GFI Product Manual

GFI EventsManager™

Administrator Guide

GFI®

Document Version: 1.0.0

Last updated (month/day/year): 24/08/2012

Contents

List of Figures

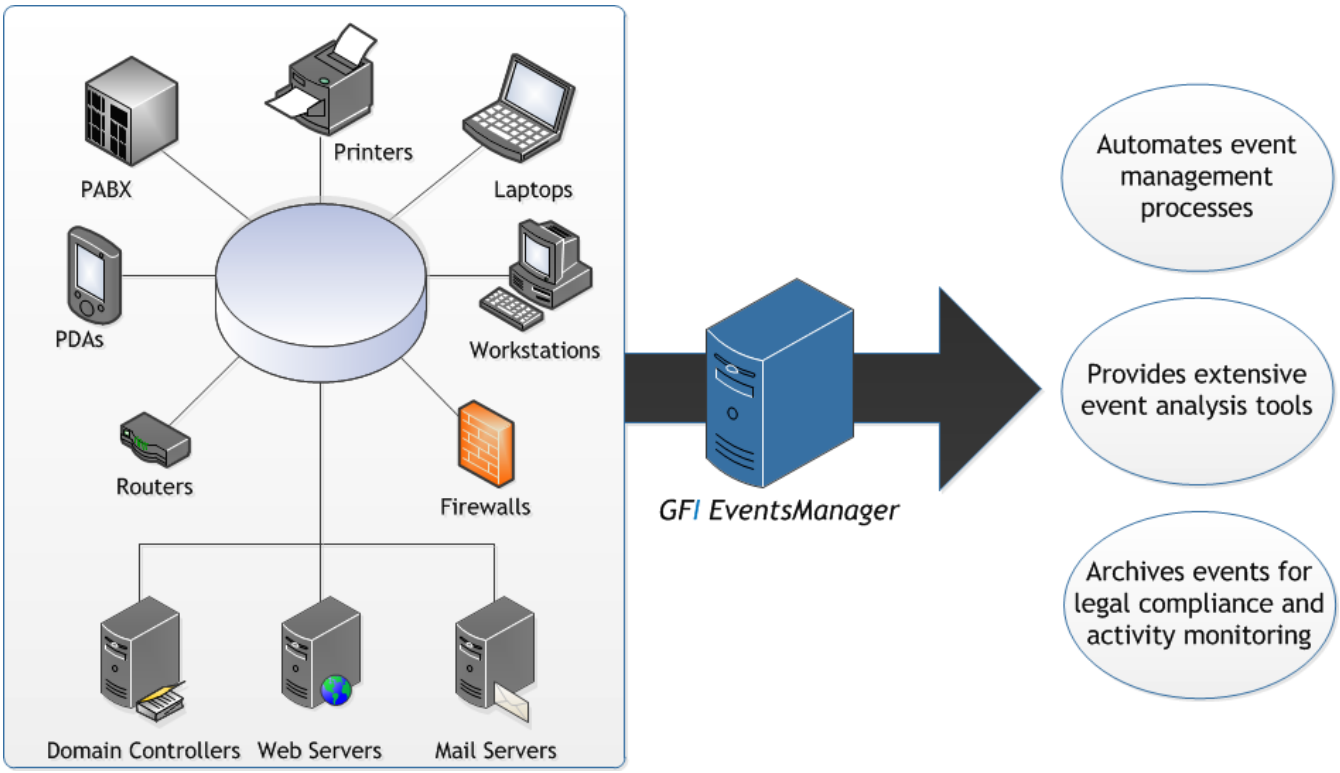
List of Tables

1 Introduction

This chapter provides you with information about how events management is achieved by GFI EventsManager. The enormous volume of system event logs generated daily is of growing importance to organizations that must record information for forensic and compliance purposes. It is essential to perform real-time network-wide event log monitoring, analysis and reporting to address any incidents or security concerns and combat threats to business continuity. GFI EventsManager assists with this monumental task by automatically and centrally monitoring and managing event logs - supporting a wide range of event types generated both by applications and devices from top vendors as well as for custom ones.

Topics in this chapter:

1.1 About GFI EventsManager



Screenshot 1: GFI EventsManagerintegrates into any existing IT infrastructure

GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager, you are able to:

» Automatically monitor computers and network devices through GFI EventsManager's wide range of event log support; such as W3C logs, Windows event logs, Syslogs, SNMP Traps and even custom

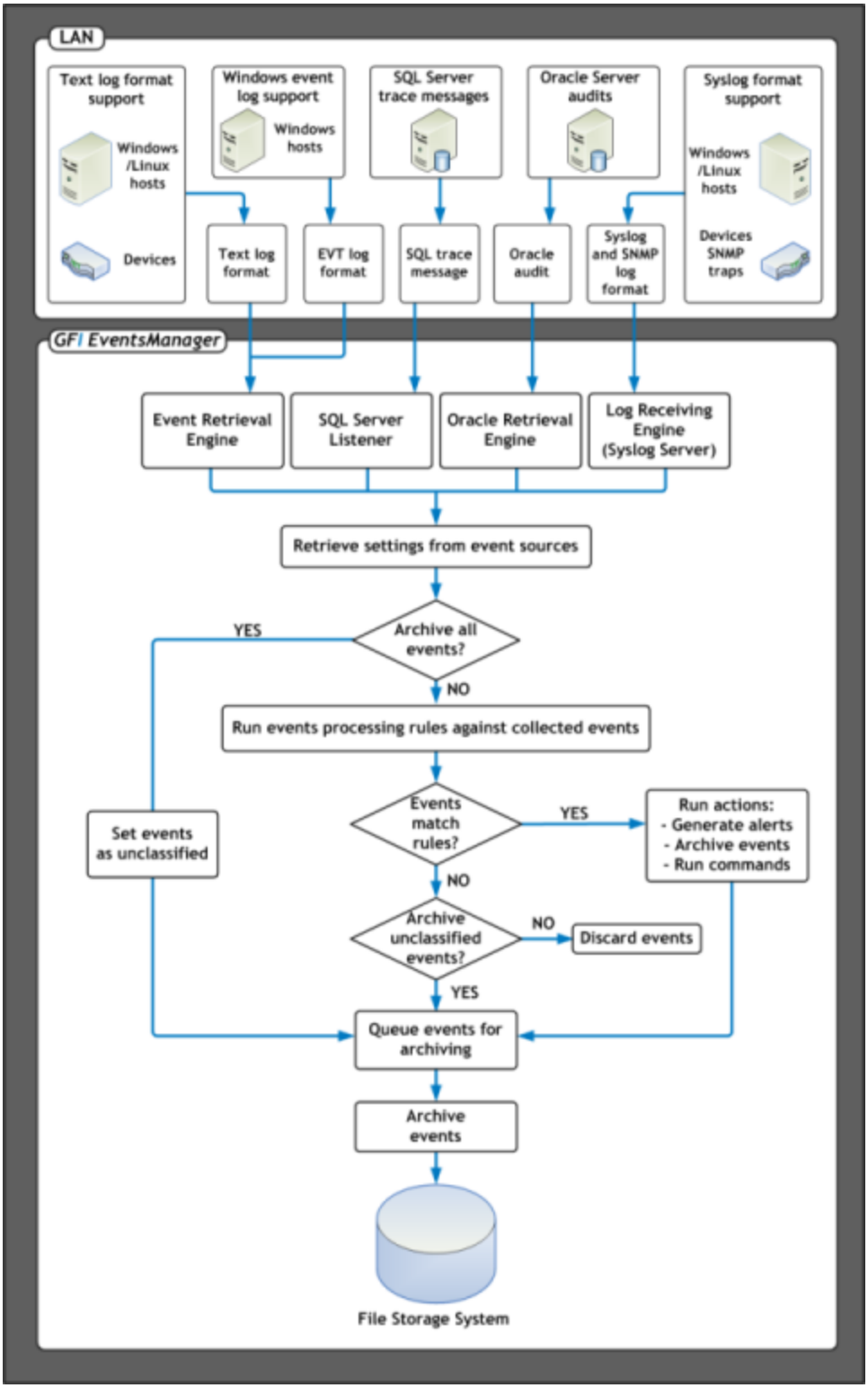
made logs

- Monitor computers and services running on your network through system monitoring features such as continuous checking of HTTP/HTTPS/FTP site availability, server roles queries, firewall queries and more
- Optimize security, performance and track operational issues by auditing your critical systems like routers, firewalls, sensors, servers and database engines
- Create and maintain an automated network security system which detects intrusion attacks
- Achieving compliance with various regulations and acts including SOX, PCI DSS, Code of Connection, HIPAA, data protection laws and others
- Proactively detect events which will lead to disaster such as hardware failure. When such events are processed, GFI EventsManager provides an early warning to give you control and take corrective action
- Minimize the risk and business loss due to systems downtime and misconfiguration
- Easily browse events from any number of databases through the extensive Events Browser; which helps you carry out forensic investigations with minimal human input
- Automatically processes and archives event logs, collecting and highlighting the information you need to know about the most important events occurring in your network so you are never caught off guard
- Generate technical IT level and management level reports from the extensive list of reports and also create new ones from existing reports or collected events
- Protect your business by tracking the security events in your network. Find who is responsible for security breaches and network threats

For a full list of features, refer to:

http://www.gfi.com/eventsmanager#features

1.2 How GFI EventsManager works



Screenshot 2: The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided in the following stages:

- Stage 1: Event Collection
- Stage 2: Event Processing

1.2.1 Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of two event collection engines: The **Event Retrieval Engine** and the **Event Receiving Engine**.

Table 1: GFI EventsManager engines

Engine	Description
The Event Retrieval Engine	Used to collect Windows Event Logs and W3C logs from networked event sources. During the Event Collection process this engine will: 1. Log-on to the event source(s) 2. Collect events from the source(s) 3. Send collected events to GFI EventsManager Server 4. Log-off from the event source(s). The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console
The SQL Server Listener	The listener receives trace messages from the scanned Microsoft SQL Server in real time. On receipt, GFI EventsManager processes the message immediately.
The Oracle Retrieval Engine	The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft Windows Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.
Log Receiving Engine	The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured. By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.

1.2.2 Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

- Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- Filter events that match specific conditions
- Trigger email, SMS and network alerts on key events
- Trigger remediation actions such as the execution of executable files or scripts on key events
- Optionally archive collected events in the database backend.

GFI EventsManager can be configured to archive events without running events processing rules. In such cases, even though no rules will be applied against collected logs, archiving will still be handled by the Event Processing stage.

Important

Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to the following KBASE article: http://kb.gfi.com/articles/SkyNet_Article/What-access-rights-are-required-by-the-GFI-EventsManager-processes?retURL=%2Fapex%2FSupportHome&popup=true

1.3 Conventions used in this manual

Table 2: Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI EventsManager.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.
`Code`	Indicates text values to key in, such as commands and addresses.

2 Installing GFI EventsManager

This chapter provides you with information about the different deployment scenarios supported by GFI EventsManager and everything you need to know about preparing your environment for installing the product. It is essential to review the requirements and best possible deployment scenario that most closely fits your requirements prior to installing GFI EventsManager.

Topics in this chapter:

2.1 Deployment scenarios

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network. If you want to collect event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a machine running Microsoft Windows Vista, 7 or Server 2008.

Use GFI EventsManager to manage the events generated:

- By the same computer where it is installed
- By all the computers that are reachable from the computer on which it is installed.

GFI EventsManager can be deployed in a:

- LAN - Monitor the activity of internal servers and workstations/end points
- DMZ - Monitor and manage the events generated on your servers running public services.

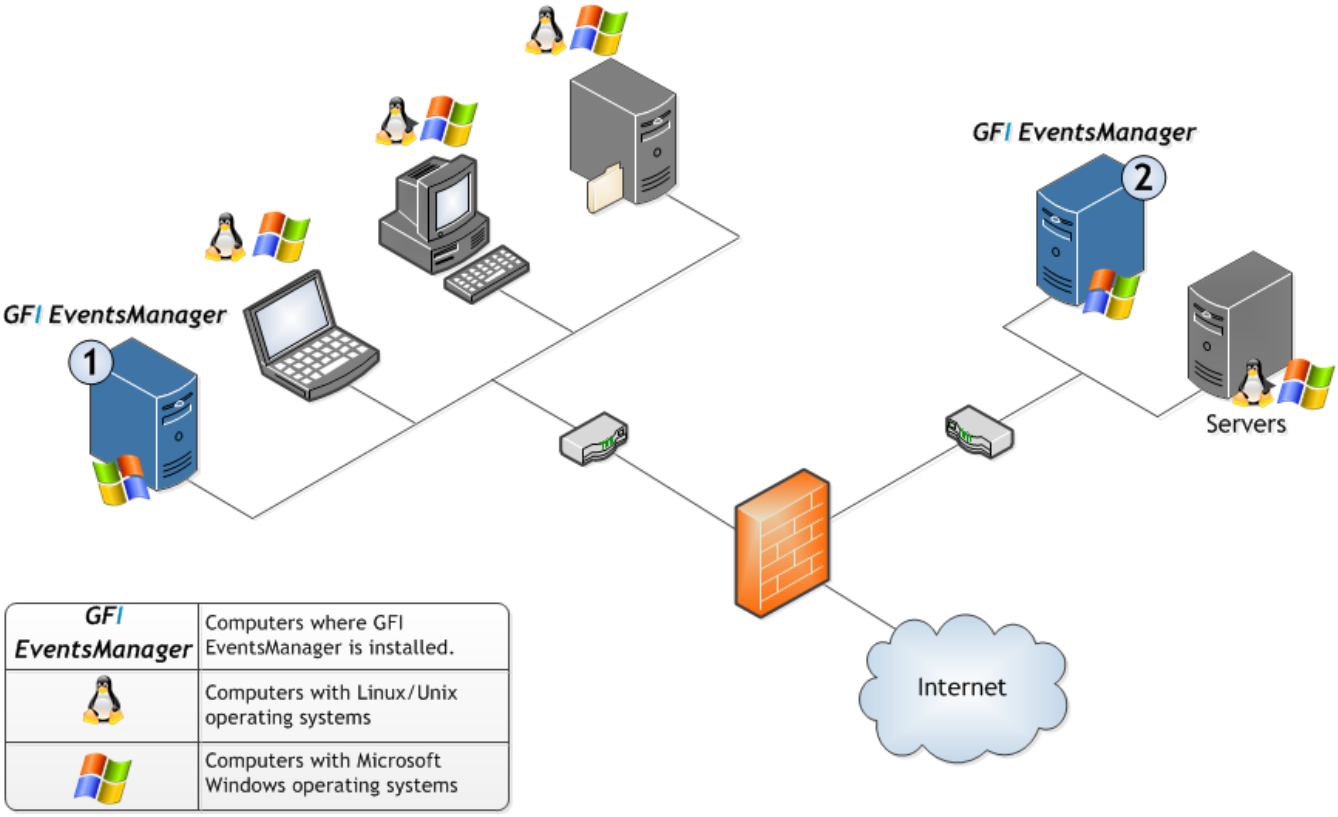


Figure 1: GFI EventsManager deployment scenario

2.1.1 Deploying GFI EventsManager on LAN

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and Unix systems are being used as well.

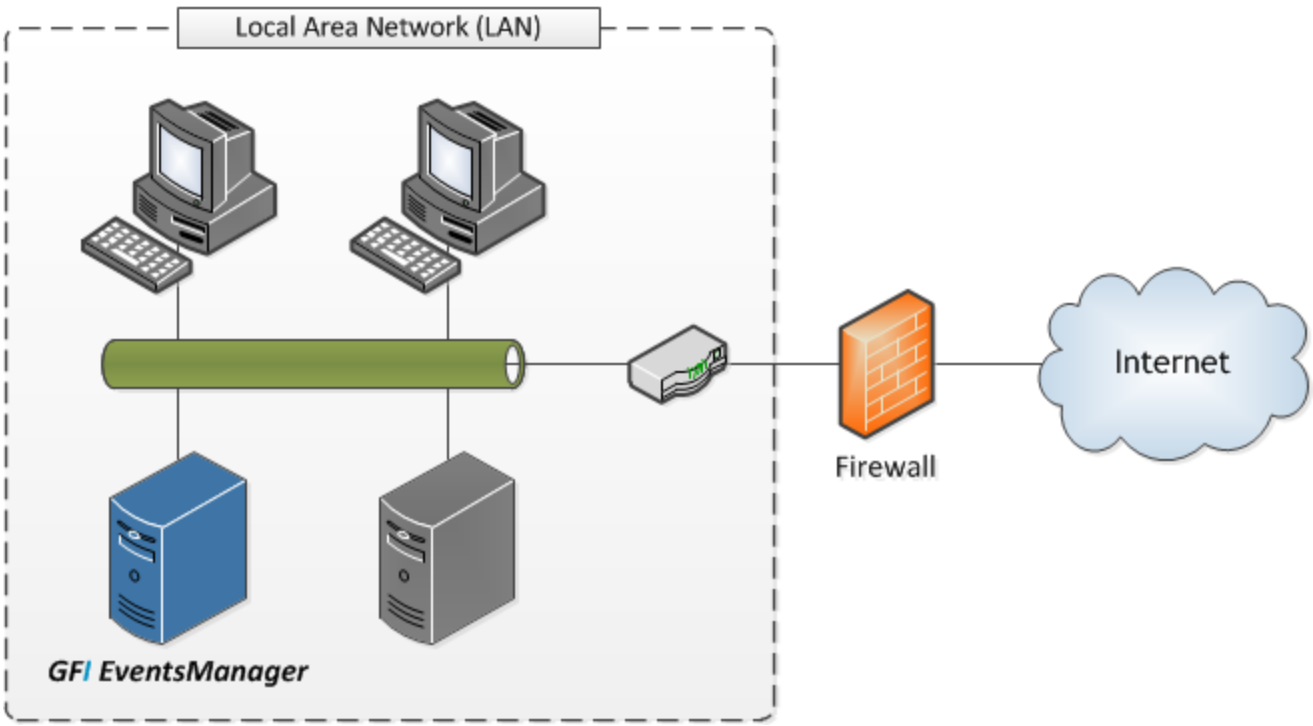


Figure 2: Deployment of GFI EventsManager in LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows events, W3C event logs, Syslog messages, SNMP Trap and SQL Server audit messages generated by any hardware or software that is connected to the LAN, including:

Table 3: Devices supported by GFI EventsManager

Device	Example
Workstations and laptops	End-user computers and systems.
Servers	Web servers, Mail servers, DNS servers and more.
Network devices	Routers, switches and any other device that generates performance logs.
Software	Including GFI EndPointSecurity, GFI LanGuard and other applications that generate logs.
Specialized Services	Microsoft Internet Information Server – IIS.
PABXs, Keyless Access Systems, Intrusion detections systems and more	GFI EventsManager enables you to monitor any device that is attached to the network.

When installed on a LAN, GFI EventsManager can also be used to collect events from hardware and software systems deployed on a Demilitarized Zone (DMZ). Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

- The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer to: http://kb.gfi.com/articles/SkyNet_Article/KBID002770?retURL=%2Fapex%2FSupportHome&popup=true.
- GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

2.1.2 Deploying GFI EventsManager on DMZ

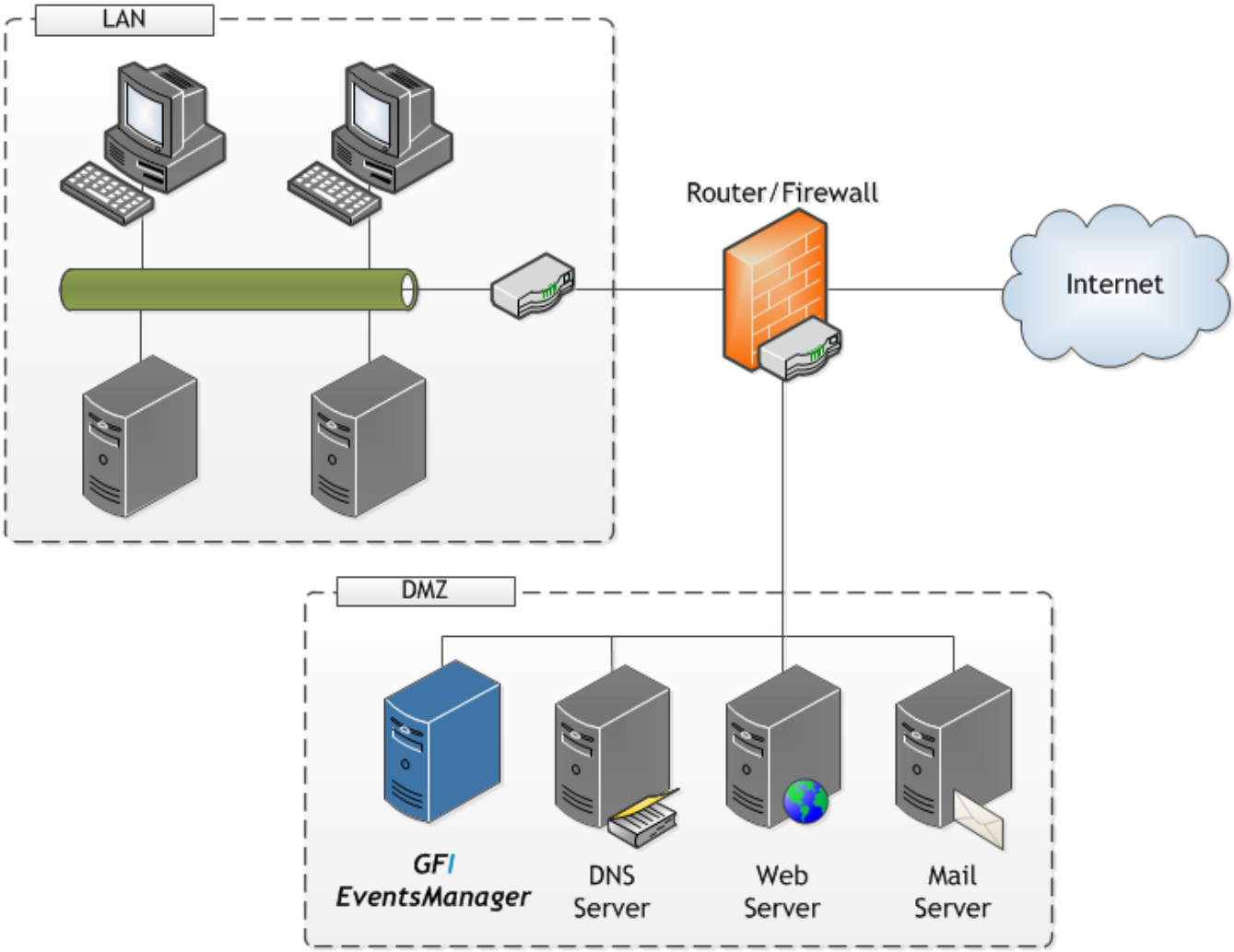


Figure 3: The DMZ sits between the internal LAN and the Internet

GFI EventsManager can also be deployed on a Demilitarized Zone (DMZ). This is the neutral network which sits between the "internal" corporate network and the "outside world" (Internet). The deployment of GFI EventsManager on a DMZ helps you automate the management of events generated by DMZ hardware and software systems; such as:

Table 4: Benefits of installing GFI EventsManager in DMZ

DMZ Automation	Description
Automate management of Web and Mail server events	DMZ networks are normally used for the running of hardware and software systems that have Internet specific roles such as HTTP servers, FTP servers, and Mail servers. Hence, you can deploy GFI EventsManager to automatically manage the events generated by: » Linux/Unix based web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms » Windows based web-servers including the W3C web-logs generated by Microsoft Internet Information Servers (IIS) » Linux/Unix and Windows based mail-servers including the Syslog auditing services messages generated by Sun Solaris v. 9 or later » Automate management of DNS server events » If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can useGFI EventsManager to automatically collect and process DNS server events including those stored in your Windows' DNS Server logs.

DMZ Automation	Description
Automate management of DNS server events	If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows' DNS Server logs.
Automate management of network appliance events	Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (example: Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems. By deploying GFI EventsManagerr on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.

2.2 System requirements

This section contains information about:

- Hardware requirements
- Storage requirements
- Supported operating systems (x86 or x64)
- Other software components
- Firewall ports and permissions
- Event source settings
- Antivirus exceptions
- Computer identification considerations
- Monitoring events logs from computers running Windows Vista or later

2.2.1 Hardware requirements

Table 5: Hardware requirements

Hardware Component	Specification
Processor	2.5 GHz dual core or higher.
RAM	3 GB.
Hard disk	10 GB free space.

> **Note**
>
> Hard disk size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.

2.2.2 Storage requirements

The following specifications are based on the average size of event logs:

Table 6: Storage space requirements

Hard Disk Space	Number of Events
Events stored per 1 Gb of storage space	2,006,994
Events stored in 500 Gb of storage space	1,003,497,032

Note

The above specifications are based on an average size of event logs, being 535 bytes per event.

2.2.3 Supported operating systems (x86 or x64)

- Windows Server 2008 - Standard or Enterprise
- Windows Server 2008 R2 – Standard or Enterprise
- Windows Server 2003 SP2 - Standard or Enterprise
- Windows 7 - Enterprise, Professional or Ultimate
- Windows Vista SP1 - Enterprise, Business or Ultimate
- Windows XP Professional SP3
- Windows SBS 2008
- Windows SBS 2003.

2.2.4 Other software components

- Microsoft .NET framework 4.0
- Microsoft Data Access Components (MDAC) 2.8 or later
- A mail server (when email alerting is required).

Note

Microsoft Data Access Components (MDAC) 2.8 can be downloaded from http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en

2.2.5 Firewall ports and permissions

Ports and protocols

Table 7: Firewall ports and protocols

Port	Protocols	Description
135	UDP and TCP	Target machines use this port to publish information regarding available dynamic ports. GFI EventsManager uses this information to be able to communicate with the target machines.
139 and 445	UDP and TCP	Used by GFI EventsManager to retrieve the event log descriptions from target machines.
162	UDP and TCP	Used by GFI EventsManagerr to receive SNMP traps. Ensure that this port is open on the machine where GFI EventsManagerr is installed.
514	UDP and TCP	Used by GGFI EventsManager to receive SYSLOG messages.
1433	UDP and TCP	Used by GFI EventsManager to communicate with the SQL Server database backend. Ensure that this port is enabled on Microsoft SQL Server and on the machine where GFI EventsManagerr is installed.

Port	Protocols	Description
1521	UDP and TCP	Used to collect Oracle Server audit logs. Port 1521 is the default port for this connection. If the port is changed manually in the Oracle Listener's configuration, adjust firewall settings accordingly.
49153	UDP and TCP	Used by GFI EventsManager to collect events from event sources with Microsoft Windows Vista or Microsoft Windows 7.

Permissions

Table 8: Firewall permissions

Firewall Permissions and Audit Policies	Windows Server 2008	Windows Server 2003	Windows XP	Windows 7	Windows Vista
Remote Event Log Management	Enable	Not applicable	Not applicable	Enable	Enable
File and Printer sharing	Enable	Enable	Enable	Enable	Enable
Network discovery	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Object access	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Process tracking	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Audit account management	Enable	Enable	Enable	Enable	Enable
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable

Note

For more information, refer to Enabling permissions on events sources manually or Enabling permissions on event sources automatically.

2.2.6 Event source settings

The below table describes what configuration is required for event sources:

Table 9: Event source settings

Log Type	Description
Windows event log processing	Enable remote registry.
W3C log processing	The source folders must be accessible via Windows shares.
Syslog and SNMP Traps processing	Configure sources/senders to send messages to the computer/IP where GFI EventsManageris installed.
Scanning machines with Windows Vista or later	Install GFI EventsManager on a computer running Windows Vista or later.
System auditing	Enable auditing on event sources. For information, refer to Miscellaneous.

2.2.7 Antivirus exceptions

If an antivirus application installed on the computer where GFI EventsManager is running, make sure that:

- Traffic is not blocked on the ports in use by GGFI EventsManager
- **esmui.exe** and **esmproc.exe** are allowed access through the firewall(s)
- GFI EventsManager folders are excluded from real-time antivirus scanning.

2.2.8 Computer identification considerations

GFI EventsManager identifies computers via computer name or IP. If NETBIOS-compatible computer names are used, ensure that your DNS service is properly configured for name resolution. Unreliable name resolution downgrades overall system performance. If you disable NETBIOS over TCP/IP, you can still use GFI EventsManager, however you must specify computer name by IP.

2.2.9 Monitoring events logs from computers running Windows Vista or later

GFI EventsManager cannot be installed on Microsoft Windows XP to monitor events of Microsoft Windows Vista or later. Microsoft Windows Vista and Microsoft Windows 7 introduced extensive structural changes in event logging and event log management. The most important of these changes include:

- A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- Event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- A new file format (evtx) that replaces the old evt file format.

Due to these changes, to collect and process event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a system running:

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows Server 2008.

Note

Windows XP events can be collected when GFI EventsManager is installed on Microsoft Windows Vista or later machines.

Note

When GFI EventsManager is using a non-domain account to collect events from Microsoft Vista machines or later, target machines must have User Account Control (UAC) disabled. For more information, refer to Disabling User Account Control (UAC) (page 254).

2.3 Upgrading GFI EventsManager

Upgrading from versions older than GFI EventsManager 2011 is not fully supported. Some settings may be lost due to the underlying technology changes.

GFI EventsManager can be upgraded:

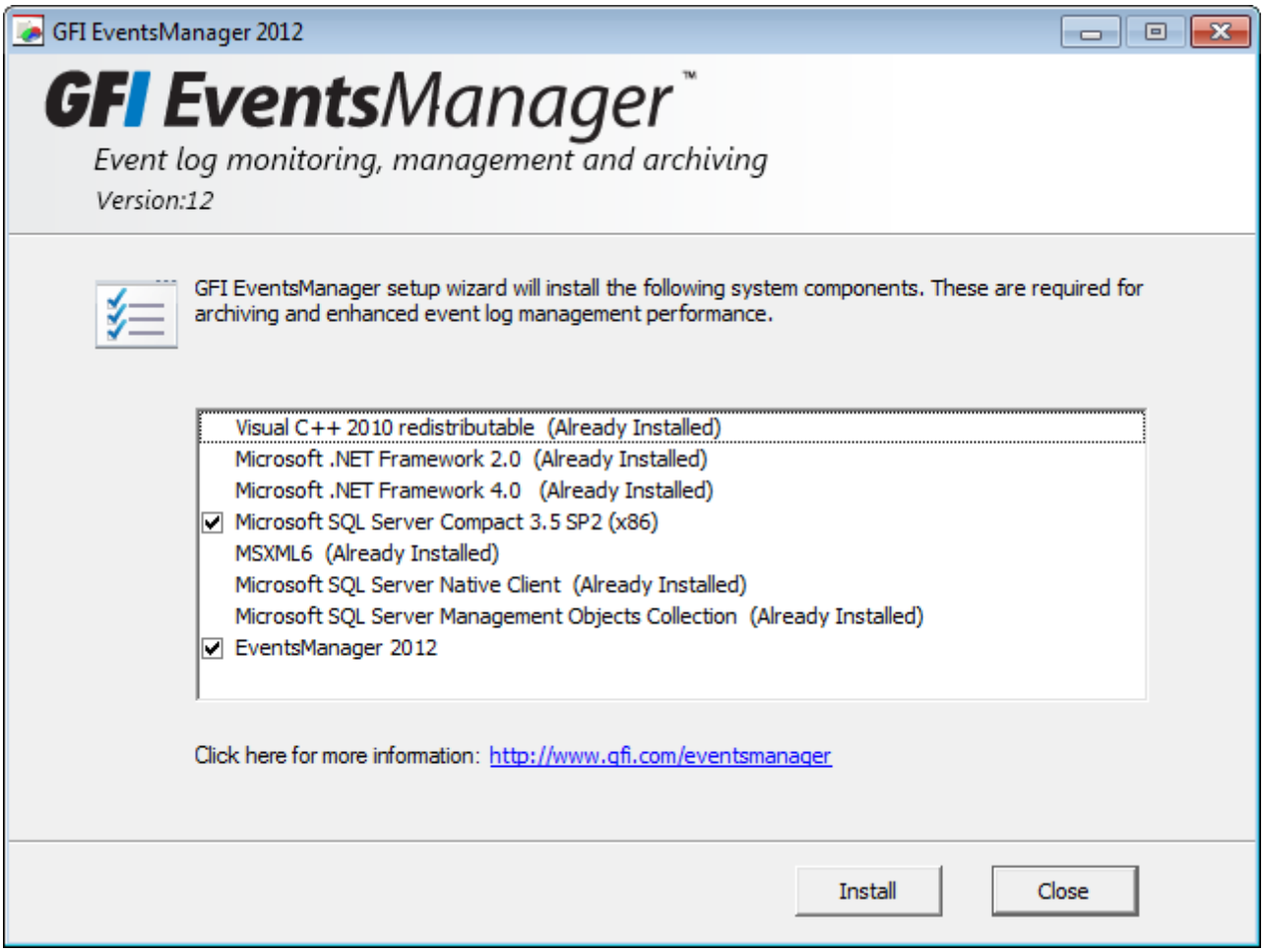
Table 10: Upgrading GFI EventsManager

Method	Description
Automatically	Launch the new setup and complete the wizard to upgrade and retain data. For more information, refer to Upgrading from a previous version (page 30).
Manually	Export events from an older version of GFI EventsManager and import it in the new one using Database Operations. For more information, refer to Creating maintenance jobs (page 203).

2.3.1 Upgrading from a previous version

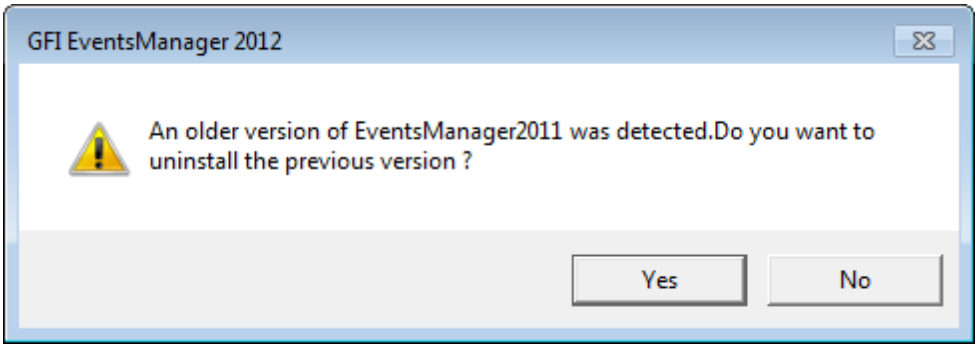
To upgrade to a new version:

1. Double-click **EventsManager.exe**.



Screenshot 3: Upgrade prerequisite check

2. Click **Install** to install the required missing components and the new version of GFI EventsManager.



Screenshot 4: Uninstall previous version

3. Before installing the new version, select whether you want to keep or remove the older version of GFI EventsManager. Select from:

Table 11: Upgrade options

Option	Description
Yes	Replaces the old version with the new one.
No	Keeps the old version and installs the new one.

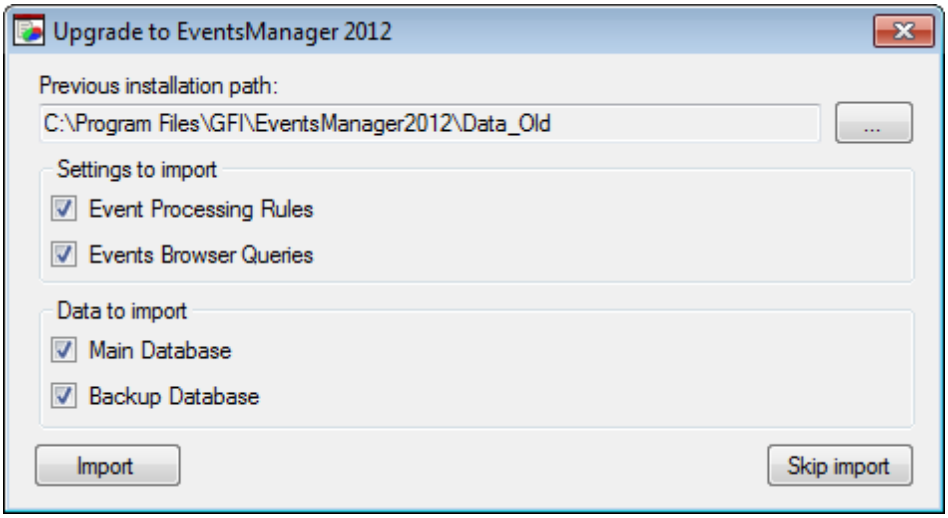
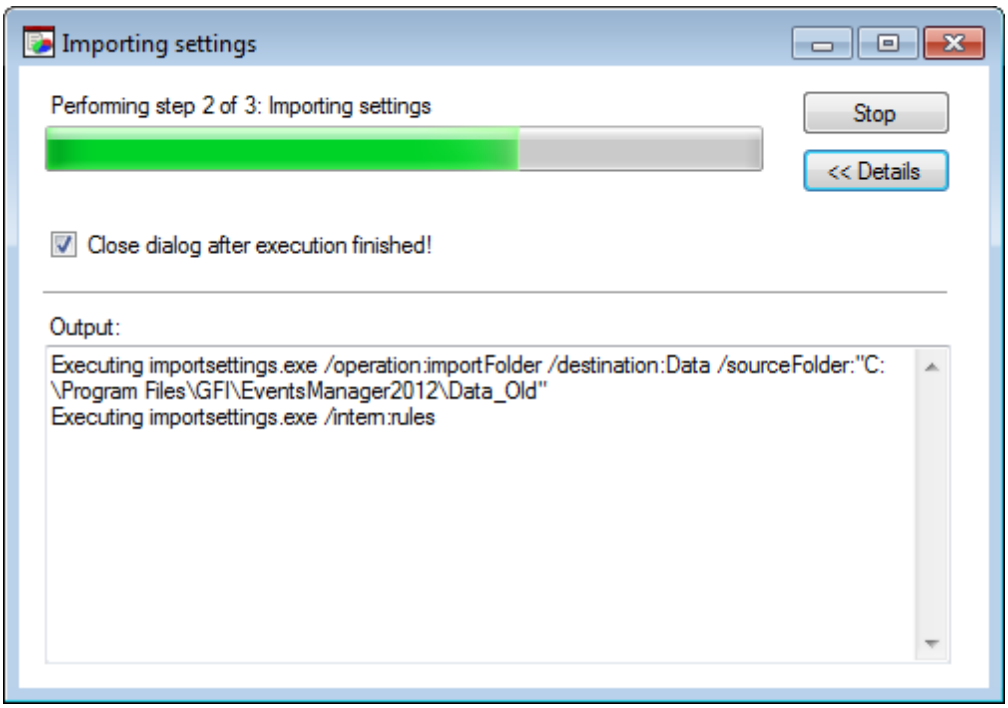


Figure 4: Upgrade import dialog

4. Once installed, the upgrade dialog is launched automatically. Select the settings to import and the location from where to import events.

5. Click **Import**.



Screenshot 5: Import progress

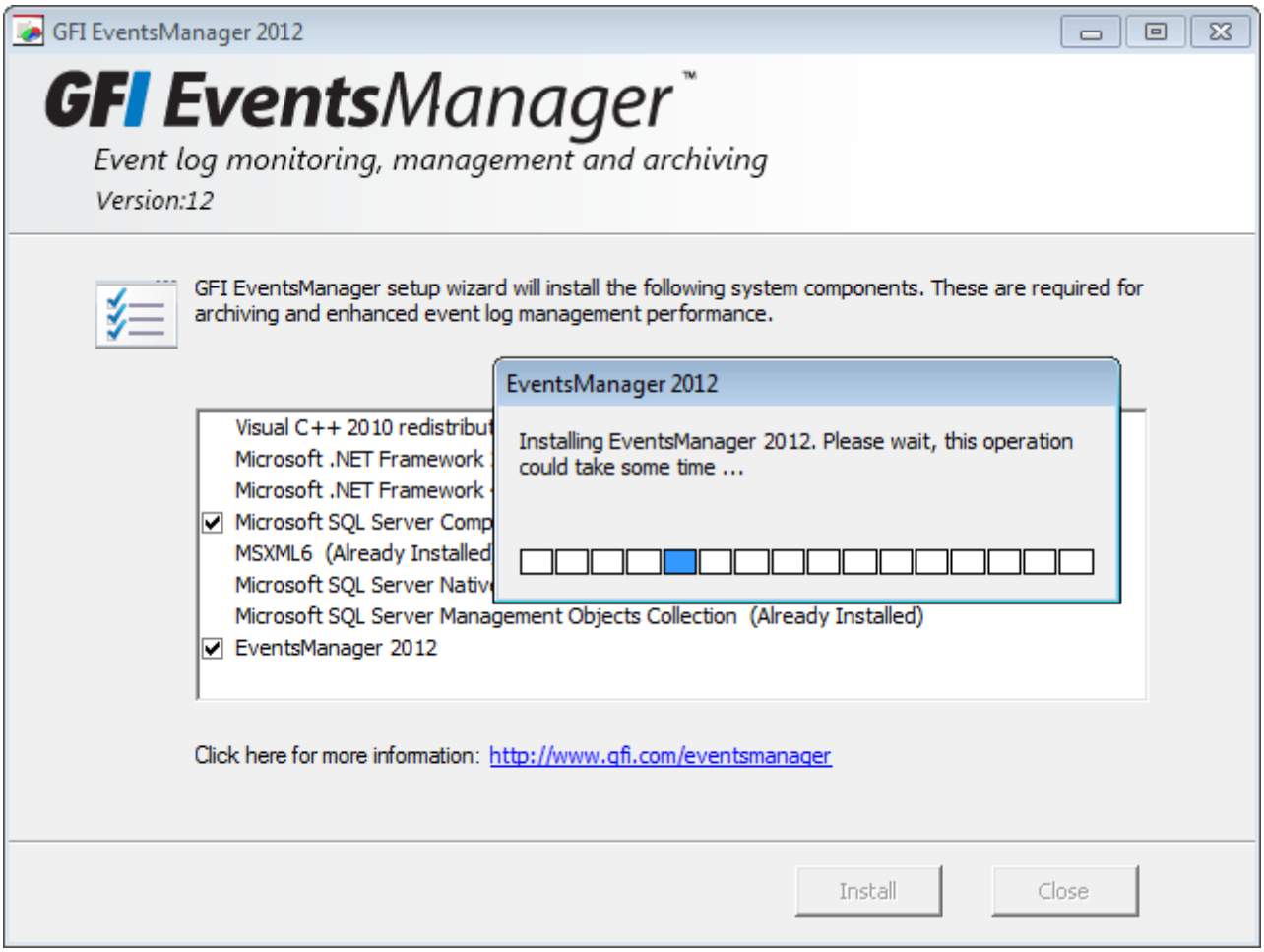
6. Wait for the import job to finish. The GFI EventsManager Management Console opens automatically on completion.

2.4 Installing a new instance of GFI EventsManager

To install GFI EventsManager:

1. Close all running applications and log on the computer using an administrator account.

2. Double-click **EventsManager.exe**.



Screenshot 6: Pre-requisite check

3. GFI EventsManager will check your system for components that are not already installed. Click **Install** to begin the installation.

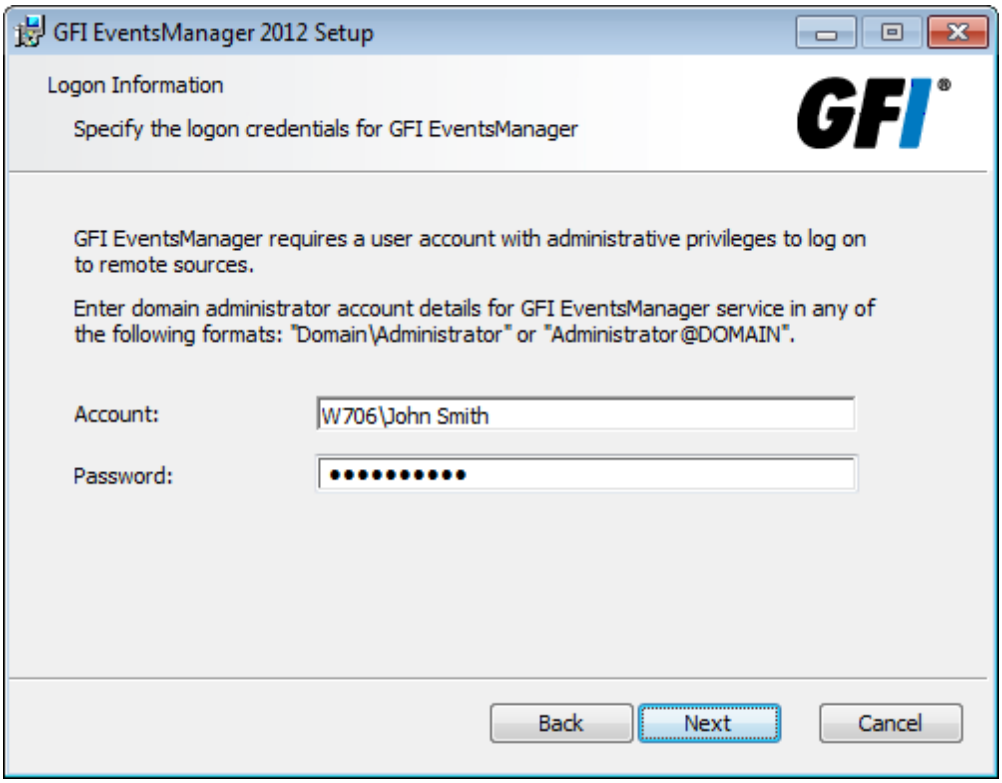
4. Click **Next** at the wizard welcome step.

Screenshot 7: End-User License Agreement

5. Read the licensing agreement carefully. Select '**I accept the terms in the License Agreement**'. Click **Next**.

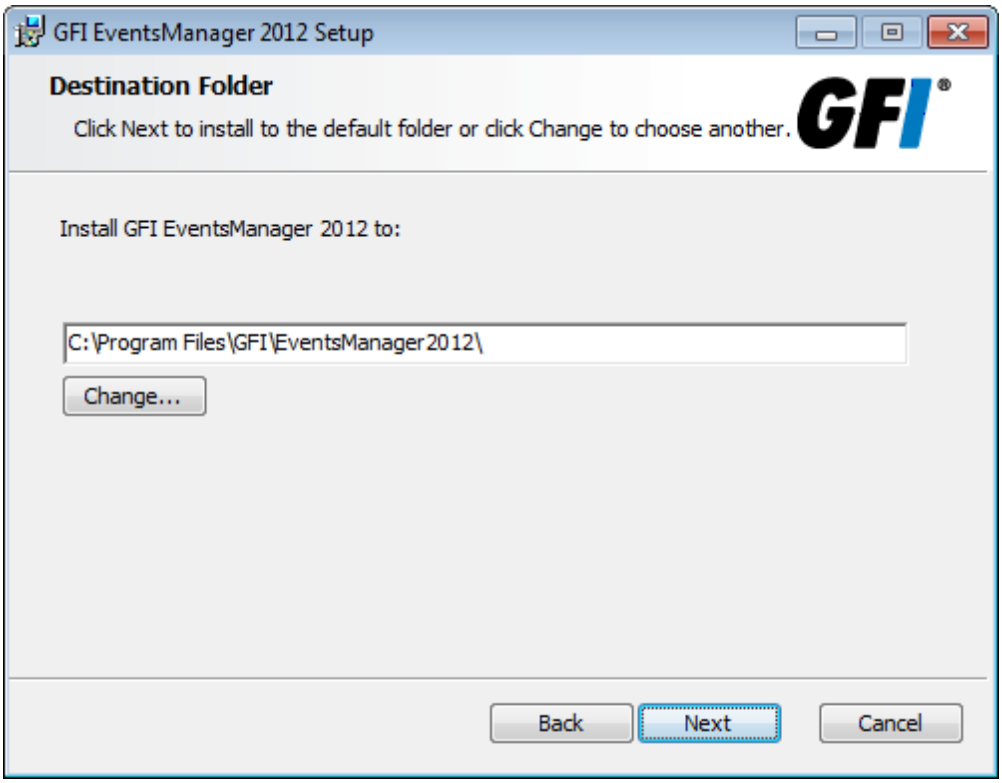
Screenshot 8: Customer and license details screen

6. Key in your **User Name** and **License Key**. Click **Next**.



Screenshot 9: Logon information screen

7. Key in a user name and password of a domain administrator account. Click **Next**.



Screenshot 10: GFI EventsManager install directory

8. (Optional) Specify an alternative installation path or click **Next** to install to default location.

Screenshot 11: Begin installing GFI EventsManager

9. Click **Install**.

2.5 Testing your installation

After installing GFI EventsManager, the Management Console is launched automatically. To launchGFI EventsManager manually, click **Start > All Programs > GFI EventsManager > Management Console**.

Follow the steps outlined below to configure GFI EventsManager for first time use:

- Step 1: Launch events processing
- Step 2: Analyze events and generate reports

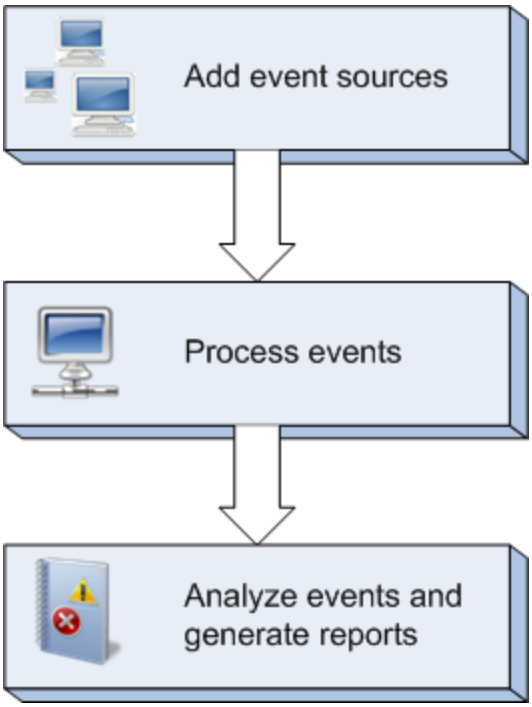
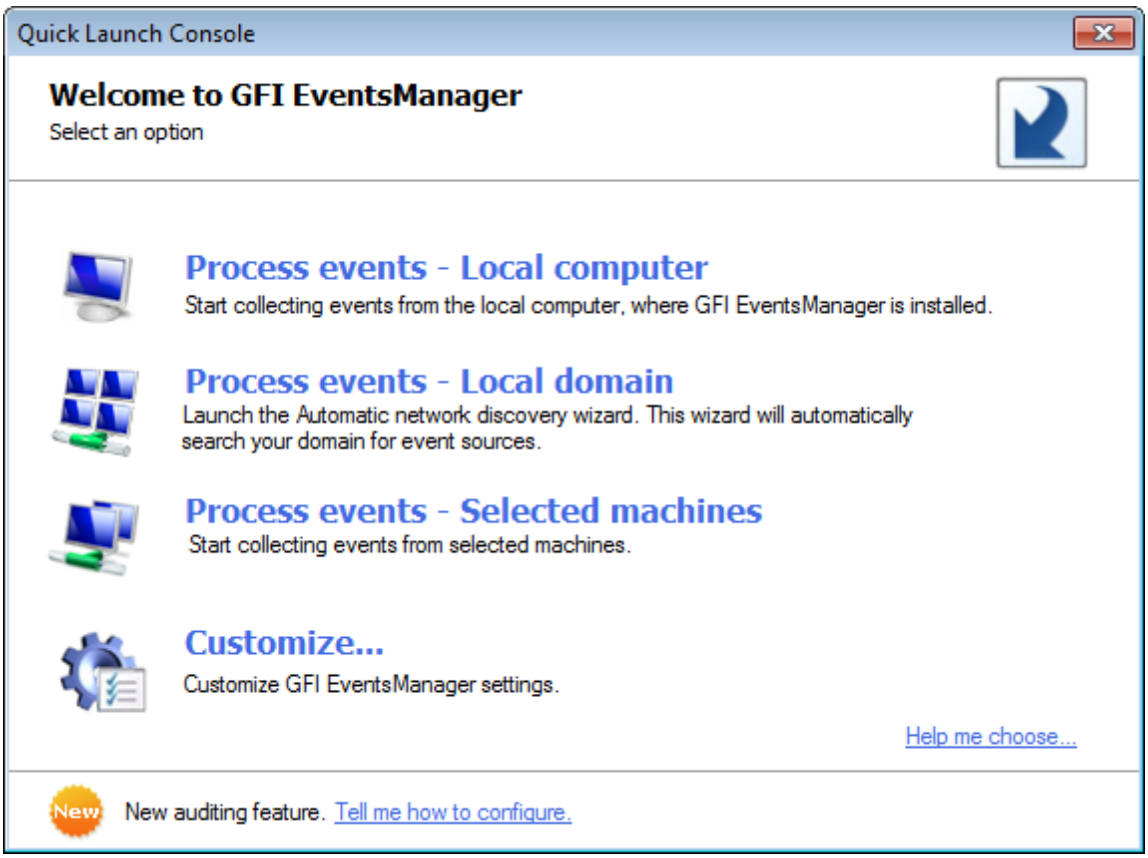


Figure 5: Running GFI EventsManager for the first time

2.5.1 Step 1 - Start collecting and processing events



Screenshot 12: Quick Start Dialog

When you run the GFI EventsManager Management Console for the first time, the **Quick Launch Console** opens automatically. To open the Quick Launch Console manually, click **Open Quick Launch Console** from the top-right corner of the **Management Console**.

Select one of the following options to test your installation:

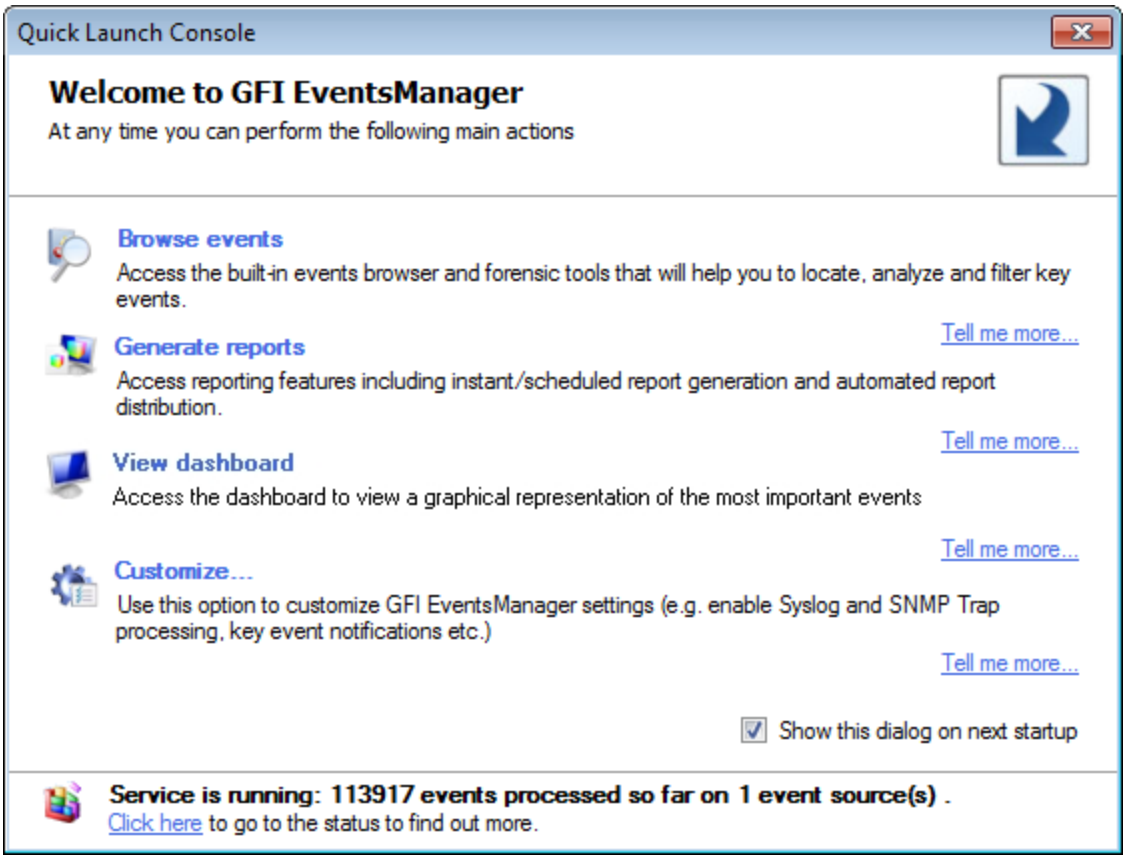
Table 12: Quick Launch Console options

Option	Description
Process events - local computer	Start collecting events from the local computer, where GFI EventsManager is installed. For more information, refer to Processing events from the local computer (page 37).
Process events - local domain	Launch the **Automatic network discovery** wizard. This wizard will automatically search your network for event sources. For more information, refer to Processing events from the local domain (page 38).
Process events - selected machines	Add event sources manually without using the wizard. For more information, refer to Processing events from selected machines (page 39).
Customize	Customize settings of: » Events sources and log types » Event processing rules » Database operations » Users and groups » Alerting options.

Processing events from the local computer

To process event logs from the local machine:

1. From **Quick Launch Console** , click **Process events - local computer**. GFI EventsManager will start to collect events from the local machine immediately.



Screenshot 13: Events processed from local machine

On completion, the number of events that have been processed is displayed in the information bar as illustrated in the screenshot above.

Processing events from the local domain

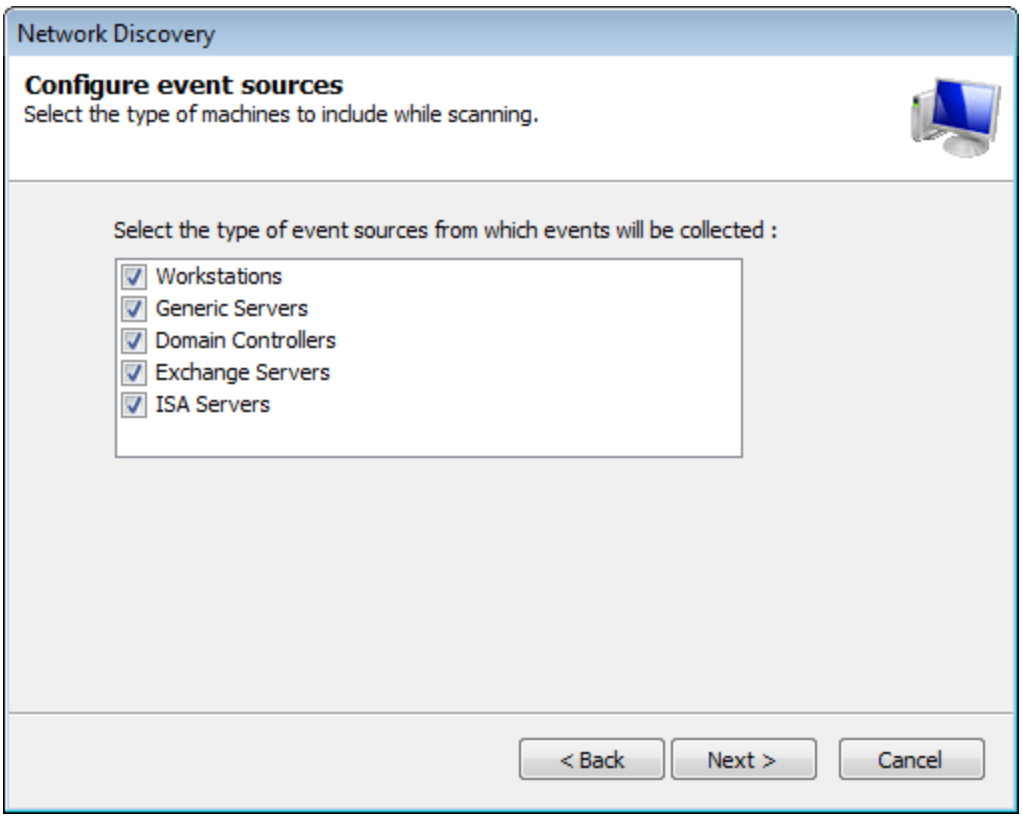
The Network discovery wizard searches the entire network for computers and servers. This will assist in adding network computers as GFI EventsManager event sources. To launch the Network discovery wizard:

1. From **Quick Launch Console** , click **Process events - Local domain**.

> **Note**
>
> The wizard can also be launched from **Configuration** tab > **Event Sources**; right-click **All event sources** and select **Scan local domain**.

> **Note**
>
> If synchronization options are configured, **Process events - Local Domain** is disabled. For more information, refer to Adding event sources automatically (page 43).

2. In the Welcome screen, click **Next**.



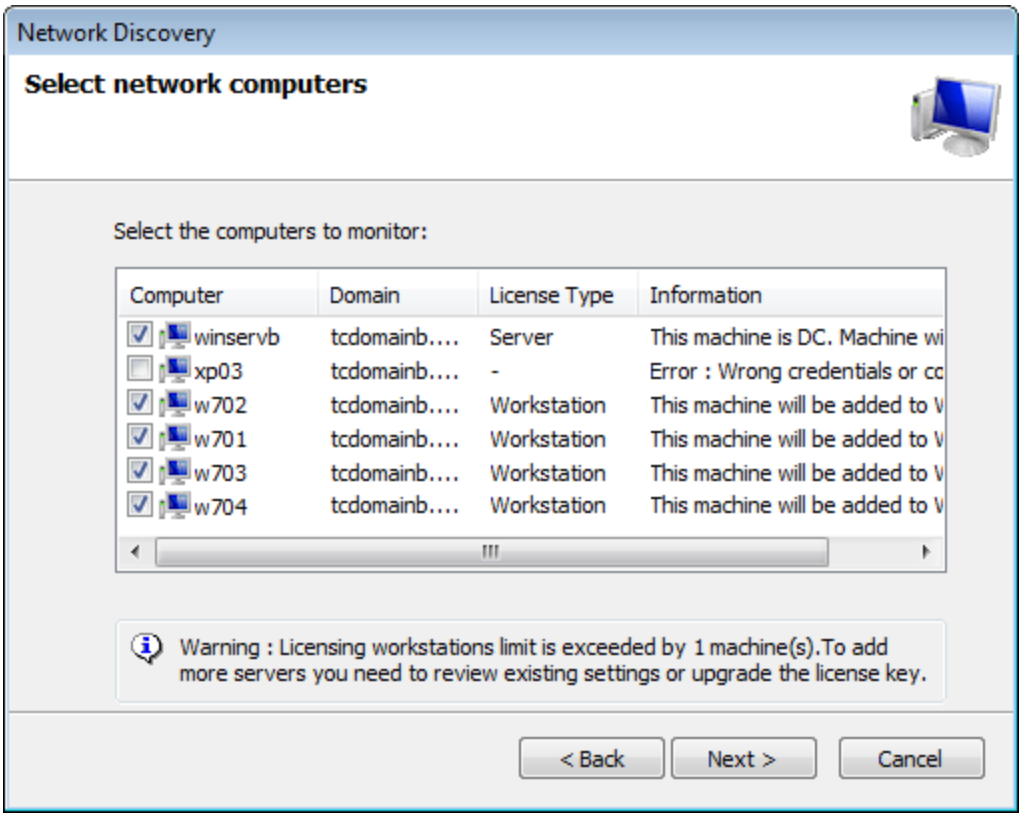
Screenshot 14: Select the type of event source

3. The wizard enables you to search the local network for specific types of event sources. Select the type of event sources to add and click **Next**.

Note

At least one event source type must be selected before proceeding to the next wizard dialog.

4. The wizard will automatically start to search for connected computers. On completion, click **Next**.



Screenshot 15: Select computers from result

Note

All discovered machines are selected by default. If the wizard fails to login to a computer, it is not selected.

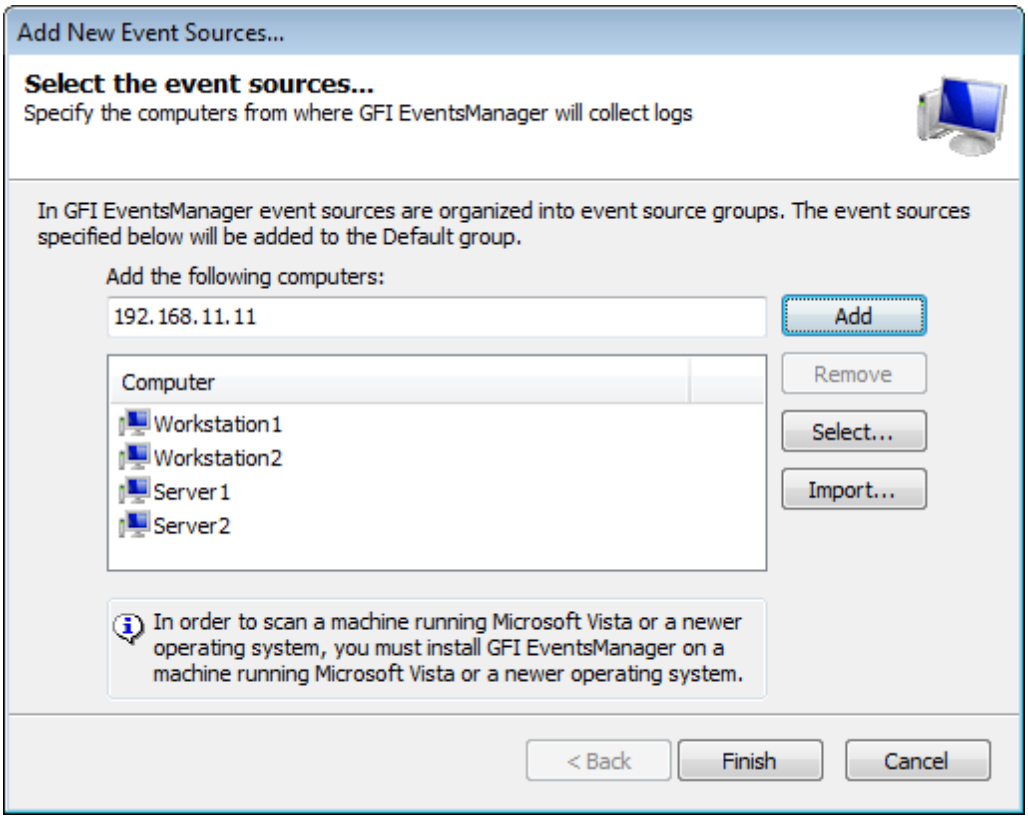
5. To add a computer not selected by default, click the respective computer and a dialog will enable you to key in alternative credentials.

6. Click **Next** and **Finish**.

Processing events from selected machines

To collect event logs from selected machines:

1. From the **Quick Launch Console** , click **Process events - selected machines** to launch the **Add New Event Sources…** wizard.



Screenshot 16: Process events from selected machines

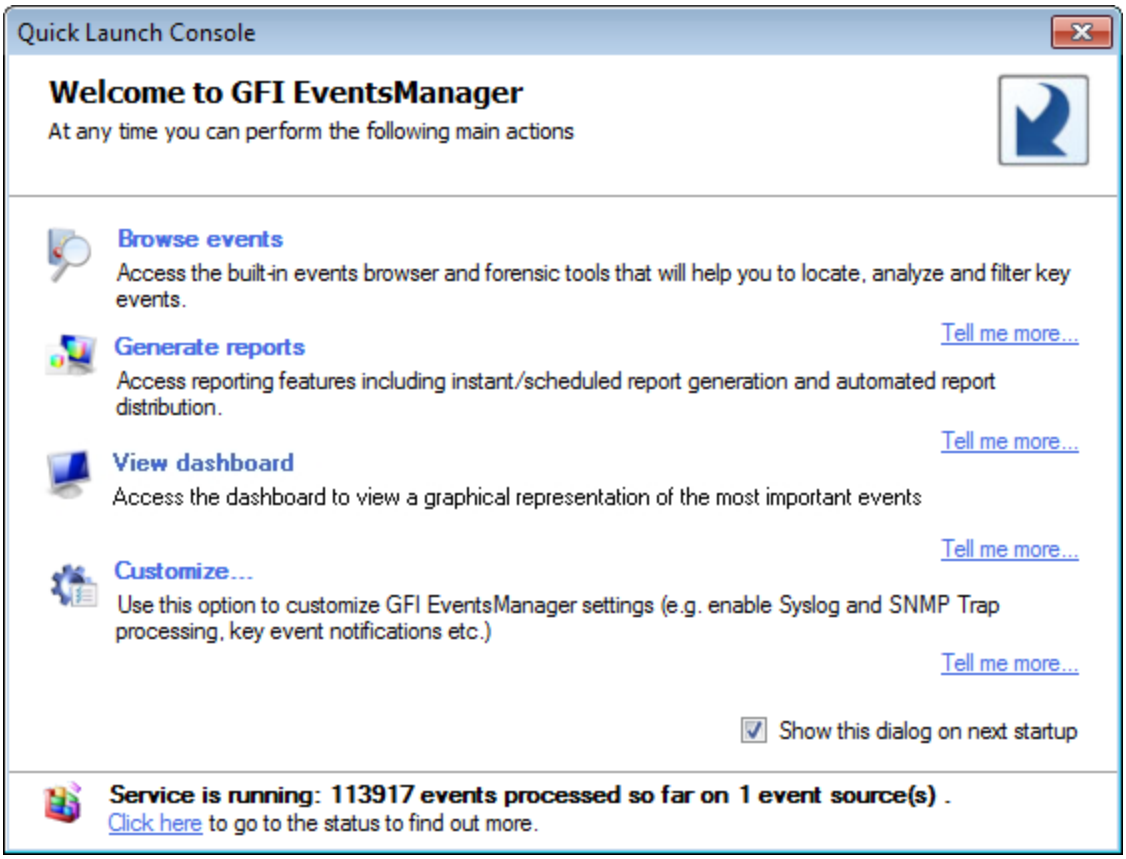
2. Specify the event source name or IP and click **Add**. Repeat until you have specified all the event sources to add to this group.

> **Note**
>
> To import the list of event sources from a text file click **Import**. To select event sources from a list, click **Select**.

3. Click **Finish** to finalize settings. GFI EventsManager will collect events from the configured sources immediately.

2.5.2 Step 2 - Analyze events and generate reports

After collecting event logs, you can analyze the information and generate reports based on the gathered data.



Screenshot 17: GFI EventsManager Quick Launch Console

To analyze events:

1. Click **Open Quick Start Dialog** from the top-right corner of the GFI EventsManager user interface. The table below describes available options:

Table 13: Quick Launch Console options

Icon	Description
	Browse events Access the built-in events and forensic tools that will help you to locate, analyze and filter key events. For more information, refer to Browsing Stored Events (page 102).
	Generate reports Access reporting features including instant/scheduled report generations and automated report distribution. For more information refer to Reporting chapter in this manual. For more information, refer to Reporting (page 112).
	View dashboard Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager. For more information, refer to Activity Monitoring (page 96).
	Customize Customize GFI EventsManagersettings, such as enabling Syslog, SNMP Trap processing, key events notifications, and more. For more information, refer to Managing Event Sources (page 42).

3 Managing Event Sources

This chapter provides you with information about adding and managing your event sources. Event sources are networked computers and devices that are accessed and processed by GFI EventsManager. The Events Sources sub-tab (**Configuration > Event Sources**), enables you to organize your event sources into specific groups. You can create new groups or use the default ones to distinctively configure and organize event sources.

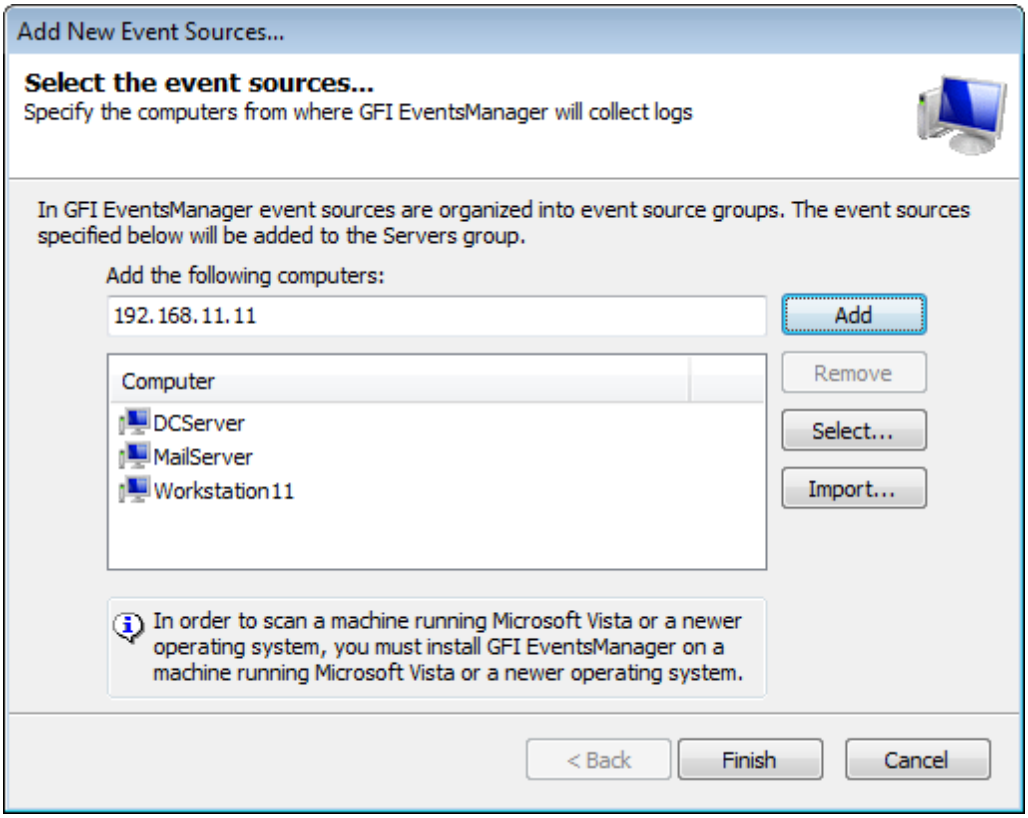
Topics in this chapter:

3.1 Adding event sources manually

To add a new event sources to a computer group:

1. Click **Configuration** tab **> Event Sources** and from **Group Type**, select **Event Sources Groups**.

2. Right-click a computer group of your choice and select **Add new event source…**



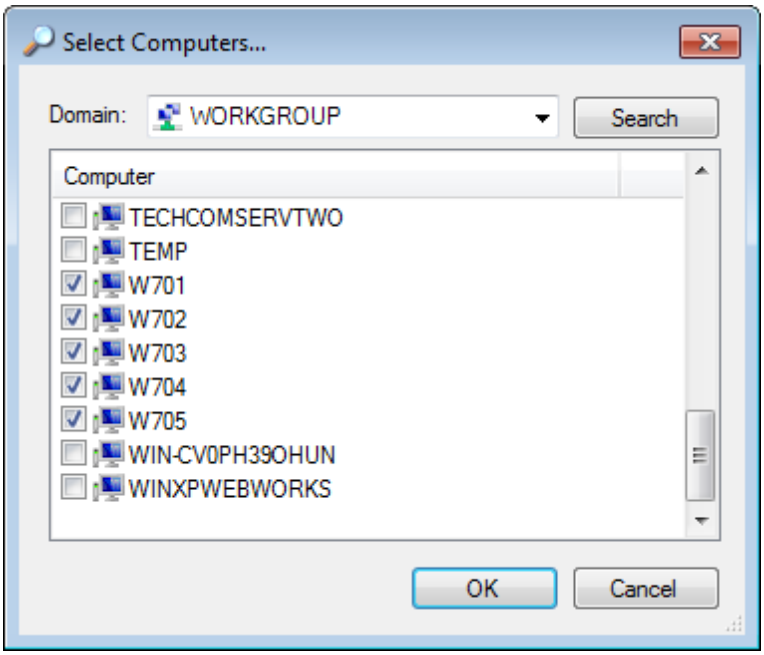
Screenshot 18: Add new event source wizard

3. Specify the name or IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.

Note

Since Syslog and SNMP traps use the IP address to determine the source of an event, it is recommended to use the source IP instead of the domain name when retrieving Syslog and SNMP traps from target machines.

4. (Optional) Click **Select...** to browse the network for existing domains and computers. Select the domain from the **Domain** drop down list and select the computers to add.



Screenshot 19: Browse the network for connected computers

5. (Optional) Click **Import…** to import computers from a text file. Ensure that the text file contains only one computer name or IP per line.

6. Click **Finish** to finalize your settings. GFI EventsManager will attempt to collect logs from the configured sources immediately.

Note

If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch **Network Discovery Wizard**, right-click **All event sources** from the event sources tree and select **Scan local domain**. For more information, refer to Adding event sources automatically (page 43).

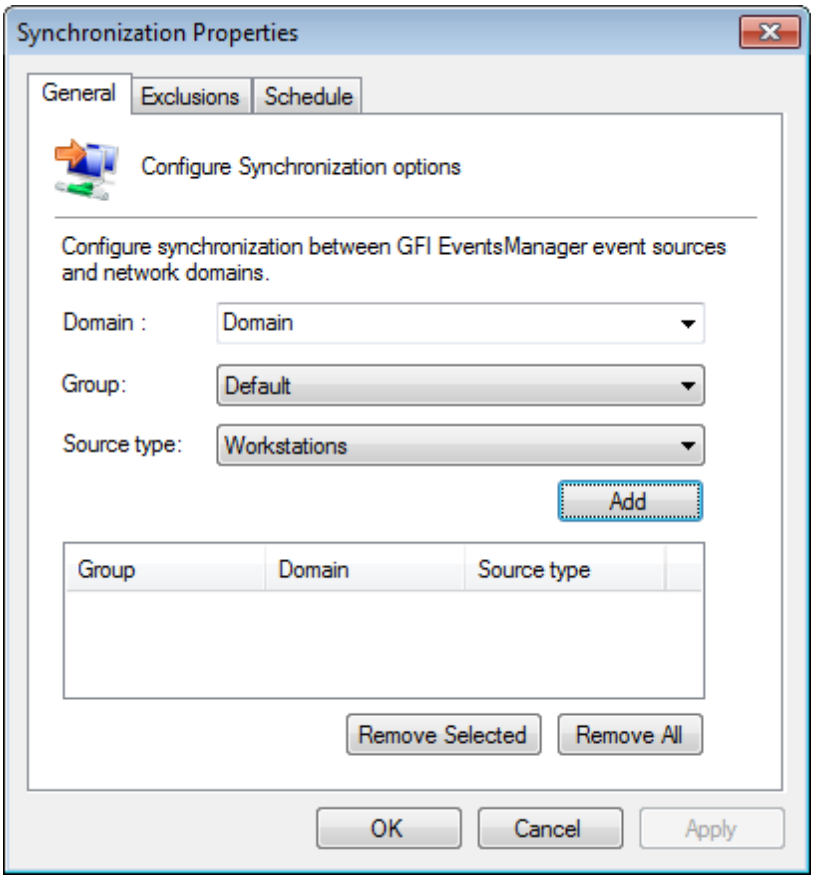
3.2 Adding event sources automatically

GFI EventsManager enables you to synchronize domains with event sources groups. When the synchronization is configured, every new domain member is added automatically to GFI EventsManager event sources.

To edit synchronization options:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. Right-click **All event sources** and select **Edit synchronization options**.



Screenshot 20: Synchronization properties - General tab

3. Select **General** tab and configure the options described below:

Table 14: Synchronization properties - General tab

Option	Description
Domain	Select the domain name from the list or key in a valid domain name.
Group	Select the GFI EventsManager group name where to add the discovered event sources.
Source type	Select the type of computers discovered in the selected domain that will be added to the selected GFI EventsManager group.

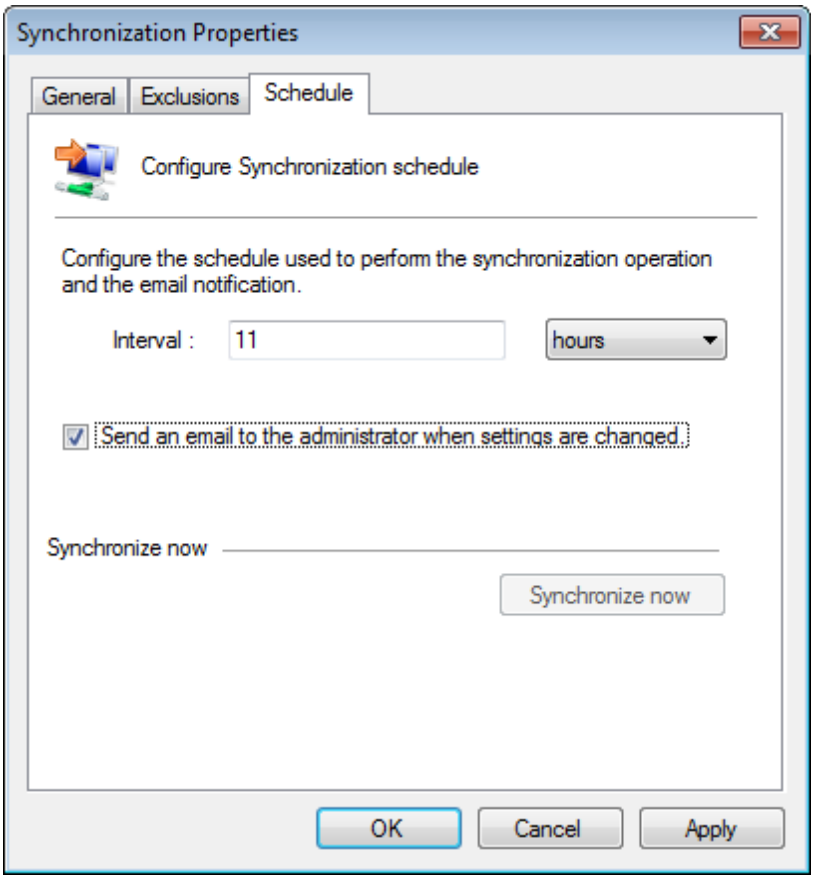
4. To include the synchronization click **Add**.

5. Repeat steps 3 to 4 for each synchronization.

6. (Optional) Select **Exclusions** tab to configure the list of computers that will be excluded from the synchronization. Click **Add** and key in a computer name to exclude.

> **Note**
>
> Event sources that are already part of an event source group will be automatically excluded from synchronization.

7. Select **Schedule** tab to configure when the synchronization should be performed.



Screenshot 21: Synchronization properties -Schedule tab

8. Key in a valid interval in hours or days.

9. (Optional) Select **Send an email to the…** to send an email notification when event sources are changed after synchronization.

10. (Optional) Click **Synchronize now** to synchronize event sources immediately.

11. Click **Apply** and **OK**.

> **Note**
>
> Adding event sources manually to a synchronized group is not allowed in GFI EventsManager.

3.3 Creating a new event source group

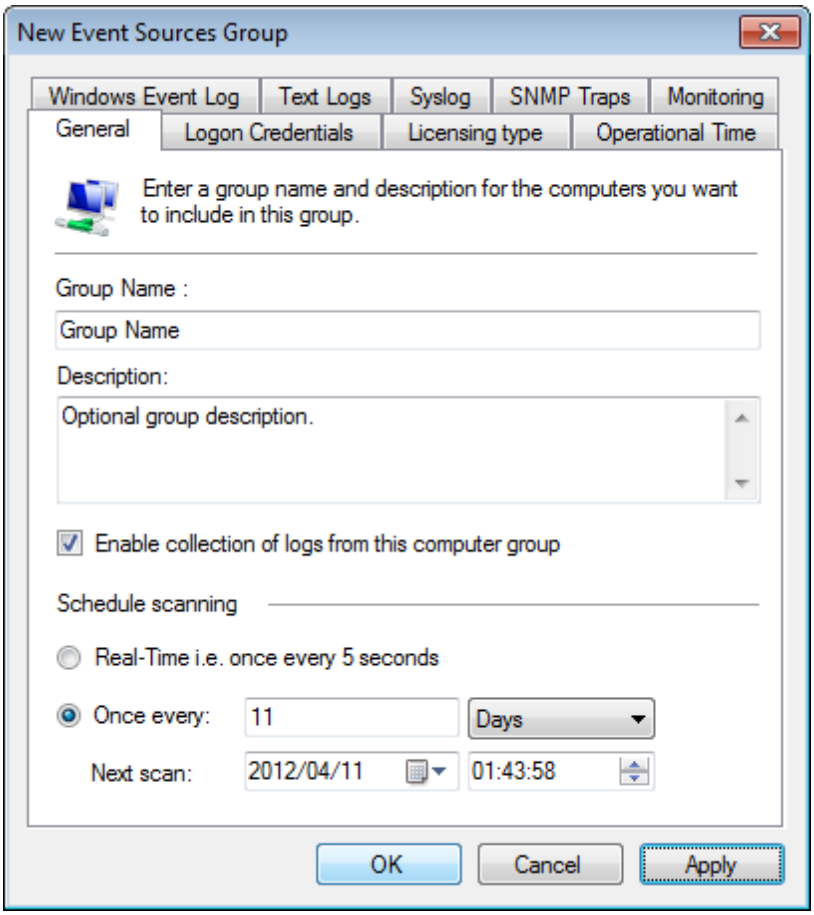
Grouping event sources into Event Source Groups improves the speed at which you configure event sources. Once an event source group is configured, every member of that particular group inherits the same settings.

To create a new event source group:

1. Click **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. Right-click **All event sources** and select **Create group…**

3. Select the license type. Choose between **Workstation** and **Server** license.



Screenshot 22: Add new event source group

4. Key in a unique name and an optional description. Select the tabs described below, and configure the available options:

Table 15: Event source group options

Tab Name	Description
General	Enable collection of events and schedule the scanning process. For more information, refer to Configuring general event source properties (page 47).
Logon credentials	Configure the username and password used to login target machines and collect information. For more information, refer to Configuring event source logon credentials (page 48).
Licensing type	Select the type of license to use. Select between **Workstation** and **Server**.
Operational time	Configure the operational time that computers are normally used. For more information, refer to Configuring event source operational time (page 50).
Monitoring	Enable GFI EventsManager system monitoring on target computers and configure the audits to perform. Monitoring checks enable administrators to identify system problems at the very early stages to prevent system down-time. For more information, refer to Configuring event source monitoring (page 51).
Windows Event Log	Specify the logs to collect and configure archive settings for Windows event logs. For more information, refer to Collecting Windows event logs (page 73).
Text Logs	Specify the logs to collect and configure settings for W3C/HTTP/CSV logs. This tab is only available when creating a server group. For more information, refer to Collecting Text logs (page 76).
Syslog	Specify the logs to collect and configure archive settings for Syslogs. This tab is only available when creating a server group. For more information, refer to Collecting Syslogs (page 79).
SNMP Traps	Specify the logs to collect and configure archive settings for SNMP Traps. This tab is only available when creating a server group. For more information, refer to Collecting SNMP Traps (page 83).

5. Click **Apply** and **OK**.

3.4 Configuring event source properties

GFI EventsManager allows you to customize the event source parameters to suit the operational requirements of your infrastructure. You can configure these parameters on single event sources or at event source group. Any member of a configured group inherits the same configuration, automatically.

This section contains information about:

- Configuring general event source properties
- Configuring logon credentials
- Configuring operational time
- Configuring event source monitoring
- Configuring event processing parameters

3.4.1 Configuring general event source properties

Use the General tab in the properties dialog to:

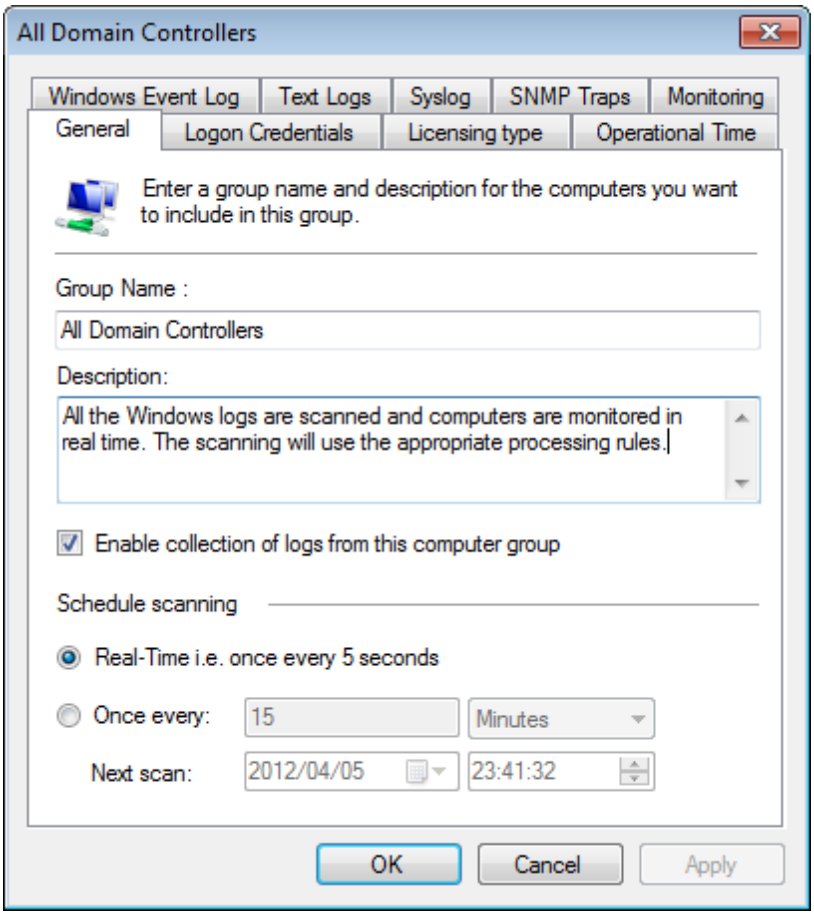
- Change the name of a computer group
- Enable/disable log collection and processing for the computers in a group
- Configure log collection and processing frequency.

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 23: Event sources properties dialog

3. From the **General** tab, configuring the options described below:

Table 16: Event source properties - General options

Option	Description
Group Name	Key in a unique name for the computer group.
Description	(Optional) Key in a description.
Enable collection of logs from this computer group	Select/unselect this option to enable/disable event log collection from the group.
Real-Time i.e. once every 5 seconds	Select this option to check for new event logs every 5 seconds. **Note** This is not recommended if members of this group generate high volumes of event logs because it may disrupt your network performance.
Once every	Specify a custom schedule for when GFI EventsManager checks for new event logs.

4. Click **Apply** and **OK**.

3.4.2 Configuring event source logon credentials

During event processing, GFI EventsManager must remotely log-on to the target computers. This is required in order to collect log data that is currently stored on the target computers and to pass this data on to the event processing engine(s).

To collect and process logs,GFI EventsManager must have administrative privileges over the target computers. By default, GFI EventsManager will log-on to target computers using the credentials of the account under which it is currently running; however, certain network environments are configured to use different credentials to log on to workstations and servers with administrative privileges.

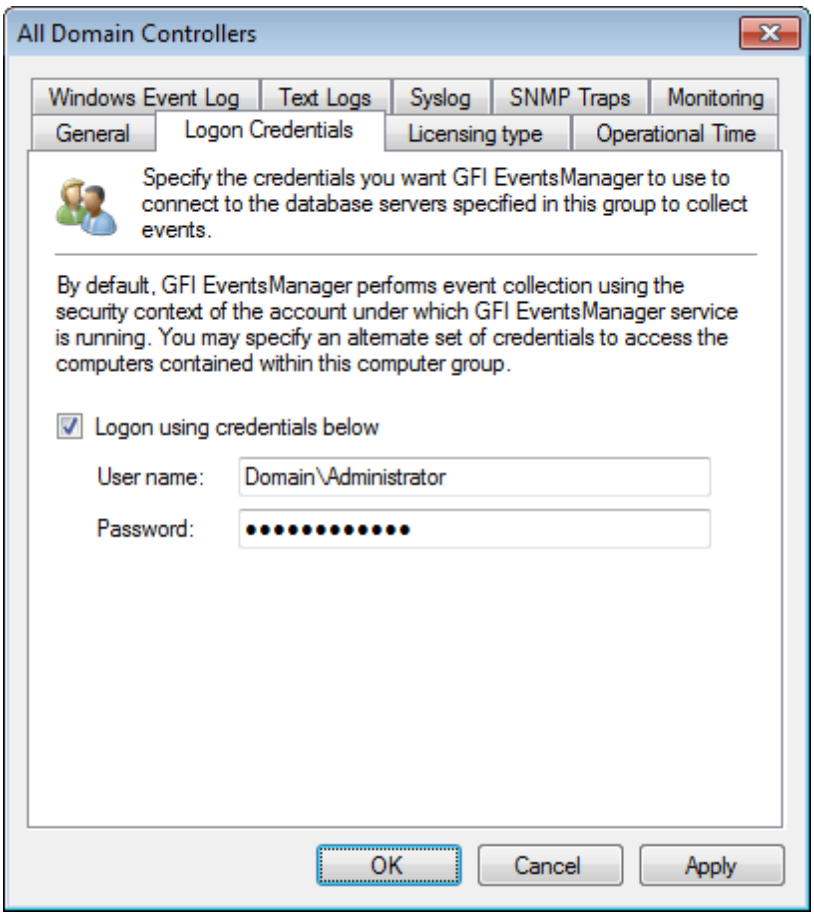
As an example, for security purposes, you might want to create an administrator account that has administrative privileges over workstations only and a different account that has administrative privileges over servers only.

To configure event source properties:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 24: Configuring alternative logon credentials

3. From **Logon Credentials** tab, select/unselect **Logon using credentials below**. By default this option is unselected, meaning that the event source will inherit the credentials from the parent group.

4. Specify the User name and Password.

5. Click **Apply** and **OK**.

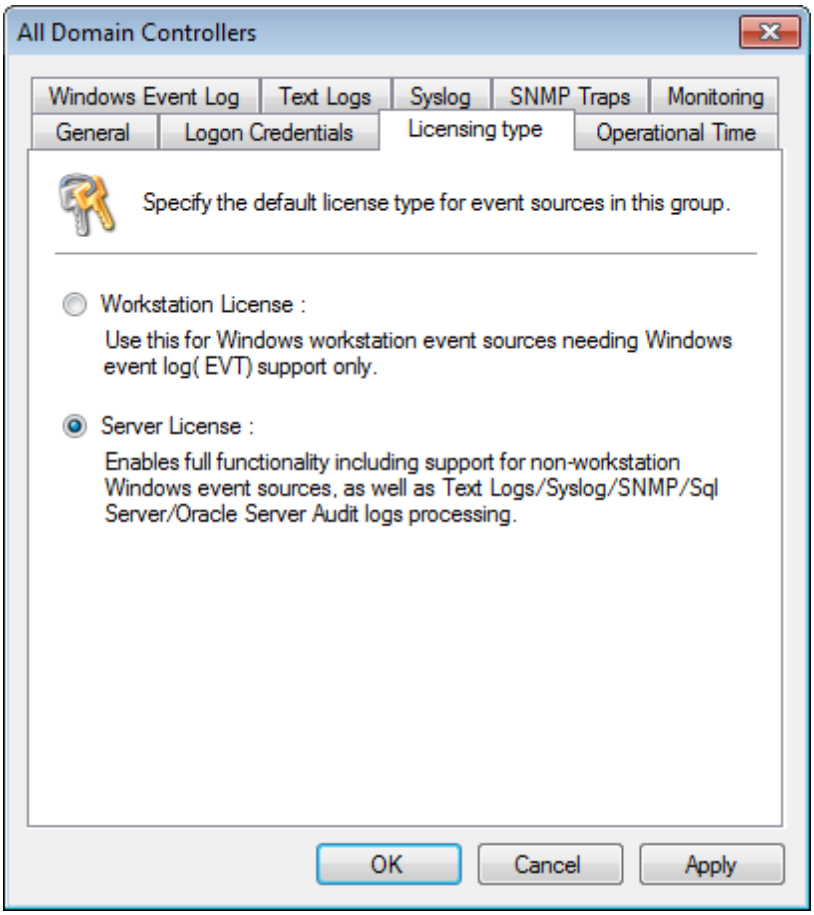
3.4.3 Configuring event source license type

To configure event source properties:

1. From **Configuration** tab > **Event Sources** > **Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 25: Configuring event source license type

3. From Licensing type tab, select from:

- **Workstation license** - enables Windows event log (EVT) support only
- **Server license** - enables full functionality for collecting Text logs, Syslogs, SNMP Traps, etc.

4. Click **Apply** and **OK**.

3.4.4 Configuring event source operational time

GFI EventsManager includes an Operational Time option through which you specify the normal working hours of your event source groups. This is required so thatGFI EventsManager can keep track of the events that occur both during and outside working hours.

Use the operational time information for forensic analysis; to identify unauthorized user access, illicit transactions carried outside normal working hours and other potential security breaches that might be taking place on your network.

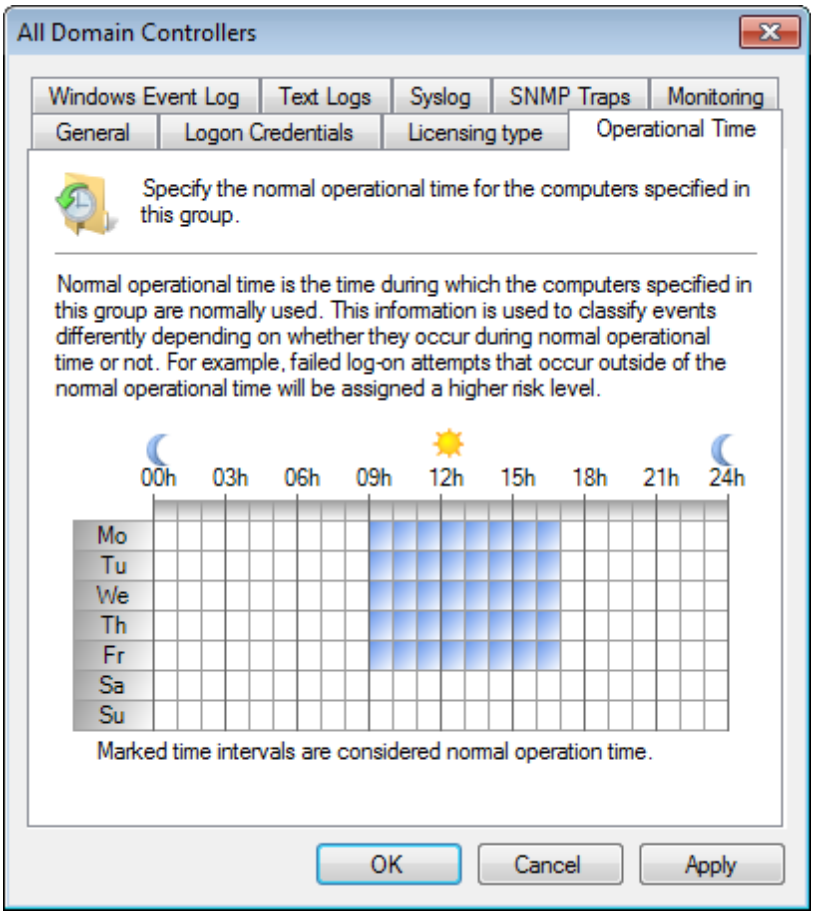
Operational time is configurable on computer group basis. This is achieved by marking the normal working hours on a graphical operational time scale which is divided into one hour segments.

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 26: Specify operational time

3. From **Operational Time** tab, mark the time intervals of your normal working hours. Marked time intervals are considered normal operational time.

4. Click **Apply** and **OK**.

3.4.5 Configuring event source monitoring

GFI EventsManager is able to collect additional information about your event sources through System Monitoring Checks. These checks generate specific events which in turn, trigger real-time notifications or execute an action.

For example, when monitoring **CPU usage** checks, GFI EventsManager queries that event source and detects whether the target machine is performing at the specified CPU usage levels.

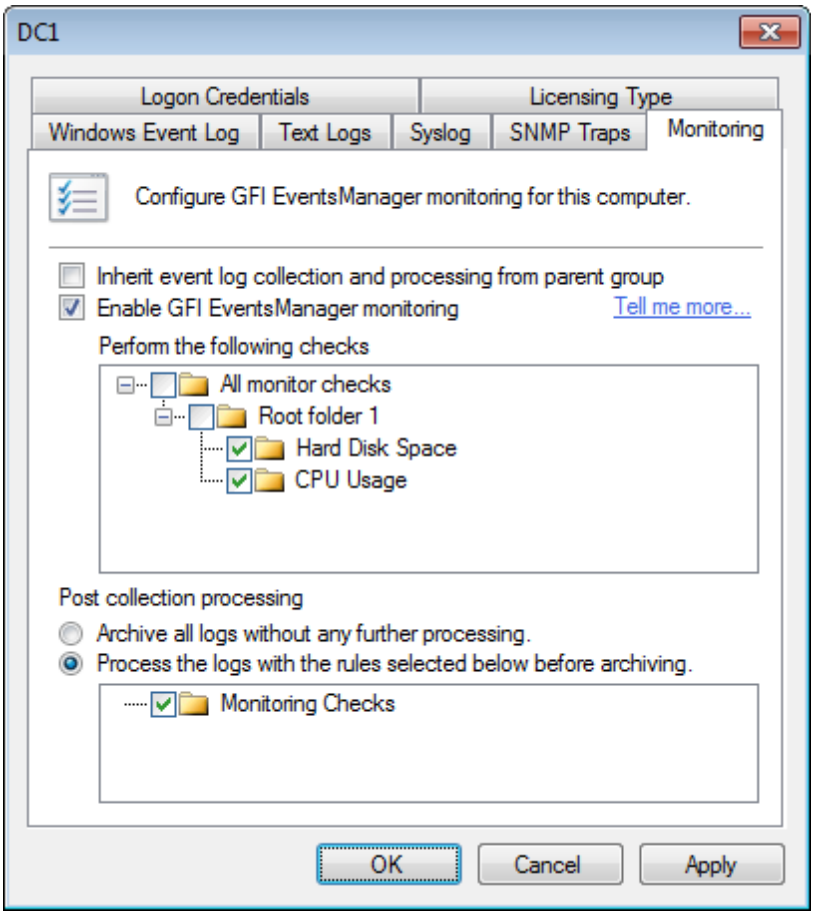
> **Note**
>
> For more information, refer to System Monitoring Checks (page 158).

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 27: Event source properties - Monitoring tab

3. From **Monitoring** tab, configure the options described below:

Table 17: Event source monitoring options

Option	Description
Inherit event log collection and processing from parent group	This option is available when enabling monitoring on a single event source. If you enabled monitoring on the group containing the event source, leave this option selected to obtain the same settings.
Enable GFI EventsManager monitoring	Select/unselect this option to enable/disable system monitoring checks.
Perform the following checks	Expand the list of checks and select the ones which you want to apply to your event source/event source group. For information about creating monitoring checks, refer to Creating a new monitoring check.
Archive all logs without any further processing	Select this option to store events without applying any further checks (from Events Processing Rules).
Process the logs with the rules selected below before archiving	Expand the list of rules which are applied to the collected logs. GFI EventsManager enables you to create custom rules and configure them to trigger when one of the system monitoring check generates an event. Then, through the configuration of the selected Event Processing Rule, actions are executed and/or alerts are generated. Once a monitoring check is enabled, browse for the event that it generates and create a rule based on that event. For more information, refer to Creating new rules from existing events (page 152).

4. Click **Apply** and **OK**.

3.4.6 Configuring event processing parameters

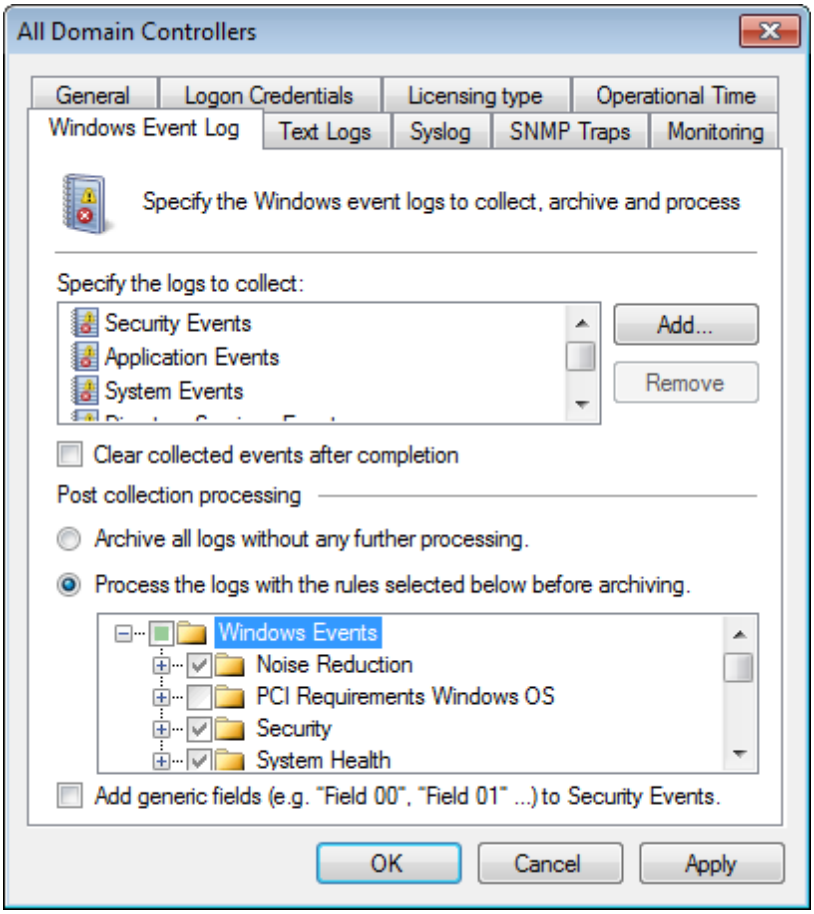
Event processing parameters are enabled only for event sources/event source groups licensed as Servers. Server event sources posses more settings than normal workstations, in order to collect Windows event logs, Text logs, Syslogs and SNMP Traps.

To configure event source properties:

1. From **Configuration** tab **> Event Sources > Group Type**, select **Event Sources Groups**.

2. To configure the parameters of:

- **Computer group** - Right-click on the computer group to be configured and select **Properties**
- **Single event source** - Right-click on the required event source and select **Properties**.



Screenshot 28: Event processing configuration tabs

3. Use the **Windows Event Log**, **Text Logs**, **Syslog** and **SNMP Traps** tabs configure the required event processing parameters.

4. Click **Apply** and **OK**.

Note

For more information, refer to:

- Collecting Windows Event Logs
- Collecting Text logs
- Collecting Syslogs
- Collecting SNMP Traps.

3.5 Database sources

GFI EventsManager can monitor and process events from database servers. Database event sources require specific configuration settings to listen to and collect events generated by database activity.

This section contains information about:

- Configuring Microsoft SQL Server sources
- Configuring Oracle Server sources

3.5.1 Microsoft SQL Server Sources

This section contains information about:

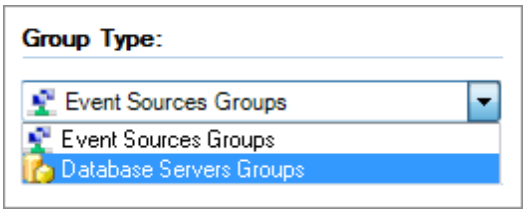
- Creating a new Microsoft SQL Server group
- Adding a new Microsoft SQL Server event source

Creating a new Microsoft SQL Server group

To create a Microsoft SQL Server group:

1. Click **Configuration** tab > **Event Sources**.

2. From **Group Type**, select **Database Servers Groups**.



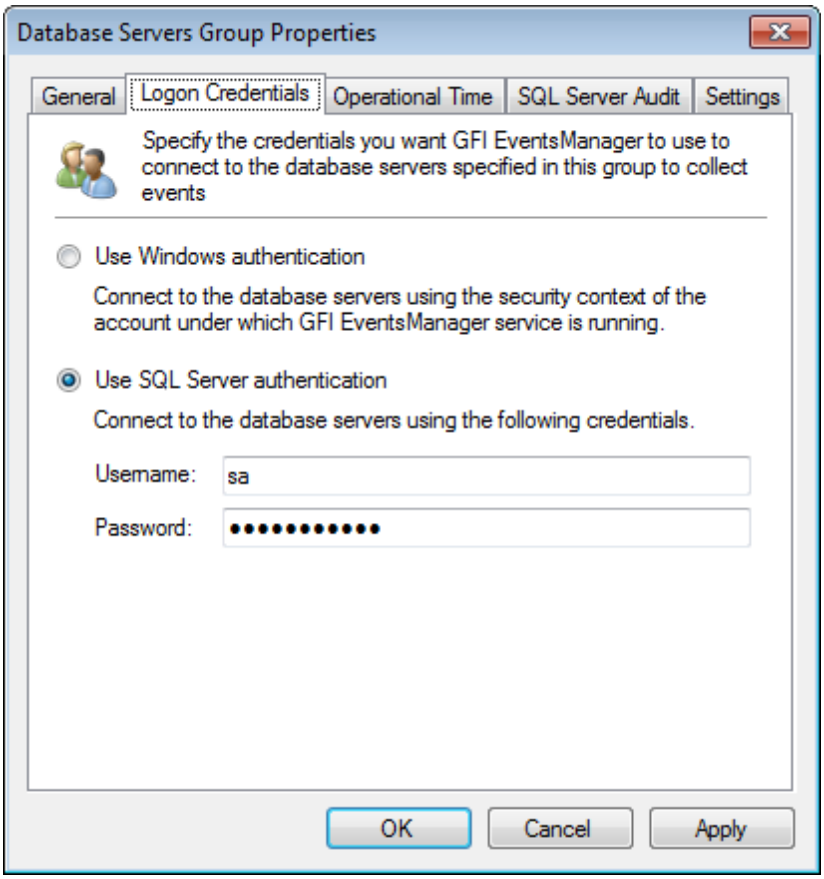
Screenshot 29: Database Servers Groups

3. From **Groups**, right-click **Microsoft SQL Servers** and select **Create group...**

4. Select **Microsoft SQL Server** as the server type and from **General** tab configure the options described in below:

Table 18: Microsoft SQL Database group: General tab

Option	Description
Group Name	Key in a group name to identify the Microsoft SQL server group.
Description	(Optional) Key in a description.
Collects logs from the database servers included in this group	Enable option to collect database events from all servers in this group.

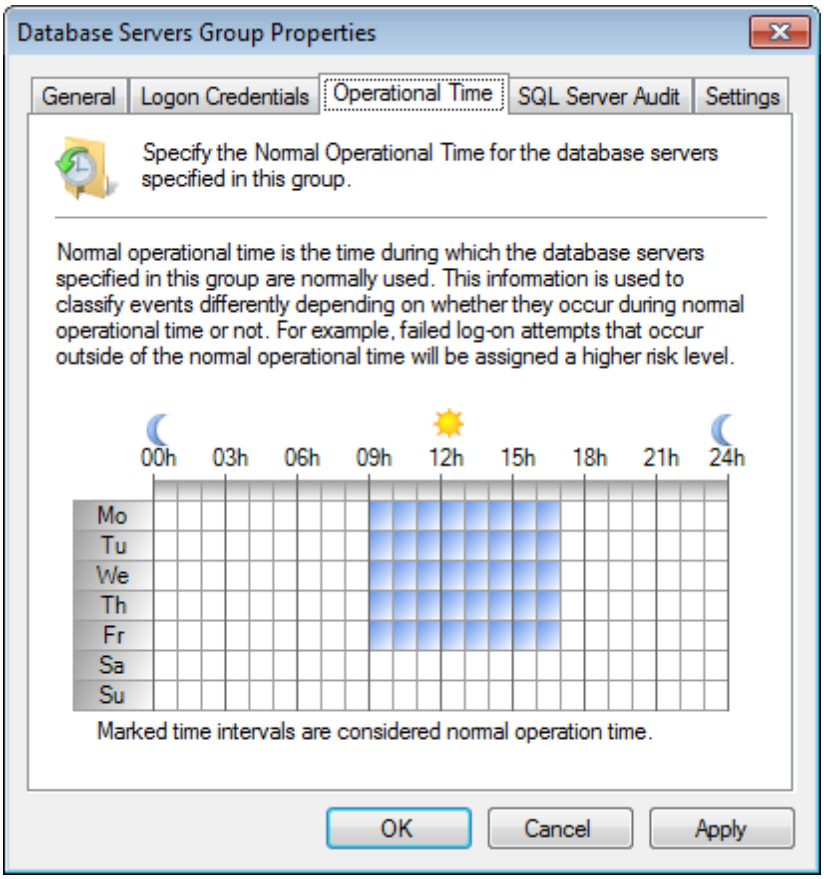


Screenshot 30: Configure logon settings from the Logon Credentials tab

4. Select **Logon Credentials** tab and configure the options described below:

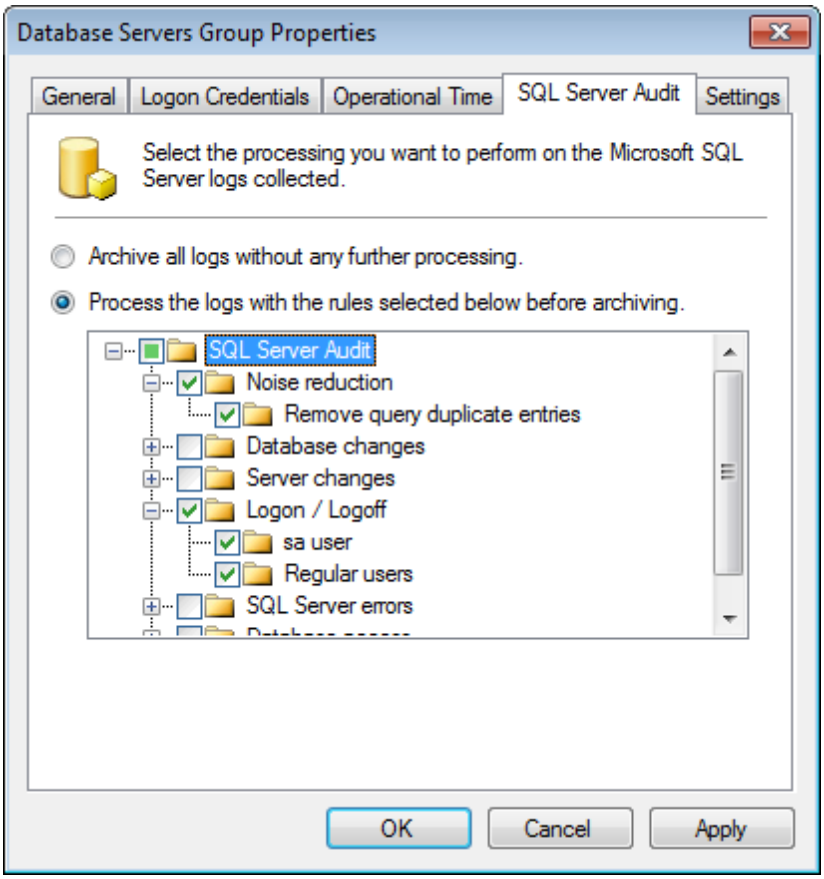
Table 19: Microsoft SQL Database group: Logon Credentials

Option	Description
Use Windows authentication	Connect to the Microsoft SQL Database using windows authentication.
Use SQL Server authentication	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.



Screenshot 31: Configure the normal working hours from Operational Time tab

5. Select **Operational Time** and configure the operational time when the database is normally used. Marked time intervals are considered normal working hours.

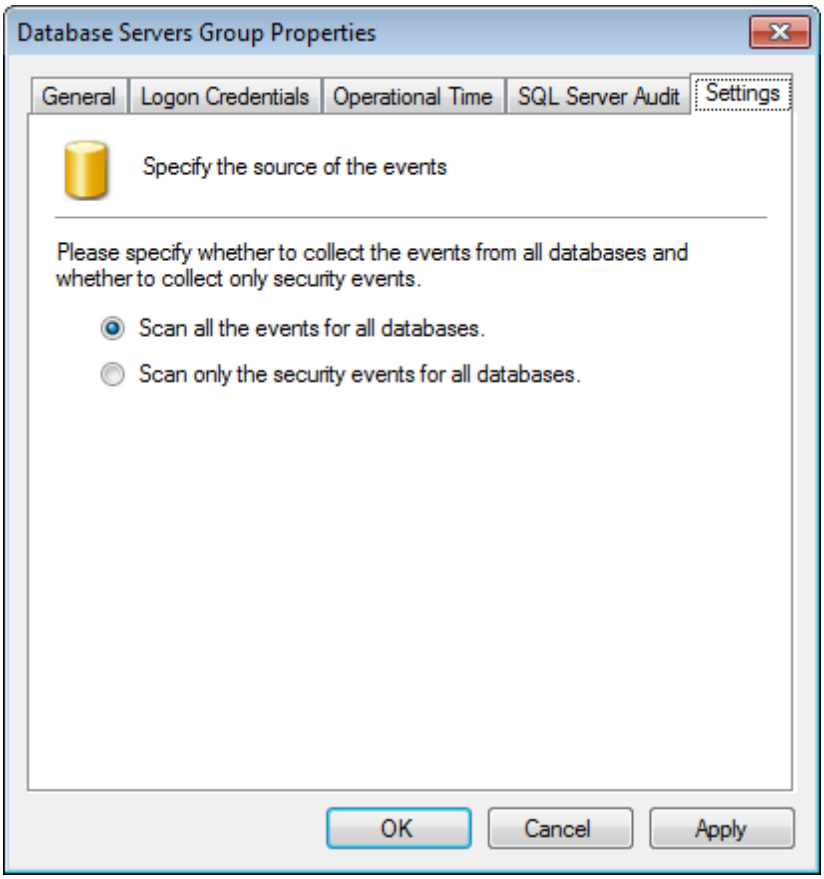


Screenshot 32: Configure SQL Server Auditing from SQL Server Audit tab

6. Select **SQL Server Audit** tab and configure the options described below:

Table 20: Microsoft SQL Database group -SQL Server Audit

Option	Description
Archive all logs without further processing	Archive events in GFI EventsManager database backend without applying processing rules.
Process the logs with the rules selected below before archiving	Specify the rules to perform before archiving events in GFI Events-Manager database backend.



7. Select **Settings** tab and configure the options described in below:

Table 21: Microsoft SQL Database group - Settings

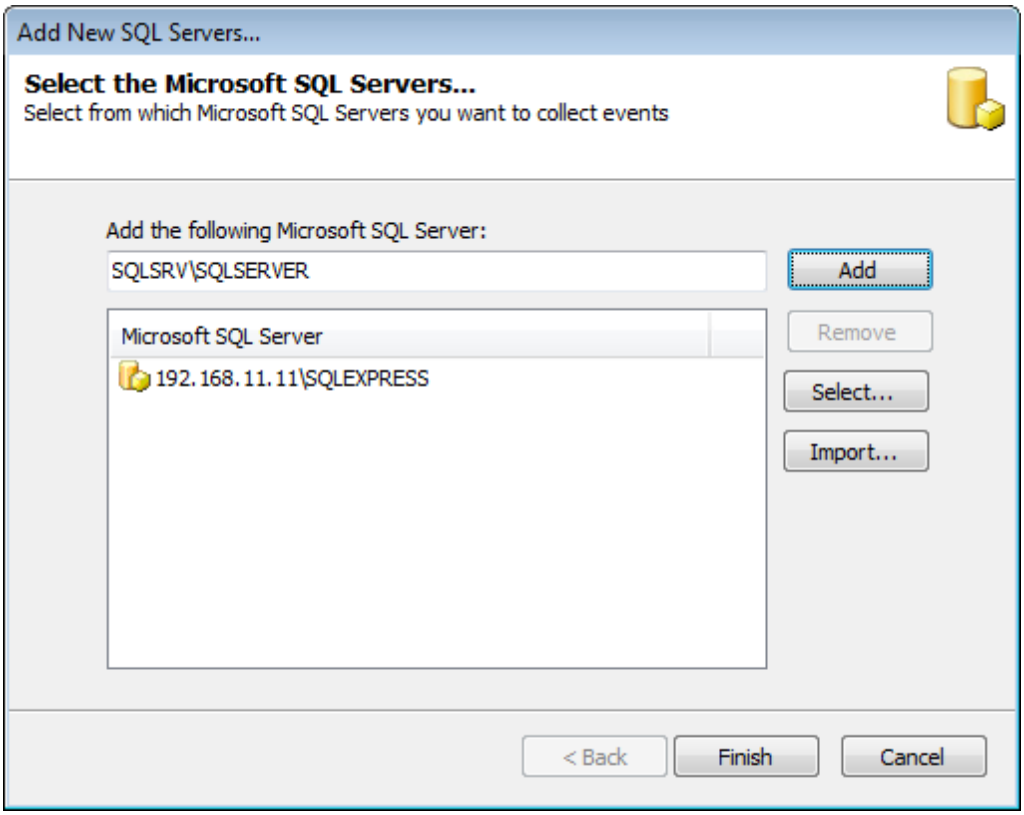
Option	Description
Scan all the events for all databases	All Microsoft SQL Server events are collected and processed by GFI EventsManager.
Scan only security events for all databases	Only security events are collected and processed by GFI EventsManager.

8. Click **Apply** and **OK**.

Adding a new Microsoft SQL Server event source

To add a new Microsoft SQL Server source:

1. Right-click a database group and select **Add new SQL Server...**



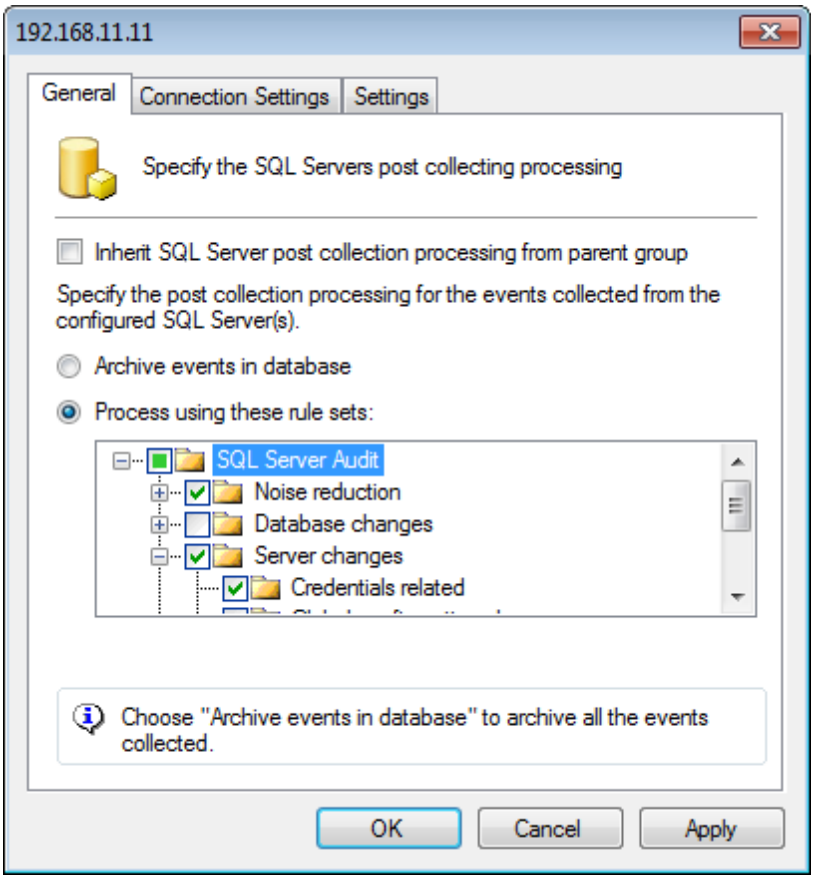
Screenshot 33: Add new Microsoft SQL server

2. Key in the server name or IP and click **Add**.

> **Note**
>
> Use **Select** and **Import** to search the network for SQL Servers or import list of SQL servers from a text file respectively.

3. Click **Finish** and the Add New SQL Servers dialog closes.

4. From **Groups**, select **SQL Servers** and from the right pane, double-click the new Microsoft SQL Database instance.

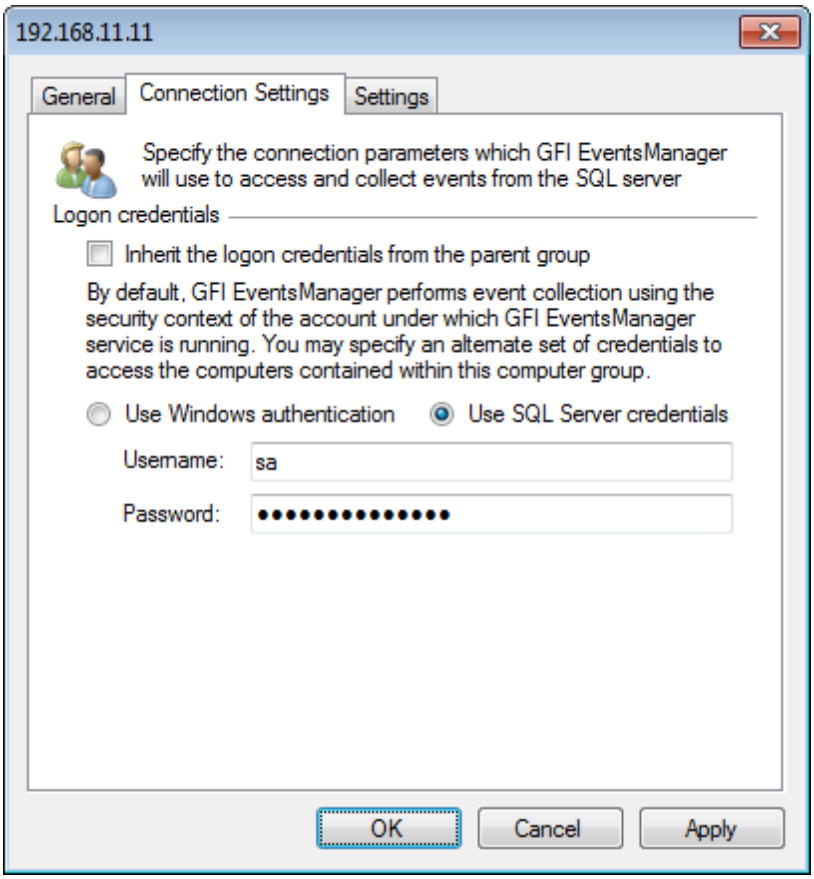


Screenshot 34: Microsoft SQL Database properties: General tab

5. From **General** tab, configure the options described below:

Table 22: Microsoft SQL Database - General tab options

Option	Description
Inherit SQL Server post collecting processing from parent group	Inherits all settings from the parent group.
Archive events in database	Archive events in GFI EventsManager database backend without applying processing rules.
Process using these rule sets	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

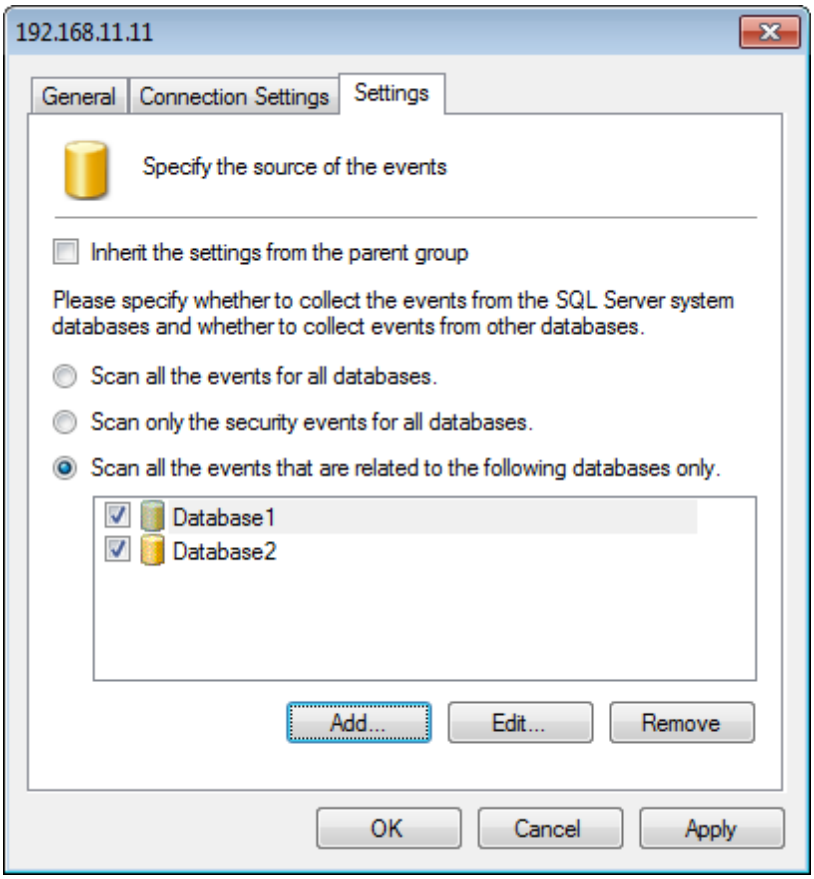


Screenshot 35: Microsoft SQL Database properties: Connection Settings tab

6. Select **Connection Settings** and configure the options described below:

Table 23: Microsoft SQL Database - Connection Settings tab

Option	Description
Inherit the logon credentials from the parent group	Select this option to inherit login settings from the parent group.
Use Windows authentication	Connect to Microsoft SQL Database using windows authentication.
Use SQL Server credentials	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.



Screenshot 36: Microsoft SQL Database properties: Settings tab

7. Select **Settings** tab and configure the options described below:

Table 24: Microsoft SQL Database - Settings tab options

Option	Description
Inherit the settings from the parent group	Inherits settings from the parent group.
Scan all the events for all databases	Scan all databases and collect all events from the Microsoft SQL Server.
Scan only the security events for all databases	Scan all databases and collect only security events from the Microsoft SQL Server.
Scan all the events that are related to the following databases only	Collect all events from the selected databases. Use Add, Edit and Remove to manage database sources.

8. Click **Apply** and **OK**.

3.5.2 Oracle server sources

GFI EventsManager enables you to collect and process events generated by Oracle Relational database management systems. The following audits are collected and processed by GFI EventsManager:

Table 25: Oracle Server supported audits

Audit	Description
Session auditing	Audit user sessions and database access.
Statement auditing	Audit processed SQL statements.
Object auditing	Audit queries and statements related to specific objects.

The following Oracle Database versions are supported:

- Oracle Database 9i
- Oracle Database 10g
- Oracle Database 11g

This section contains information about:

- Pre-configuration settings for Oracle Servers event sources
- Creating a new Oracle Server group
- Adding a new Oracle Server event source

Pre-configuration settings for Oracle Servers event sources

Before adding Oracle Server event sources, follow the steps below on each Oracle Server instance you want to monitor:

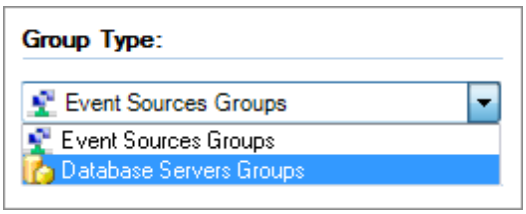
Table 26: Oracle Server configuration stages

Pre-configuration Step	Description
Step 1	Ensure the logon credentials used to connect, set audits and access the audit table has the necessary permissions.
Step 2	Enable auditing on the Oracle Server by changing startup parameters. To enable auditing: 1. Startup parameters for the Oracle servers are stored in: `<Oracle Home Directory>\admin\<Oracle SID>\pfile\init.ora.` 2. Locate and open the parameters file using a text editor. 3. Locate **AUDIT_TRAIL** parameter and change the default value to '**db**' or '**db_extended**' ('db, extended' on latest versions of Oracle). 4. Save and restart the Oracle server.

Adding a new Oracle Server group

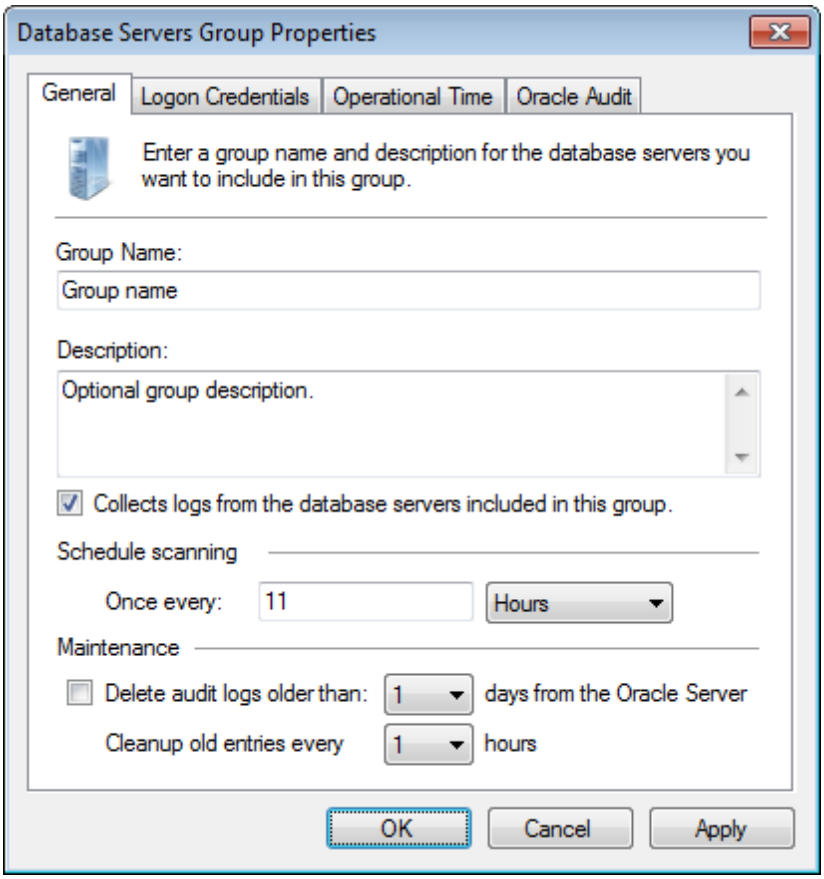
To add a new Oracle Database group:

1. Click **Configuration** tab > **Event Sources**. From **Group Type**, select **Database Servers Groups**.



Screenshot 37: Database Servers Groups

2. From **Groups**, right-click **Oracle Servers** and select **Create group…**

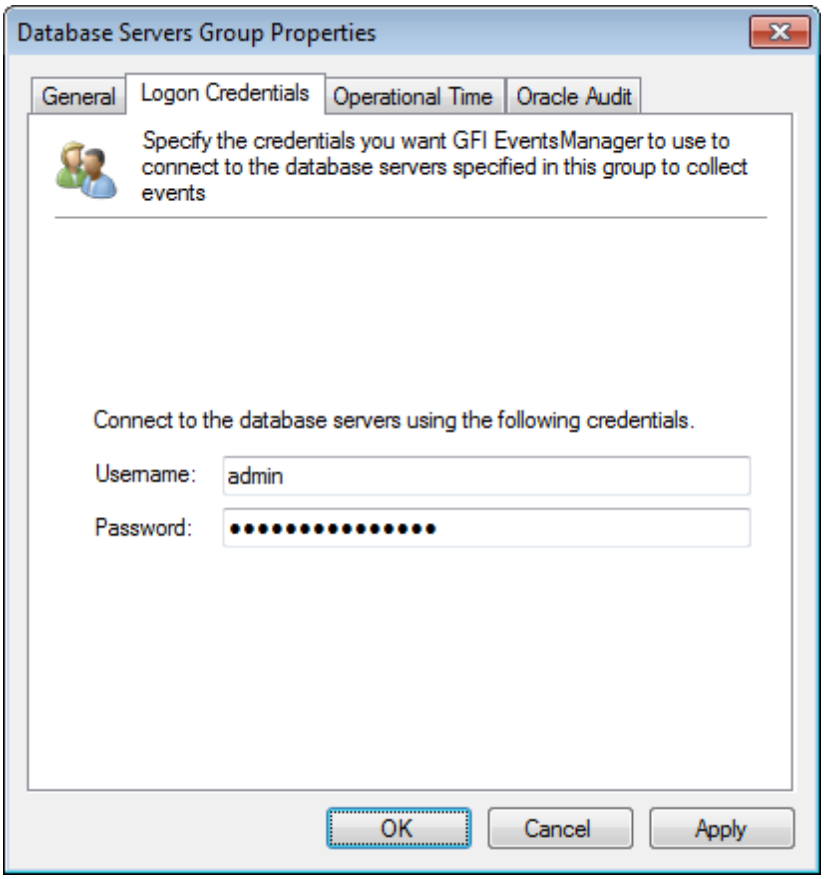


Screenshot 38: Oracle Database group - General tab

3. From **General** tab, configure the options described in below:

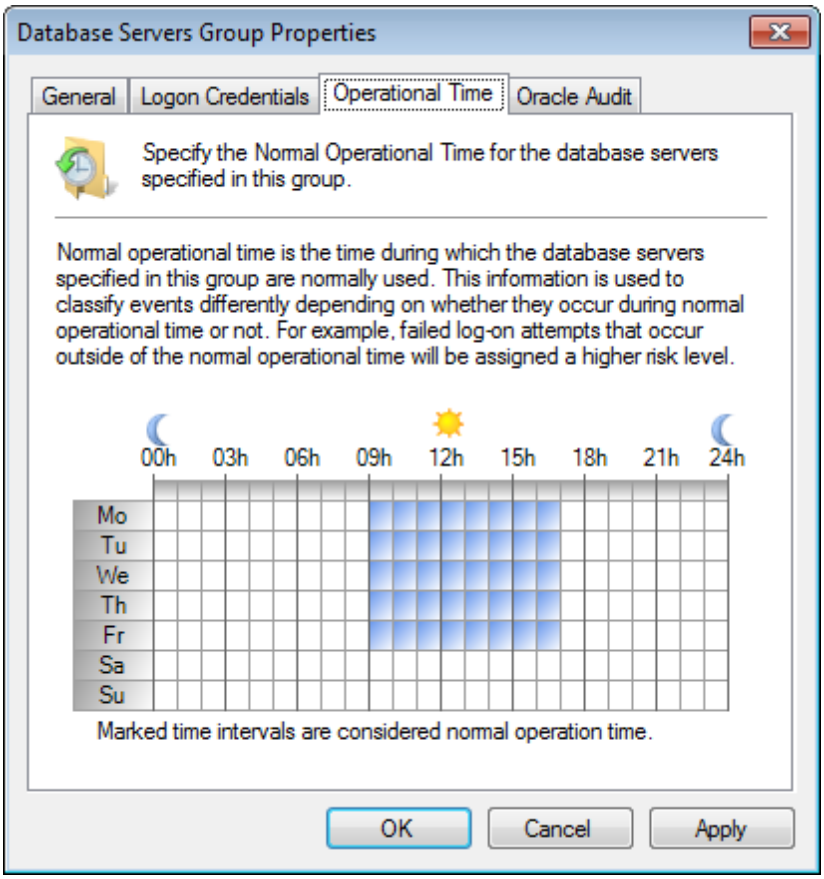
Table 27: Oracle Database group - General tab

Option	Description
Group Name	Key in a group name to identify the Oracle Database group.
Description	Optionally, key in a description.
Collects logs from the database servers included in this group	Collects events from the event sources in the Oracle group. Once this option is enabled, configure the Schedule scanning and Maintenance options.
Schedule scanning	Specify the frequency to collect events on a pre-defined schedule.
Maintenance	Oracle audit events are stored in a specific audit table on the Oracle server. To prevent excessive audit table growth, configure the options in this section to delete audit logs and old entries on a pre-defined time.



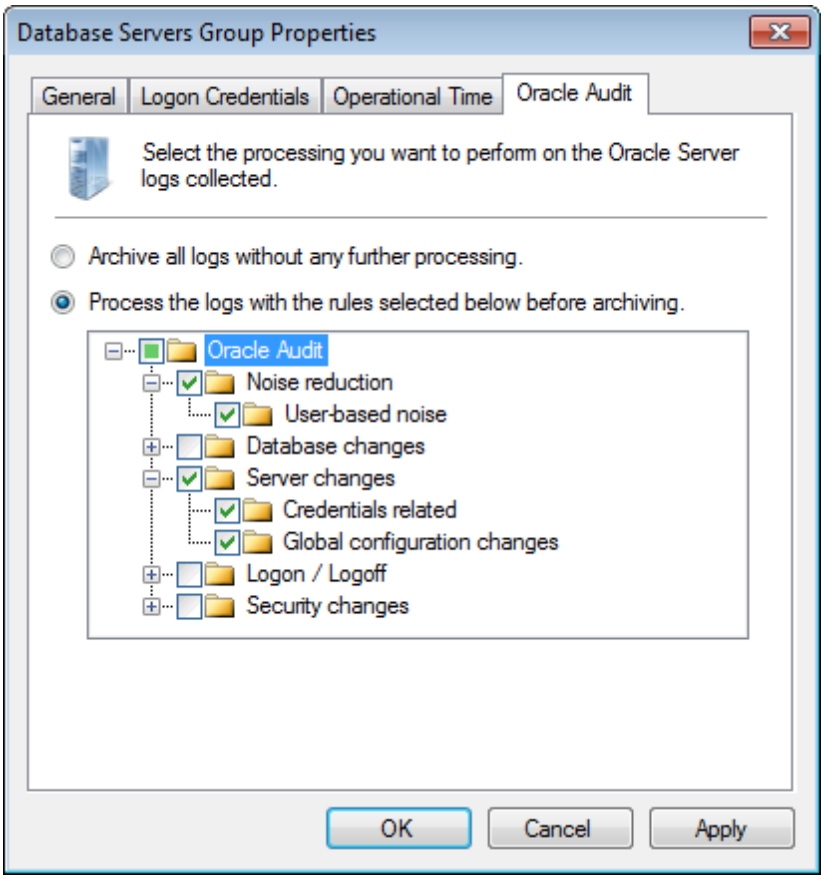
Screenshot 39: Oracle Database group - Logon Credentials tab

4. Select **Logon Credentials** tab and key in a valid username and password to connect to the Oracle server.



Screenshot 40: Oracle Database group - Operational Time tab

5. Select **Operational Time** tab and configure the normal operational time of the Oracle Database servers in this group.



Screenshot 41: Oracle Database group - Oracle Audit tab

6. Select **Oracle Audit** and configure the options described below:

Table 28: Oracle Database group - Oracle Audit

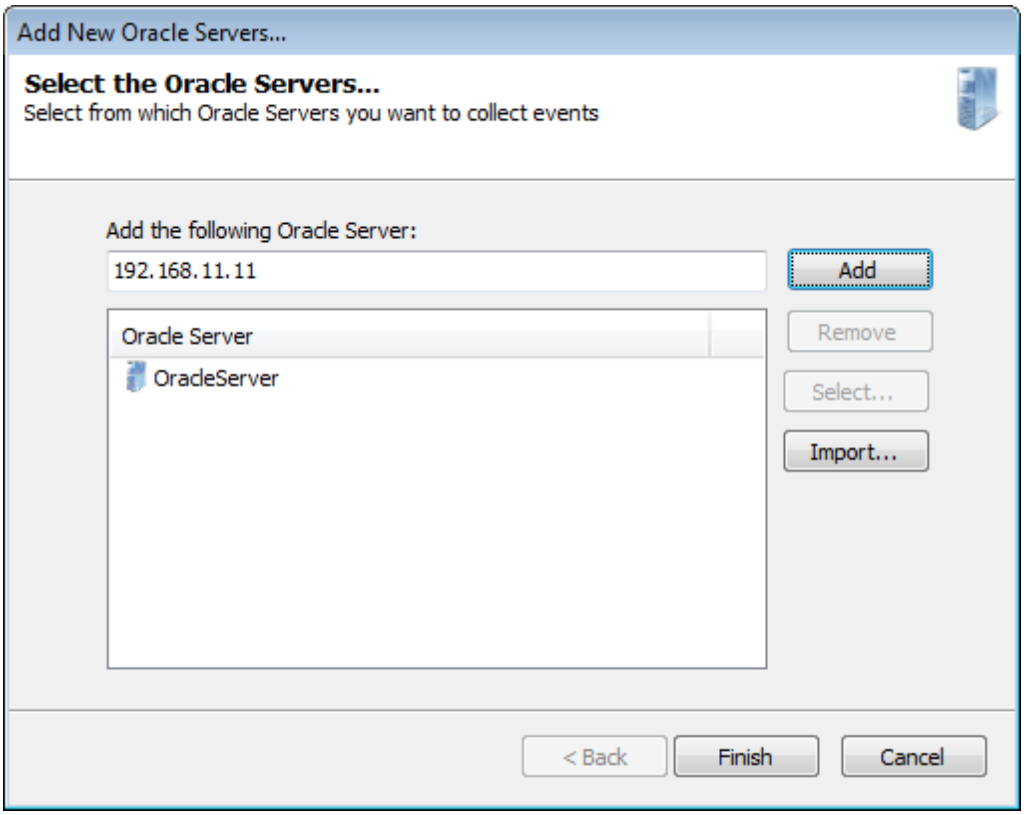
Option	Description
Archive all logs without further processing	Archive events in GFI EventsManager database backend without applying processing rules.
Process the logs with the rules selected below before archiving	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

7. Click **Apply** and **OK**.

Adding a new Oracle Server event source

To add a new Oracle Database to a database group:

1. Right-click an Oracle Server group and select **Add new Oracle Server...**

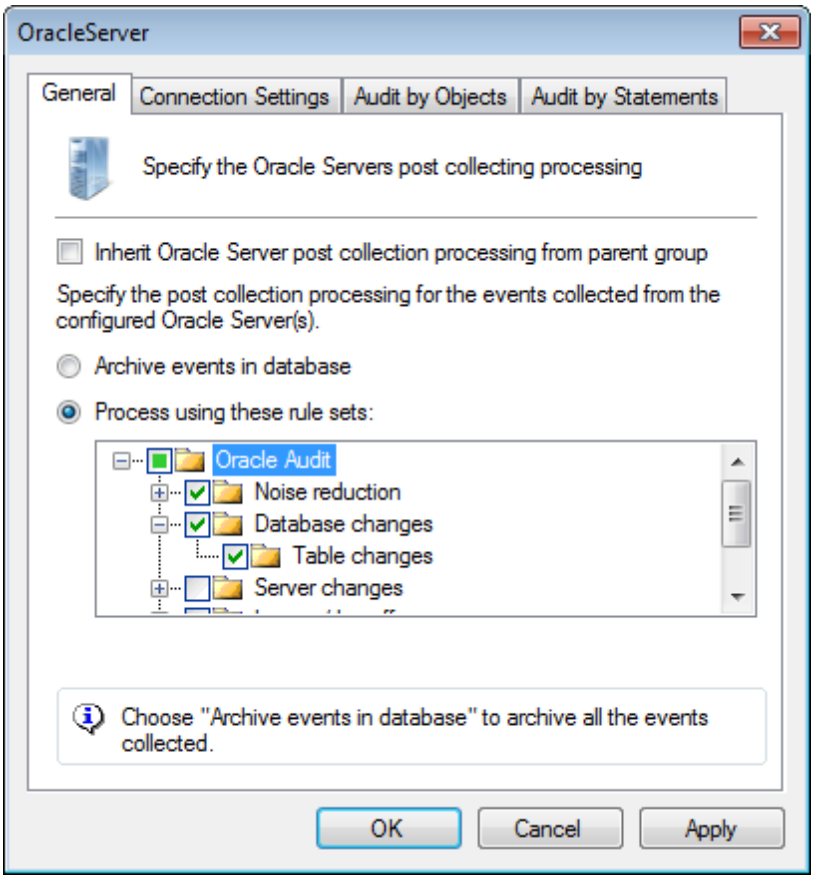


Screenshot 42: Add new Oracle server

2. Key in the server name or IP and click **Add**.

3. Click **Finish** and the Add New Oracle Servers dialog closes.

> **Note**
>
> Use **Select** and **Import** to search the network for SQL Servers or import list of SQL servers from a text file respectively.

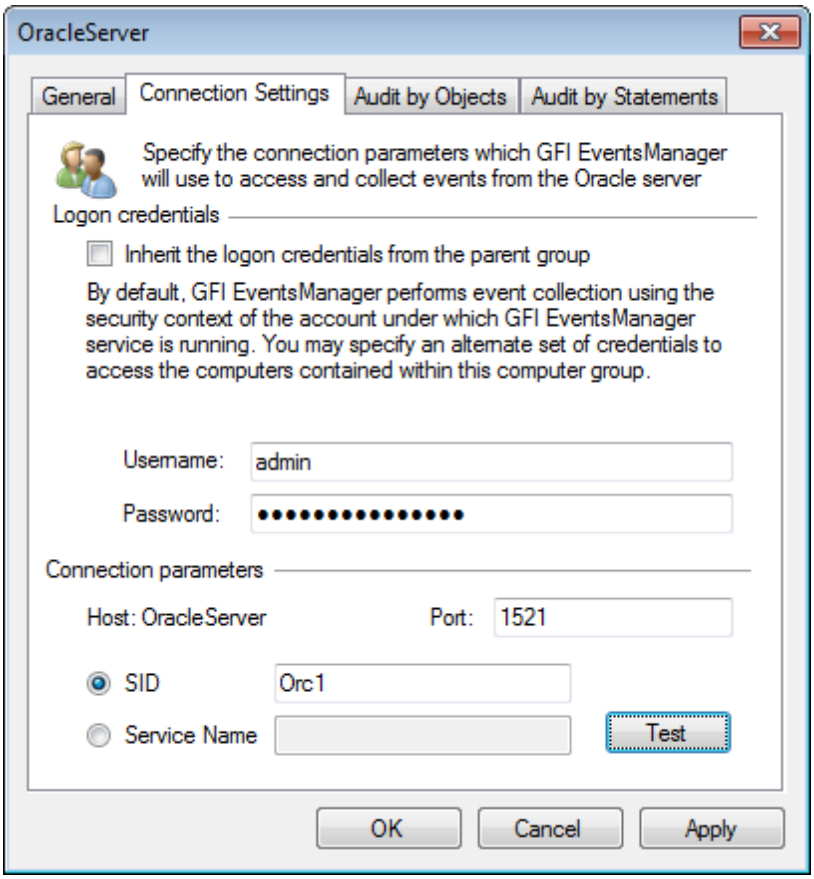


Screenshot 43: Oracle Server properties - General tab

4. From the right pane, double-click the new oracle server event source and configure the options described below:

Table 29: Oracle Server properties - General tab

Option	Description
Inherit Oracle Server post collecting processing from parent group	Select to inherit all settings from the parent group.
Archive events in database	Archive events in GFI EventsManager database backend without applying processing rules.
Process using these rule sets	Specify the rules to perform before archiving events in GFI Events-Manager database backend.

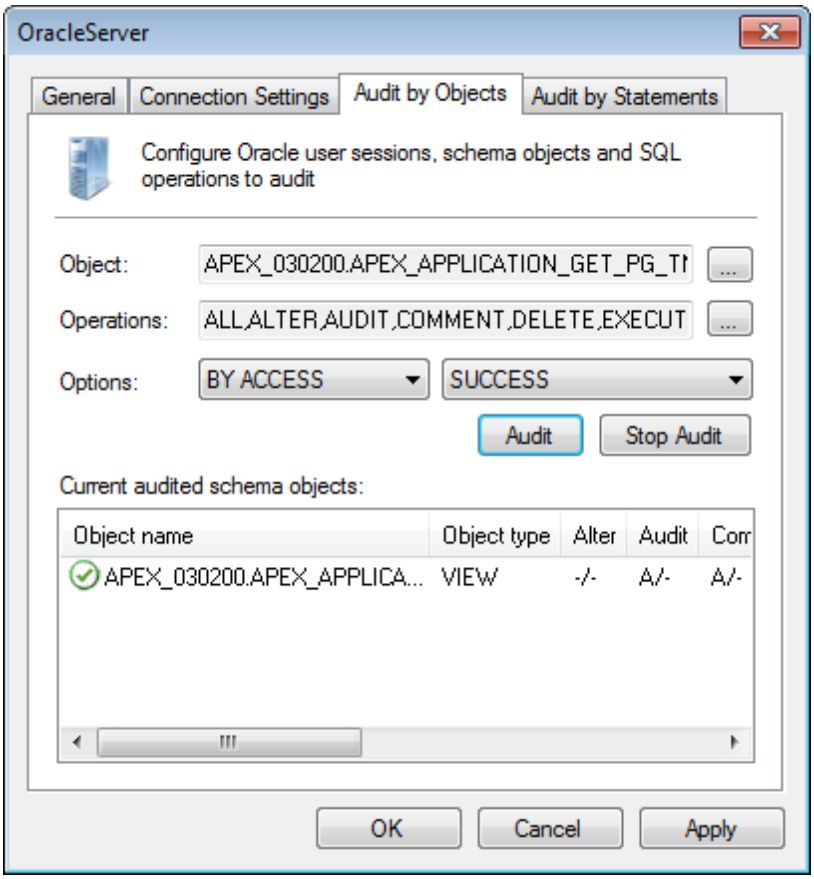


Screenshot 44: Oracle Server properties - Connection Settings tab

5. Select **Connection Settings** and configure the options described below:

Table 30: Oracle Server properties - Connection Settings tab

Option	Description
Inherit the logon credentials from the parent group	Select to inherit login settings from the parent group.
Port	Key in the port to use to connect to the Oracle Database.
SID	The SID is a unique name to identify an Oracle Database instance. Key in the SID of the database to audit.
Service Name	The Service name is the alias used to identify the Oracle Database. Key in the Service name of the database to audit.
Test	Test the connection with the Oracle Database server.

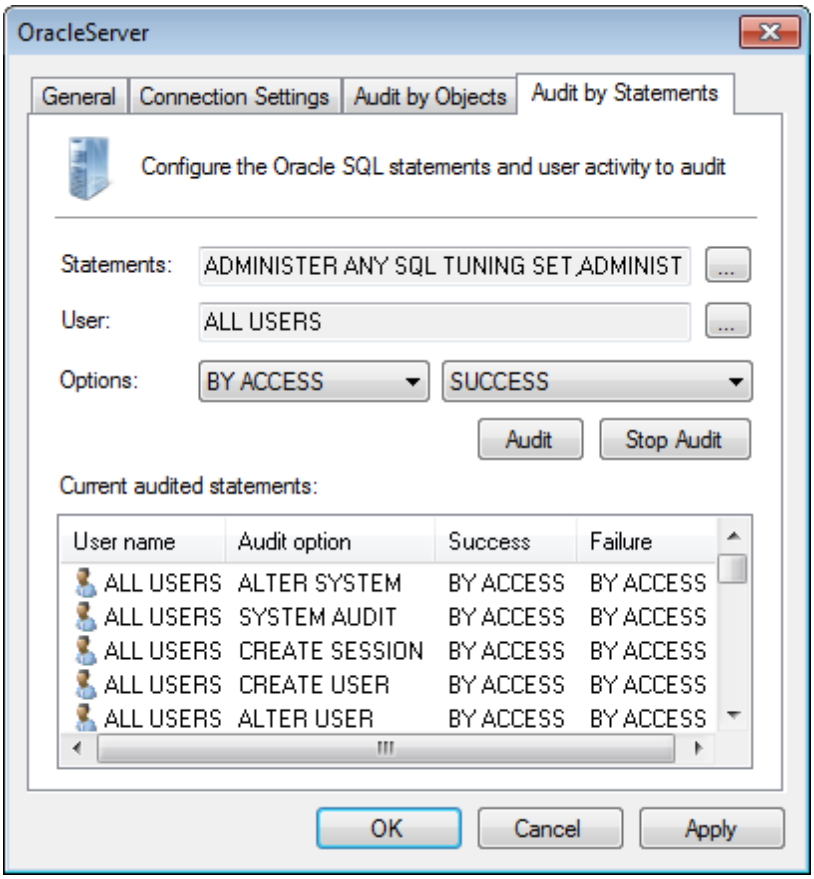


Screenshot 45: Oracle Server properties - Audit by Objects tab

6. Select **Audit by Objects** and configure the options described below:

Table 31: Oracle Server properties - Audit by Objects tab

Option	Description
Object	Click **Browse** to launch a list of available Oracle objects. Select the object to audit and click **OK**. **NOTE**: Amongst others, Oracle objects can be procedures, views, functions and tables.
Operations	Operations are actions that modify or query an object. Click **Browse** to launch a list of available operations. Select the operations to audit and click **OK**.
Options	Select the audit options: » **By Access** - Creates an audit log per object operation execution. » **By Session** - Creates an audit log per operation and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Select to process only successful audits. » **Failure** - Select to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Current audited schema objects	A list that displays all current Oracle audited schema.



Screenshot 46: Oracle Server properties - Audit by Statements tab

7. Select **Audit by Statements** and configure the options described below:

Table 32: Oracle Server properties - Audit by Statements tab

Option	Description
Statements	Click **Browse**to launch a list of available Oracle statements. Select the Oracle statements to audit and click **OK**. **NOTE**: Amongst others, Oracle statements can be **ALTER**, **CREATE** and **SELECT** .
User	Oracle enables you to audit statements for a specific user. Click **browse** button to launch a list of available users. Select the user and click **OK**.
Options	Select audit options: » **By Access** - Creates one audit log for each statement execution. » **By Session** - Creates one audit log per user and per schema object. A session is the time between a connection and a disconnection to/from the database. » **Success** - Processes only successful audits. » **Failure** - Select option to process only failed audits. Oracle will create an audit log if an audit fails to complete. » **Both** - Select option to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (such as users, statements, etc.)
Current audited state-ments	A list that displays all current Oracle audited statements.

8. Click **Apply** and **OK**.

4 Collecting Event Logs

This chapter provides you with information about how to configure your event sources to apply events processing rules to collected events. Assign existing or custom events processing rules to precisely process the events wanted only.

Topics in this chapter:

4.1 Collecting Windows event logs

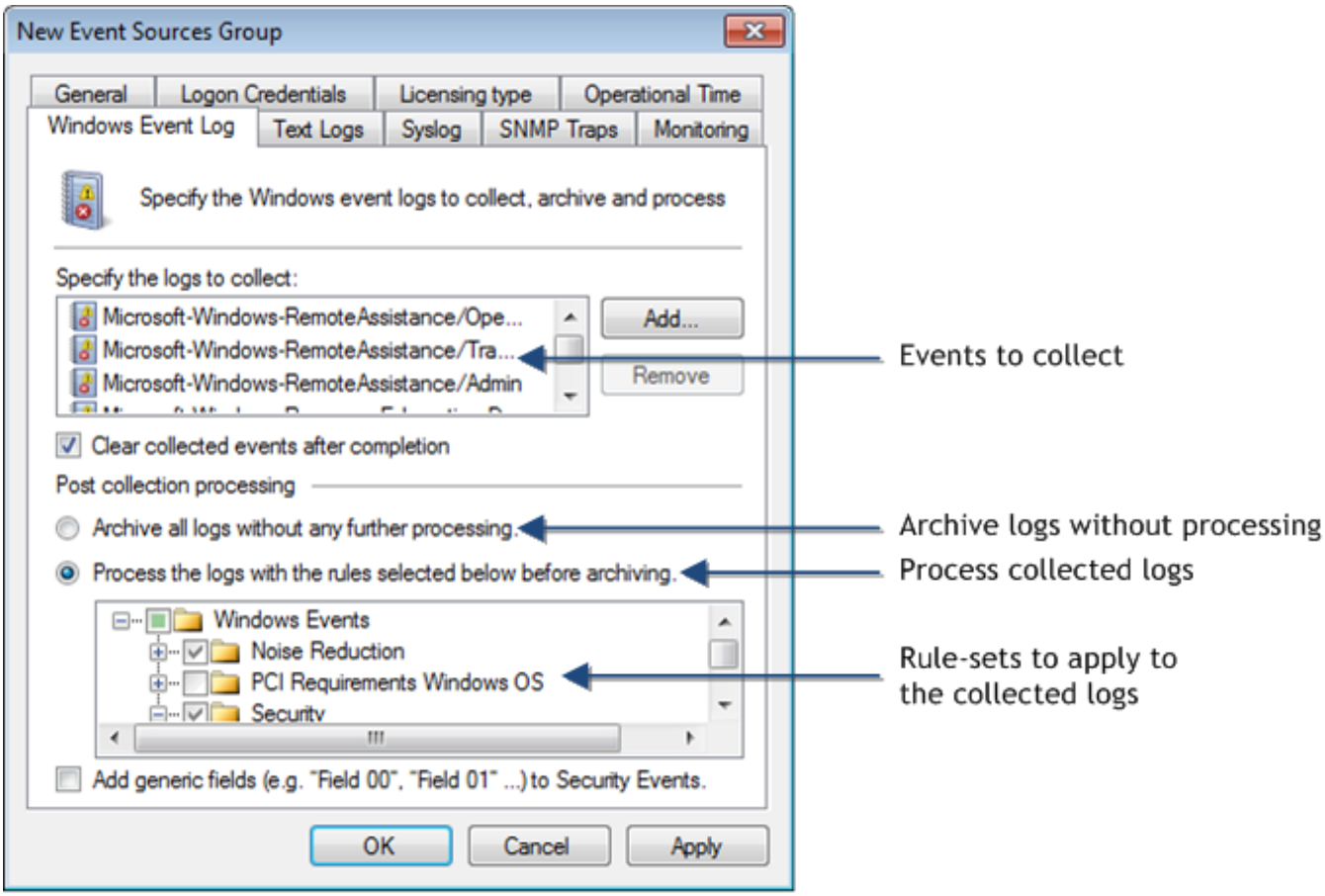
Windows events are organized into specific log categories; by default computers running on Windows NT or higher, record errors, warnings and information events in three logs namely **Security**, **Application** and **System logs**.

Computers that have more specialized roles on the network such as Domain Controllers, and DNS Servers have additional event log categories.

As a minimum, Windows Operating Systems record events in the following logs:

Table 33: Windows Event Logs collected by GFI EventsManager

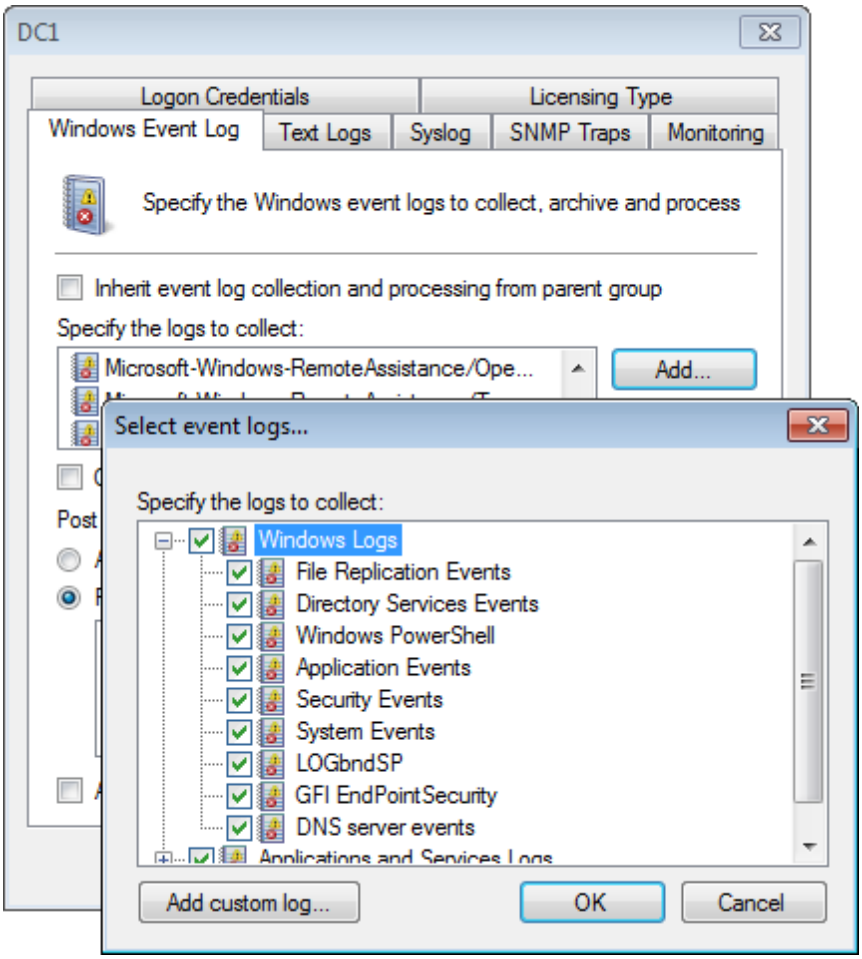
Log Type	Description
Security event log	This log contains security related events through which you can audit successful or attempted security breaches. Typical events found in the Security Events log include valid and invalid logon attempts.
Application event log	This log contains events recorded by software applications/programs such as file errors.
System event log	This log contains events logged by operating system components such as failures to load device drivers.
Directory service log	This log contains events generated by the Active Directory including successful or failed attempts to make to update the Active Directory database.
File Replication service log	This log contains events recorded by the Windows File Replication service. These including file replication failures and events that occur while domain controllers are being updated with information about Sysvol.
DNS server log	This log contains events associated with the process of resolving DNS names to IP addresses.
Application and Services Logs	These logs contain events associated with Windows VISTA and the relative services/functionality it offers.



Screenshot 47: Computer group properties: Configuring Windows Event Logs parameters

To configure Windows Event Log collection and processing parameters:

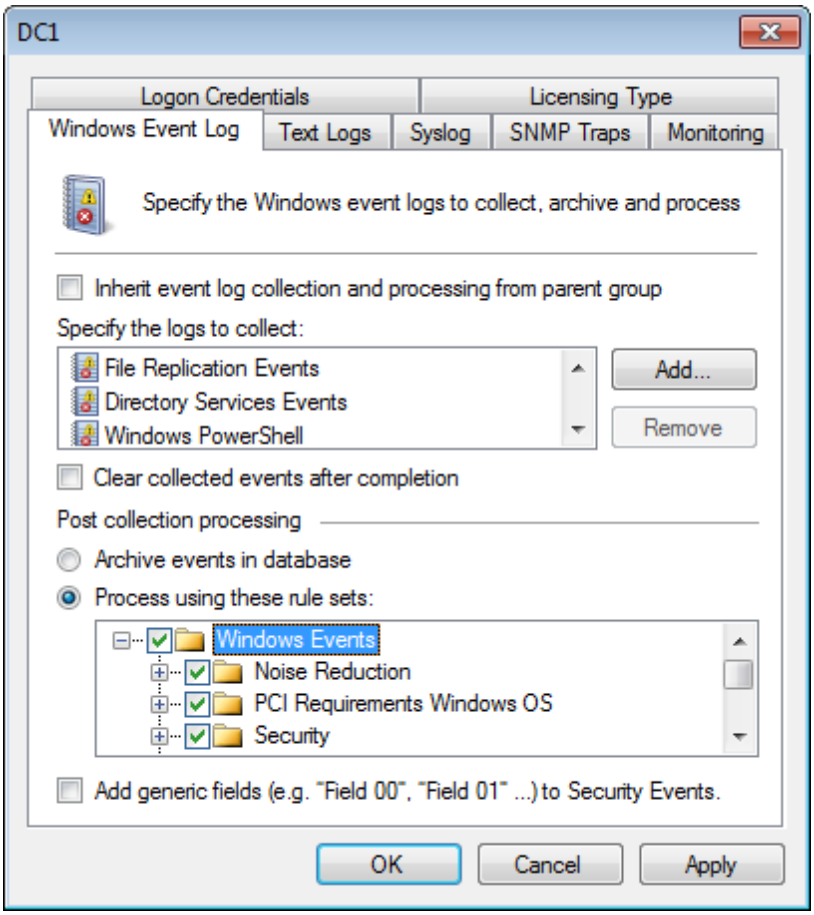
1. From **Configuration** tab **>** **Event Sources**, right-click an event source and select **Properties**.



Screenshot 48: Selecting event logs to collect

2. Click **Windows Event Log** tab > **Add...** to select the logs you want to collect. Expand **Windows Logs** and/or **Applications and Services Logs** and select from the list of available logs.

3. (Optional) Click **Add custom log...** and key in a unique name for the unlisted event log.



Screenshot 49: Configuring Windows Event Log Processing parameters

4. Select **Clear collected events after completion** to clear the collected events from the respective event source.

5. Select **Archive events in database** to archive collected events without applying events processing rules.

6. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

7. Select **Add generic fields** to add extended fields to the database. Extended fields contain data from event descriptions and are added by a common name (example: "Field01" "Custom field name").

8. Click **Apply** and **OK**.

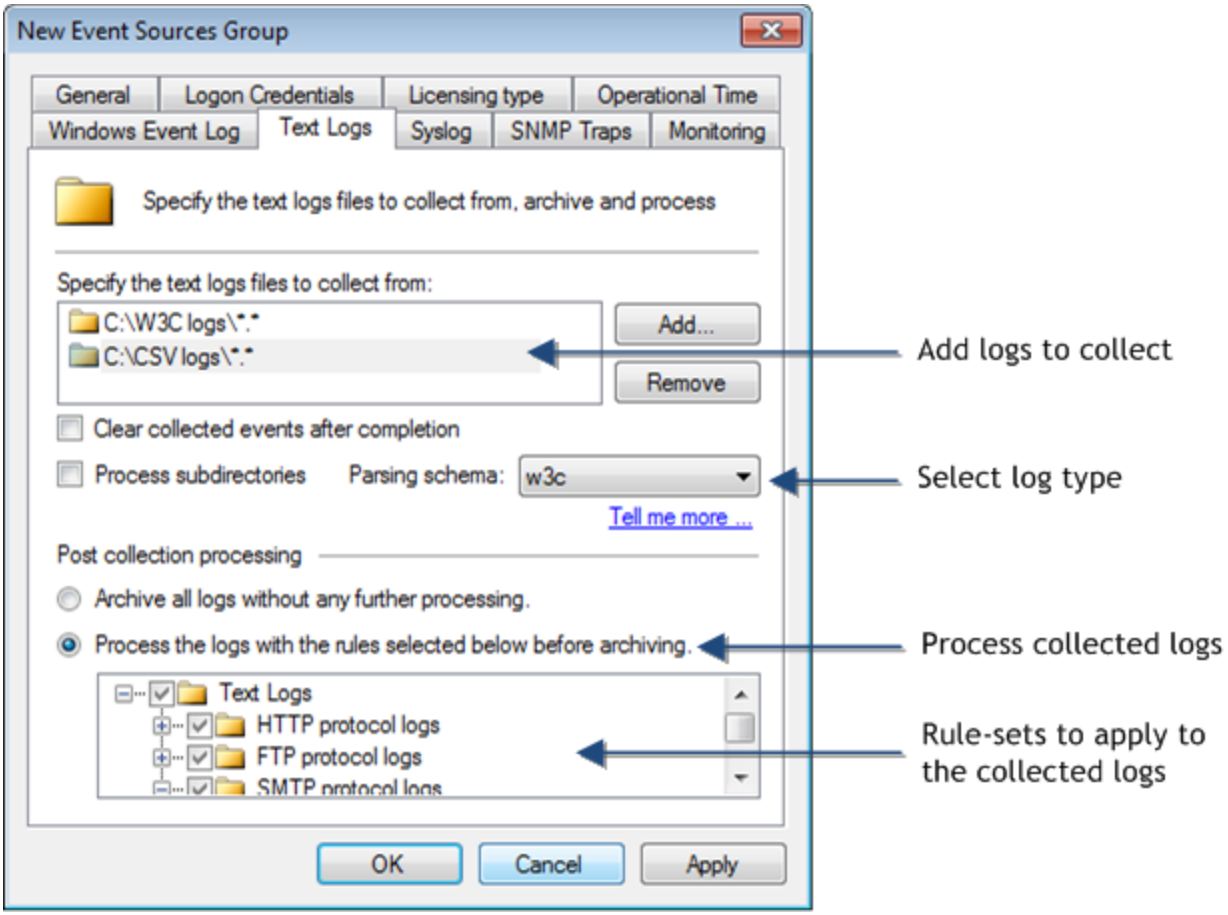
> **Important**
>
> Deleting event logs without archiving may lead to legal compliance penalties.

4.2 Collecting Text logs

W3C and CSV are other log formats supported by GFI EventsManager. W3C logs are text-based flat files containing various event details delimited by special characters.

The W3C log format is most commonly used by hardware systems (Example: servers and appliances) which have Internet specific roles. Microsoft Internet Information Server (IIS) service and Apache web servers for example, can collect web related events such as web logs, in the form of W3C formatted text files.

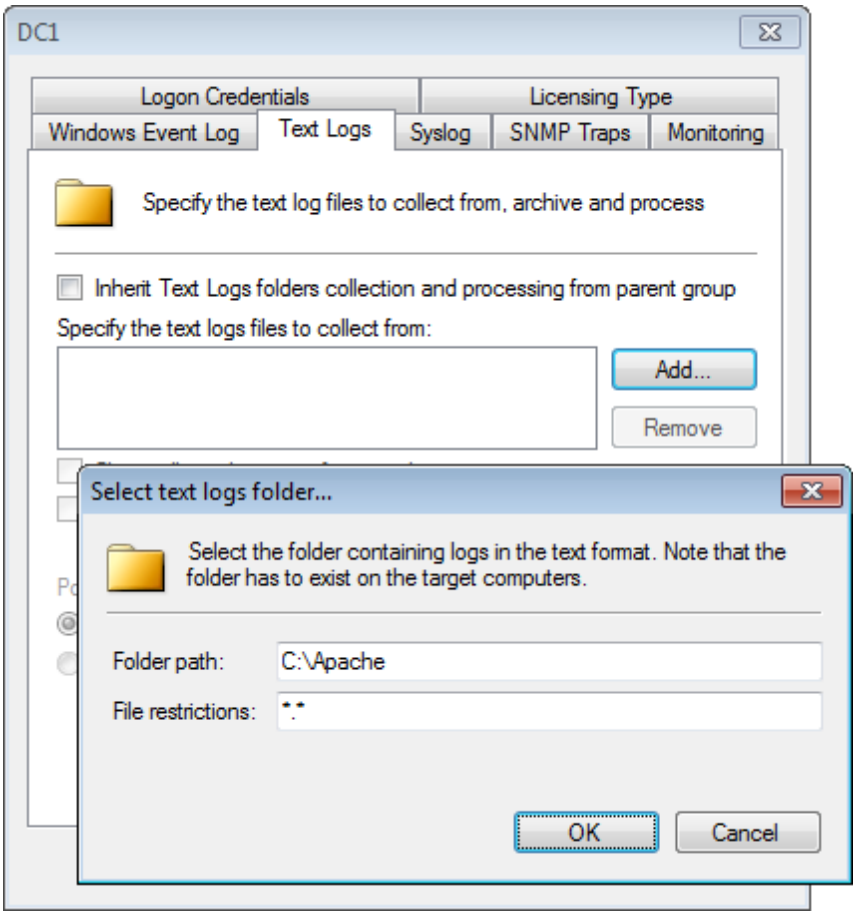
In GFI EventsManager, the configuration process of W3C log parameters is identical to that performed for Windows event processing, with one exception. Unlike Windows Event Logs, there is no standard which dictates a specific or centralized folder location where W3C log files are stored on disk. Therefore, in order to collect W3C logs, you must specify the complete path to these text-based log files.



Screenshot 50: Text logs options

To collect Text logs:

1. From **Configuration** tab > **Event Sources**, right-click an event source and select **Properties**.



Screenshot 51: Adding folders containing Text Logs

2. Click **Text Logs** tab > **Add...** to add folder paths containing Text Logs. Click **OK**.

3. Select **Clear collected events after completion** to clear the collected events from the respective event source.

4. Select **Process subdirectories** to recursively scan the specified path that contains W3C/CSV logs.

5. From **Parsing schema** drop-down menu, select the schema in which Text Logs are interpreted. Select from:

- W3C
- CSV
- EMS Logs.

6. Select **Archive events in database** to archive collected events without applying events processing rules.

7. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

8. Click **Apply** and **OK**.

Important

Deleting event logs without archiving may lead to legal compliance penalties.

4.3 Collecting Syslogs

Syslog is a data logging service that is most commonly used by Linux and UNIX based systems. The concept behind Syslogs is that the logging of events and information is entirely handled by a dedicated server called 'Syslog Server'.

Unlike Windows and W3C log based systems, Syslog enabled devices send events in the form of data messages (technically known as 'Syslog Messages') to a Syslog server that interprets and manages message and saves the data in a log file.

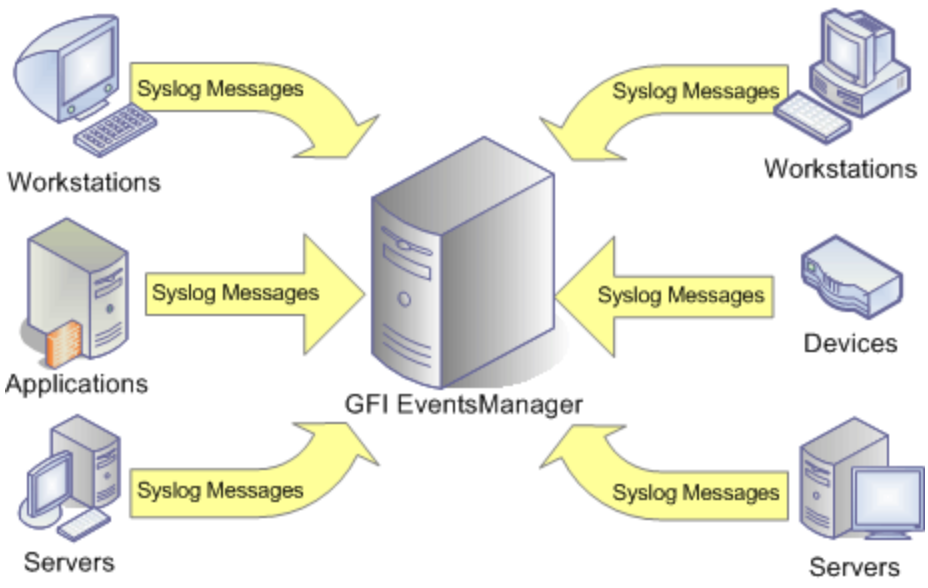
In order to process Syslog messages, GFI EventsManager ships with a built-in Syslog Server. This Syslog server will automatically collect, in real-time, all Syslog messages/events sent by Syslog sources and pass them on to the event processing engine. Out-of-the-box, GFI EventsManager supports events generated by various network devices manufactured by leading providers including Cisco and Juniper.

Note

For more information about supported devices visit the following KBASE article: http://kb.gfi.com/articles/SkyNet_Article/KBID002868?retURL=%2Fapex%2FSupportHome&popup=true

Note

A built-in buffer allows the Syslog server to collect, queue and forward up to 30 Syslog messages at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.



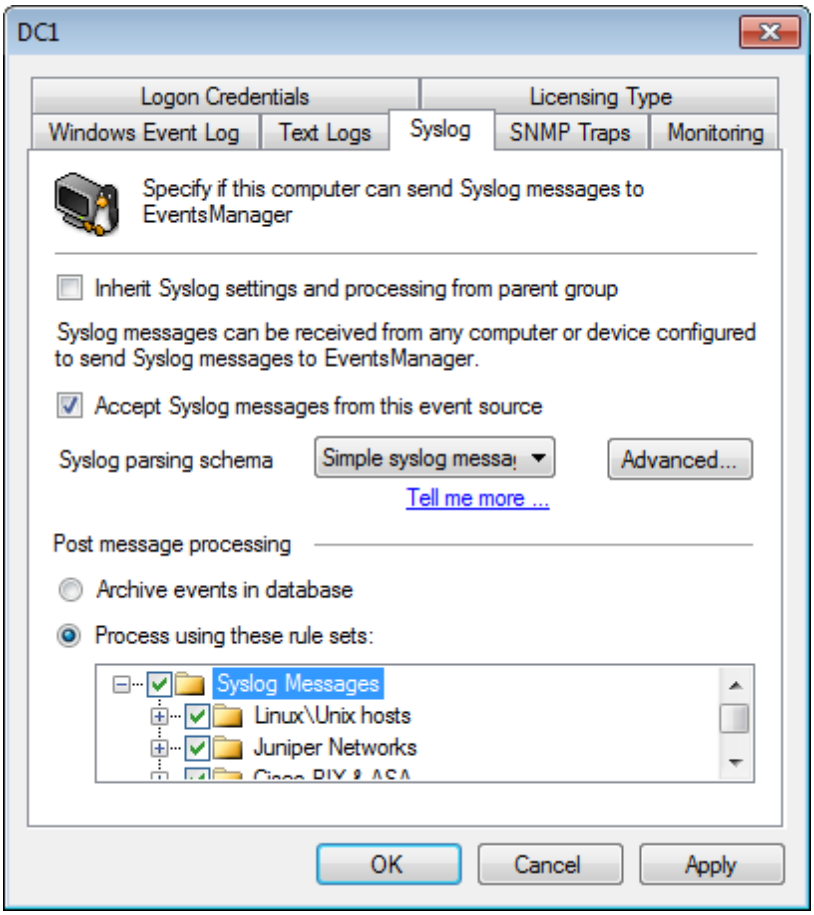
Screenshot 52: Syslog messages must be directed to the computer running GFI EventsManager

Important

Before you start collecting Syslogs, every Syslog event source (workstations, servers and/or network devices) must be configured to send their Syslog Messages to the computer name or IP where GFI EventsManager is installed.

To collect Syslogs:

1. From **Configuration** tab > **Event Sources**, right-click an event source group and select **Properties**.



Screenshot 53: Collecting Syslogs - Syslogs options

2. Click **Syslog** tab and select **Accept Syslog messages to EventsManager** to enable the collection of Syslogs from that event source/event source group.

3. From the **Syslog parsing schema** drop-down, select the method that GFI EventsManager Syslog Server interprets Syslog Messages from network devices. Select from:

- Simple Syslog message
- Standard Linux message
- Juniper Network Firewall
- Cisco ASA.

4. Click **Advanced…** to use custom windows code page. Specify the code and click **OK**.

Note

Windows code page is used to encode international characters to ASCII strings. Since Syslog is not Unicode compliant, GFI EventsManager uses a code page to decode the events. This is only applicable if GFI EventsManager is installed on a machine using a different language than the monitored machines.

For more information, refer to:
http://www.microsoft.com/globaldev/reference/wincp.mspx

5. Select **Archive events in database** to archive collected events without applying events processing rules.

6. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

7. Click **Apply** and **OK**.

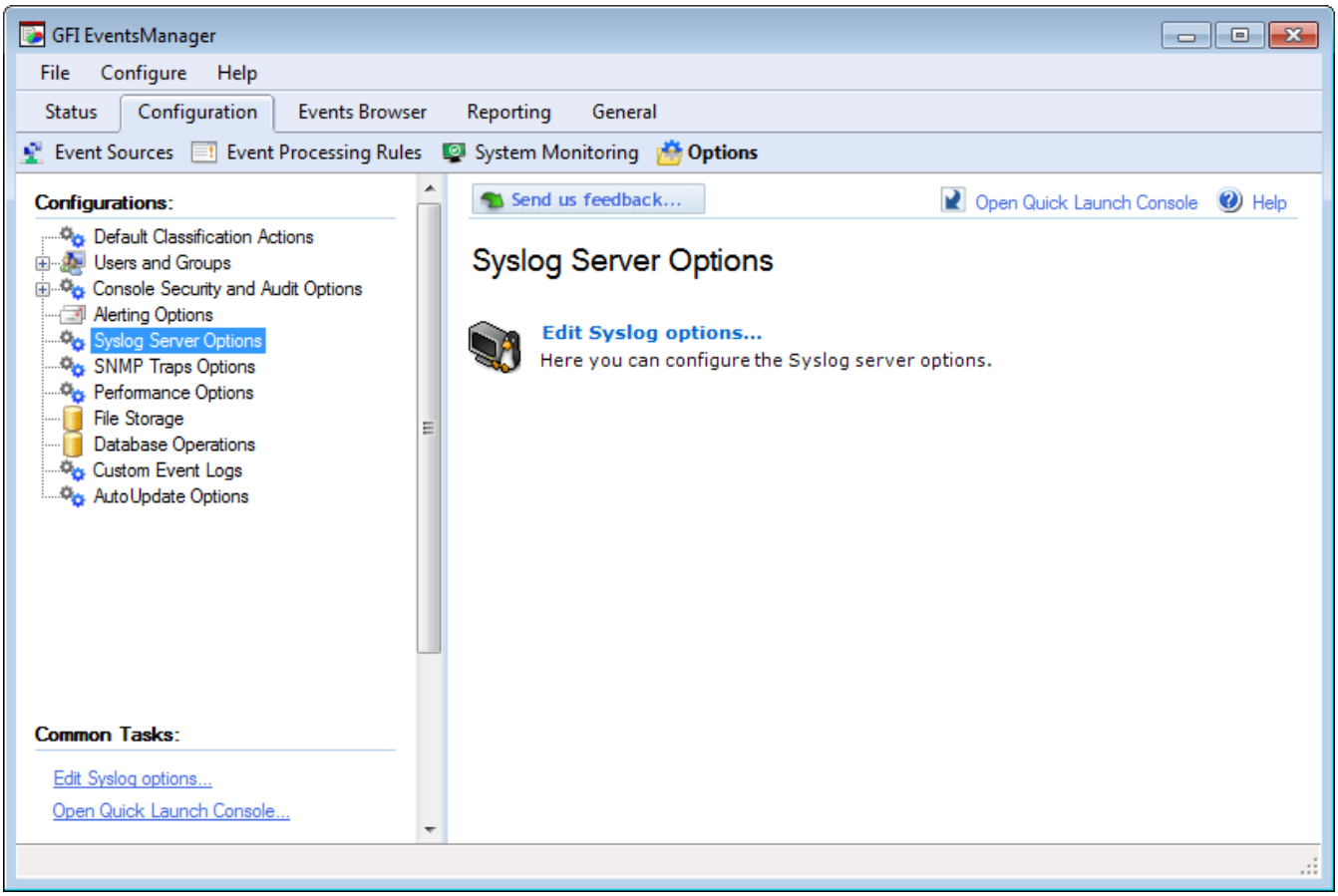
Note

The GFI EventsManager Syslog server is by default configured to listen for Syslog messages on port **514**. For more information, refer to Configuring the Syslog server communications port (page 82).

Important

Deleting event logs without archiving may lead to legal compliance penalties.

4.3.1 Configuring the Syslog server communications port

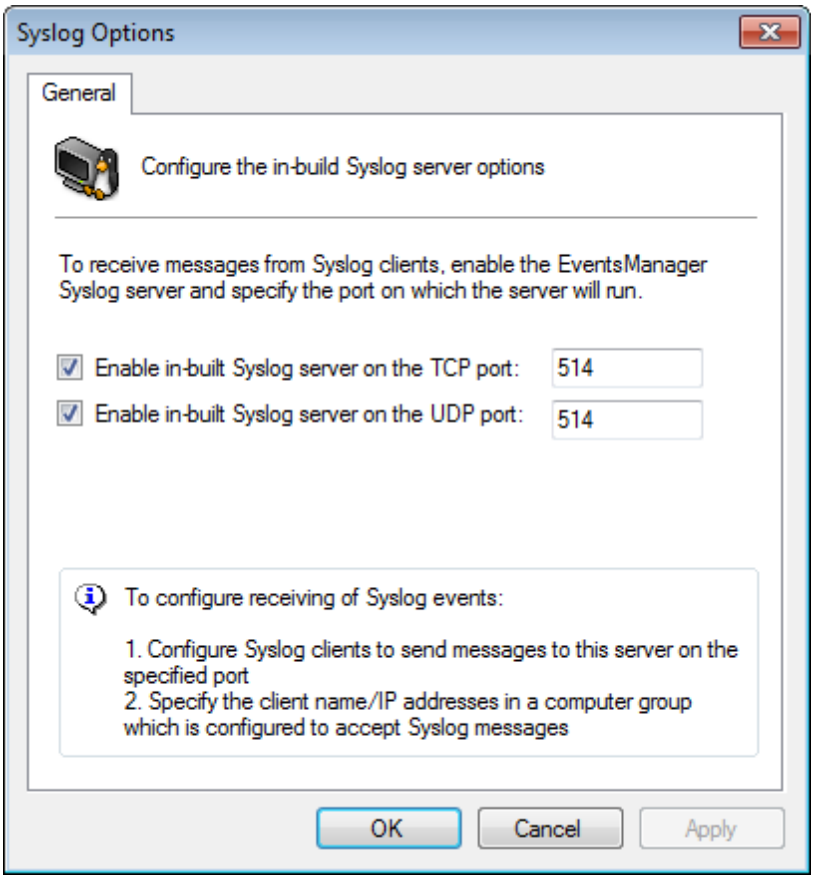


Screenshot 54: Configuring Syslog Server communication port

To change the default Syslog ports settings:

1. Click **Configuration** tab **> Options**.

2. Right-click **Syslog Server Options** and select **Edit Syslog options…**



Screenshot 55: Syslog server options

4. Select **Enable in-built Syslog server on TCP port:** and specify the TCP port on which GFI EventsManager will receive/listen for Syslog messages.

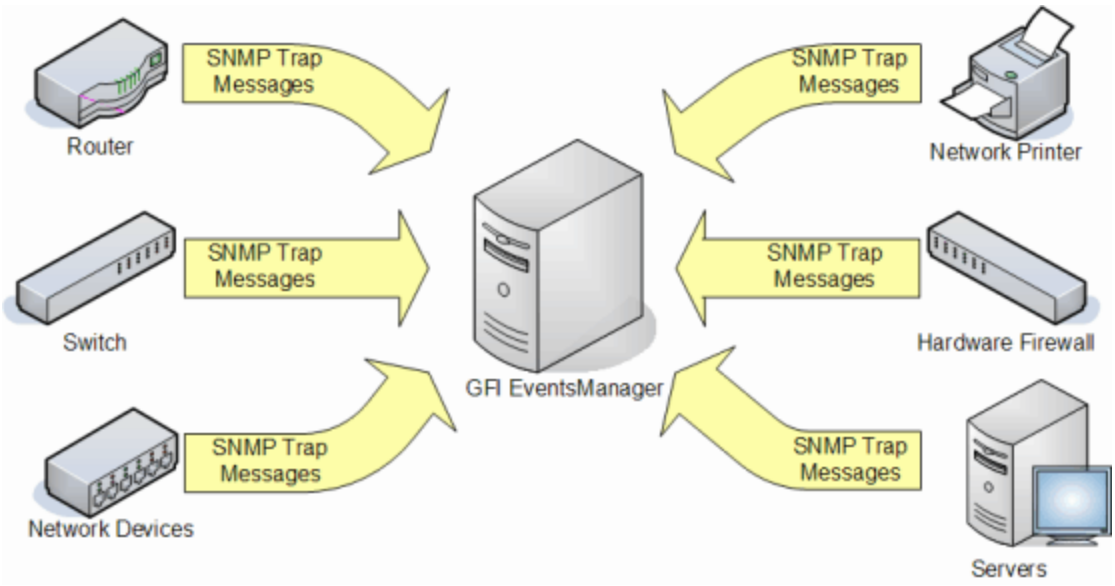
5. Select **Enable in-built Syslog server on UDP port:** and specify the UDP port on which GFI EventsManager will receive/listen for Syslog messages.

6. Click **Apply** and **OK**.

> **Note**
>
> When configuring Syslog server port settings, make sure that the configured port is not already in use by other installed applications. This may affect the delivery of Syslog messages to GFI EventsManager.

4.4 Collecting SNMP Traps

SNMP is a data logging service that enables networked devices to log events and information through data messages (technically known as SNMP Traps). SNMP messaging technology is similar in concept to Syslogs - where unlike Windows and W3C log based environments, devices that generate SNMP messages do not record events data in local logs. Instead events information is sent in the form of data messages to an SNMP Trap Server which manages and saves SNMP message data in a local (centralized) log file.



Screenshot 56: SNMP Trap messages must be directed to the computer running GFI EventsManager

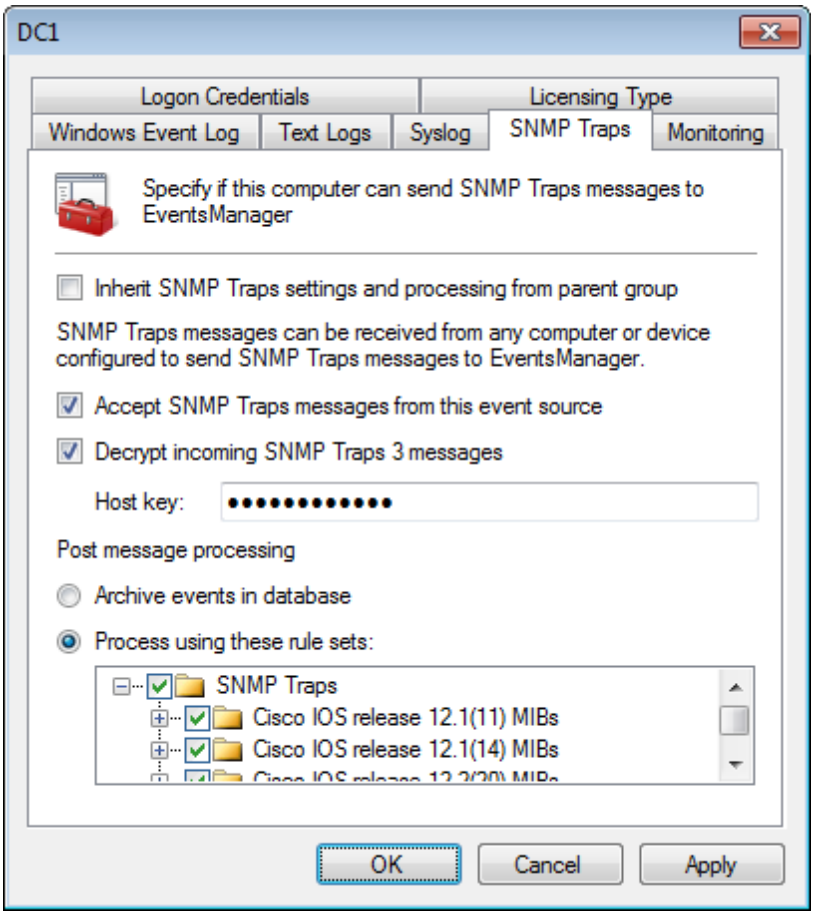
> **Note**
>
> GFI EventsManager natively supports an extensive list of SNMP devices and Management Information Bases (MIBs). For a full list of supported devices, view the following KBASE article: http://kb.gfi.com/articles/SkyNet_Article/KBID002868?retURL=%2Fapex%2FSupportHome&popup=true

GFI EventsManager includes a dedicated SNMP Trap Server through which SNMP Traps are handled. A built-in buffer allows the SNMP Trap Server to collect, queue and forward up to 30 SNMP Trap at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.

> **Important**
>
> Before you start collecting SNMP Traps messages, every SNMP event source (workstations, servers and/or network devices) must be configured to send their SNMP Traps Messages to the computer name or IP where GFI EventsManager is installed.

To collect SNMP Traps:

1. From **Configuration** tab > **Event Sources**, right-click an event source group and select **Properties**.



Screenshot 57: Collecting SNMP Traps

2. Click **SNMP Traps** tab and select **Accept SNMP Traps messages from this event source** to enable the collection of SNMP Traps.

3. Select **Decrypt incoming SNMP Traps 3 messages** and specify the security key in the **Host key** text box.

4. Select **Archive events in database** to archive collected events without applying events processing rules.

5. Select **Process using these rule sets** and select the rule sets you want to run against the collected events.

6. Click **Apply** and **OK**.

Note

The GFI EventsManager SNMP Trap Server is by default configured to listen for SNMP Trap messages on port **162**. For more information, refer to Configuring the SNMP Trap server (page 86).

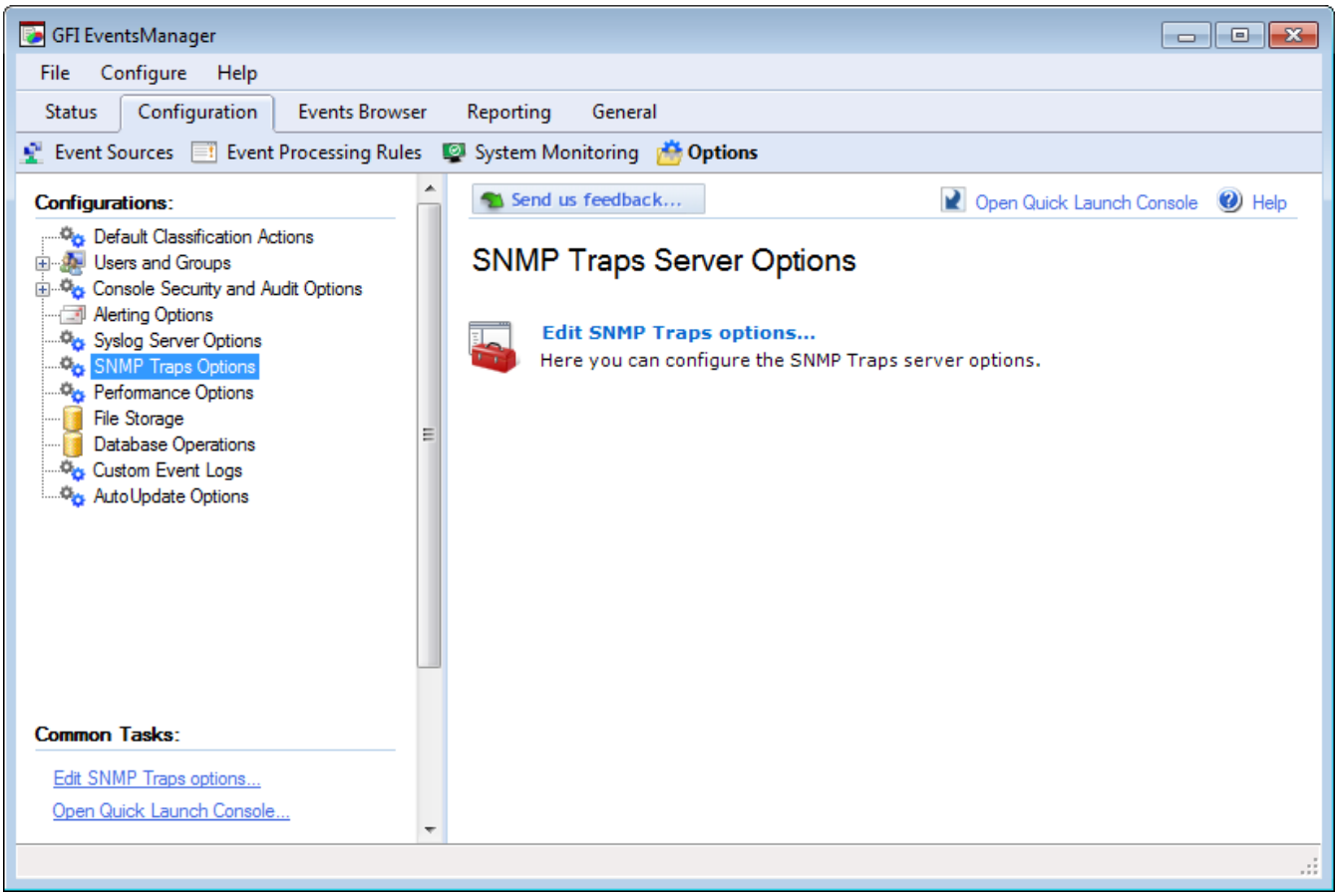
Note

The built in SNMP Trap Server supports SNMP version 3 Traps with encryption. For encrypted SNMP messages the encryption host key must be provided in the decrypt incoming SNMP Traps 3 message field.

Important

Deleting event logs without archiving may lead to legal compliance penalties.

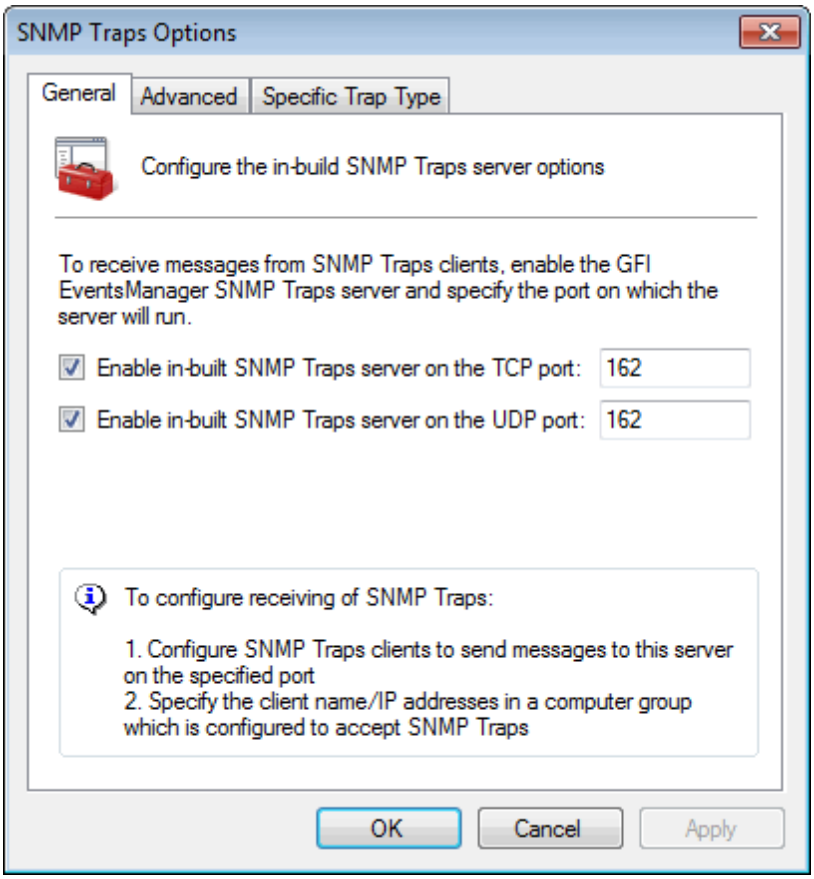
4.4.1 Configuring the SNMP Trap server



Screenshot 58: Configuring SNMP Traps

To change the default SNMP Trap Server settings:

1. Click **Configuration** tab > **Options**.
2. Right-click **SNMP Traps Options** and select **Edit SNMP Traps options…**



Screenshot 59: SNMP Traps options

3. Enable the required TCP/UDP SNMP server. Specify the TCP/UDP port on which GFI EventsManager will listen for SNMP messages.

4. Click **Advanced** tab to add, edit or remove SNMP Trap object identifiers (OIDs).

5. Click **Specific Trap Type** tab to add, edit or remove trap types.

6. Click **Apply** and **OK**.

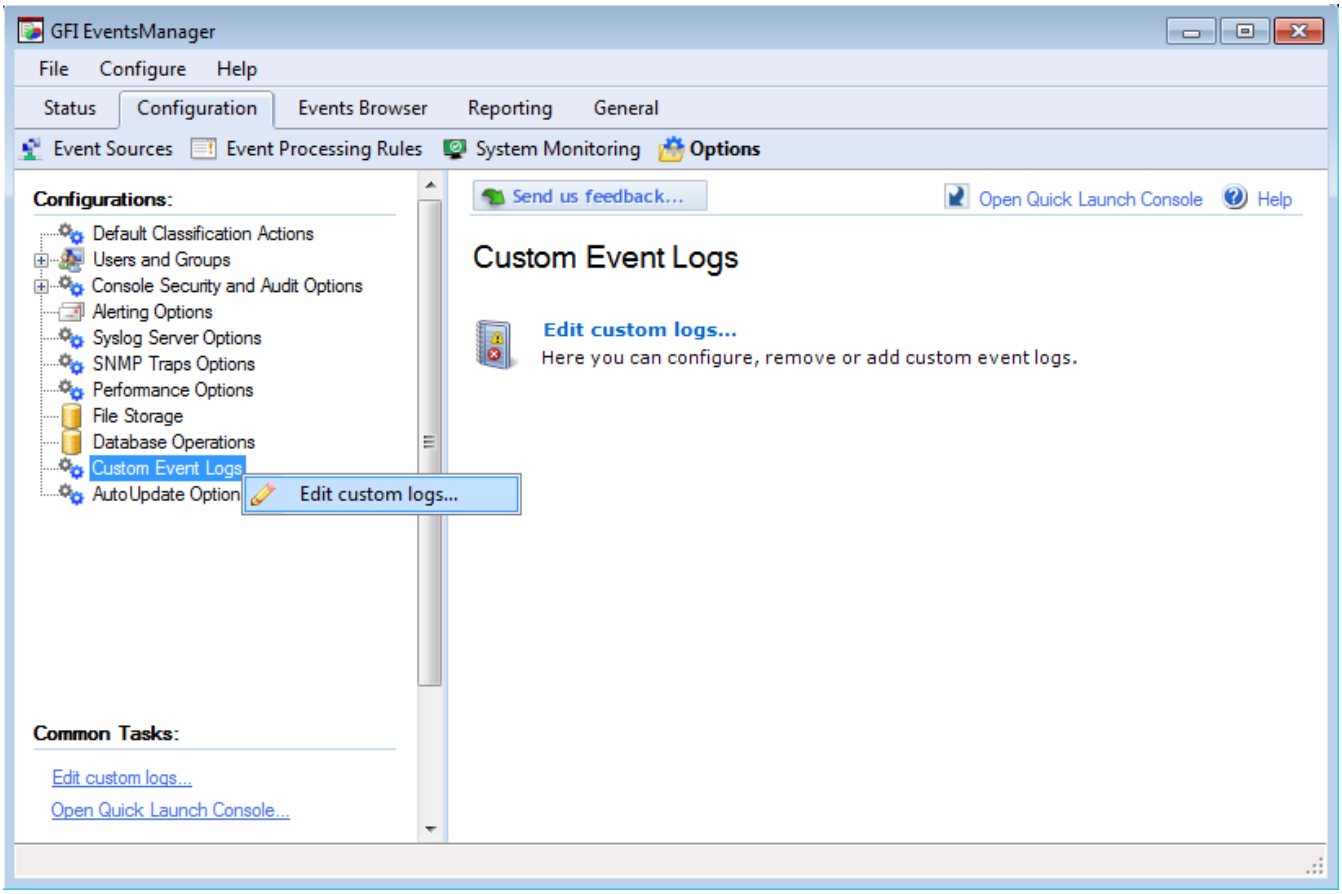
> **Note**
>
> When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

4.5 Collecting custom logs

GFI EventsManager is configured to collect and process standard event logs. However, GFI EventsManager can also be configured to manage events recorded in third party application logs such as anti-virus logs, software firewall logs and other security software.

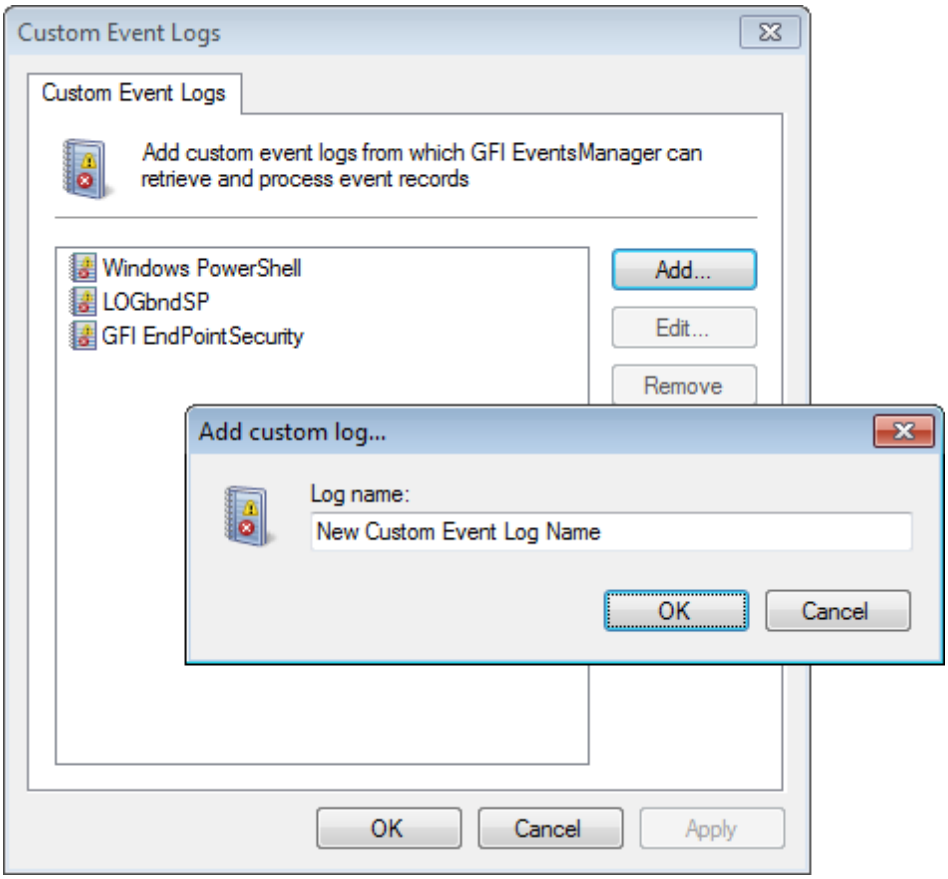
To configure custom events:

1. Click **Configuration** tab > **Options**.



Screenshot 60: Custom event logs setup

2. From **Configurations**, right-click **Custom Event Logs** and select **Edit custom logs...**



Screenshot 61: Custom event logs dialog

3. Click **Add…** button and specify the name of your custom event log.

4. Click **OK**.

5. (Optional) Click **Edit** to rename the selected custom event, or click **Remove** to delete the selected custom event.

6. Click **Apply** and **OK**.

4.6 Collecting GFI LanGuard event logs

GFI EventsManager enables you to monitor events generated by GFI LanGuard. GFI LanGuard is a network vulnerability scanner that audits your network for weaknesses that can be exploited by users for malicious purposes. During network audits, GFI LanGuard creates events in the '**Application Log**' of the machine where it is installed.

For each machine scanned by GFI LanGuard, an 'Application log' entry having '**Event ID: 0**' and '**Source**' set as **GFI LanGuard** will be generated. These events denote network vulnerability information extracted from scanned computers including:

Table 34: Information gathered by GFI LanGuard

Gathered Information	Description
Threat level	Gather information about the overall network threat level. This rating is generated through an extensive algorithm after GFI LanGuard audits the network.
Missing patches and service packs	Find out which machines have missing updates and which updates need to be installed to strengthen the security level.
Open ports	Discover any unwanted open TCP and/or UDP ports.

Gathered Information	Description
Antivirus operational and malware definition status	GFI LanGuard is able to check if your virus database definitions are up to date. If it is not, you will be alerted and GFI LanGuard will attempt to update it.
Applications detected on scanned targets	GFI LanGuard enumerates applications installed on scan targets. You can create an inventory of wanted and/or unwanted applications and configure GFI LanGuard to automatically uninstall applications categorized as unwanted.

Note

For more information about GFI LanGuard, refer to http://www.gfi.com/network-security-vulnerability-scanner.

Note

GFI EventsManager can process events generated by GFI LanGuard version 9.5 or later.

4.6.1 How to enable GFI LanGuard event logging?

There are two key steps needed to enable event log integration between GFI LanGuard and GFI EventsManager:

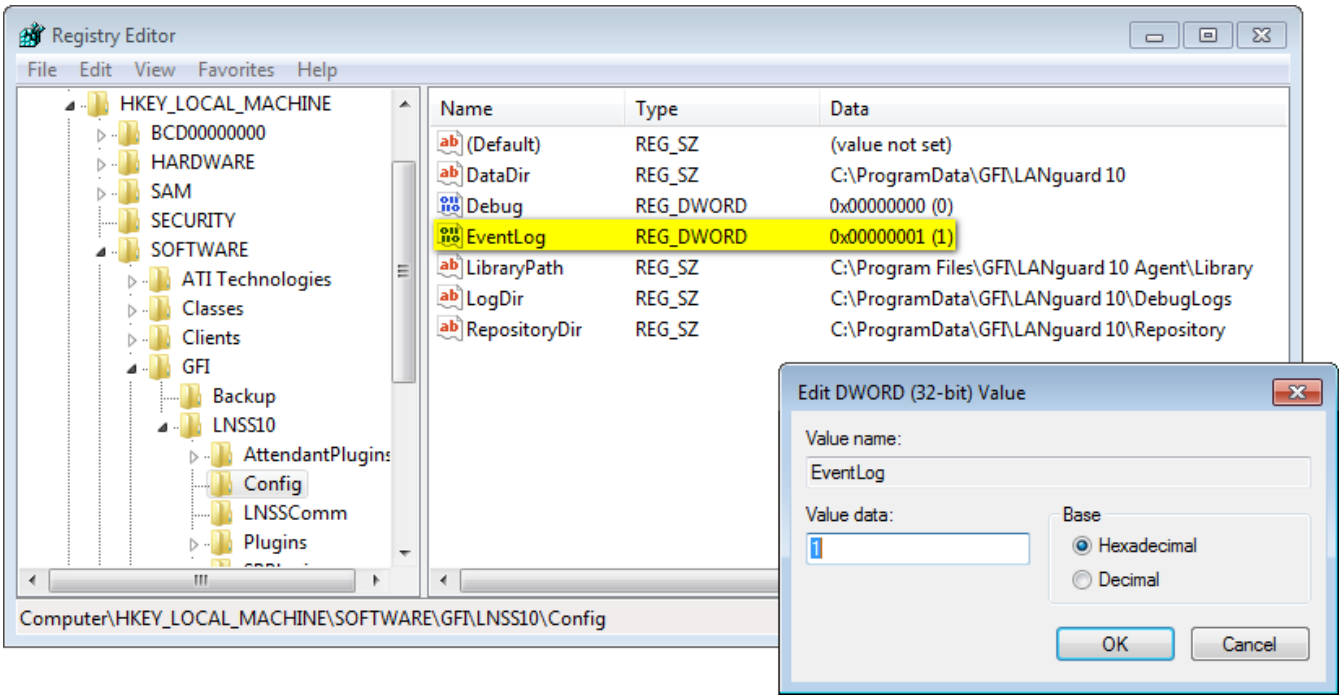
- Step 1: Enable logging
- Step 2: Configure GFI EventsManager to collect Application logs

Step 1: Enable GFI LanGuard logging

To enable GFI LanGuard to output event logs on completion of system audits:

1. Add the machine where GFI LanGuard is installed as an event source.

2. Click **Start > Run** and key in **regedit**. Press **Enter**.



Screenshot 62: Enabling GFI LanGuard logging through the registry

3. Go to the following registry key and edit the value to enable event logging:

» **Windows x86 platforms:**

- `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS[n]\Config`
- Set value of **REG_DWORD EventLog** to **1**

» **Windows x64 platforms:**

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GFI\LNSS[n]\Config`
- Set value of **REG_DWORD EventLog** to **1**

Important

[n] is the major version number of GFI LanGuard.

Example: HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS**9**\Config\EventLog = 1(dword)

Note

To stop GFI LanGuard from generating 'Application Log' entries, remove the registry value described above or change the registry value to **0**.

Step 2: Configure GFI EventsManager to collect Application logs

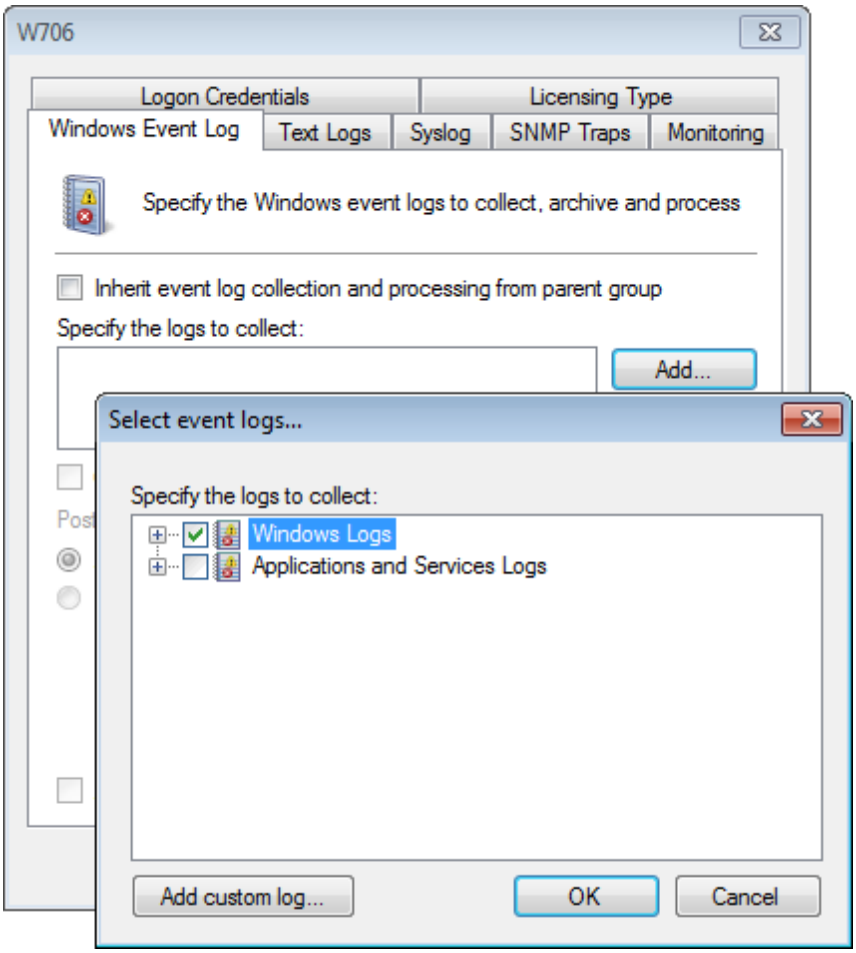
GFI LanGuard outputs windows event logs to the 'Application Log' category. Ensure that the collection of Application logs is enabled on the GFI LanGuard event source.

To enable processing of GFI LanGuard events:

1. Open GFI EventsManager Management Console.

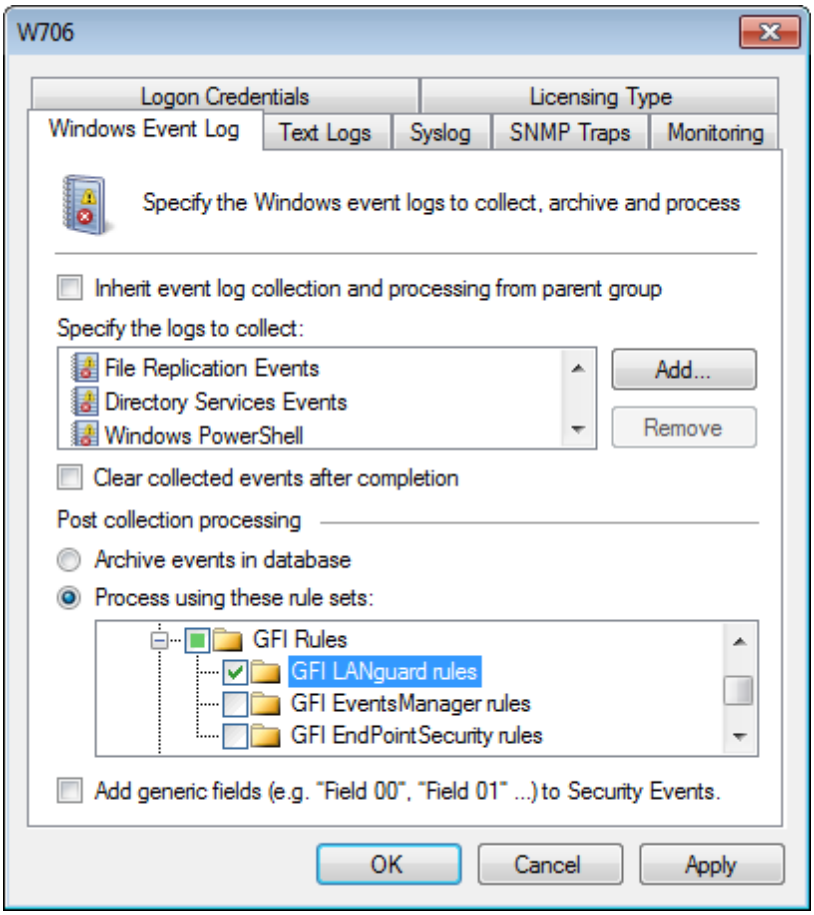
2. Click **Configuration** tab > **Event Sources**.

3. Right-click on the GFI LanGuard event source and select **Properties**.



Screenshot 63: Add Windows Application logs

4. From **Windows Event Log** tab, click **Add** and select **Windows Logs**. Click **OK**.



Screenshot 64: Add GFI LanGuard rules

5. Select **Process using these rule sets**. Expand **Windows Events > GFI Rules** node and select **GFI LanGuard rules**.

6. Click **OK**.

> **Note**
>
> GFI EventsManager has built-in processing rules for GFI LanGuardevents that are enabled by default. To monitor events generated by GFI LanGuard, select **Status** tab > **General** and locate the **Critical and High Importance Events** section.

> **Note**
>
> To configure GFI LanGuard event processing rules, click **Configuration** tab > **Event Processing Rules**. From the left pane select **GFI Rules > GFI LanGuardrules**. For more information, refer to Events Processing Rules (page 144).

Testing and troubleshooting

To check if GFI LanGuard events are being generated:

1. Open GFI LanGuard and run a security audit scan on the localhost.

2. When the scan finishes, open **Event Viewer** from **Start > Run** and key in **eventvwr**. Press **Enter**.

3. Go to Event Viewer (local) Windows Logs Application.

4. Once the stored events are loaded, search for an entry with:

- Source: GFI LanGuard
- Event ID: 0.

In case the event log is not created, typically the GFI LanGuard scan was already initiated once the registry key to output event logs was modified. Re-run the scan. Alternatively ensure that the registry value was created in the right location as the location for x86 platforms is different from that of x64 platforms.

4.7 Collecting GFI EndPointSecurity events

GFI EndPointSecurity enables you to maintain data integrity by preventing unauthorized access, and, the transfer of content to and from the following devices or connection ports:

Table 35: GFI EndPointSecurity supported devices

Device	Example
USB Ports	Flash/Memory card readers and pen drives.
Firewire ports	Digital cameras and Fire-wire card readers.
Wireless devices	Bluetooth and Infrared dongles
Floppy disk drives	Internal and external (USB) floppy drives.
Optical drives	CD, DVD and Blu-ray discs.
Magneto Optical drives	Internal and external (USB) drives.
Removable storage	USB hard-disk drives.
Other drives such as Zip drives and tape drives	Internal or External (USB/Serial/Parallel) drives.

Note

For more information about GFI EndPointSecurity, refer to http://www.gfi.com/endpointsecurity.

Enable GFI EndPointSecurity logging

By default, GFI EndPointSecurity generates logs with information about:

- The GFI EndPointSecurity service
- Devices connected and disconnected on your network
- Access allowed or denied by GFI EndPointSecurity to users.

To configure logging options in GFI EndPointSecurity:

1. From the machine running GFI EndPointSecurity machine, launch GFI EndPointSecurity Management Console.

2. Click **Configuration** tab > **Protection Policies**.

3. From the left pane, select the protection policy and click **Set Logging Options**.

4. Customize the settings available in Logging Option dialog.

Note

For more information on how to configure GFI EndPointSecurity logging options, refer to the GFI EndPointSecurity documentation available from http://www.gfi.com/products/gfi-endpointsecurity/manual.

Monitor GFI EndPointSecurity Events

GFI EventsManager has built-in processing rules for GFI EndPointSecurity events that are enabled by default. To monitor events generated by GFI EndPointSecurity, select **Status** tab > **General** and locate the **Critical and High Importance Events** section.

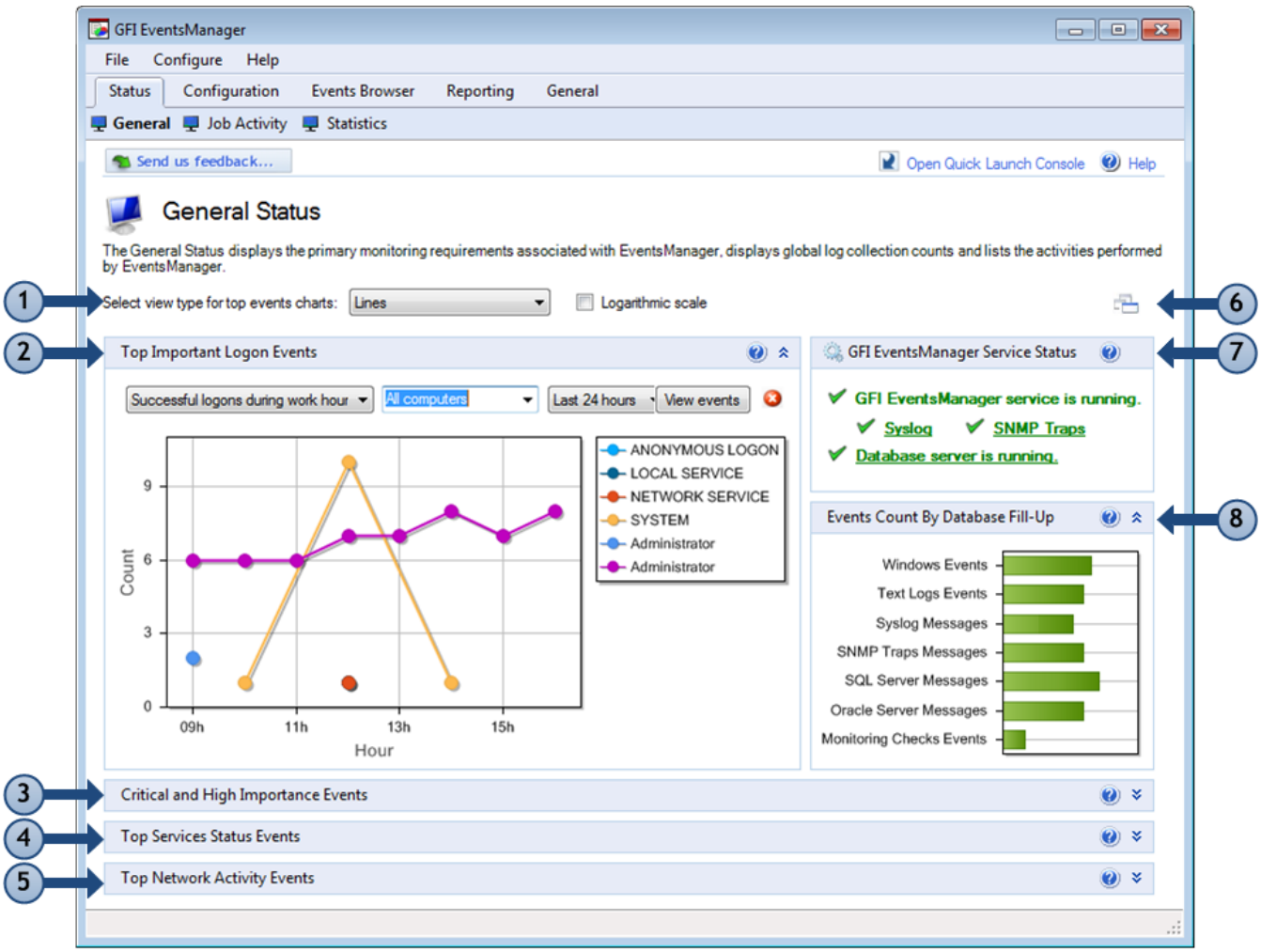
To configure GFI EndPointSecurity event processing rules, click **Configuration** tab > **Event Processing Rules**. For more information, refer to Events Processing Rules (page 144).

5 Activity Monitoring

This chapter provides you with information about monitoring the events collection processes. The **Status** tab is a dashboard that shows the status of GFI EventsManager as well as statistical information related to the events collected, processed and archived. The status monitor consists of three different dashboard views: **General** view, **Job Activity** view and **Statistics** view.

Topics in this chapter:

5.1 General Status view



Screenshot 65: GFI EventsManager Status: General view

To access the **General** view, go to **Status** tab > **General**. This view is used to:

- View the status of the GFI EventsManager event processing engine
- Access statistical information such as the number of logon events, critical events and service status events.

The General view consists of the sections described below:

Table 36: Status monitoring: General view sections

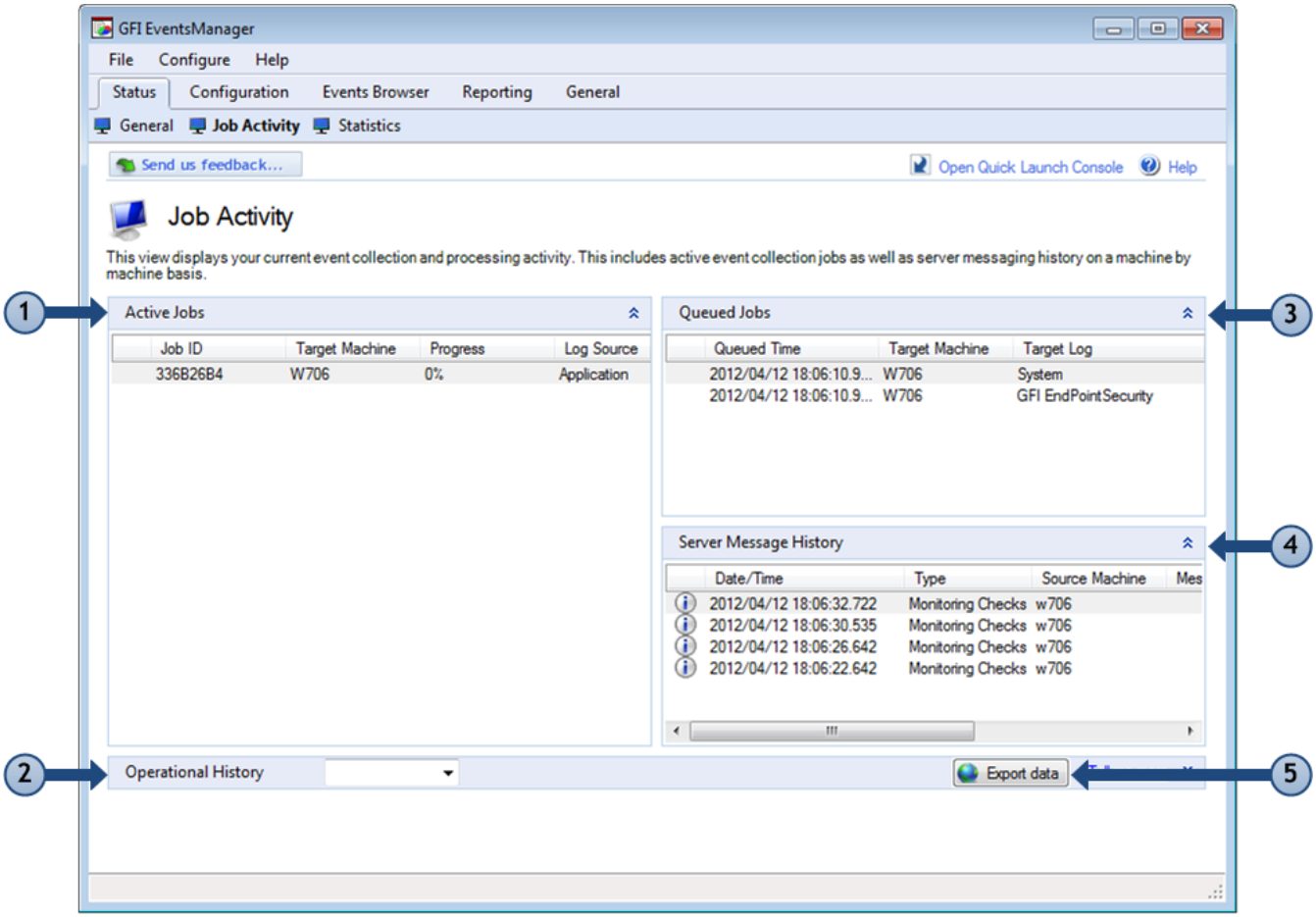
Section	Description
1	Use this section to select the chart type for top events.
2	The **Top Important Log Events** section provides statistical information about: » Top 10 successful Logon events outside working hours » Top 10 important Logon events during working hours » Top 10 failed Logon events. Events in this section are filtered by: » **Machine**: Select a machine or key in a machine name in the drop down list » **Period**: The time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).
3	The **Critical and High Importance Events** section provides statistical/graphical information about critical events collected from all event sources. This graph shows the event processing rules that collected and processed the events for a particular period. From the drop down lists, select the type of information to display. Select from: » **Grouping**: Determines how events are grouped; such as Events, Computers, Computer groups, Events/Computers or Events/Computer groups » **Event type**: Select the type of data to display (Windows, W3C, Syslog, SNMP, SQL and Oracle audit) » **Alert type**: Specify the alert severity; such as All alerts, Critical or High » **Period**: Specify the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date). **NOTE 1** This section also displays the vulnerability results monitored by GFI LanGuard. **NOTE 2** For detailed information about the different types of important events shown in this view, download the Microsoft Security Monitoring and Attack Detection Planning Guide from http://www.gfi.com/ms-security-mointoring-and-attack-detection-planning/.
4	The **Top Service Status Events** displays the top 10 services that caused the selected event. A service can generate events when: » Terminated with an error » Failed to load » Failed to start » Timed out » Stopped » Started. The graph shows the frequency of these events sorted by service type and/or by computer generating the event. Select a machine or service from the drop down lists or key in the required criteria to customize the graph results. **NOTE** To collect services information, event sources must have Audit system events policy enabled. For more information, refer to Enabling event source permissions manually (page 242).

Section	Description
5	The **Top Network Activity Events** section displays details of the top 10 network activities (inbound and outbound). Network activity consists of all type of traffic that is generated by various protocols including SMTP, HTTP, FTP and MSN traffic. The network activities displayed can be filtered by: » Applications » Source Addresses » Destination Addresses » Computers » Ports » Users. Select parameters from the drop down lists or key in the values to filter the type of chart displayed. **NOTE 1** The network activity shown in the chart applies only to computers running Microsoft Windows Vista or later. **NOTE 2** To collect network activities, event sources must have Object auditing and Process tracking enabled. For more information refer to Enabling event source permissions manually.
6	Click the **Arrange Window** icon to automatically fit all graphs in the management console.
7	The GFI EventsManager **Service Status** is used to view: » The operational status of GFI EventsManager service/event processing engine » The operational status of the Syslog server » The operational status of the SNMP Traps server » The operational status of the database server currently in use by GFI EventsManager. **NOTE** Click the service name to edit the service settings.
8	The **Events Count By Database Fill-Up** displays: » The horizontal bars represent the number of events stored in the database backend, sorted by event log type » The date and time of the last backup » The date and time of the next scheduled backup. The bar color turns from green to red as the database is populated with events.

Note

Double-click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph. Use the **Export to image** button to export the graph.

5.2 Job Activity view



Screenshot 66: GFI EventsManager Status: Job Activity view

To access the **Job Activity** view, go to **Status** tab > **Job Activity**.

This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.

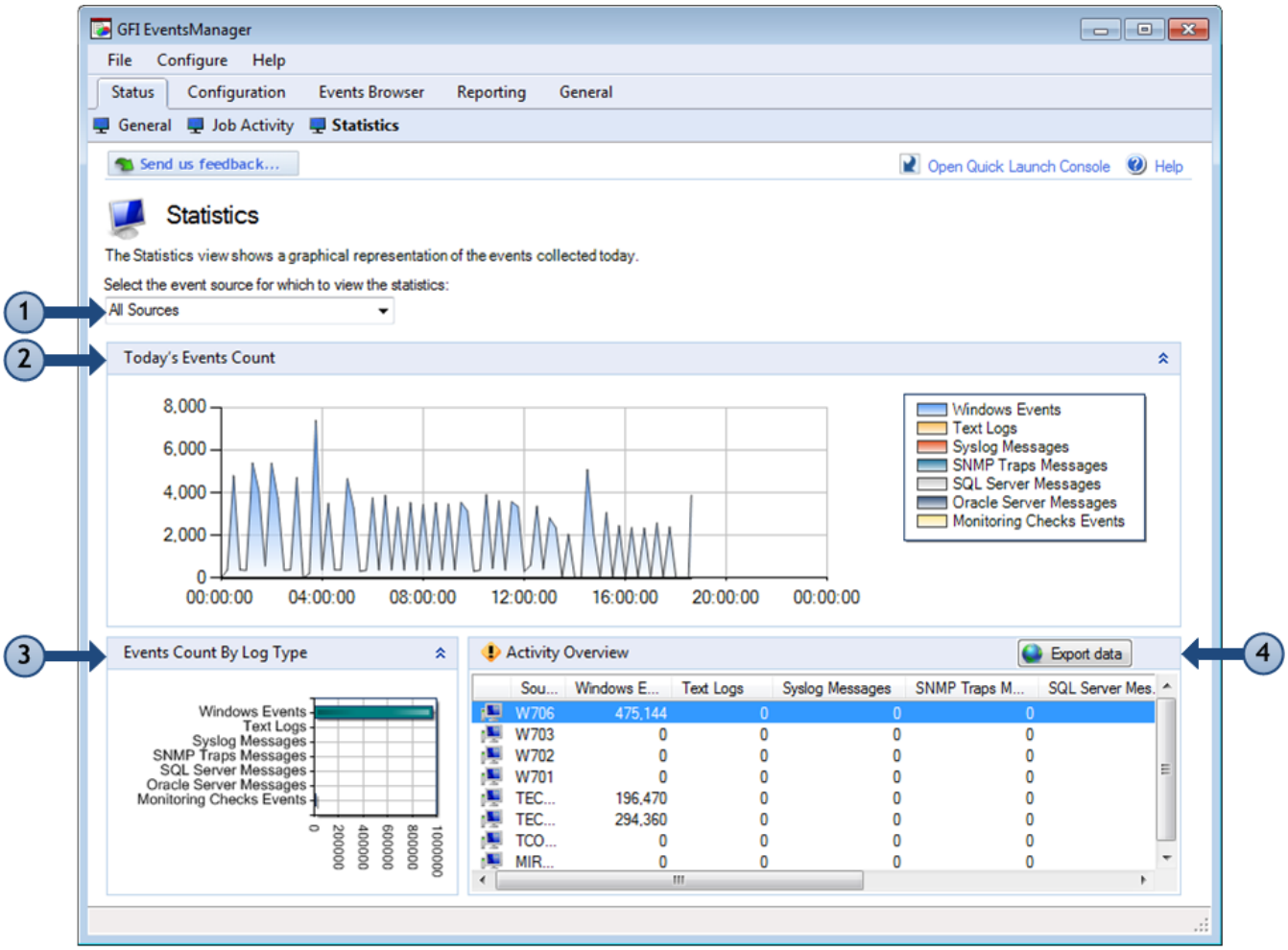
The information provided in this view is divided into the following dedicated sections:

Table 37: Status monitoring: Job activity view

Section	Description
1	The **Active Jobs** section provides a list of all event collection jobs currently taking place on every event source/machine. The information provided includes the job progress as well as the Log Source from which events are being collected.
2	The **Operational History** section shows an audit trail of the event collection operations performed by GFI EventsManager. The information provided includes errors and information messages generated during the event collection process as well as the name of the log file that was being processed on the event source. **NOTE** Operational history logs can be exported using the Export data button. For more information, refer to Generating reports (page 130).
3	The **Queued Jobs** section provides a list of all pending event collection jobs on a machine by machine basis. The information provided includes the event source from which events will be collected as well as the queuing time and type of log to collect.
4	The **Server Message History** section displays a list of all server messages (SNMP Traps and Syslog) that were received by GFI EventsManager. The information provided includes the total number of messages sent by every event source, message count and the date/time when the last message was received.

Section	Description
5	Click **Export data** to generate Operational History reports.

5.3 Statistics view



Screenshot 67: GFI EventsManager Status: Statistics view

To access the **Statistics** view, go to **Status** tab > **Statistics**.

The **Statistics** view is used to display the daily event activity trends and statistics of a particular computer or entire network. The information provided in this view is divided into the following dedicated sections:

Table 38: Status monitoring: Statistics view

Section	Description
1	Use this drop-down menu to select what information is displayed. Select between **All sources** or select specific sources to view their information accordingly.
2	The **Today's Events Count** graphically represents the daily event collection trend on a machine by machine basis as well as on a network by network basis. A color scheme is used to differentiate between Windows, W3C, Syslog and SNMP Traps events.
3	The **Events Count By Log Type** represents the number of Windows, W3C, Syslog and SNMP Traps events collected by GFI EventsManager from a particular machine or network.

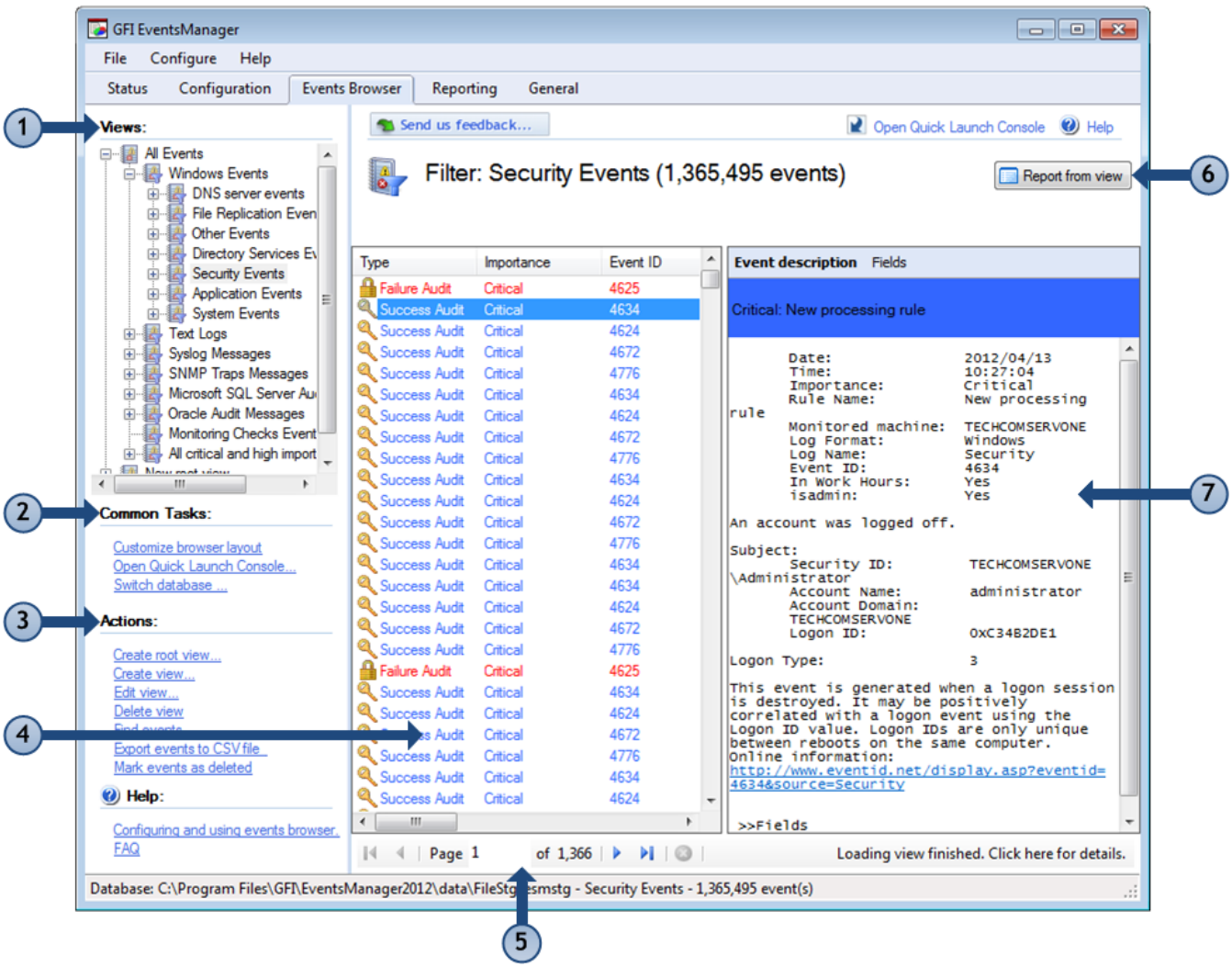
Section	Description
4	The **Activity Overview** section provides information about: » The total number of Windows, W3C, Syslog and SNMP Traps events processed on a machine by machine basis » The date/time of the last event collection performed from every machine. Click **Export data** to generate Activity Overview reports.

6 Browsing Stored Events

This chapter provides you with information about using the Events Browser. The Events Browser is equipped with tools for event analysis and forensic investigation. It also enables you to easily browse through multiple events databases as well as export events to encrypted databases for legal compliance purposes.

Topics in this chapter:

6.1 Navigating the Events Browser



Screenshot 68: Events Browser

The Events Browser is made up of the following sections:

Table 39: Navigating the Events Browser

	Section	Description
1	**Views**	The **Views** section includes a wide range of predefined views. Use this section to view specific logs such as Windows Event Logs, W3C logs, SQL Server audits and more.
2	**Common Tasks**	**Common Tasks** enable you to customize the look of the Events Browser and switch database to view exported and/or archived event logs.
3	**Actions**	Use the **Actions** section to run common functions related to analyzing event logs. This enables you create or edit custom views, export events for further analysis and more.
4	**Events**	The **Events** section is used to browse through the events categorized under the selected view (from section 1).
5	**Navigation controls**	Use the navigation controls to browse through collected events.
6	**Reporting**	The **Report from view** option enables you to generate graphical and statistical reports based on the selected view (from section 1).
7	**Event Description Pane**	The **Events Description Pane** provides an extensive breakdown of the selected event (from section 4). Use this section to analyze the event details and find out when the event was generated, what was the cause and by whom it was generated. The header color coding enables you to quickly identify the severity of the event. The description section enables you to switch between two views: » **General** - Contains event information in the legacy format that was standard for pre-Microsoft Windows Vista event logs. » **Fields** - Contains a list of event information categorized by fields. The link provided in the event description gives you access to: » A more detailed description of the event » Information and links that explain what causes this type of event » Hints and tips on how to possibly solve any existing issues.

6.2 Using the Events Browser

Event analysis is a demanding task; GFI EventsManager is equipped with specialized tools that simplify this process. Use the Events Browser for forensic analysis of events. All events accessible through the Events Browser are organized by log type in the Views section.

This section contains information about:

» Exporting events to CSV

» Creating reports from events browser views

» Deleting events

» Searching stored events

» Identifying rules using the rule finder tool

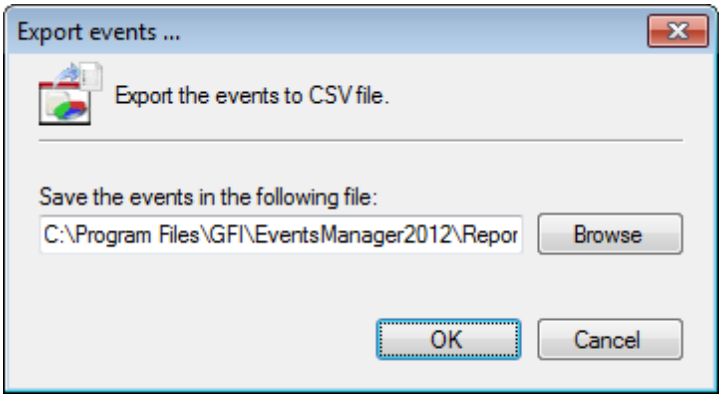
6.2.1 Exporting events to CSV

GFI EventsManager enables you to export event data to CSV files directly from Events Browser. This is extremely convenient especially when further processing of event data is required. This includes:

- Distribution of key event data via email
- Running automated scripts that convert CSV exported events data to HTML for upload on web/company intranet
- Generation of graphical management reports and statistical data using native tools such as Microsoft Excel
- Generation of custom reports using third party applications
- Interfacing events data with applications and scripts built in-house.

To export events to CSV:

1. From **Events Browser > Views**, right-click a view and select **Export events**.



Screenshot 69: Export events tool

2. Specify or browse to the location where exported events are saved. Click **OK**.

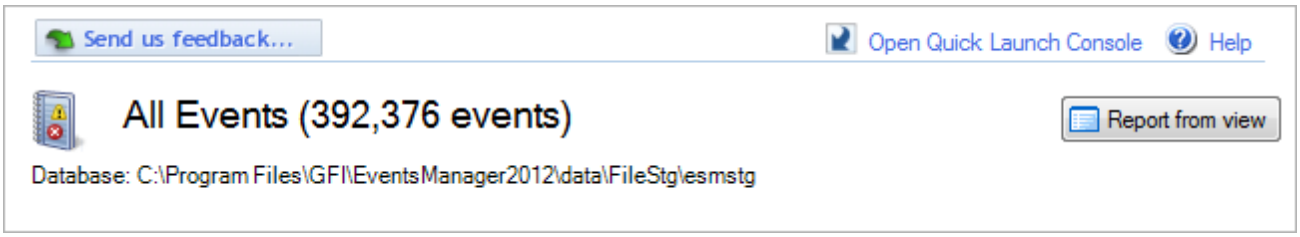
6.2.2 Creating reports from views

GFI EventsManager enables you to build your own custom reports (with graphs and statistics) based on a selected View from Events Browser.

> **Note**
>
> GFI EventsManager ships a selection of predefined reports. We recommend that you check the available reports prior to creating new ones to avoid having duplicate reports.

To generate a report from a view:

1. From **Events Browser > Views**, select a view.



Screenshot 70: Report from view button

2. From the top-right corner of the Events Browser, click **Report from view**.
3. From the **Create Report** dialog, configure the options from the tabs described below:

Table 40: Event Browser: Create new report

Tab	Description
General	Specify the new report name and add conditions.
Layout	Select the columns that you want to be visible in the report. You can also customize the order of appearance.
Chart	Select **Use graphical charts** to generate a report showing information in a chart. The available chart types are: » Pie chart » Bar chart » Line graph.
Schedule	Select **Use schedule** to enable report scheduling. Configure the generation date and frequency for the new report.

Note

For more information, refer to Creating custom reports (page 121).

6.2.3 Deleting events

When collecting and processing event logs from a significantly large number of event sources, a number of unwanted logs are collected. To help you remove such event logs, GFI EventsManager includes a delete option. When events are deleted, they are:

- Removed from events browser
- No longer included in export/import jobs
- No longer included in reports.

After deleting an event, every other event of the same type, category and containing view are deleted as well.

Important

Before you delete event logs, ensure that you are abiding by legal compliance regulations. Deleting event logs may lead to legal penalties.

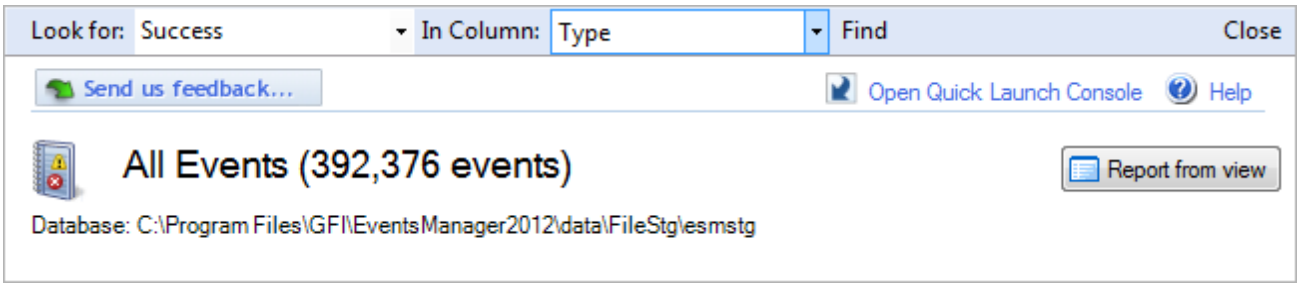
To delete events:

1. From **Events Browser > Views**, select a view.
2. Select an event that you want to delete. From **Actions**, click **Delete events**.
3. Click **Yes** to confirm delete or click **No** to cancel.

6.2.4 Searching stored events

Use the event finder tool to search and locate specific events using simple customizable filters. To search for a particular event:

1. Click **Events Browser > Actions > Find events**.



Screenshot 71: Event finder tool

2. Configure the event search parameters through the options provided on top of the right pane. To trigger a case sensitive search, click **Options** and select **Match whole word**.

3. Click **Find** to start searching.

6.2.5 Identifying rules using the rule finder tool

GFI EventsManager enables you to identify the event processing rule which triggered the selected event log.

To identify the rule(s) used for a specific event:

1. From **Events Browser**, right-click an event log.

2. Click **Find Rule**. Doing so will take you to **Configuration** tab > **Event Processing Rules**. For more information, refer to Events Processing Rules (page 144).

6.3 Managing Events Browser views

This section contains information about:

- Creating Root Views / Views
- Editing a view
- Deleting a view

6.3.1 Creating Root Views / Views

In Events Browser, GFI EventsManager enables you to create two different types of custom views, described below:

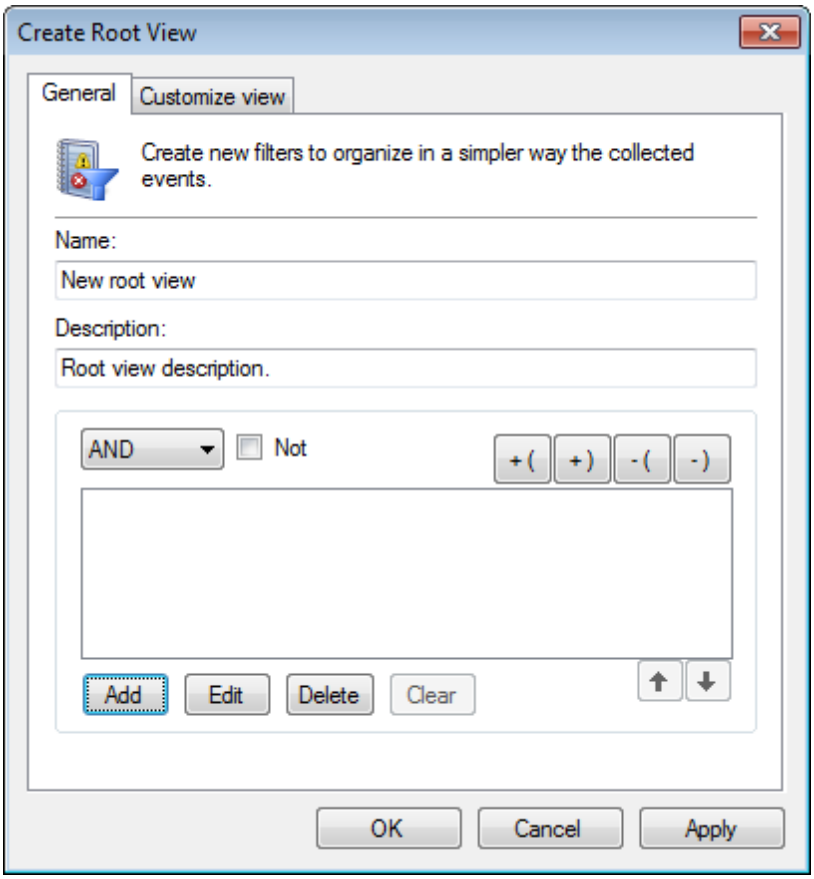
Table 41: Event Browser: Create new view

View	Description
Create root view...	Enables you to create top-level views which may contain a number of sub-views. This creates a new set of views beneath the ones that ship with the product (Example: **All Events** view).
Create view...	Create views within root views. Custom views can be added to the default root views and views.

To create a Root view/View:

1. From **Events Browser** > **Actions**, click **Create root view.../Create view...**

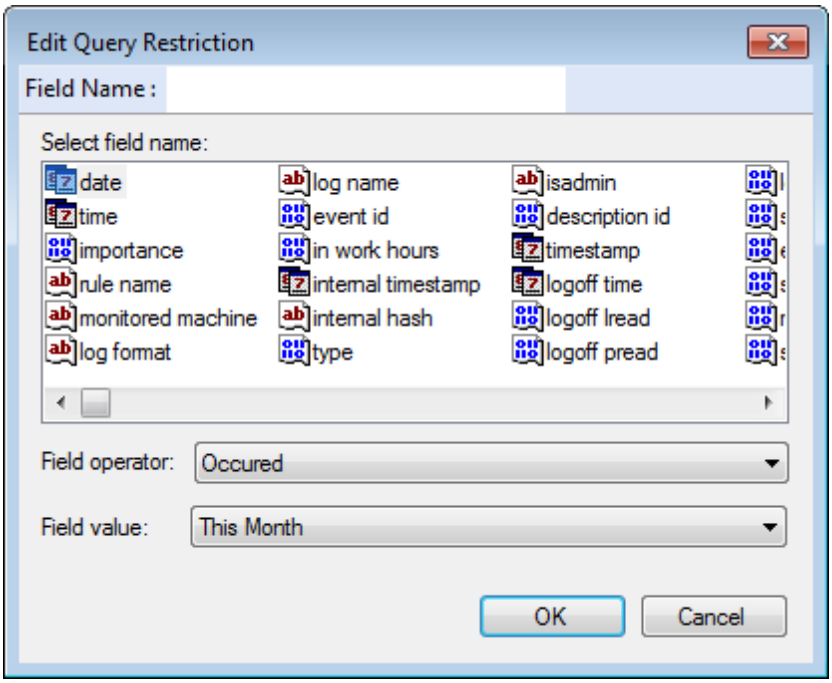
> **Note**
>
> Both options launch the same **Create view** dialog and are both configured in the same way. The difference is the positioning of the new custom view.



Screenshot 72: Custom view builder

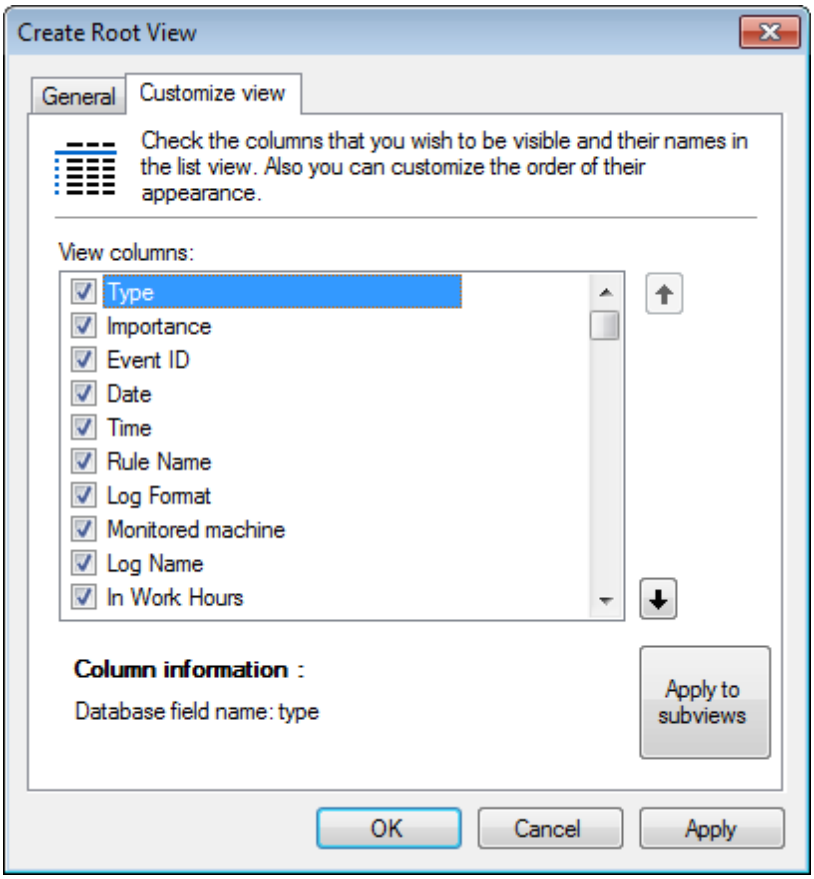
2. Key in a name and description for the new view.

3. Click **Add** to add filtering conditions to your view. If no conditions are specified, the view will display information from every event that is generated.



Screenshot 73: Edit view restriction

4. Select a field from the list of available fields and specify the **Field operator** and **Field value**. Repeat this step until all required conditions are specified. Click **OK**. For more information, refer to Defining Restrictions.

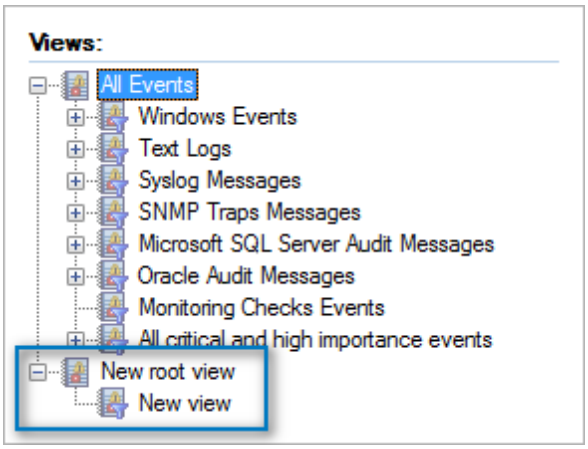


Screenshot 74: Customize View tab

4. Click **Customize view** tab to select the columns to show in the new custom view. You can also arrange their order of appearance using the **Up** and **Down** arrow buttons.

5. (Optional) Click **Apply to subviews** to apply the selected columns to all subviews of the root view.

6. Click **Apply** and **OK**.



Screenshot 75: Sample: New Root Views and Views

6.3.2 Deleting a view

1. From **Events Browser > Views**, select the view to delete.

2. From **Actions**, click **Delete view**. Alternatively, right-click on the view you want to delete and select **Delete view**.

6.3.3 Editing a view

1. From **Events Browser > Views**, select the view to edit.

2. From **Actions** click **Edit view...**

3. From the View Properties dialog, add, edit or delete conditions according to your requirements.

6.4 Customizing Events Browser layout

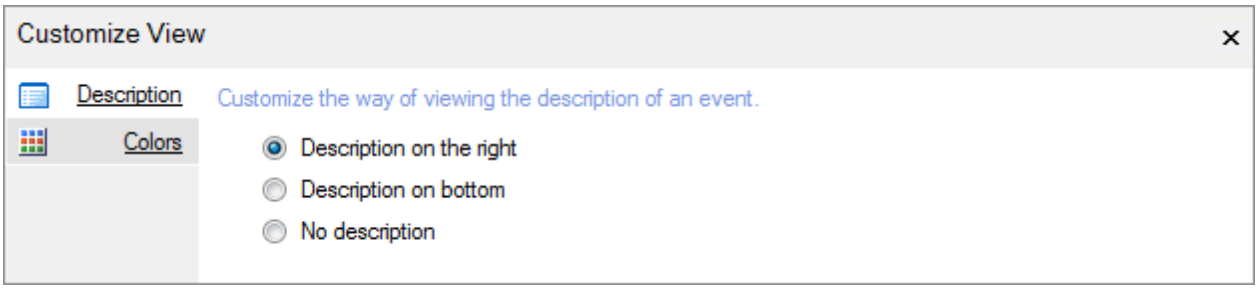
This section contains information about:

- Customizing description position
- Event color-coding options

6.4.1 Customizing description position

To change the position of the event description pane:

1. From **Events Browser > Common Tasks**, click **Customize browser layout > Description**.



Screenshot 76: Customize browser description

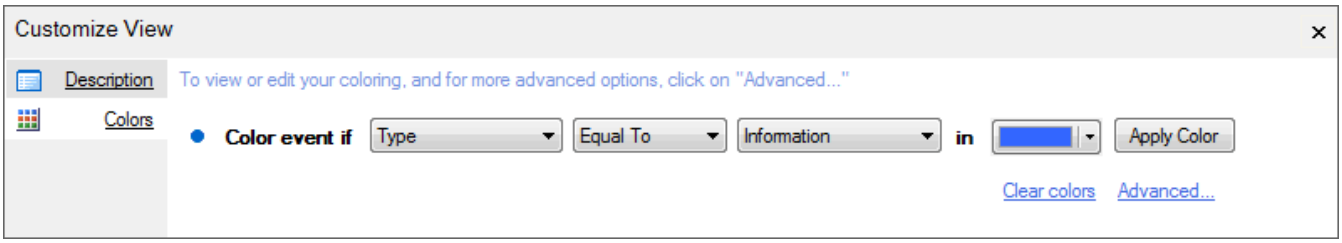
2. Select one of the options described below:

Table 42: Description pane positions

Option	Description
Description on the right	Places the description pane to the right of the events list.
Description on bottom	Places the description pane at the bottom of the events list.
No description	Removes description pane.

6.4.2 Event color-coding options

Use the event color-coding tool to tint key events in a particular color. This way the required events are easier to locate during event browsing.



Screenshot 77: Color coding configuration

To assign a color code to a specific event:

1. From **Events Browser > Common Tasks** select **Customize browser layout > Colors**.

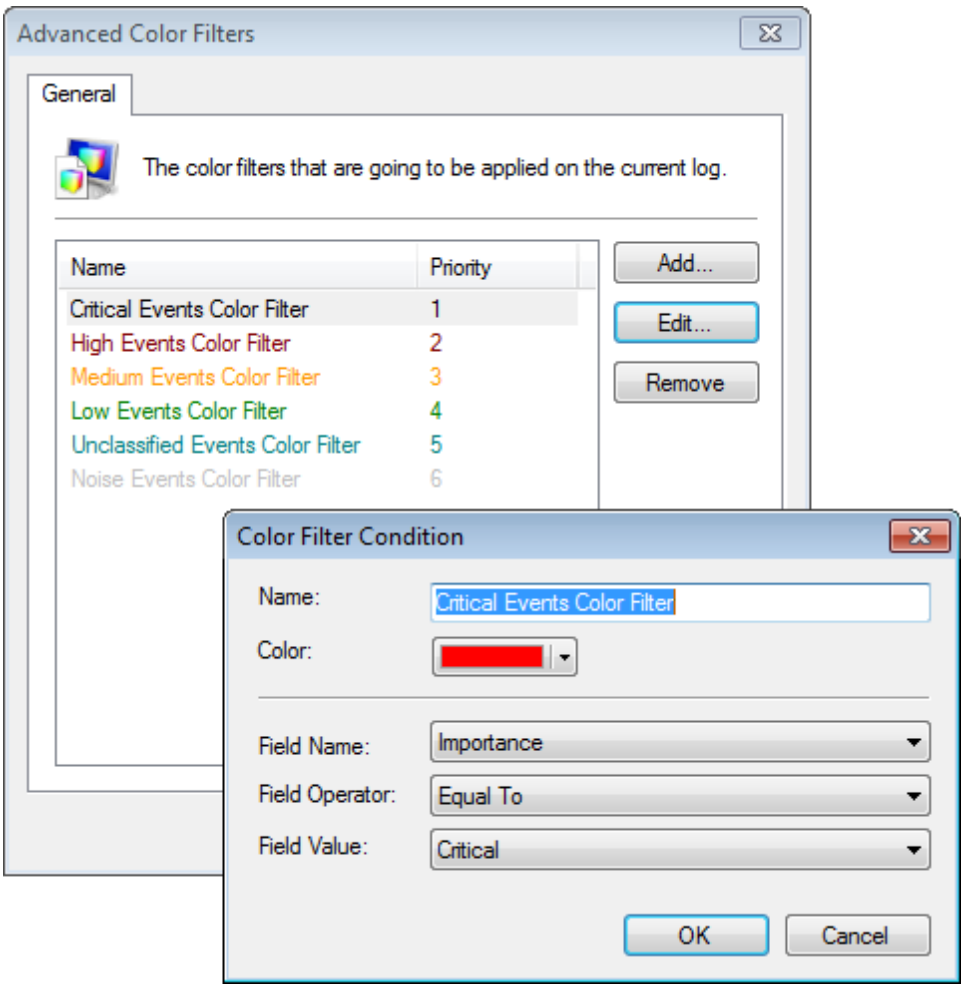
2. Specify event filtering parameters including the color to be applied to the sifted events.

3. Click **Apply Color**.

> **Note**
>
> Use the **Clear color** option to clear all color settings.

To assign different color-codes to multiple events:

1. From **Events Browser > Common Tasks** select **Customize view > Colors > Advanced…**



Screenshot 78: Advanced Color Filter

3. Click **Add** button. Specify filter name and configure event filter parameters.

4. Click **OK**.

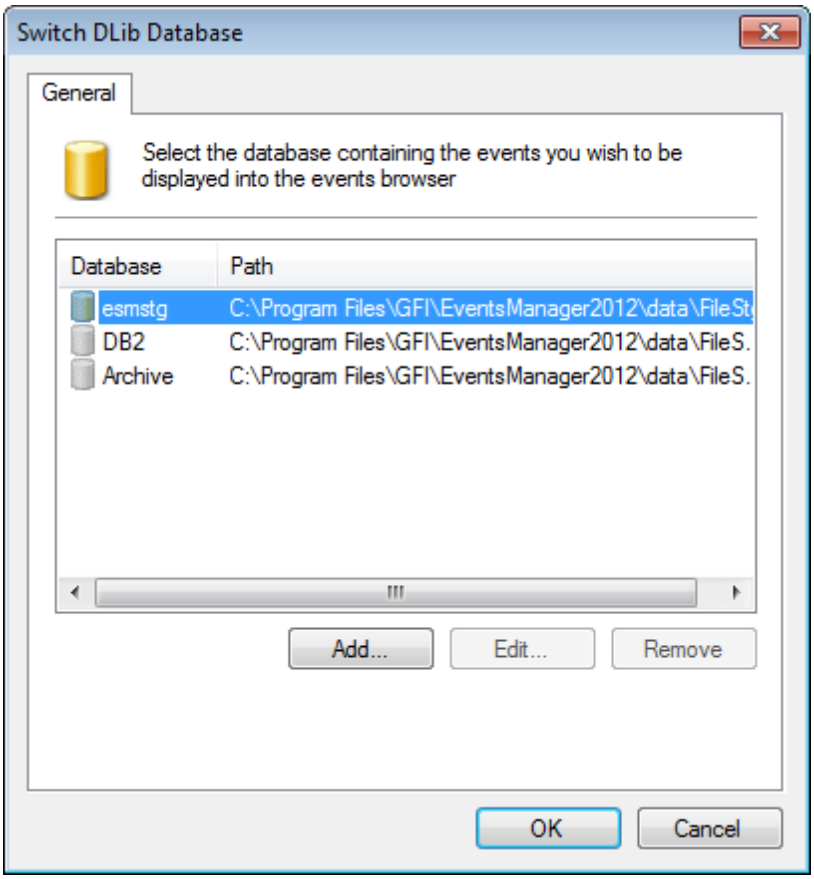
5. Repeat until all required event filter conditions have been configured. Click **OK**.

6.5 Browsing events from different databases

GFI EventsManager enables you to switch between different databases. Use this feature to browse events that have been exported or archived for further analysis or stored in different databases.

To switch databases:

1. Click **Events Browser > Common Tasks > Switch database**.



Screenshot 79: Switch database dialog

2. Select the database from the list of databases and click **OK**.

Note

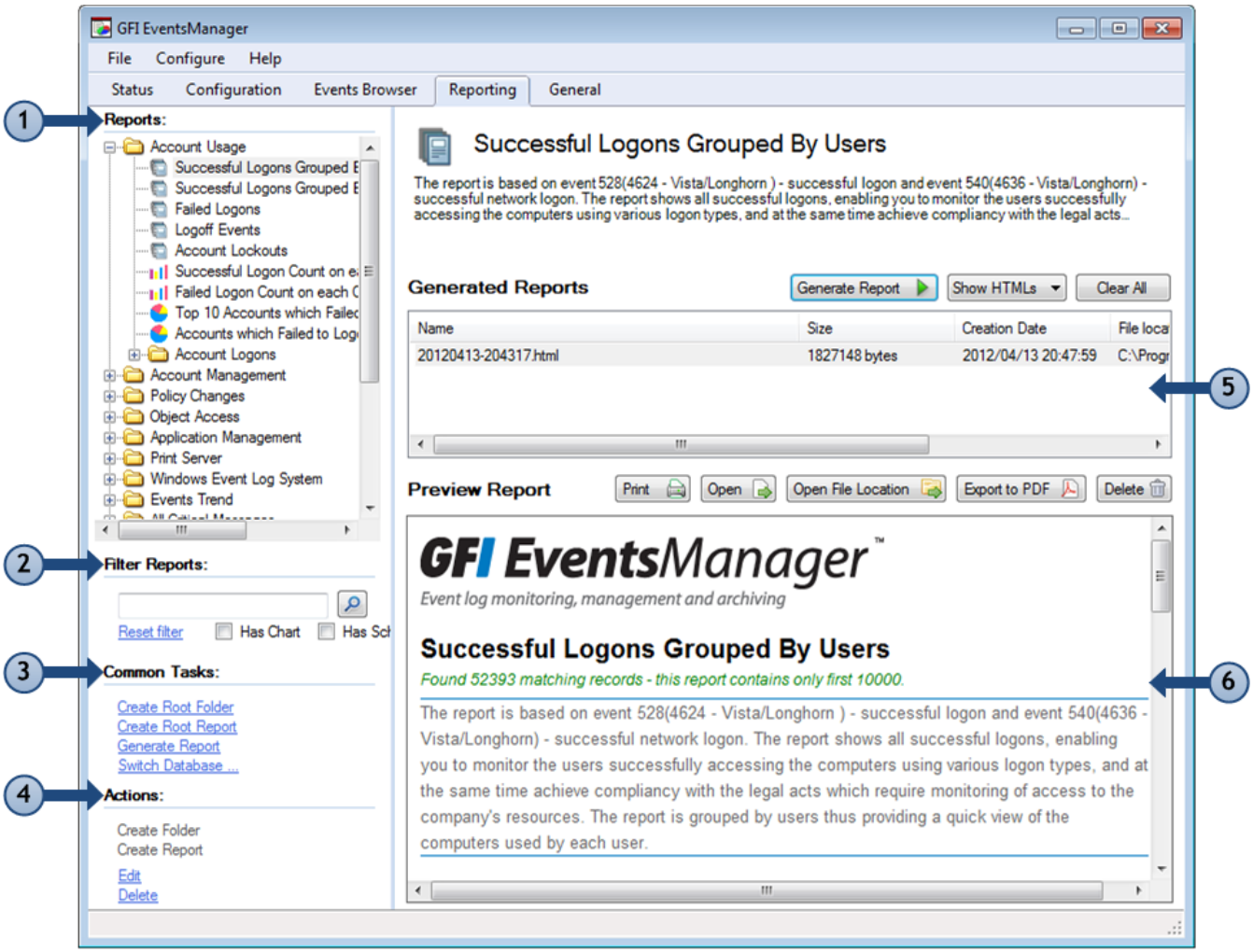
You can click **Add…** to specify a path and a unique name to create a new database. Click **Edit…** to edit the specified information.

7 Reporting

This chapter provides information about the fully-fledged reporting engine of GFI EventsManager. It ships with a number of reports including technical and executive level reports showing graphical and statistical information based on hardware and software managed by GFI EventsManager.

Topics in this chapter:

7.1 Navigating the Reports tab



Screenshot 80: Navigating the Reporting UI

The Reporting tab consists of the sections described below:

Table 43: Navigating the Reporting tab

Section	Description
1	The **Reports** section contains all the predefined reports that ship with the product. Use this section to organize and generate various reports from technical to executive type.
2	Find reports rapidly, using the available filtering options. Through **Filter Reports** options, you are able to search for reports that contain charts and are generated based on a schedule.
3	The **Common Tasks** section enables you to quickly launch typical operations such as creating folder and report views to organize reports and generating reports.
4	From **Actions**, create, edit or delete reports according to your needs.
5	Use the **Generated Reports** section to view the history of a selected report (from Section 1). This enables you to regenerate and export the report to HTML and/or PDF.
6	The **Preview Report** section provides a view of a selected, generated report. Use the control buttons to Print, Open, Export or Delete reports directly from this section.

7.2 Available reports

GFI EventsManager's extensive report list contains reports for various requirements designed to facilitate reporting as much as possible. The following report categories are included in GFI EventsManager by default. GFI EventsManager allows you to use the existing reports as templates to create your own ones. Each category in the table below contains a number of reports that can be used out of the box or customized to fit your requirements:

Table 44: Available reports

Category	Description
Account Usage	Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
Account Management	Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
Policy Changes	Use the reports in this category to identify policy changes effected on your network.
Object Access	Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects that have been deleted.
Application Management	Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications that have been installed or removed as well as applications, which are crashing and hanging.
Print Server	Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
Windows Event Log System	Use the reports in this category to identify audit failures and important Windows event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
Events Trend	Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer-by-computer basis. Reports in this category can be generated for each main time - by hour, day, week or month.

Category	Description
All Critical	Use the reports in this category to display information related to critical Windows events, Syslog, W3C, Custom Events, SNMP Traps and SQL Server Audit events. The charts provided enumerate the 10 most critical events.
Miscellaneous, Customizable	Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows event log, using filtering conditions and grouping modes that are not covered by the other default reports.
PCI DSS Compliance / GCSx Code of Connection Requirements / SOX Compliance / HIPAA Compliance / GLBA Compliance	Use the reports in these categories to generate legal compliance regulations reports.
General and Security Requirements	Use the reports in this category to generate various reports required by several GCSx Code of Connection memos.
LOGbinder SP reports	Use the reports in this category to generate reports related to Microsoft SharePoint audit events.

7.3 Managing reports

Reports are organized in a tree structure enabling you to easily find and generate the required report. GFI EventsManager includes various options that allow you to easily maintain the reports structure as the number of reports increase by time.

This section contains information about:

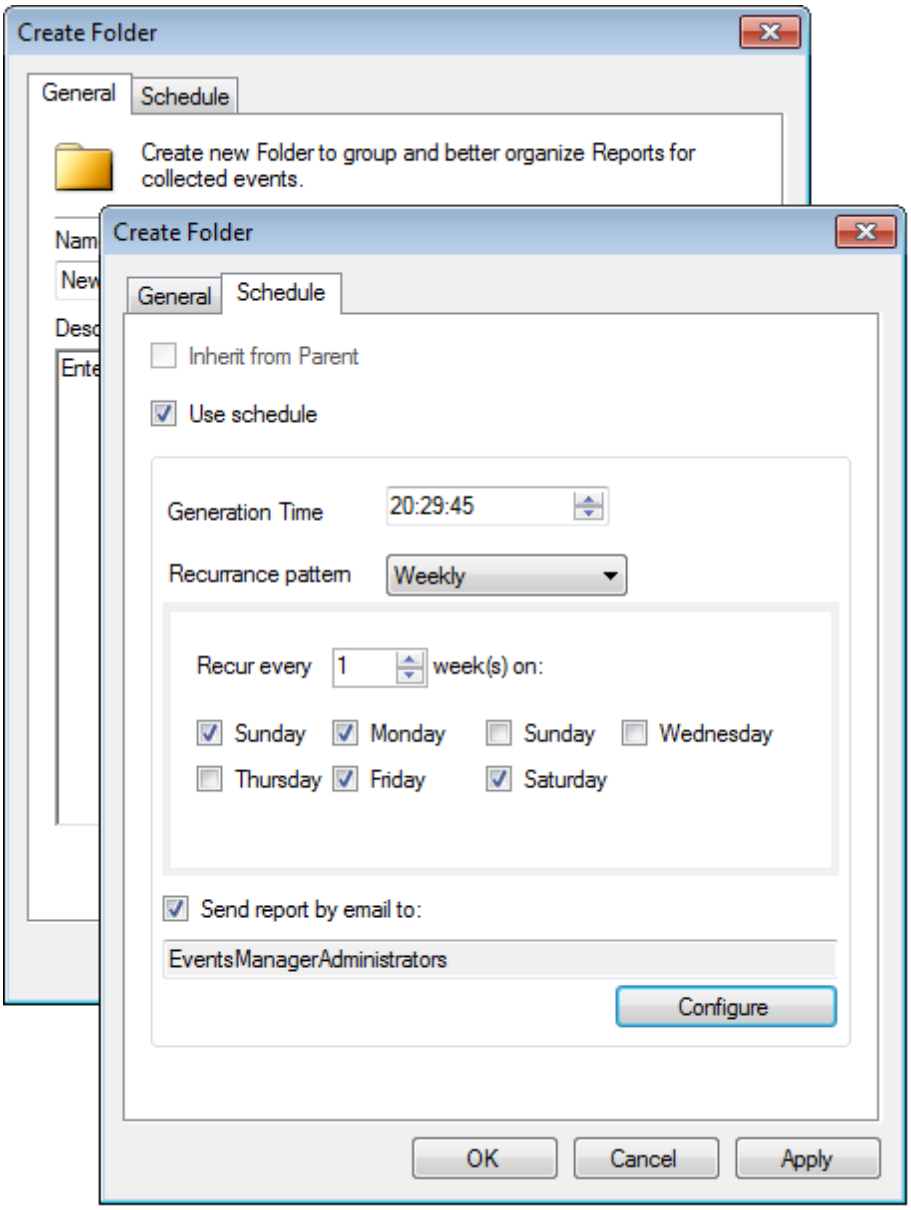
- Creating a root folder
- Creating a folder
- Creating a root report
- Creating custom reports
- Defining report restrictions
- Defining column headings
- Reporting on events from different databases

7.3.1 Creating a root folder

Root folders are top-level folders which may contain one or more sub-folders or reports.

To create a root folder:

1. From **Reporting** tab > **Common Tasks**, click **Create Root Folder**.



Screenshot 81: Create Report Folder dialog

2. From the **General** tab, specify a name and a description (optional) for the new folder.

3. Click **Schedule** tab and select **Use schedule** to configure a schedule for the reports included in this new folder. Configure the options described below:

Table 45: Create report folder: Schedule options

Option	Description
Inherit from Parent	Select when the new folder is part of a root folder that already has scheduling configured.
Use schedule	Select **Use Schedule** to enable scheduling of the reports contained in the new folder.
Generation time	Specify the time when reports are generated.
Recurrence pattern	Specify the report generation frequency. Select from **Daily**, **Weekly** or **Monthly** pattern and configure the respective parameters.
Send report by email to	Select this option to enable email notifications. Click Configure to select the users from the Select users and groups… dialog. **NOTE** Configure alerting options before using this feature. For more information, refer to Configuring Alerting Options (page 187).

4. Click **Apply** and **OK**.

7.3.2 Creating a folder

GFI EventsManager allows you to create as many recurring folders as required.

To create a folder:

1. From **Reporting** tab > **Reports**, right-click a root or sub-folder and select **Create Folder**.

2. From the **General** tab, specify the name and description (optional) for the new group.

3. Click **Schedule** tab and configure the required schedule settings.

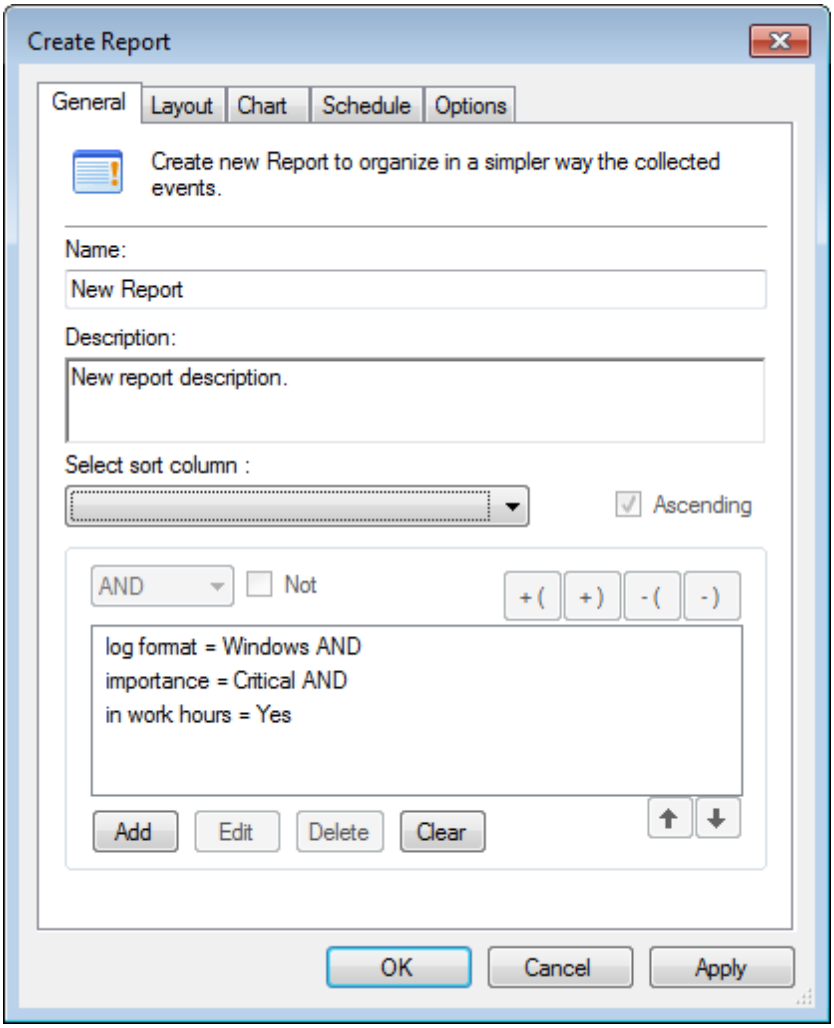
4. Click **Apply** and **OK**.

7.3.3 Creating a root report

Root reports behave in the same way as root folders. These are created at the top level and may contain a number of sub reports. For example, you can create a root report that generates on monthly basis, and contains information about successful logons, failed logons and account lockouts. It's sub-reports would only contain information about specific parts of the root report, such as failed logons only, generated on daily basis.

To create a root report:

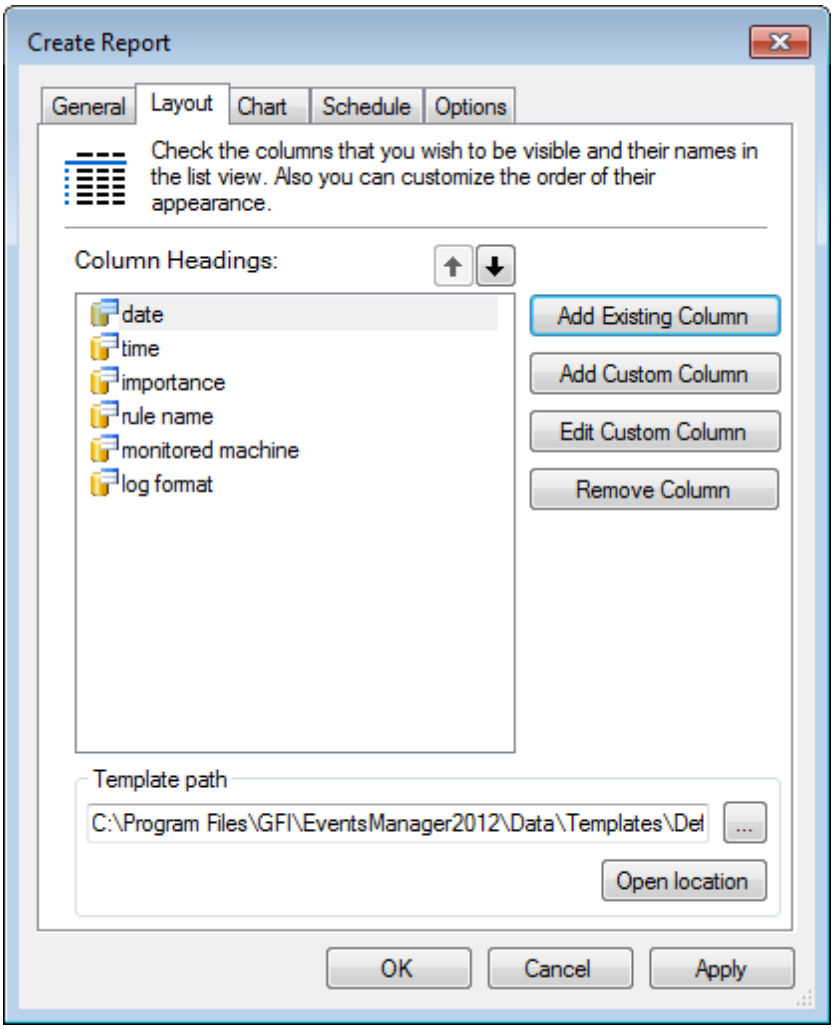
1. From **Reporting** tab > **Common Tasks**, click **Create Root Report**.



Screenshot 82: Creating a root report

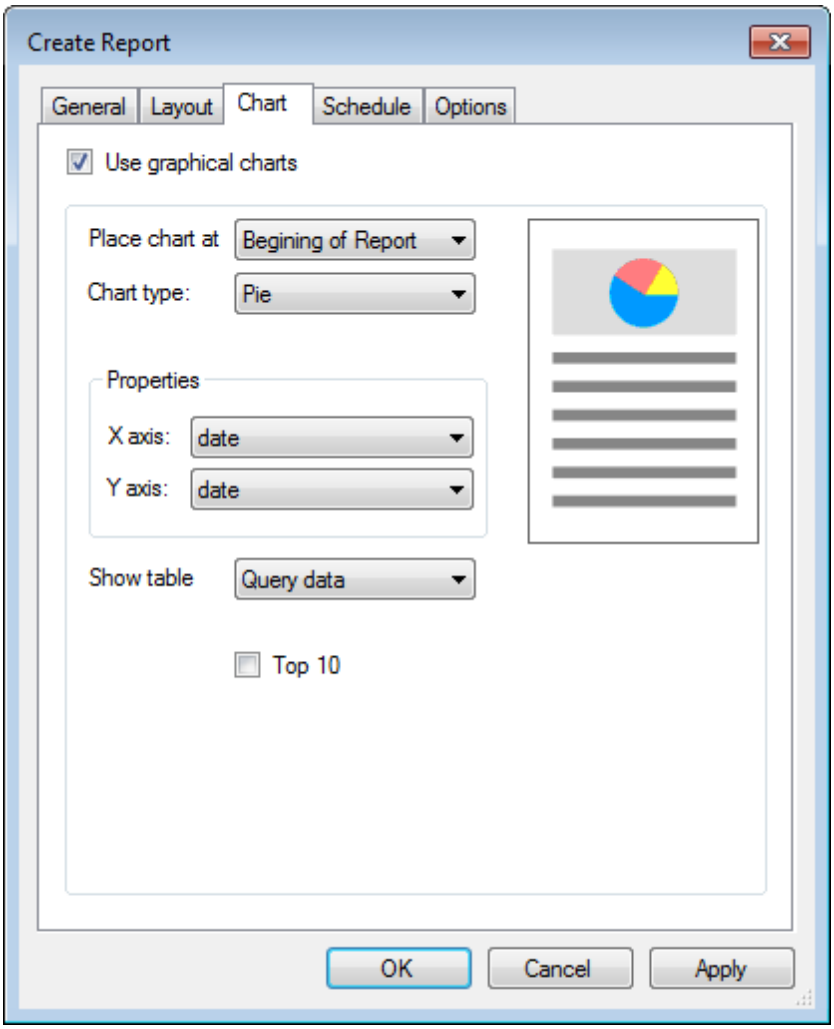
2. From the **General** tab, specify a name and description (optional) for the new root report.

3. Click **Add** to add conditions to your new report. For more information, refer to Defining restrictions (page 126). Repeat this step until all required conditions have been specified.



Screenshot 83: Configuring new root report layout options

4. Click **Layout** tab and add the column headings that you want to be visible in the report. For more information, refer to Defining column headings (page 128). If you have a saved report template, click **Open location** to browse and load your template.



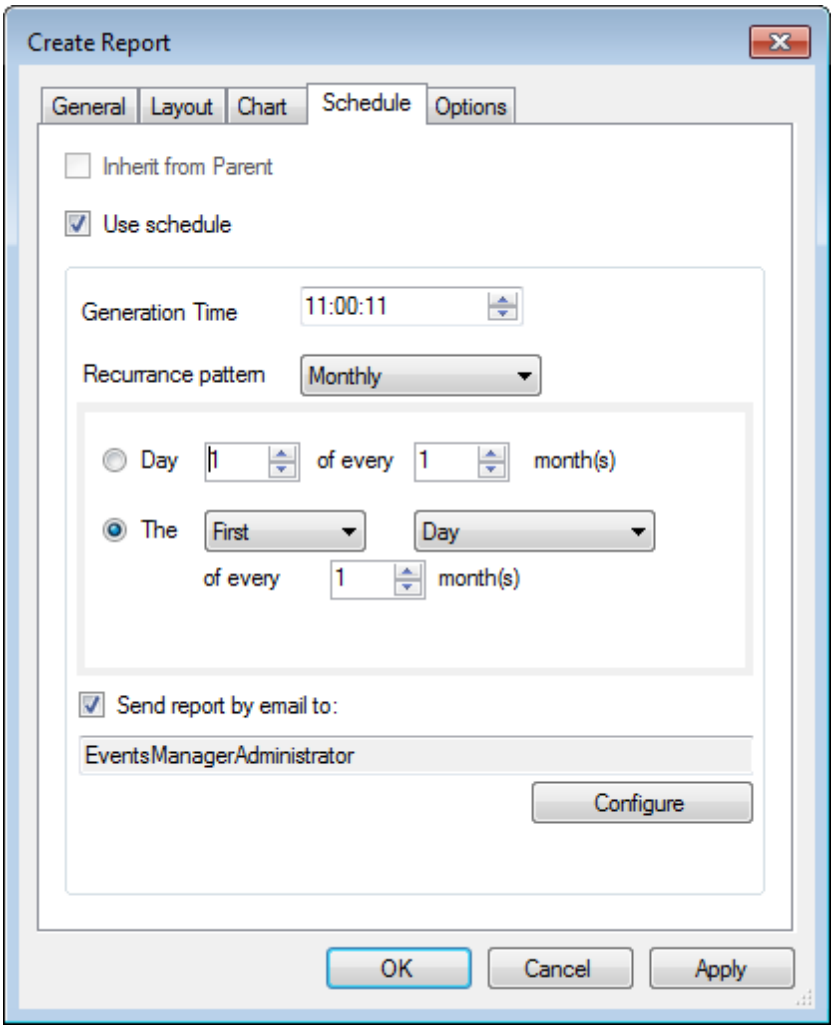
Screenshot 84: Inserting a chart in a new root report

5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.

6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:

- Beginning of Report
- End of Report.

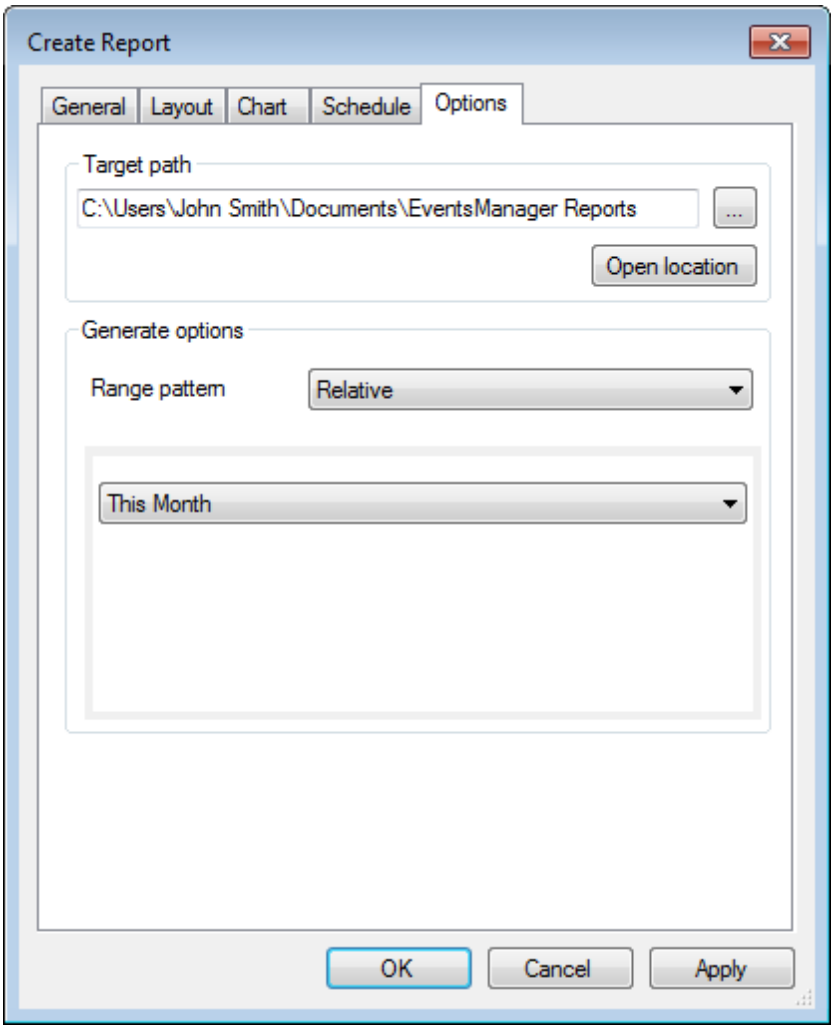
7. From **Properties > X axis** and **Y axis**, configure the X and Y Axis properties. I.e. select the data represented in the chart.



Screenshot 85: Configuring the schedule for when the report is generated

8. (Optional) Click **Schedule** tab and configure schedule settings.

9. Select **Send report by email to** and click **Configure** to select the recipients of this report.



Screenshot 86: Create new report Options

10. Click **Options** tab and specify the path to where the report generates to in the **Target path** area.

11. From the **Range pattern** drop-down menu, select the options described in the table below:

Table 46: Range pattern options

Pattern	Description
All Time	Select **All Time** to generate the report based on information from all the related logs.
Relative	Generate the report based on events from: » Today » Yesterday » Last 7 Days » This Month » Last Month.
Day	Specify a single day that you want to base your report on.
Month	Specify a month and year that you want to base your report on.
Date Range	Specify a **From** and **To** date to base report information on events collected in the specified time period.

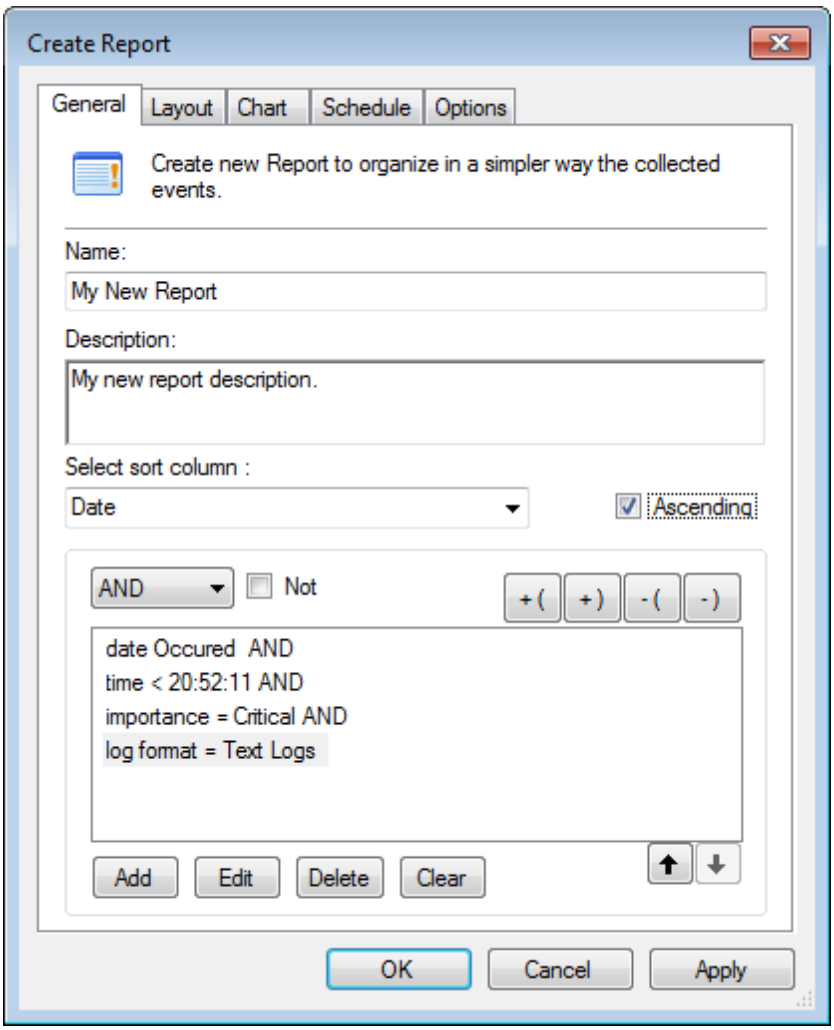
12. Click **Apply** and **OK**.

7.3.4 Creating custom reports

Creating custom reports requires planning while setting up conditions. Conditions are set to determine what is filtered and presented in the report. Failing to configure conditions properly generates unwanted noise and inaccurate information.

To create a new custom report:

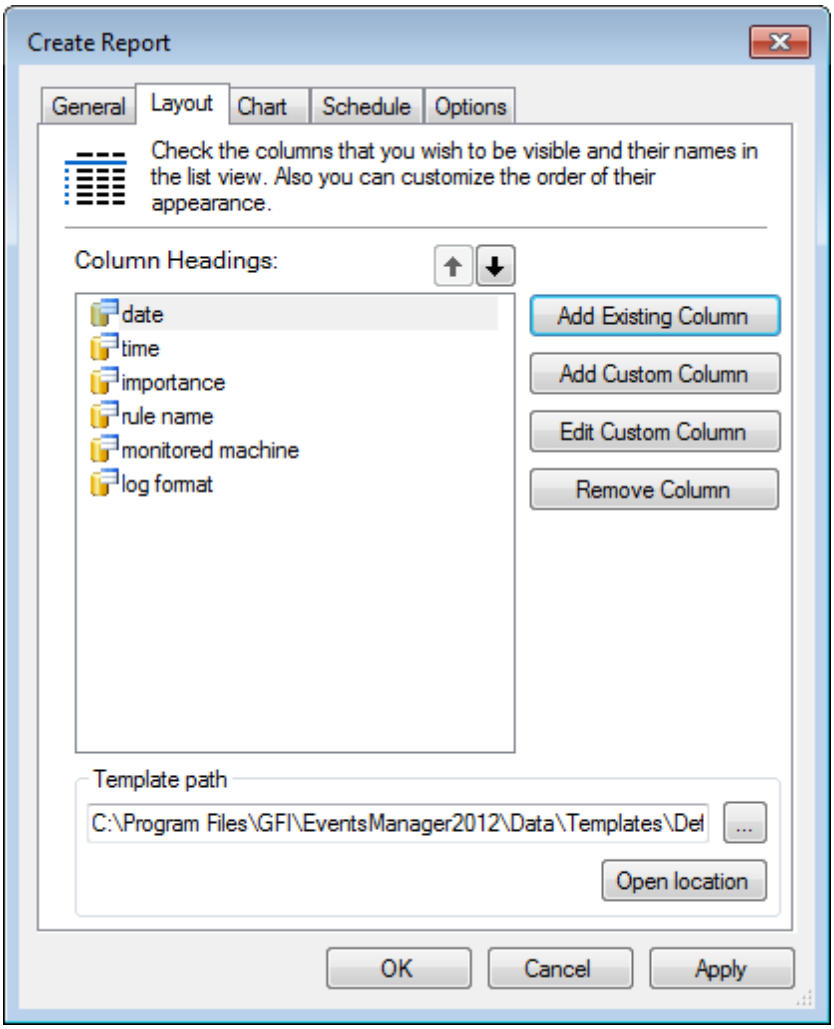
1. From **Reporting** tab > **Reports**, right-click a root folder/folder/root report and select **Create Report**.



Screenshot 87: Creating a report: General options

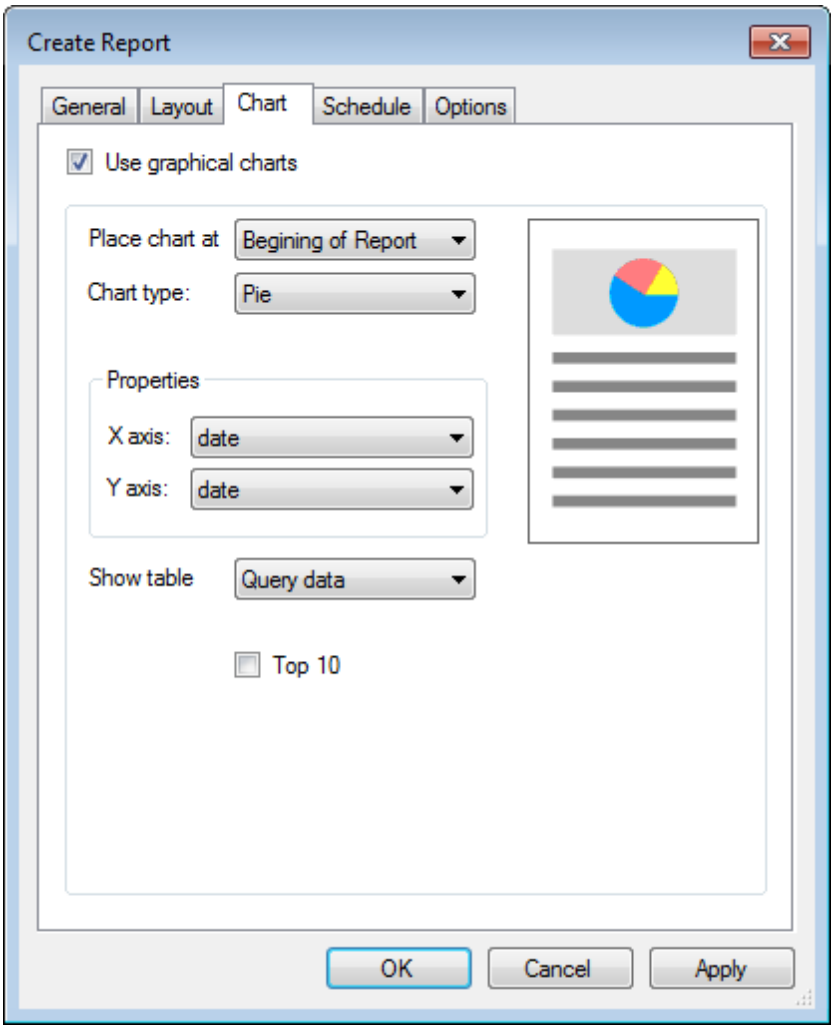
2. From the **General** tab, specify a name and description (optional) for the new root report.

3. Click **Add** to add conditions to your new report. For more information, refer to Defining restrictions (page 126). Repeat this step until all required conditions have been specified.



Screenshot 88: Configuring new root report layout options

4. Click **Layout** tab and add the column headings that you want to be visible in the report. For more information, refer to Defining column headings (page 128). If you have a saved report template, click **Open location** to browse and load your template.



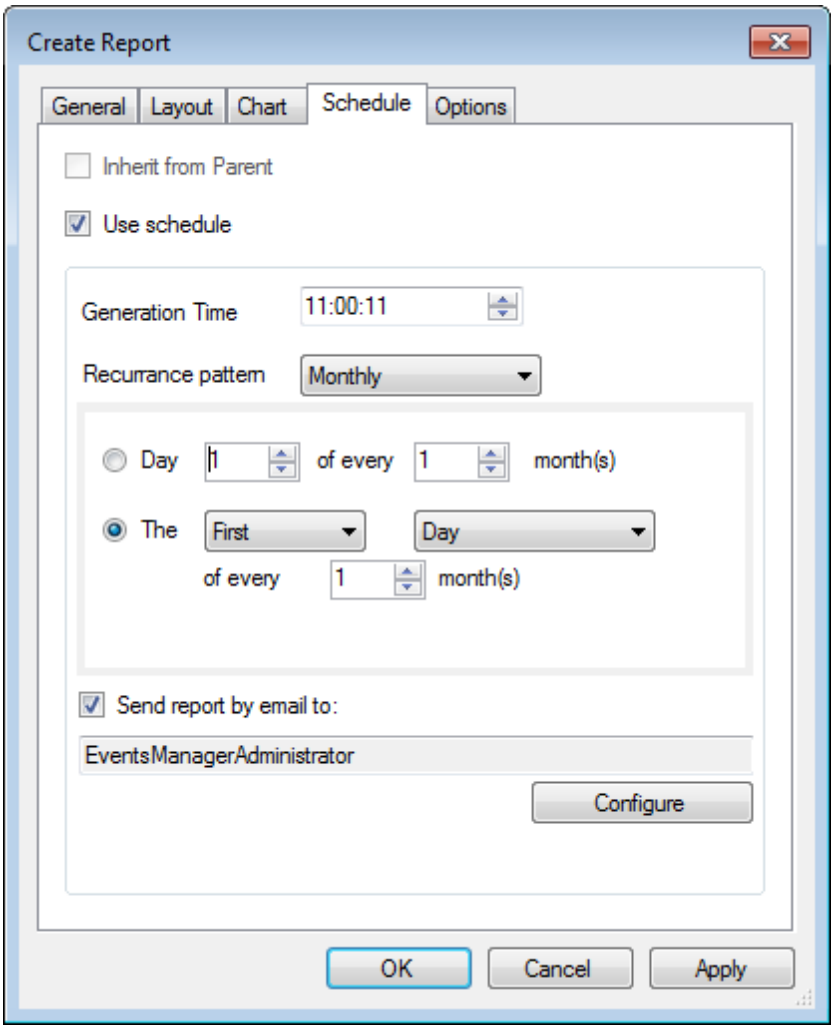
Screenshot 89: Inserting a chart in a new root report

5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.

6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:

- Beginning of Report
- End of Report.

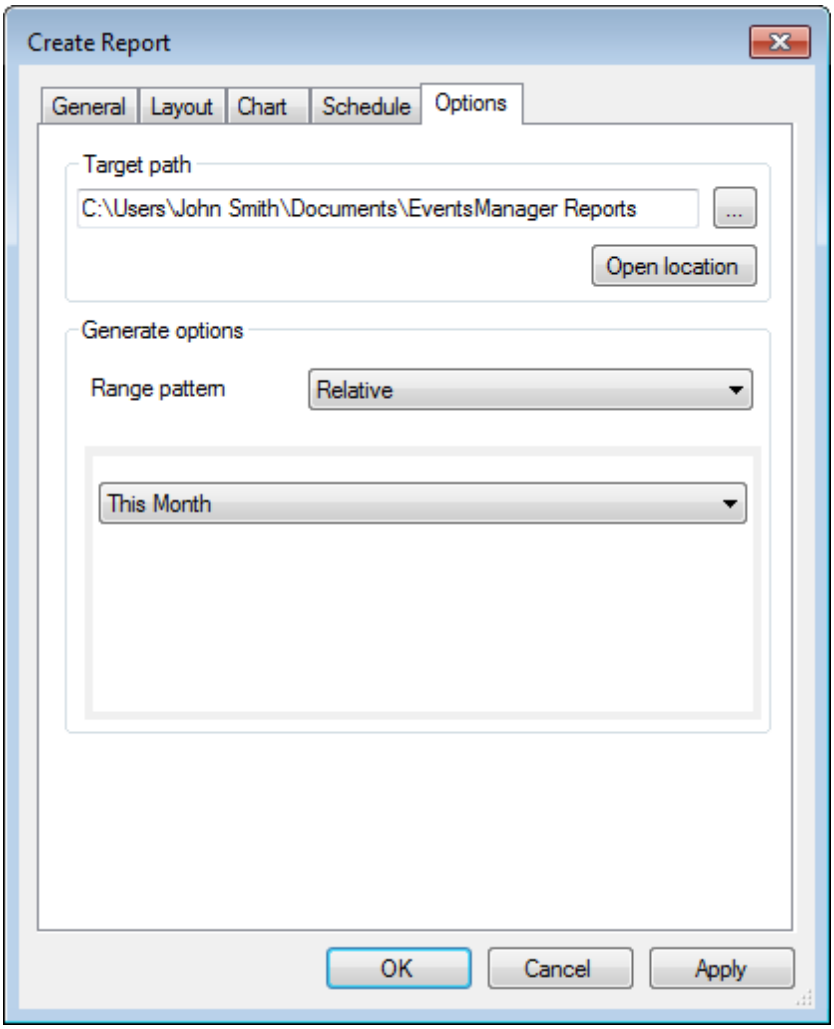
7. From **Properties > X axis** and **Y axis**, configure the X and Y Axis properties. I.e. select the data represented in the chart.



Screenshot 90: Configuring the schedule for when the report is generated

8. (Optional) Click **Schedule** tab and configure schedule settings.

9. Select **Send report by email to** and click **Configure** to select the recipients of this report.



Screenshot 91: Create new report Options

10. Click **Options** tab and specify the path to where the report generates to in the **Target path** area.

11. From the **Range pattern** drop-down menu, select the options described in the table below:

Table 47: Range pattern options

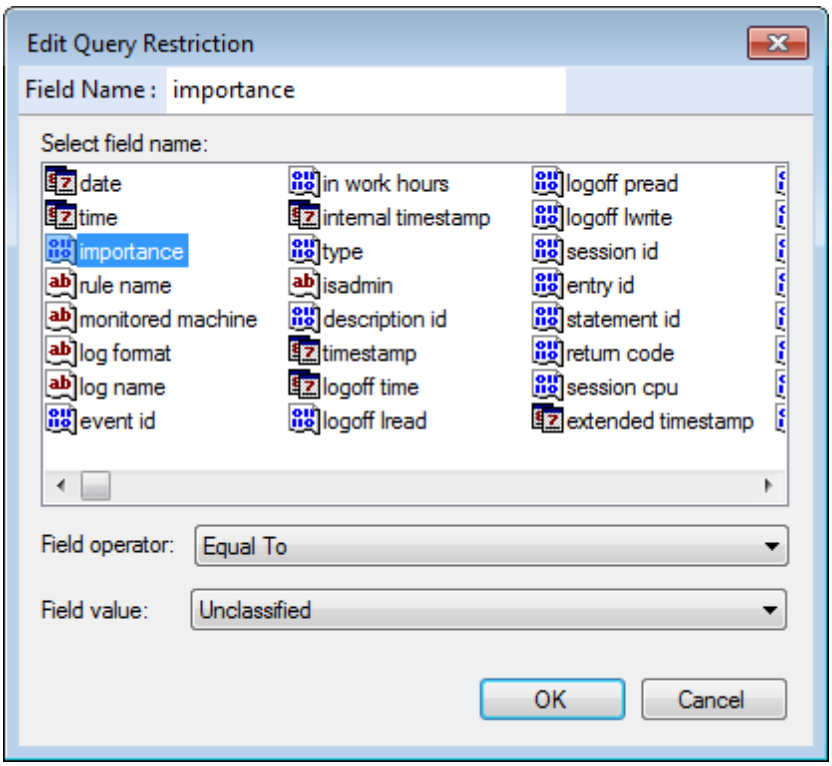
Pattern	Description
All Time	Select **All Time** to generate the report based on information from all the related logs.
Relative	Generate the report based on events from: » Today » Yesterday » Last 7 Days » This Month » Last Month.
Day	Specify a single day that you want to base your report on.
Month	Specify a month and year that you want to base your report on.
Date Range	Specify a **From** and **To** date to base report information on events collected in the specified time period.

12. Click **Apply** and **OK**.

7.3.5 Defining restrictions

Report/view restrictions are used to define what is filtered and presented in your reports/views. To configure conditions:

1. From the Create View/Create Report dialog, click **Add** to launch the **Edit Query Restriction** dialog.



Screenshot 92: Defining restrictions: Editing a query restriction

2. From the list of available fields, select a field. Optionally, you can key in the name in **Field Name** text box to search for the required field.

3. Specify a **Field Operator** for the selected field. Available operators include:

Table 48: Defining restrictions: Field Operators

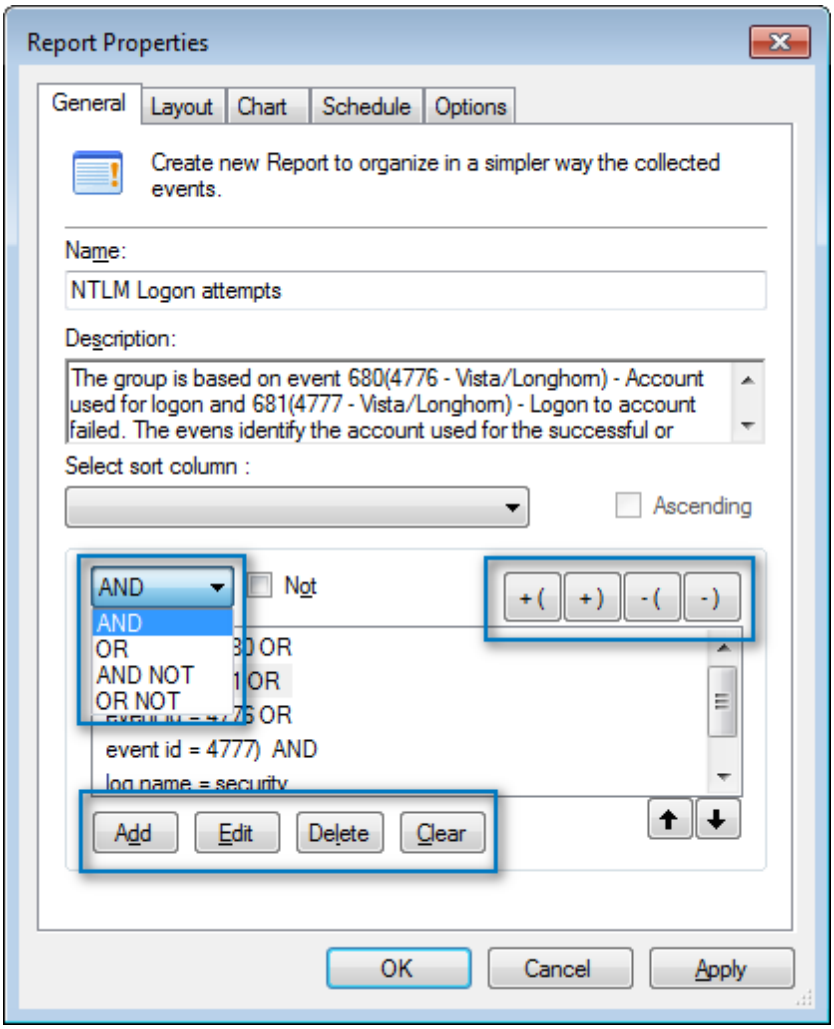
Field Operator	Description
Equal To	When the event field is equal to the value configured.
Less than	When the event field is has a smaller value than the value configured.
Greater than	When the event field is has a larger value than the value configured.
Occurred (Related to date/time fields)	When the event field date occurred before the value date.
Like	When the event field has similar text as the value text.
Contains	When the event field contains the value text.
Value in List	When the event field is equal to one of the values in a list.

4. Specify a **Field Value** for the selected field and operator. Some fields have predefined values while others require you to specify a value.

5. Click **OK**. Repeat this step until all the required filtering conditions are added.

Note

You can copy report restrictions from existing reports. From **Reporting** tab > **Reports**, right-click a report and select **Copy Report Restrictions**.



Screenshot 93: Defining restrictions: Customizing the condition

6. Once all the restrictions are defined, use the options described below to customize the condition according to your requirements:

Table 49: Defining restrictions: Query Condition tools

Options	Description
AND	Select the condition to configure and select AND. The selected condition AND the following condition(s) must be met for the query to be valid.
OR	Select the condition to configure and select OR. The selected condition OR the following condition(s) must be met for the query to be valid.
AND NOT	Select the condition to configure and select AND NOT. This means that the selected condition has to match the restriction parameters but the following conditions must not.
OR NOT	Select the condition to configure and select OR NOT. This means that the selected condition has to match the restriction parameters OR the following conditions must not.
+ (	Click '+ (' to add an opening bracket to the selected condition. Conditions enclosed in brackets are processed first.

Options	Description
+)	Click '+)' to add a closing bracket to the selected condition. Conditions enclosed in brackets are processed first.
- (	Click '- (' to remove an opening bracket from the selected condition.
-)	Click '-)' to remove a closing bracket from the selected condition.
Add	Click Add to launch the restrictions dialog and add more fields to the condition.
Edit	Click Edit to access the restrictions dialog and customize the selected condition.
Delete	Click Delete to delete a condition.
Clear	The Clear button deletes all the query conditions.
Up arrow	Use the Up arrow key to move the selected condition up in the list.
Down arrow	Use the Down arrow key to move the selected condition down in the list.

7. Click **Apply** and **OK**.

7.3.6 Defining column headings

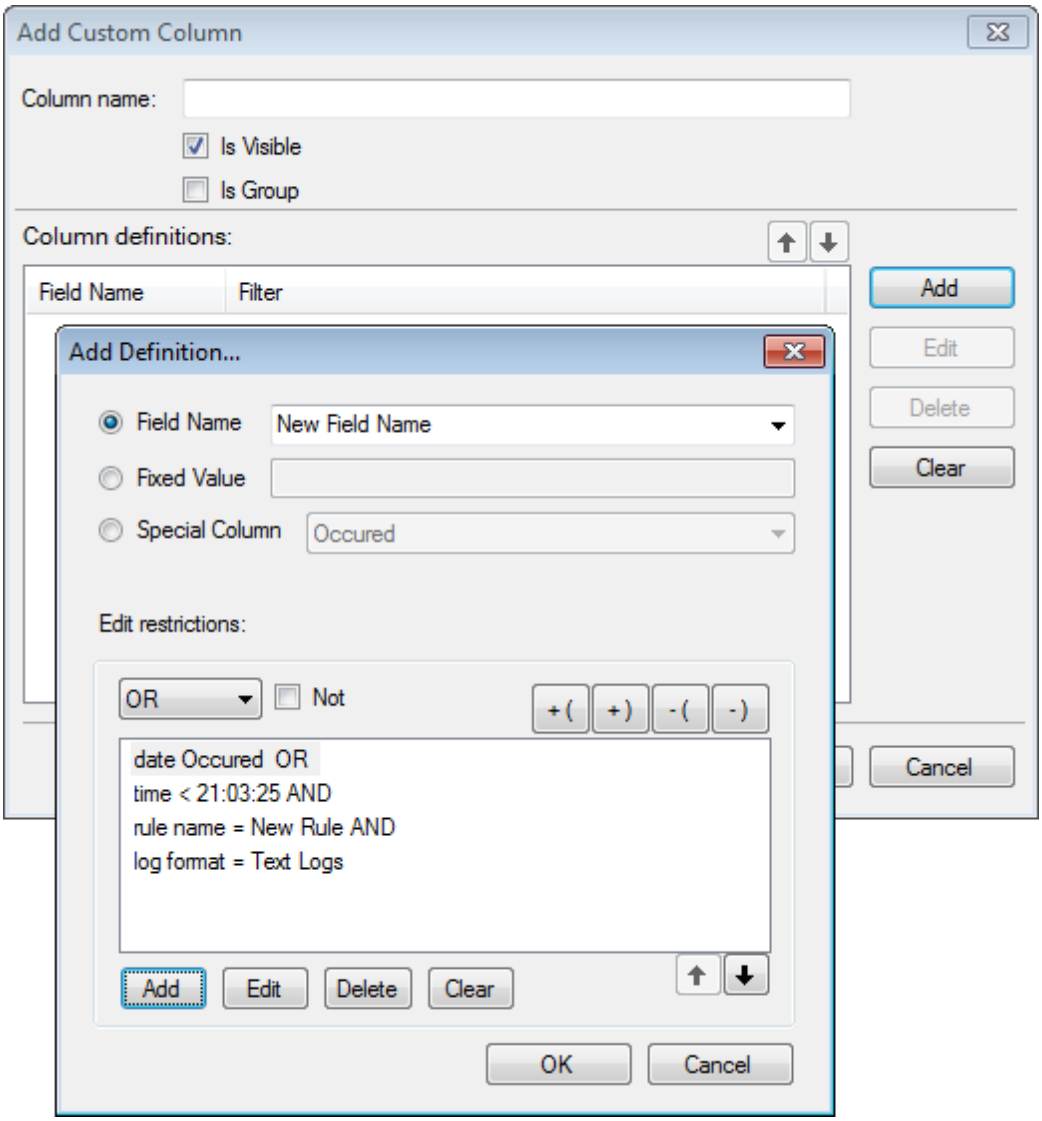
GFI EventsManager enables you to create custom columns through the **Add Custom Columns** dialog. This dialog allows you specify conditions, create a new field and add them to your report(s). Also based on conditions, this dialog enables you to further customize existing or new reports.

To add custom columns:

1. From **Reporting** tab **> Actions**, click **Create Report**.

2. Click **Layout** tab **> Add Existing Column**, to add default columns.

3. Click **Add Custom Column** to launch the **Add Custom Columns** dialog.



Screenshot 94: Define custom column conditions

4. From the **Add Custom Column** dialog click **Add**.

5. From the **Add Definition…** dialog, configure the options described below:

Table 50: Add Column Definition options

Option	Description
Field Name	Specify a name for the new field.
Fixed Value	Select **Fixed Value** if the value of the new field is going to be fixed. Specify a value as a field name. For example, to check that events always occur after 5pm, specify 5 as the fixed value instead of defining a time field and assign a value of 5.
Special Column	Special columns are predefined columns that may be used in your condition.
Edit restrictions	This section enables you to add, edit or delete field restrictions. For more information, refer to Defining restrictions (page 126).

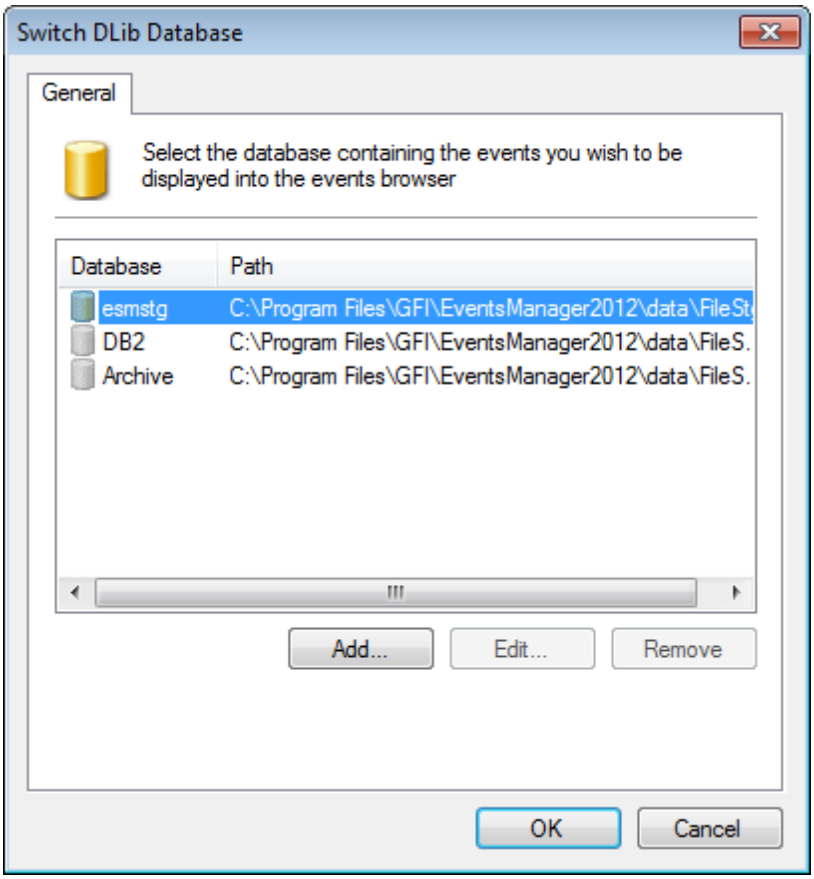
6. Click **Apply** and **OK**.

7.3.7 Reporting on events from different databases

For reporting purposes, GFI EventsManager enables you to switch between different databases. Use this feature to report on events that have been exported/archived for further analysis or stored in different databases.

To switch database:

1. From **Reports** tab > **Common Tasks**, click **Switch database**.



Screenshot 95: Switch database dialog

2. Select the database from the list of databases and click **OK**. Click **Add…** to specify a new database name and it's relevant path. Click **Edit…** to edit the specified information.

7.4 Generating reports

GFI EventsManager enables you to generate a number of different reports, containing information about GFI EventsManager configuration settings, network activity and product activity.

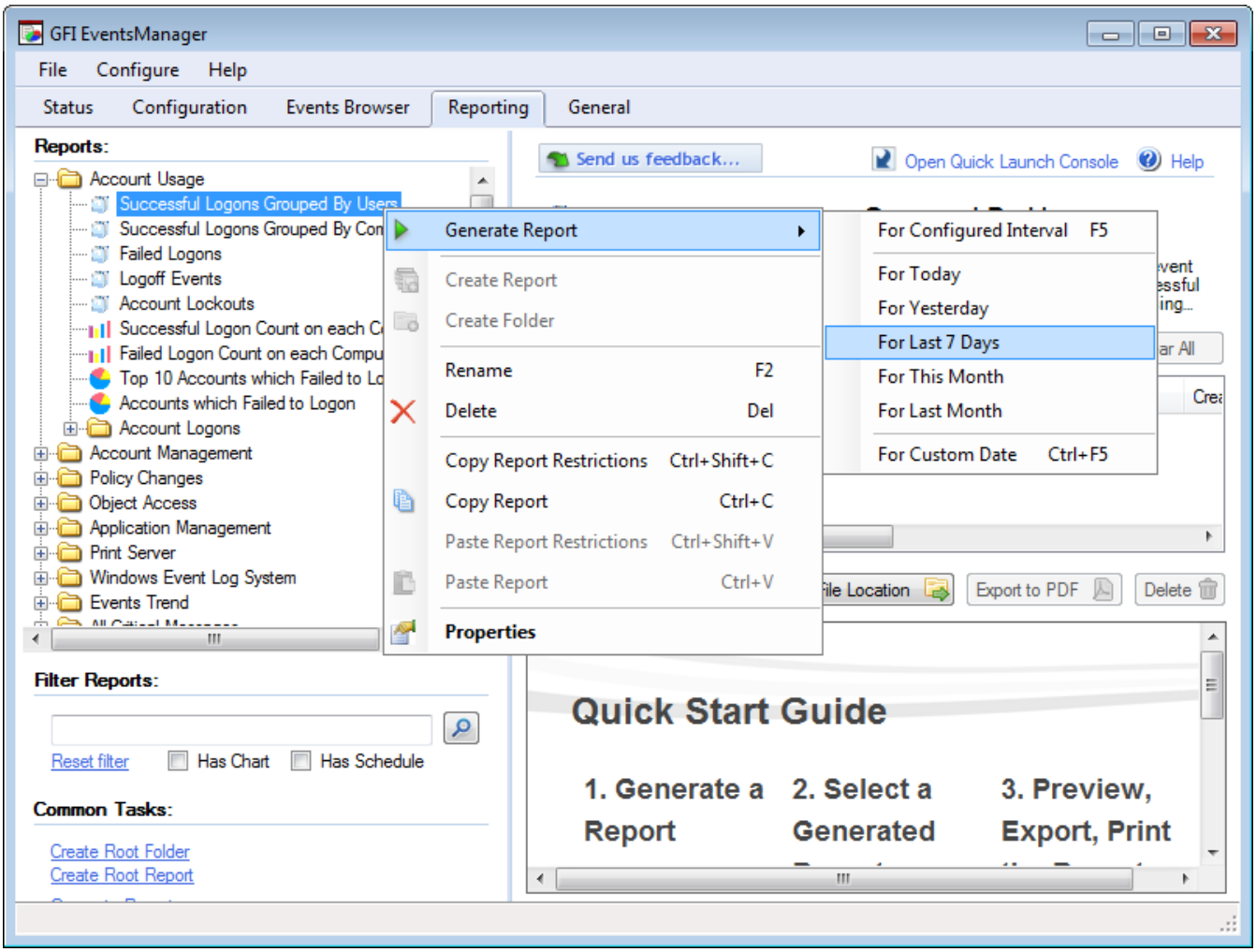
This section contains information about:

- Generating a report
- Generating daily digest reports
- Generating settings reports
- Generating rules reports
- Generating operational history reports
- Generating activity overview reports

7.4.1 Generating a report

To generate a report:

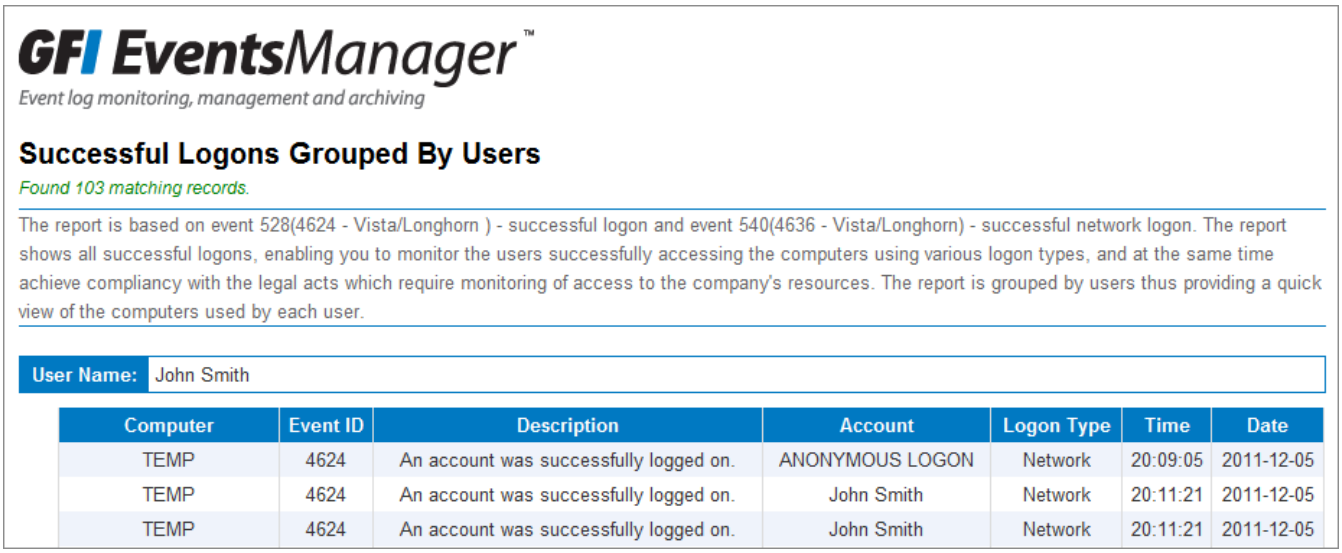
1. From **Reporting** tab > **Reports**, right-click a report and select **Generate Report**.



Screenshot 96: Generating a report

2. Wait for the report to generate and view results in **Preview Report** section.

> **Note**
>
> Reports can also be generated by selecting a report from the list and clicking **Generate Report** at the top of the reporting page.



GFI EventsManager™

Event log monitoring, management and archiving

Successful Logons Grouped By Users

Found 103 matching records.

The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliancy with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.

User Name: John Smith

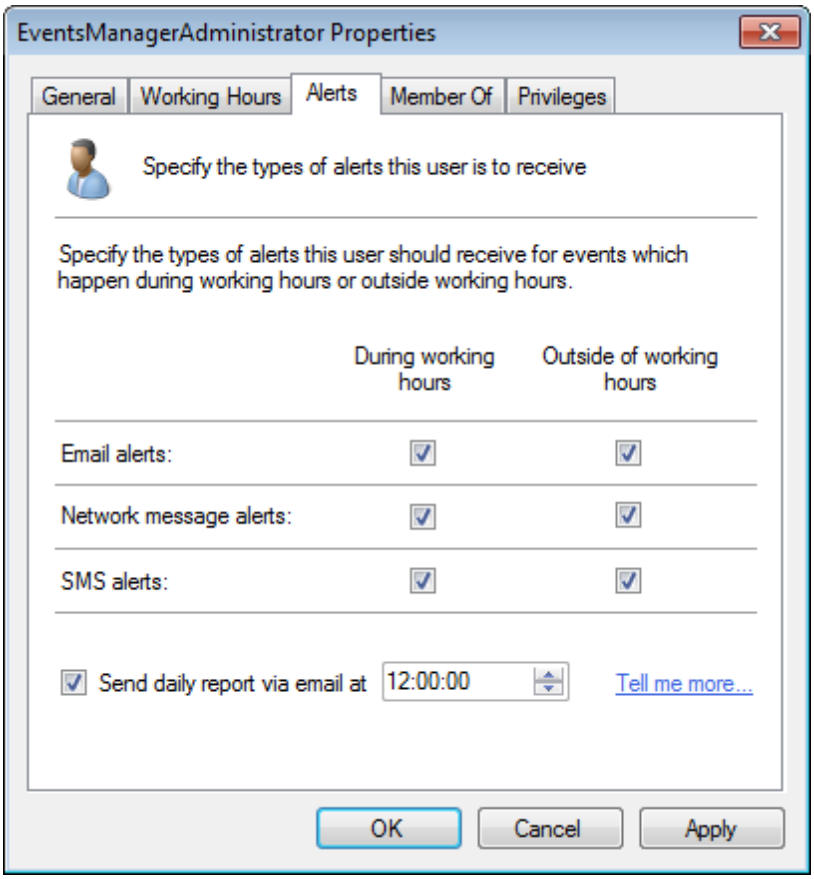
Computer	Event ID	Description	Account	Logon Type	Time	Date
TEMP	4624	An account was successfully logged on.	ANONYMOUS LOGON	Network	20:09:05	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05

Screenshot 97: Report sample

7.4.2 Generating daily digest reports

GFI EventsManager can be configured to send a summary report by email on a daily basis. The report contains a summary of the most important events collected and processed during the last 24 hours. To configure a user to receive Daily Digest emails:

1. From **Configuration** tab > **Options**. Expand **Users and Groups** and select **Users**.
2. Right-click a user from the right pane and select **Properties**.
3. From the **General** tab, ensure that a valid email address is configured.
4. From the **Alerts** tab, select **Send daily report via email**.



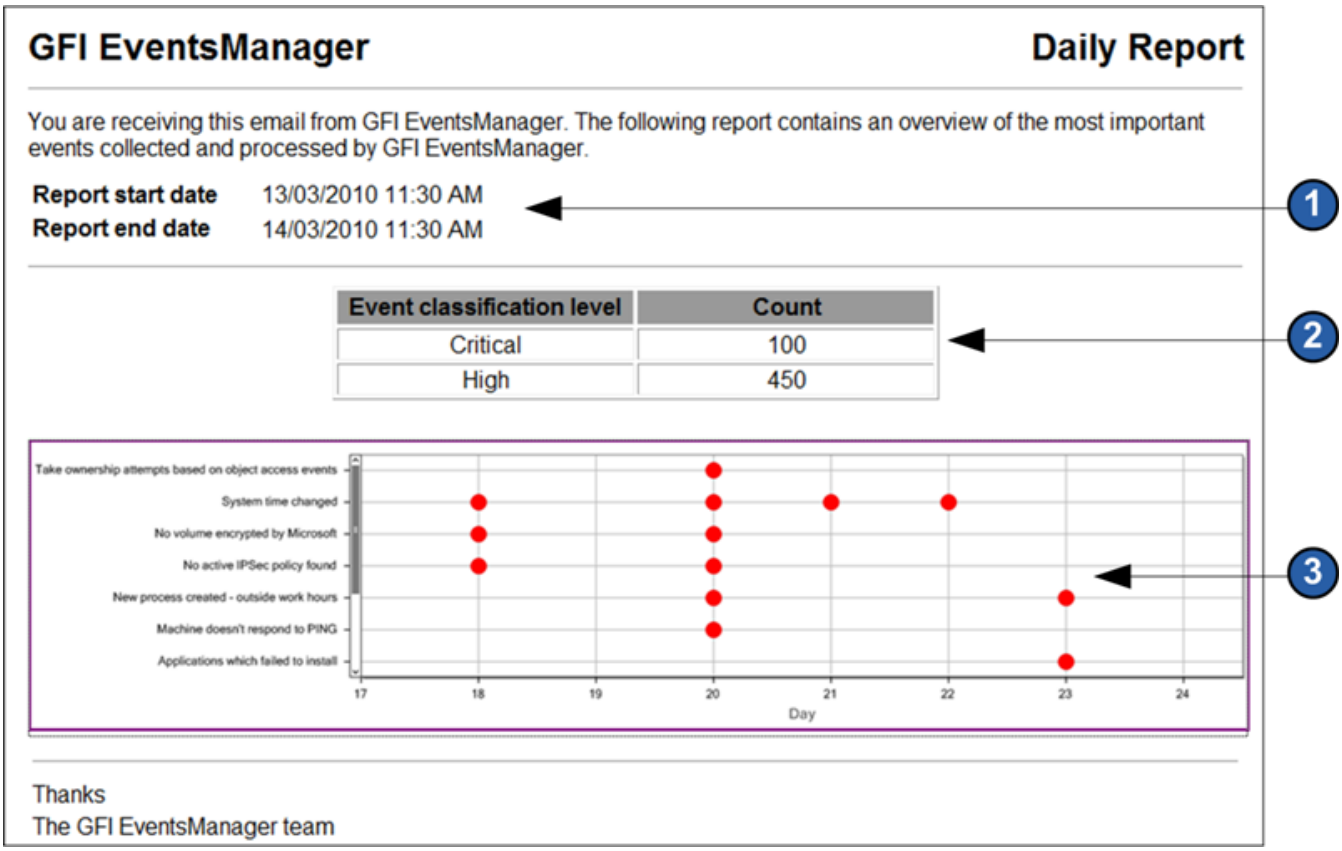
Screenshot 98: Daily Digest email settings

5. Configure the time when the Daily Digest email is sent.

6. Click **Apply** and **OK**.

Note

For more information, refer to Users, Groups and Console Security (page 163).



Screenshot 99: Daily digest email

Table 51: Daily digest email description

Section	Description
1	The start and end date of the report. The report displays the most important events collected by GFI EventsManager between the start and end date.
2	The number of Critical and High events collected in the last 24 hours.
3	This graph provides statistical information about critical events collected from all event sources in the last 24 hours.

7.4.3 Generating settings reports

GFI EventsManager enables you to generate settings reports on event source groups. The provided information is described below:

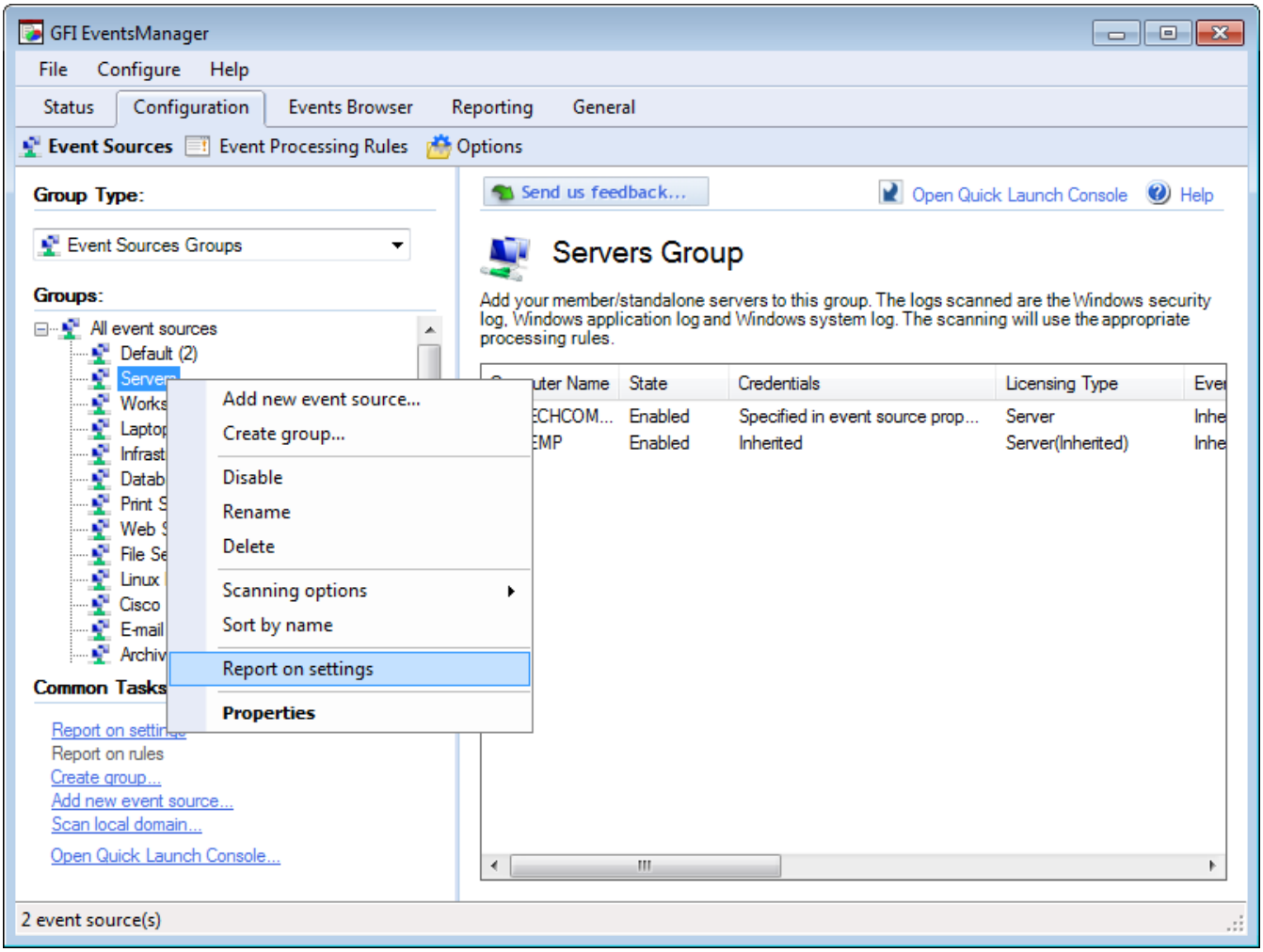
Table 52: Settings report heading information

Heading	Description
Group name	The name of the group the report is based on.
Computer name	A list of every event source in the selected group.
Scan intervals	Scanning interval for every event source in the selected group; shown in **Days : Hours : Minutes : Seconds**.

Heading	Description
Rules folder	Provides a list of rule categories applied to the selected group, such as: » Noise reduction » Security » System health » PCI DSS requirements.
Rule sets	A granular list of rules applied on the selected group.

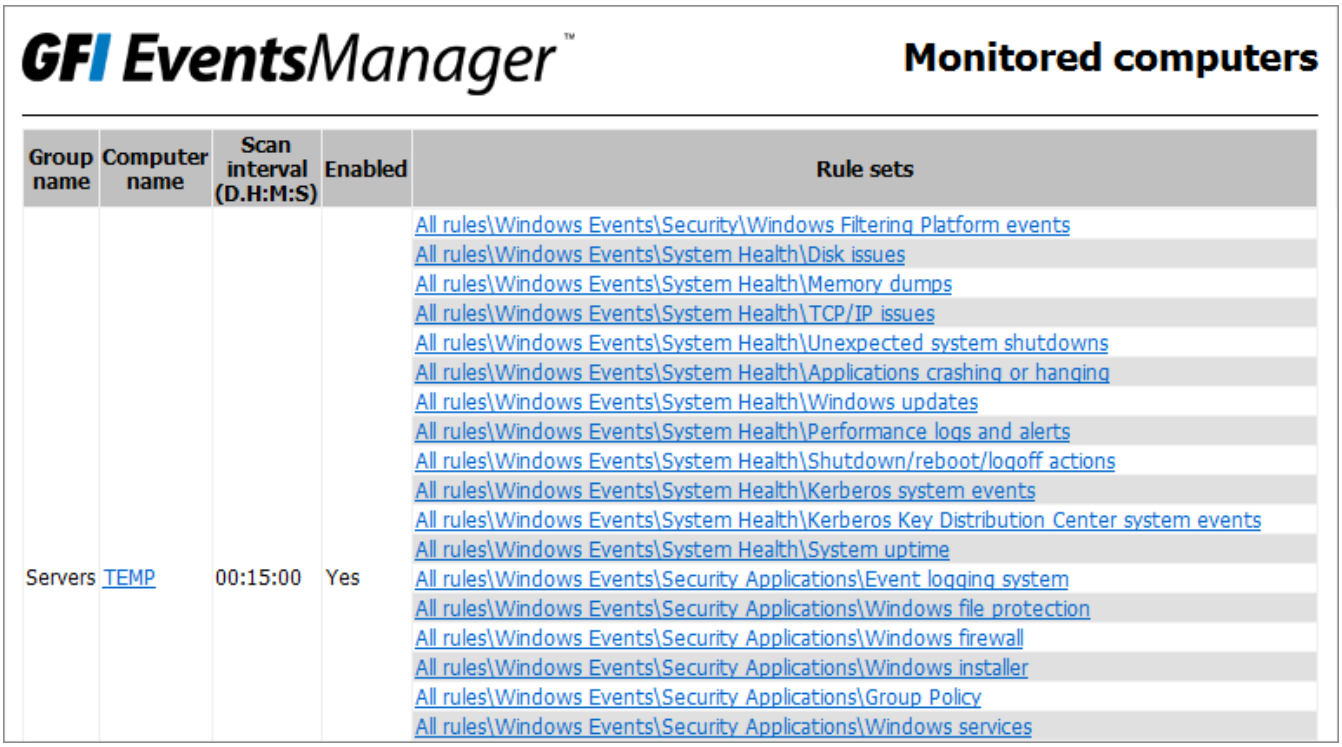
To generate settings report:

1. Click **Configuration** tab > **Event Sources**.



Screenshot 100: Generate configuration report

2. Right-click an event source group and select **Report on settings**.



GFI EventsManager™ **Monitored computers**

Group name	Computer name	Scan interval (D.H:M:S)	Enabled	Rule sets
Servers	TEMP	00:15:00	Yes	All rules\Windows Events\Security\Windows Filtering Platform events All rules\Windows Events\System Health\Disk issues All rules\Windows Events\System Health\Memory dumps All rules\Windows Events\System Health\TCP/IP issues All rules\Windows Events\System Health\Unexpected system shutdowns All rules\Windows Events\System Health\Applications crashing or hanging All rules\Windows Events\System Health\Windows updates All rules\Windows Events\System Health\Performance logs and alerts All rules\Windows Events\System Health\Shutdown/reboot/logoff actions All rules\Windows Events\System Health\Kerberos system events All rules\Windows Events\System Health\Kerberos Key Distribution Center system events All rules\Windows Events\System Health\System uptime All rules\Windows Events\Security Applications\Event logging system All rules\Windows Events\Security Applications\Windows file protection All rules\Windows Events\Security Applications\Windows firewall All rules\Windows Events\Security Applications\Windows installer All rules\Windows Events\Security Applications\Group Policy All rules\Windows Events\Security Applications\Windows services

Screenshot 101: Settings report sample

7.4.4 Generating rules reports

Rules repots provide a detailed view of applied rules on event sources. The information provided in rules reports are described below:

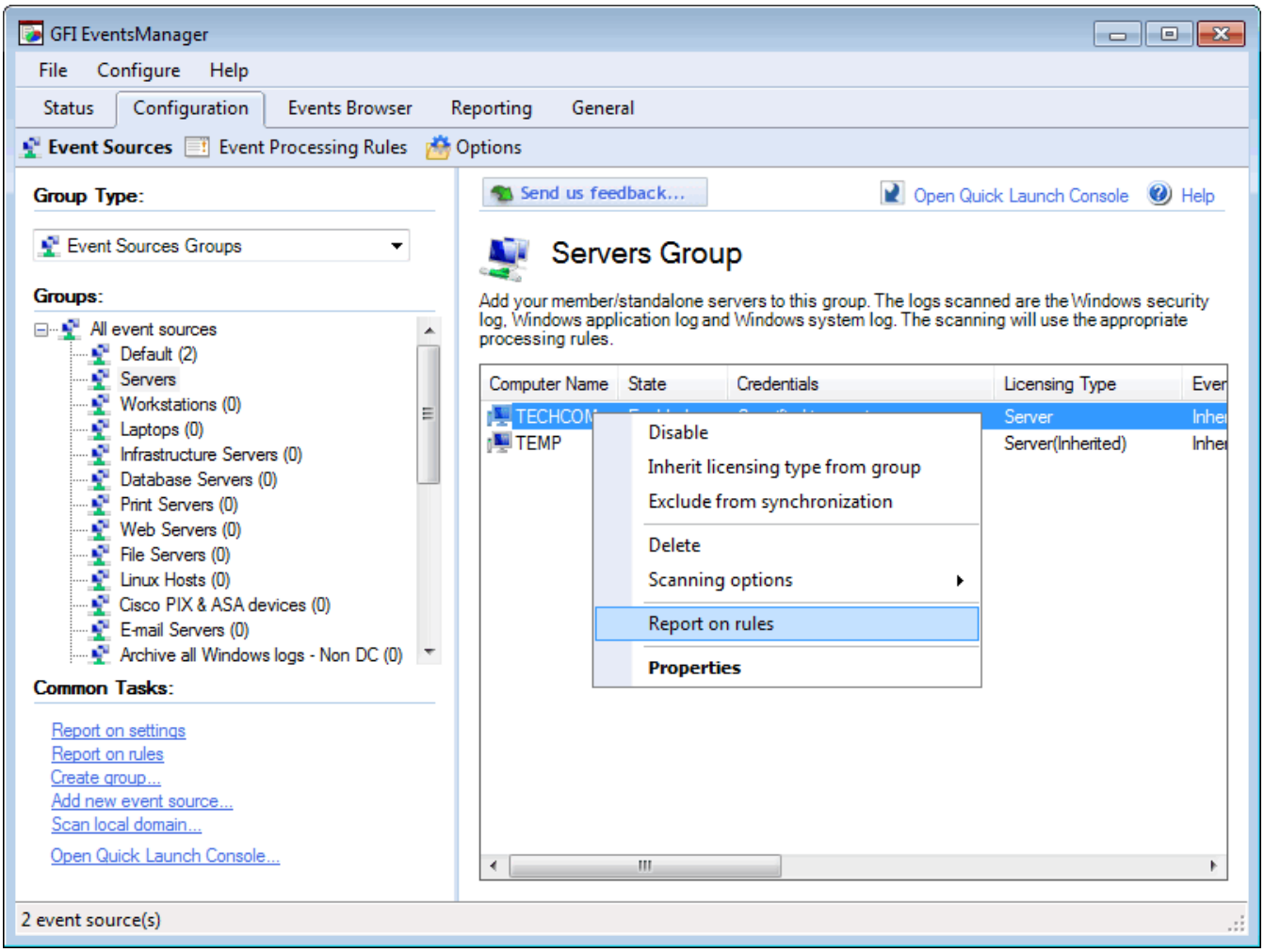
Table 53: Rules report heading information

Heading	Description
Rule name	Name of the applied rule.
Importance	The classified importance level of the collect event log, such as: » Critical » High » Medium » Low » Noise event.
Logfile monitored	Provides the category name of the collected event log, such as: » Security » System Health » Application » System.
Conditions	The processing condition(s) for the selected rule. This includes: » Event IDs » Source » Category » User » Type » Advanced.

Heading	Description
Actions	Describes the actions taken when the event is processed, including: » Archiving settings » Mail to settings » Threshold settings.

To generate rules report:

1. Click **Configuration** tab > **Event Sources**.



Screenshot 102: Generate configuration report

2. Right-click an event source and select **Report on rules**.

7.4.5 Generating operational history reports

GFI EventsManager's operational history can be exported for further analysis and archiving purposes. Operational history messages provide administrators with information as described below:

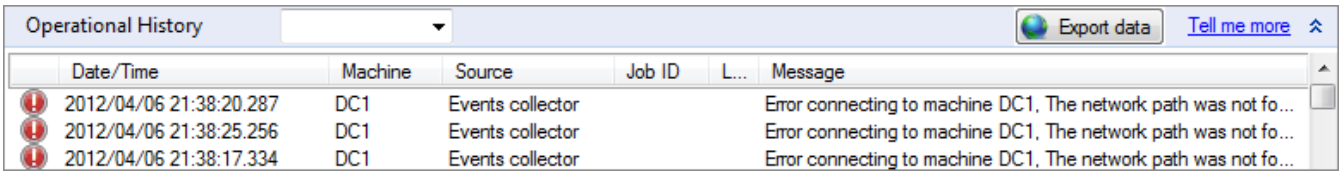
Table 54: Operational History report description

Date/Time	Date and time when the message was generated.
Machine	Event source that generated the message.

Source	Source operation that cause the message to be generated. Amongst others these include: » EvtCollector - message generated while collecting event logs » SNMP TrapsServer - message generated while collecting SNMP Traps Messages » EnetrpriseMaintenance - message generated during database maintenance jobs.
Job ID	An internal ID associated with the job.
Log file/name	Type of logs collected. Amongst others: Application Security Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity.
Message	The actual message generated while performing the job.

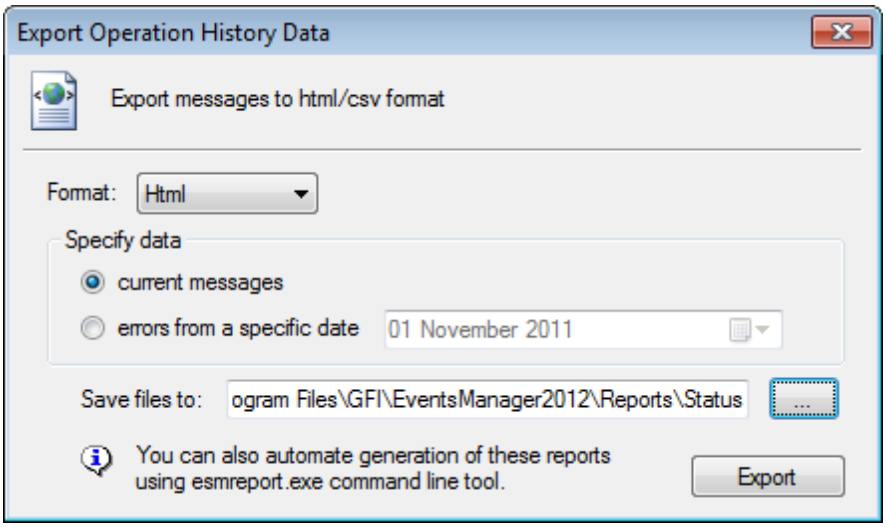
To generate Operational History reports:

1. Click **Status** tab > **Job Activity**.



Screenshot 103: Operational History report

2. Click **Export data**.



Screenshot 104: Operational History dialog

3. Specify the options described below and click **Export**.

Table 55: Operational History export options

Option	Description
Format	Select the report output format. Available formats are HTML and CSV.
Current messages	Export all messages displayed in Job Activity tab.
Errors from a specific date	Specify a date and export all the messages generated on that date.
Save file to	Select checkbox to specify output location. If not selected, reports are saved in the default location within the GFI EventsManager directory.

GFI EventsManager

Operational History for period: 2011-11-01

Date/Time	Type	Machine	Source	Job ID	Log file/name	Message
31/10/2011 18:41:03	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Start executing checks on machine 192.168.3.1..
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Executed 5 checks on machine 192.168.3.1
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	B3789E4A	Security	Start the collection on machine 192.168.3.1, log Security
31/10/2011 18:41:30	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.
31/10/2011 18:41:33	Information	192.168.3.1	EvtCollector	1017473C	Application	Start the collection on machine 192.168.3.1, log Application
31/10/2011 18:41:45	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.

Screenshot 105: Operational History report sample

7.4.6 Generating activity overview reports

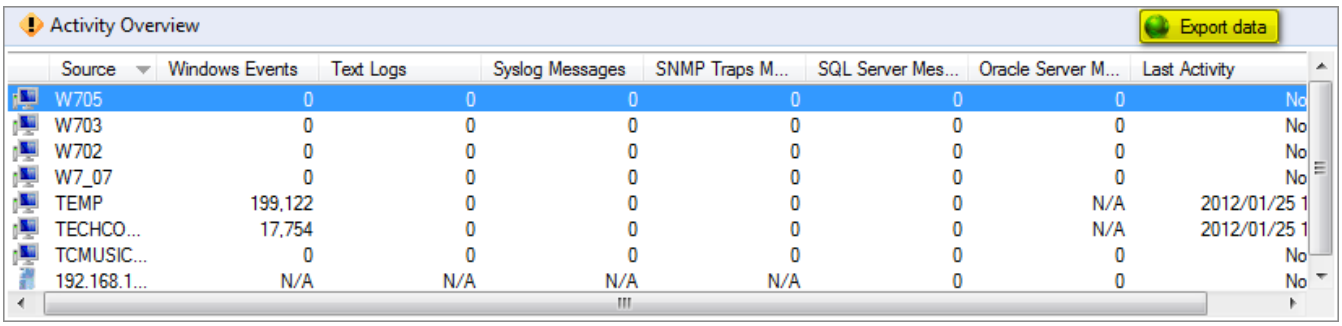
GFI EventsManager enables you to export Activity Overview data. Activity overview reports provide the information described below:

Table 56: Activity overview report headings

Heading	Description
Date/Time	Date and time when the message was generated.
Machine	Event source that generated the message.
Source	Source operation that cause the message to be generated. Amongst others these include: » **EvtCollector** - message generated while collecting event logs » **SNMP TrapsServer** - message generated while collecting SNMP Traps Messages » **EnetrpriseMaintenance** - message generated during database maintenance jobs.
Job ID	An internal ID associated with the job.
Log file/name	Type of logs collected. Amongst others: » Application » Security » Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity
Message	The actual message generated while performing the job.

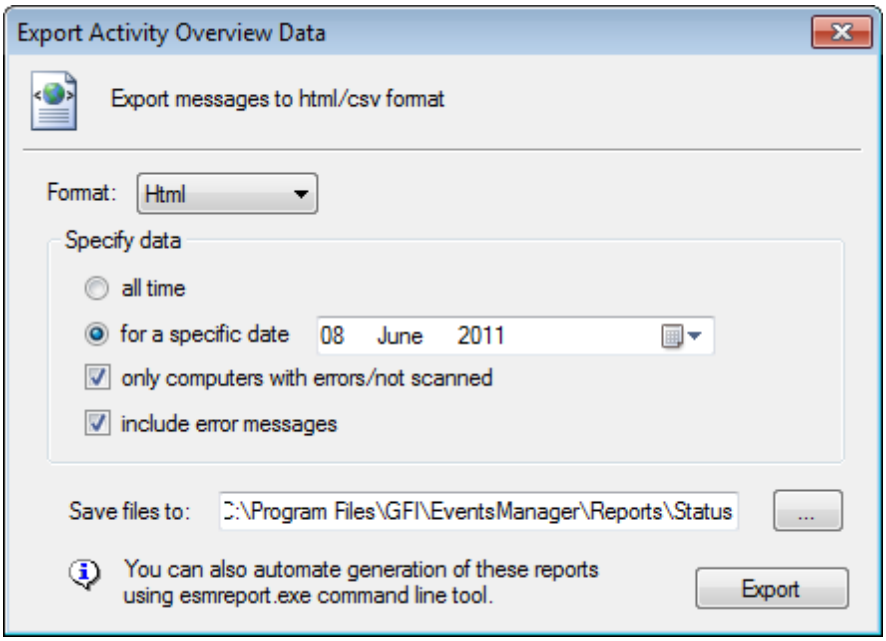
To export Activity Overview:

1. Click **Status > Statistics**.



Screenshot 106: Activity overview : Export button

2. Click **Export data**.



Screenshot 107: Activity overview dialog

3. Configure the options described in and click **Export**.

Table 57: Export Operational History options

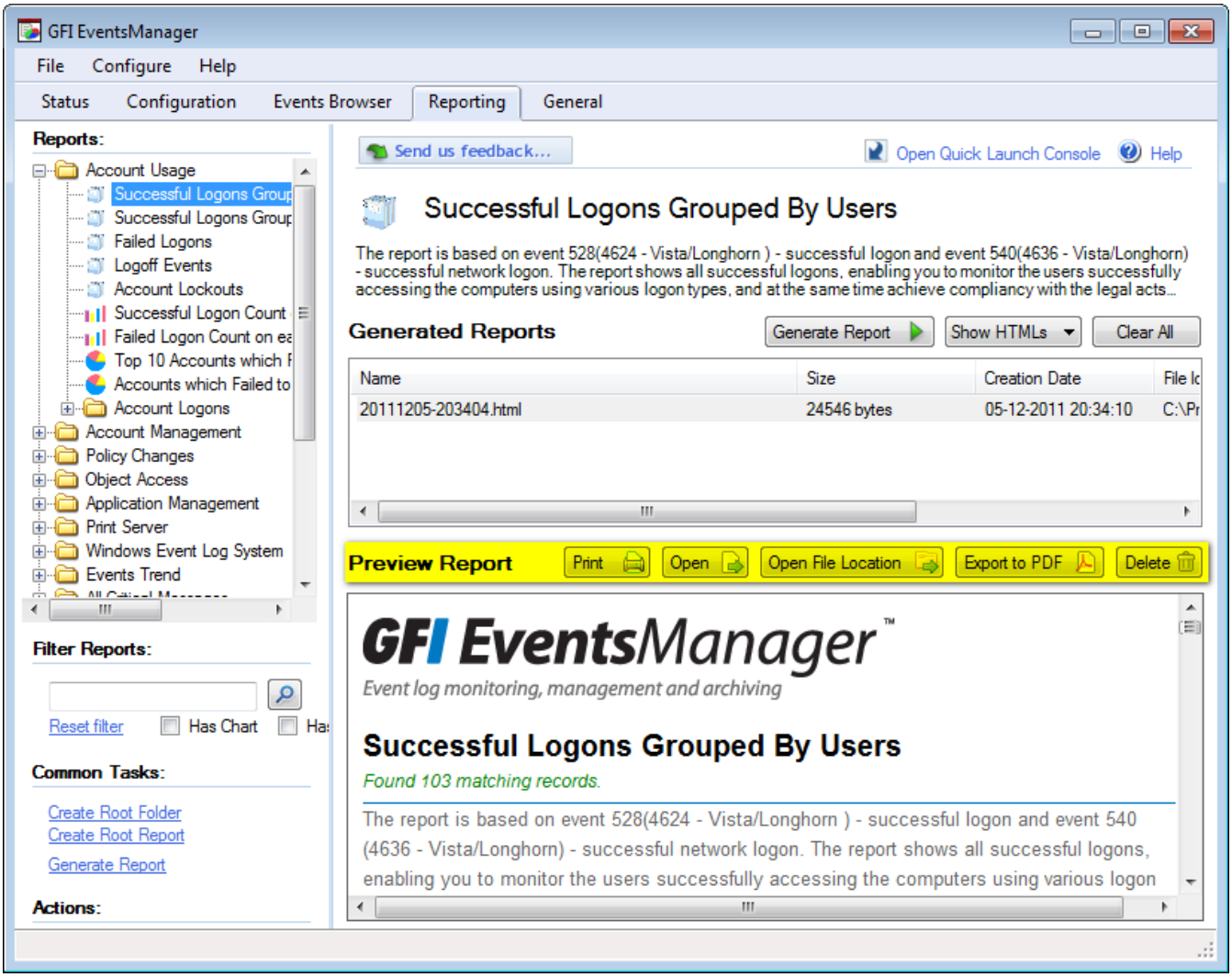
Option	Description
Format	The report output format. Available formats are HTML and CSV.
All time	Export all messages displayed Activity Overview.
From a specific date	Specify a date to export all messages generated on that date.
Only computers with errors/not scanned	Export only data of computers with scanning issues.
Include error messages	Select this option to include the generated error message.
Save files to	Displays the default export location.

GFI EventsManager™ **Activity Overview for period: 2012/01/25**

Source	Windows Events	Text Logs Events	Syslog Messages	SNMP Traps Messages	SQL Server Messages	Oracle Server Messages	Last Activity
TCMUSICSERVER	0	N/A	N/A	N/A	N/A	N/A	No Activity
TECHCOMSERVTWO	23753	N/A	N/A	N/A	N/A	N/A	2012/01/25 18:08:00.933
TEMP	196799	N/A	N/A	N/A	N/A	N/A	2012/01/25 17:55:47.542
W7_07	0	N/A	N/A	N/A	N/A	N/A	No Activity
W702	0	N/A	N/A	N/A	N/A	N/A	No Activity
W703	0	N/A	N/A	N/A	N/A	N/A	No Activity
W705	0	N/A	N/A	N/A	N/A	N/A	No Activity
192.168.11.11	N/A	N/A	N/A	N/A	N/A	0	No Activity

Screenshot 108: Activity overview report sample

7.5 Analyzing reports



Screenshot 109: Analyzing reports

The reporting system of GFI EventsManager comes with dedicated tools to help you analyze and export reports. Once a report is generated, select it from the list of Generated Reports and use the common controls which help you run common report analysis commands. The available tools are described below:

Table 58: Analyzing reports: Tools

Option	Description
Print	Use the **Print** option to view a print preview, configure printer settings and print the selected report.
Open	Use the **Open** button to open the selected report in a browser. GFI EventsManager uses your default browser to view reports in HTML.
Open File Location	**Open File Location** enables you access the folder containing the report for backup or archiving purposes.
Export to PDF	Use **Export to PDF** to export the selected report to Portable Document Format.
Delete	Click **Delete** to remove a generated report from the list.

7.6 Customizing HTML reports

HTML report templates are customizable, enabling you to further tweak GFI EventsManager to suit your daily requirements. To edit the available templates, knowledge of HTML and CSS is required.

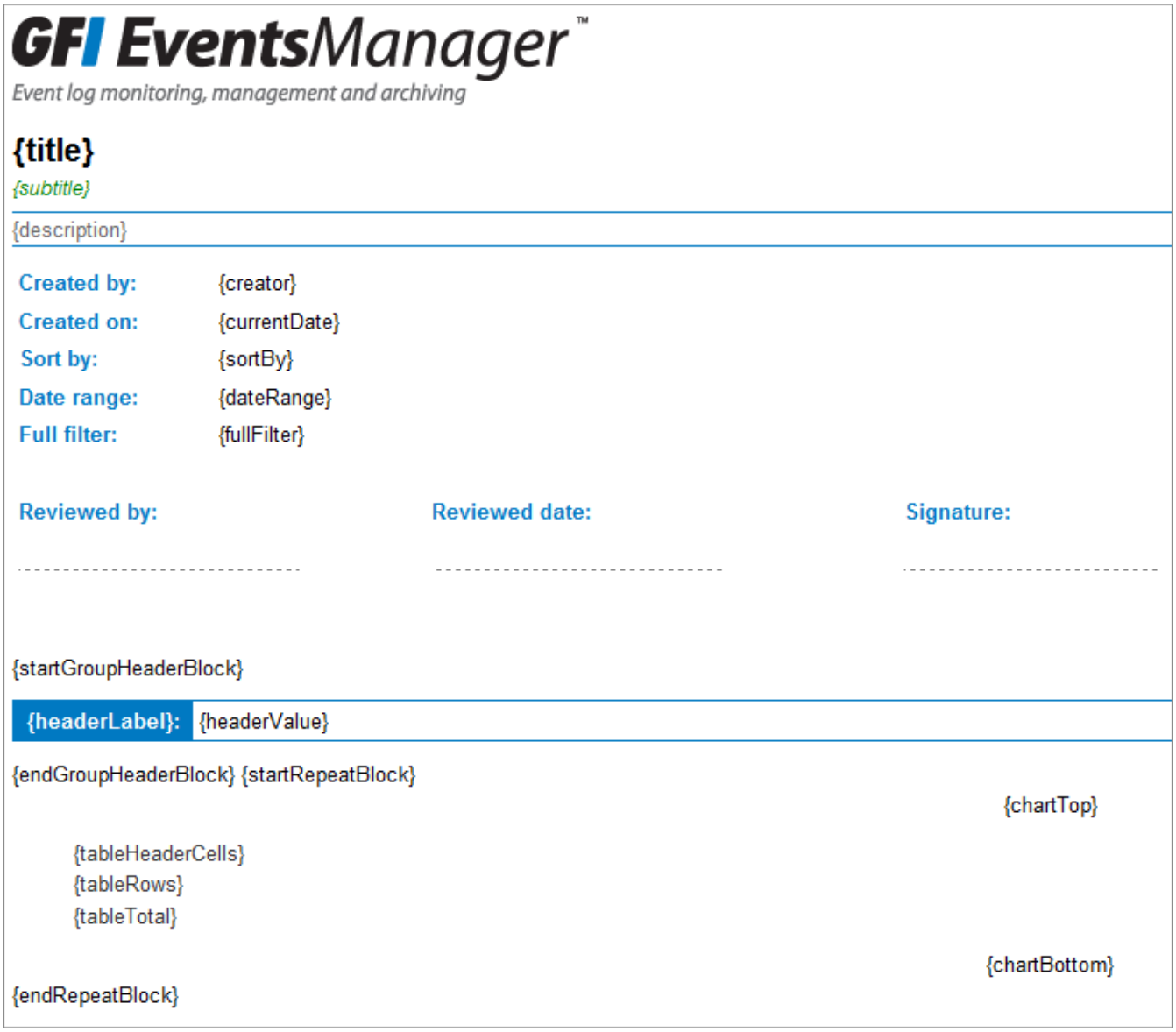
Important

Before editing the default report template, save a copy of the original so that you can easily revert to default for troubleshooting.

To edit the layout of HTML reports:

1. Go to GFI EventsManager install directory:

```
%Program Files\GFI\EventsManager2012\Data\Templates\DefaultReportLayout
```



Screenshot 110: Editing HTML report templates

2. From **DefaultReportLayout** folder, edit the templates described below:

Table 59: Default HTML templates

Template	Description
template_group_new.html	This template is used when generating reports which contain data about grouped sources. Grouping can be by users, sources, event data and more.
template_new.html	Use this template to generate statistical and graphical reports which do not organize data into groups.

3. Using an HTML editor, edit the following elements of the templates:

Table 60: HTML template: Editable sections

Section	Description
Report logo	Replace GFI EventsManager logo with a logo of your choice. Add more logos or completely remove them from your reports.
Labels and text	Rename and reposition labels according to your needs.
Placeholders	Although you are able to move placeholders around the report, renaming them will cause GFI Events-Manager reporting engine to fail to return the respective data.

Available placeholders include:

Table 61: HTML report template placeholders

Placeholder	Description
{title}	Title of report.
{subtitle}	Subtitle of report.
{description}	Description of report.
{creator}	User who generated report.
{currentDate}	Date when report is generated.
{sortBy}	Sort field.
{dateRange}	Report data is gathered from the specified time period.
{fullFilter}	List of Restrictions set for the Report.
{startGroupHeaderBlock}	Beginning of Header section of the repetitive block.
{headerLabel}	Name of grouping header.
{headerValue}	Value of grouping header.
{endGroupHeaderBlock}	Ending of Header section of the repetitive block.
{startRepeatBlock}	Beginning of the Body section of the repetitive block.
{tableHeaderCells}	The Header section of the table data.
{tableRows}	The Body section of the table data.
{tableTotal}	For charts. Contains the Sum or Count value of the computed field.
{chartTop}	Places the chart at the beginning of the report.
{chartBottom}	Places the chart at the end of the report.
{endRepeateBlock}	Ending of the Body section of the repetitive block.

4. Save the HTML template and generate a report using the new layout. For more information, refer to Generating reports (page 130).

Note

Using the same HTML/CSS structure of the HTML templates, you are also able to create your own customized templates. Copy the template, rename it and reuse the same placeholders.

8 Events Processing Rules

During events processing, GFI EventsManager runs a configurable set of rules against the collected logs in order to classify events and trigger alerts/actions accordingly. By default, GFI EventsManagerships with a pre-configured set of events processing rules that allow you to gain network-wide control over computer logs - with negligible configuration effort. You can also customize these default rules or create tailored ones for your organization's requirements.

Topics in this chapter:

8.1 About events processing rules

Events processing rules are checks/conditions which help you:

Table 62: Use of Events Processing Rules

Condition	Description
Classify processed events	Configure GFI EventsManager to classify processed events. By default, events are categorized into five main categories; however, more categories may be added according to your requirements.
Filter out noise (repeated events) or unwanted events	GFI EventsManager is able to filter out unwanted events. This helps you maintain only wanted events and ignore unwanted noise.
Trigger email, SMS and network alerts on key events	Configure automated actions to run when specific events are processed. For more information, refer to Configuring Alerting Options (page 187).
Attempt remedial actions by executing specific scripts and executable files on key events	Run executable files, commands and/or scripts upon detecting a specified event and/or number of events.
Filter events that match specific criteria	Example: Create and run a rule which filters out low severity or duplicate events.
Archive filtered events	Event archiving is based on the severity of the event and on the configuration settings of the event processing rules. Example: you can configure GFI EventsManager to archive only events that are classified as critical or high in severity and discard all the rest

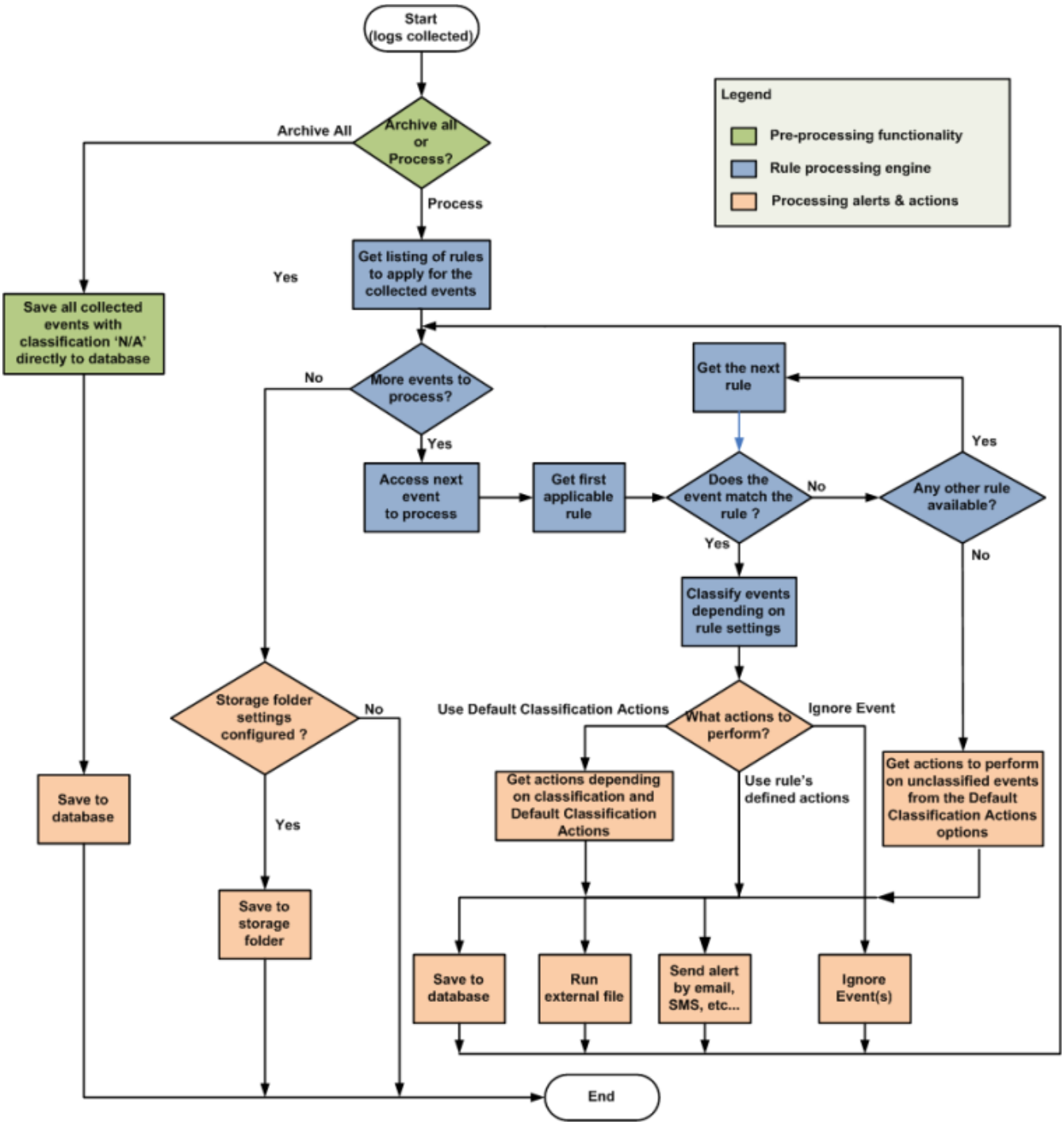
8.1.1 Event classification

Event classification is based on the configuration of the rules that are executed against the collected logs. Events that don't satisfy any event classification conditions are tagged as unclassified. Unclassified events may also be used to trigger the same alerts and actions available for classified events.

GFI EventsManager classifies events in the standard importance levels such as Critical, High, Medium, Low and Noise (unwanted or repeated log entries).

8.2 How events processing rules work

The flowchart chart below illustrates the event processing stages performed by GFI EventsManager.



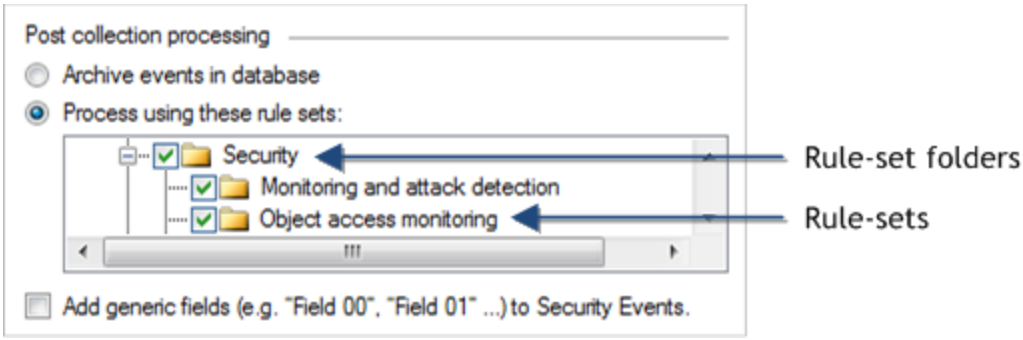
Screenshot 111: How Events Processing Rules work

8.3 Managing rules-set folders

This section contains information about:

8.3.1 About rules-set folders

In GFI EventsManager, event processing rules are organized into 'Rule-sets'; and every rule-set can contain one or more specialized rules which can be run against collected logs.



Screenshot 112: Rule-sets folder and Rule-sets

Rule-sets are further organized into Rule-set Folders. This way you can group rule-sets according to the functions and actions that the respective rules perform. By default, GFI EventsManager ships with pre-configured folders, rule-sets and event processing rules that can be further customized to suite your event processing requirements.

The table below lists some of the most common rule-set folders in GFI EventsManager:

Table 63: Common available rule-set folders

Rule-Set Folder	Description
Windows Events	Contains rules tailored for PCI Requirements, Security logs, System Health logs, noise reduction and more.
SQL Server Audits	Contains rules tailored for SQL Server Audit monitoring. Amongst others, these include: » Database changes » Server changes » Database access.
SNMP Traps	Contains rules tailored for SNMP Traps Messaging. Amongst others, these include: » Cisco IOS 12.1 » Cisco IOS 12.2 » Allied Telesis.
Oracle Audits	Contains rules tailored for Oracle Server Audit monitoring. Amongst others, these include: » Database changes » Server changes » Database access.
Syslog Messages	Contains rules tailored for the processing LINUX and UNIX system logs. Amongst others, these include: » Juniper network rules » IBM iSeries rules » LINUX\UNIX host rules.

Rule-Set Folder	Description
Text Logs	Contains rules tailored for the processing of web transfer protocols. Amongst others, these include: » HTTP rules » FTP rules » SMTP rules.

8.3.2 Adding a rule-set folder

To create a new rule-set folder:

1. Click **Configuration** tab and select **Event Processing Rules**.

2. From **Common Tasks**, select **Create folder**.

4. Specify a unique name for the new rule-set folder.

> **Note**
>
> To create sub rule-set folders, right-click on the parent folder and select **Create new folder…**

8.3.3 Renaming and Deleting a rule-set folder

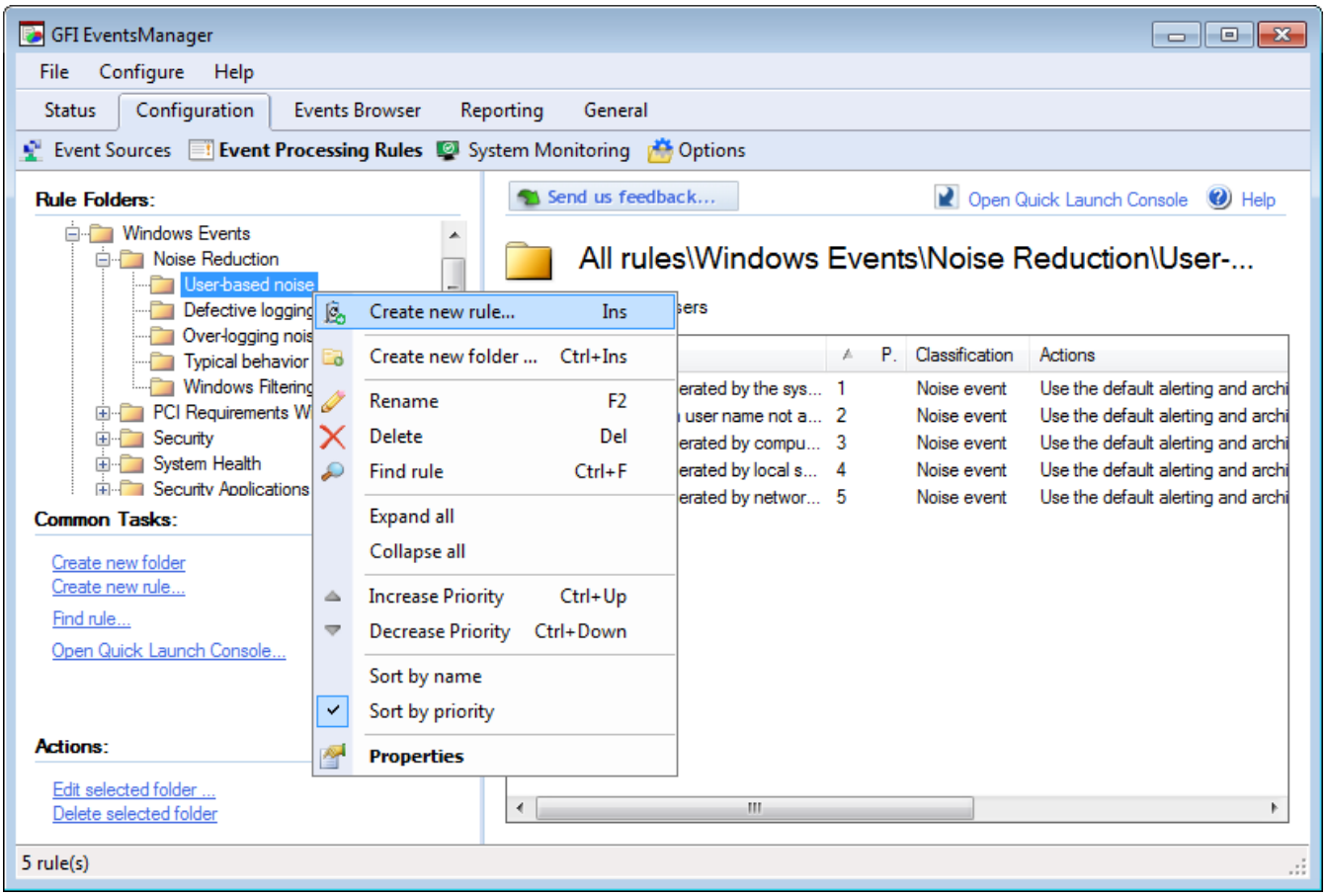
To rename or delete existing rule-set folders, right-click on the target rule-set folder and select **Rename** or **Delete** accordingly.

Deleting a rule-set folder will lead to the deletion of all the rules and rule-sets contained within the deleted folder.

8.4 Creating new events processing rules

To create a new event processing rule:

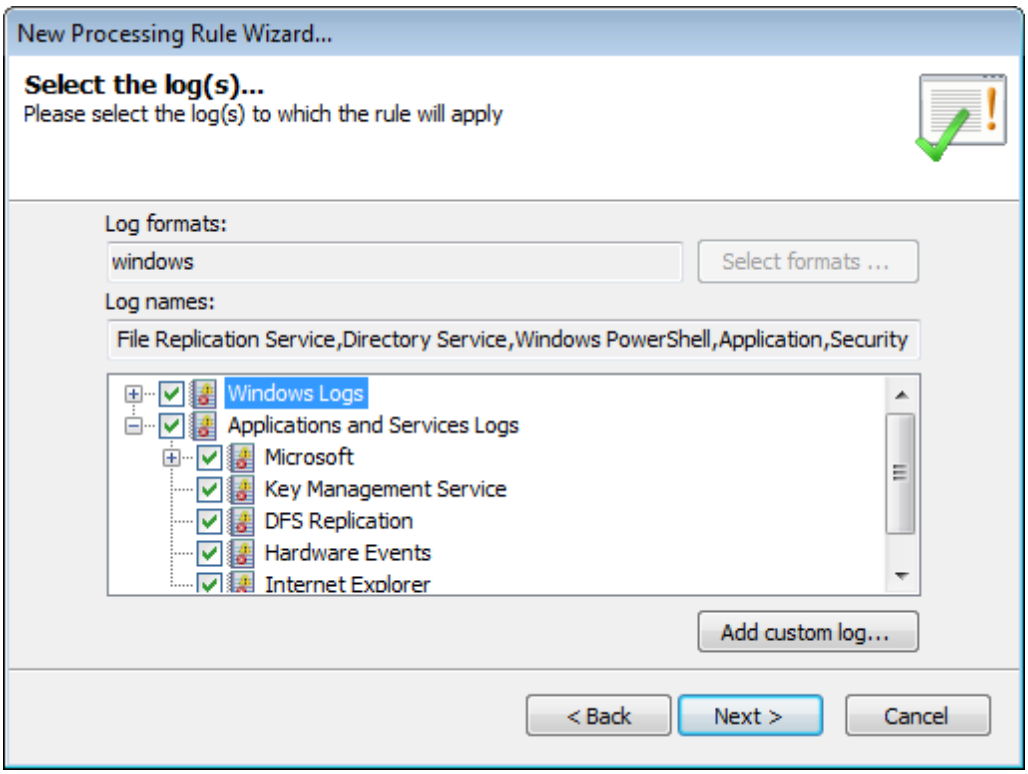
1. Click **Configuration** tab > **Event Processing Rules**.



Screenshot 113: Creating a new rule

2. Right-click the rule-set where the new rule will be created and click **Create new rule...**

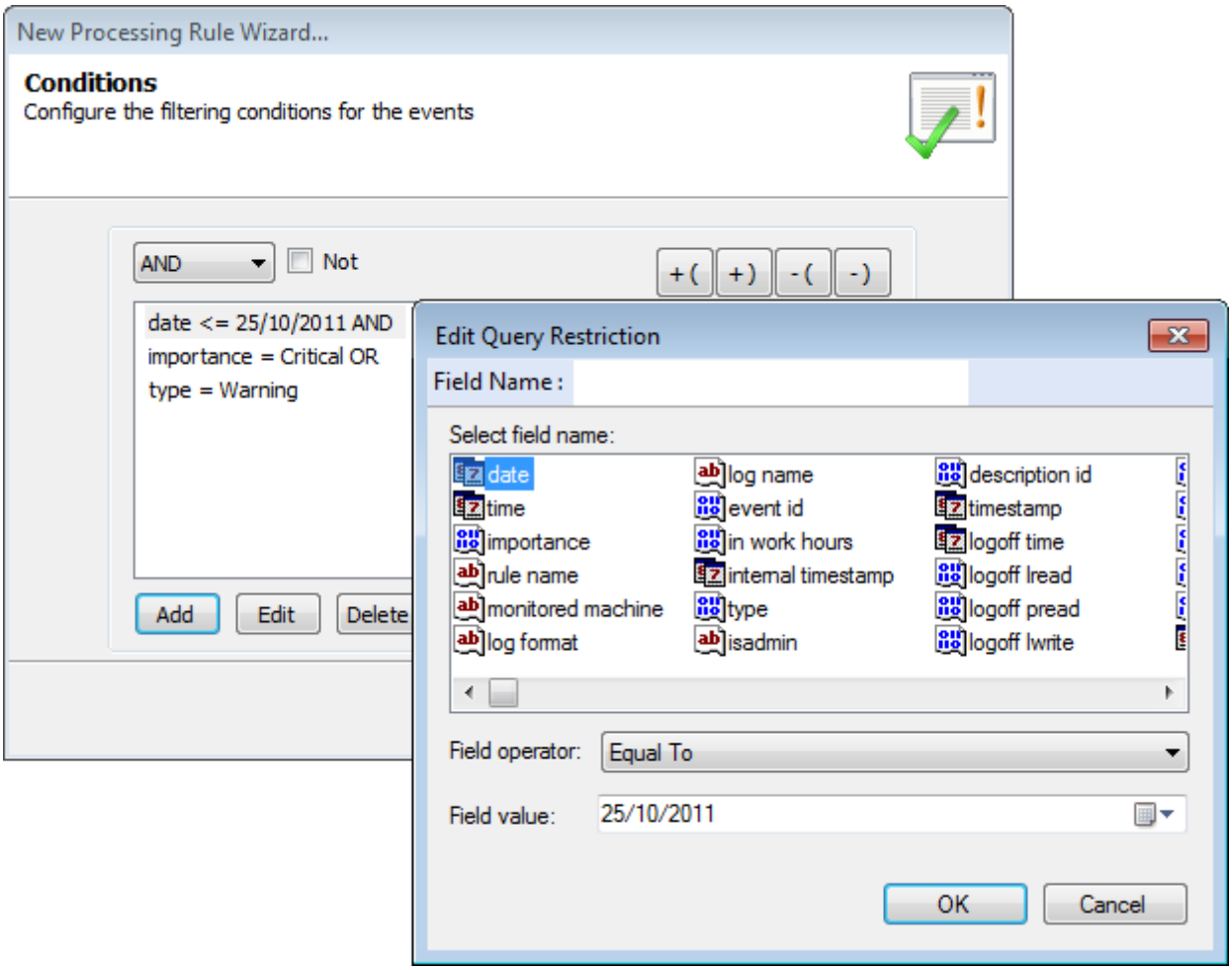
3. Specify the name and description (optional) for the new rule. Click **Next**.



Screenshot 114: Select the logs which the rule will be applied to

4. Select the event logs to which the rule applies and click **Next**. Optionally, click **Add custom log…** to insert an event log which you pre-configured. For more information, refer to Collecting custom logs (page 87).

> **Note**
>
> For SQL Audit, Oracle Audit, Syslogs, W3C logs and SNMP Traps messages, specify the full path of the object's log folder; example: "**C:\W3C\logs**".



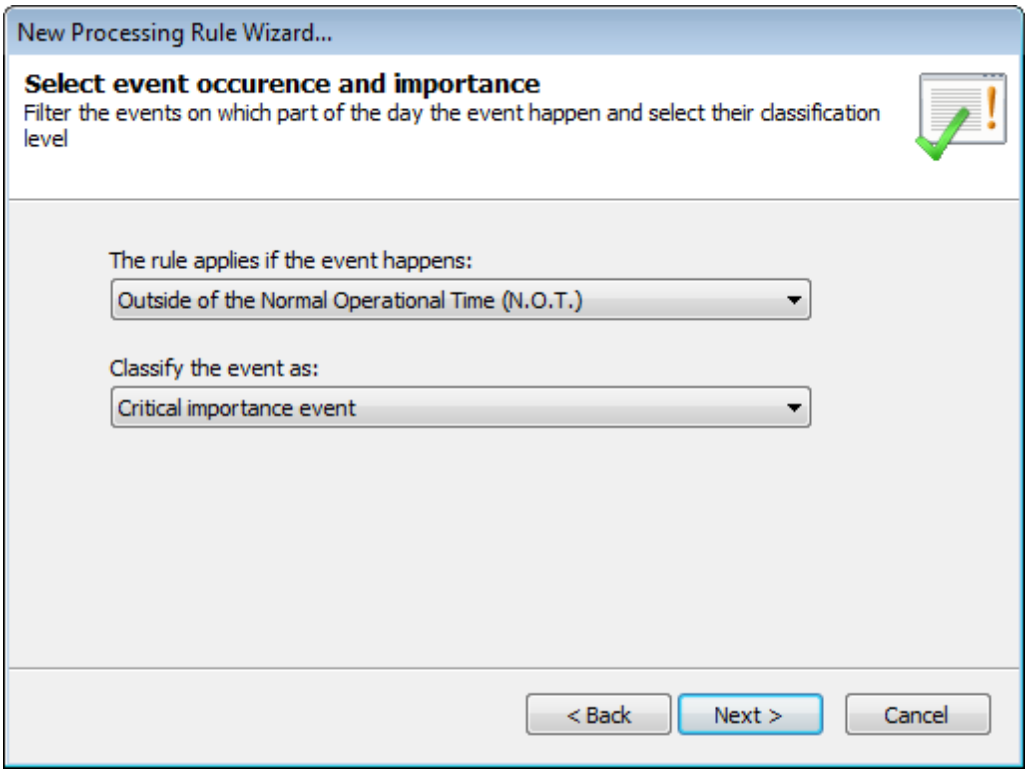
Screenshot 115: Configure the rule conditions

5. Click **Add** to select a field from the list of available fields. Specify the **Field Operator** and **Field Value** and click **OK**. Repeat this step until all filtering conditions are added. For more information, refer to Defining Restrictions. Click **Next**.

> **Note**
>
> To create a rule that applies to all events, do not specify conditions.

Note

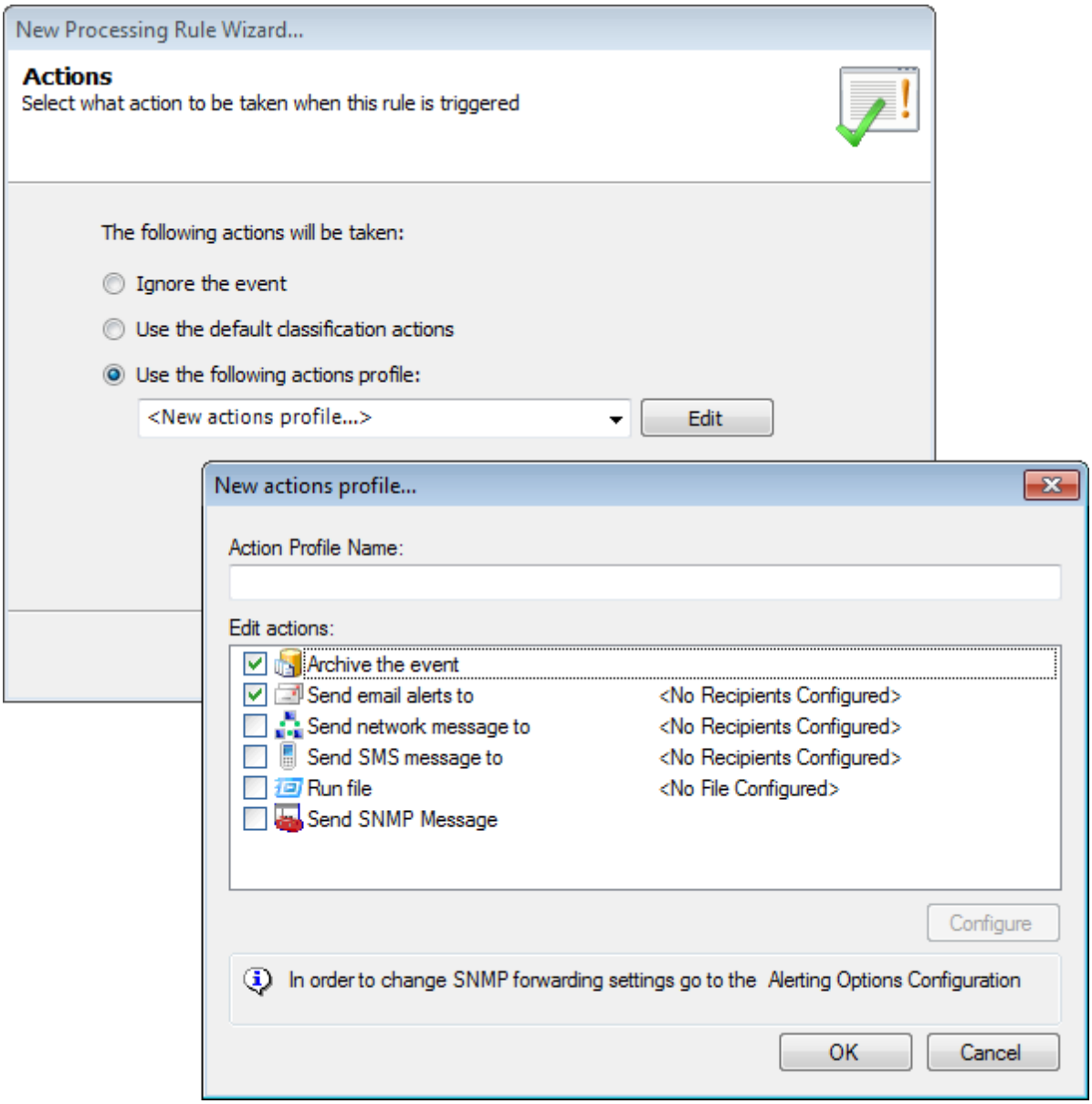
To filter events that refer to an administrator user (events having the security identifier SID that identifies a logon administrator session), ensure that if the event source is a domain member, the domain controller must also be added as an event source. For more information, refer to Creating a new event source group (page 45).



Screenshot 116: Select event occurrence and importance

6. Specify the time when the rule is applicable. Example: anytime, during working hours or outside working hours. Working and non-working hours are based on the operational time parameters configured for your event sources. For more information, refer to Configuring event source operational time (page 50).

7. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next**.



Screenshot 117: Select the triggered action

8. Specify which actions are triggered by this rule and click **Next**. Available actions are:

Table 64: Configuring new events processing rules: Actions

Action	Description
Ignore the event	Select this option so that GFI EventsManager will ignore the event and not trigger any actions or notifications.
Use the default classification actions	Select this option to use the pre-configured **Default Classification Actions**. For more information, refer to Configuring Default Classification Actions (page 185).
Use the following actions profile	Click **Edit** and select an action from the **New actions profile**.... Available actions include: » Archive the event » Send email alerts to » Send network message to » Send SMS message to » Run file » Send SNMP Message.

9. Click **Apply** and **OK**.

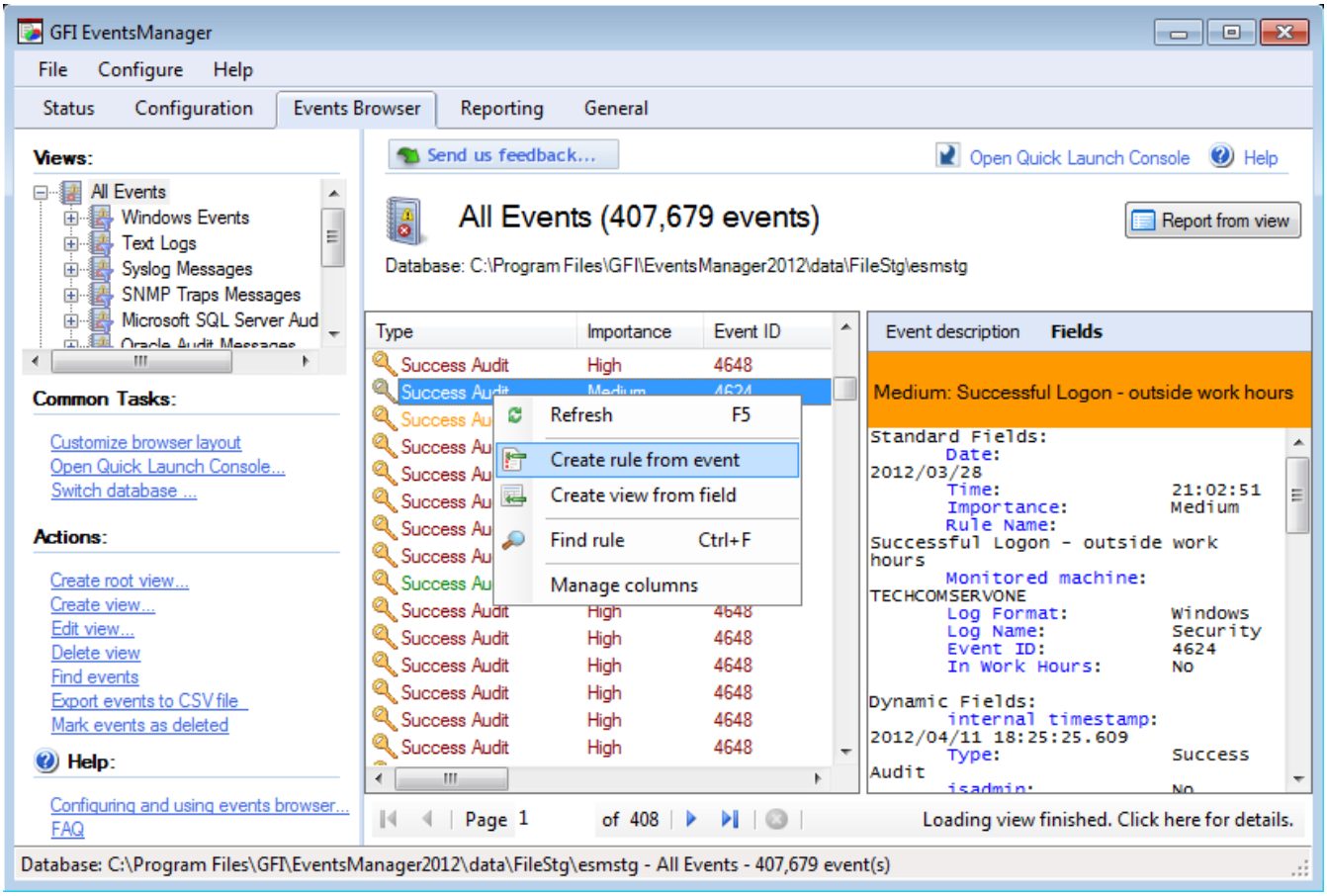
10. Assign the new rule(s) to your event sources. For information about how to collect event logs and process them using the specified events processing rules, refer to Collecting Event Logs.

8.5 Creating new rules from existing events

GFI EventsManager enables you to create new rules based on the information of existing events.

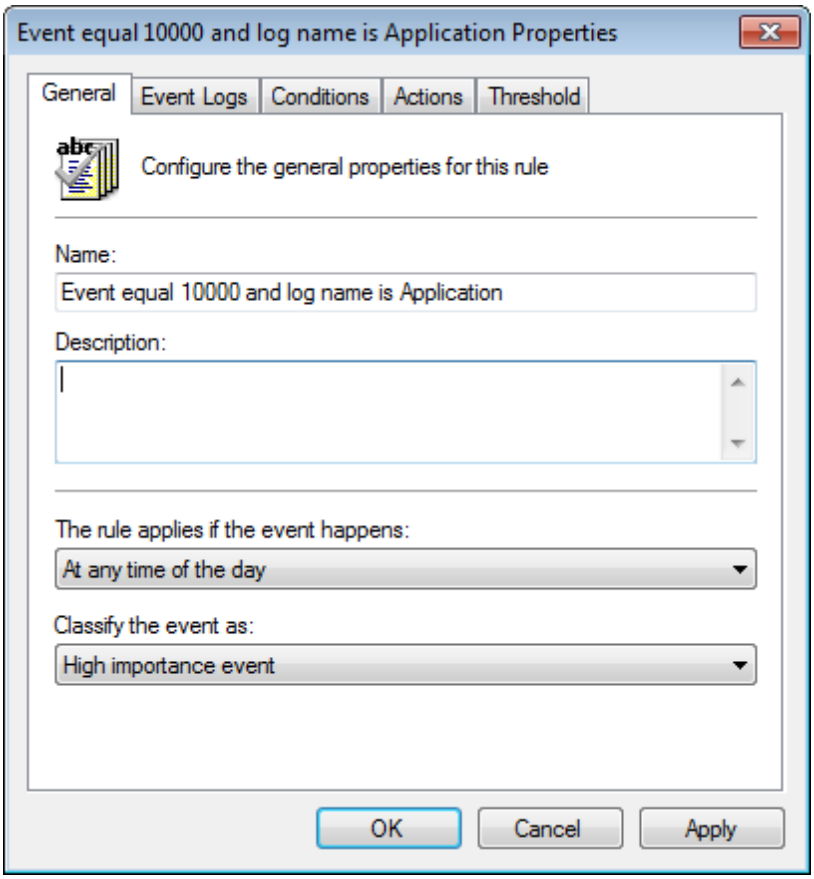
To create a new rule from an existing event:

1. From **Events Browser**, locate the event log that you want to base the rule upon.



Screenshot 118: Creating a rule from an existing event

2. Right-click the event and select **Create rule from event**.



Screenshot 119: New rule from event - General settings

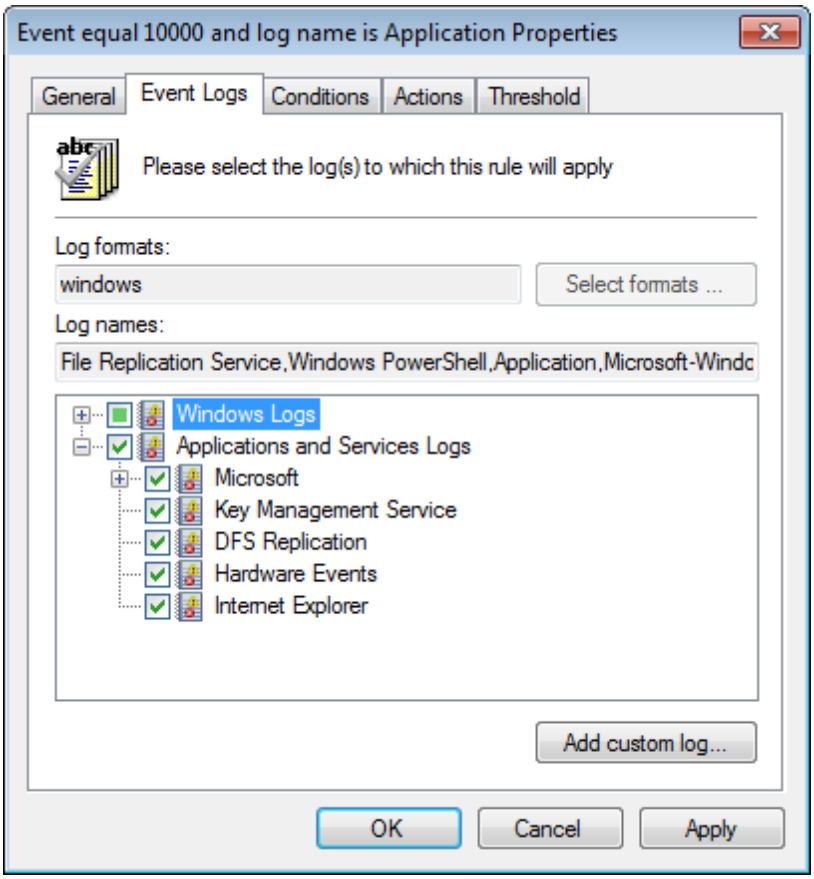
3. Specify a unique name and an optional description for the new rule.

4. From **The rule applies if the event happens** drop-down menu, select the time when the rule is applicable. Select from:

- At any time of the day
- During Normal Operational Time
- Outside the Normal Operational Time.

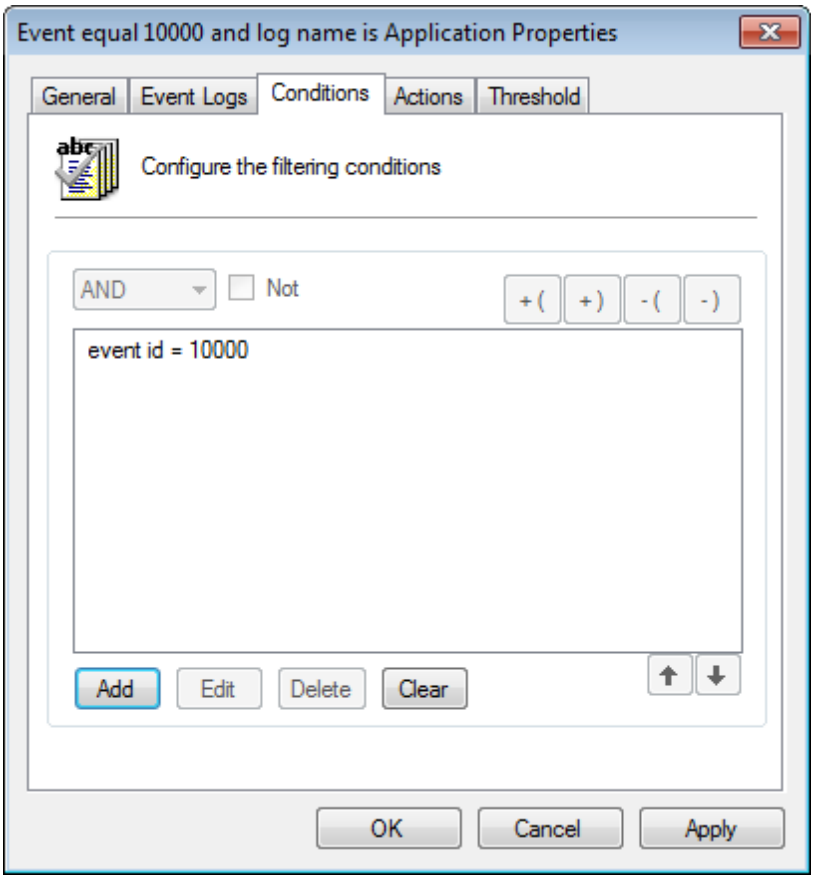
For more information, refer to Configuring event source operational time (page 50).

5. From the **Classify the event as** drop-down menu, select the classification level you want to assign to the event when it is generated.



Screenshot 120: New rule from event - Select logs to collect

6. From the **Event Logs** tab, select the logs you want to collect. To add custom logs, click **Add custom log...**, specify the custom log name and click **OK**.



Screenshot 121: New rule from event - Add conditions

7. From the **Conditions** tab, click **Add** to add conditions to the new rule. Leave blank to collect all the logs from the log types selected in the previous step. For more information, refer to Defining Restrictions.

8. Click **Actions** tab and select what action is taken when the rule is triggered. Available options are described below:

Table 65: Available event processing rule actions

Option	Description
Ignore the event	Ignores the event until a new instance of the event is generated.
Use the default classification actions	Use the actions configured in Default Classification Actions. For more information, refer to Configuring Default Classification Actions (page 185).
Use the following actions profile	From the drop-down menu, select a profile or <New action profile...> and click **Edit** to configure the action profile.

9. Click **Threshold** tab and configure the event threshold value. I.e. the number of times that an event must be detected prior to triggering alerts and remedial actions. This helps reducing false positives triggered by noise (repeated events) in your event logs.

10. Click **Apply** and **OK**.

8.6 Advanced event filtering parameters

GFI EventsManager allows systems administrators to set up advanced event filtering parameters. These options are available only for Windows Events and Syslogs.

This section contains information about:

- Windows event filtering parameters
- Syslog filtering parameters

8.6.1 Windows event filtering parameters

The **Event IDs:** field allows systems administrators to setup parameters described in the table below:

Table 66: Windows event filtering parameters: Event ID field

Parameter	Description
Single events	Event IDs: 575
List of events	Event IDs: 550, 570
Range of events	Event IDs: 575-600
Combination of events	Event IDs: 550, 570, 575-600

The **Source**, **Category** and **User fields** allow systems administrators to setup parameters described in the table below:

Table 67: Windows event filtering parameters: Source, Category and User fields

Parameter	Description
Single source name	Message: session opened

Parameter	Description
List of sources	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

8.6.2 Syslog filtering parameters

The **Message** and **Process** fields allow systems administrators to setup parameters described in the table below:

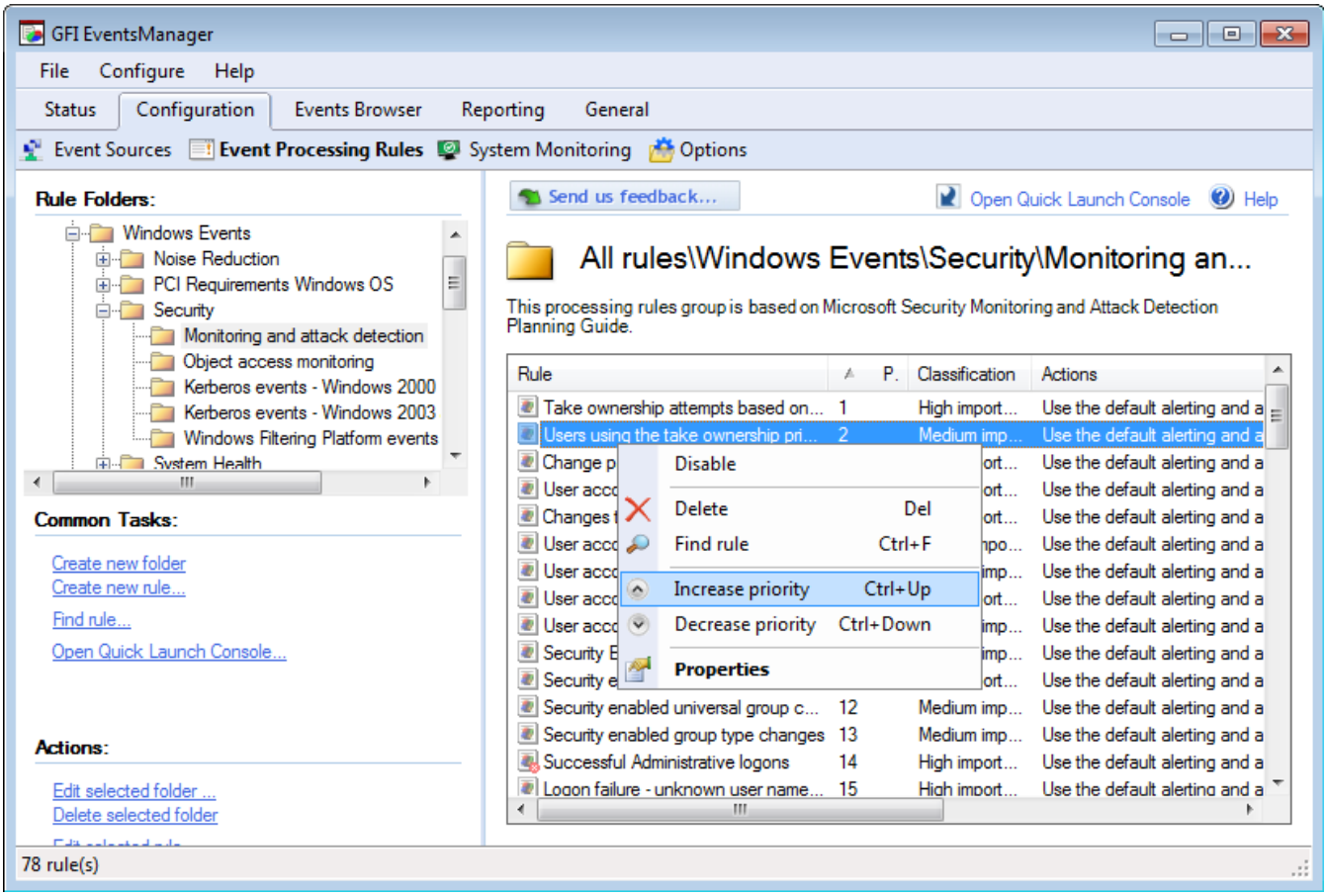
Table 68: Syslog filtering parameters: Message and Process fields

Parameters	Description
Single message	Message: session opened
List of messages	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

8.7 Prioritizing events processing rules

Events Processing Rules are executed in order of priority. To change the order of execution:

1. From **Configuration** tab > **Events Processing Rules** > **Rule Folders**, expand a rule-set folder.



2. From the right pane, right-click a rule and select **Increase priority** or **Decrease priority** accordingly. Alternatively, select a rule and press **Ctrl+Up** to increase or **Ctrl+Down** to decrease priority.

9 System Monitoring Checks

This chapter provides information about managing and using system monitoring checks. Monitoring checks scan your network for failures or irregularities. This is done automatically so that you can identify issues and proactively fix unexpected problems before they happen.

Topics in this chapter:

9.1 About system monitoring checks

Event logs are useful to track different operational aspects of devices, computers and servers, but in many cases users need more than logs to granularly inspect this activity. System monitoring checks help you monitor system activity network-wide. GFI EventsManager ships with a set of predefined checks, specifically designed to cater for Windows operating systems, Linux/Unix operating systems, SNMP devices and Network/Internet protocols and services.

System monitoring checks, generate events. You can create events processing rules, based on the generated event(s). For more information, refer to Creating new rules from existing events (page 152). By doing so, you can configure GFI EventsManager to trigger email, SMS or network alerts and also execute scripts to take remedial actions on the issues detected by the monitoring checks. For more information refer to Creating new events processing rules and Configuring Default Classification Actions.

9.2 Managing system monitoring checks

This section contains information about:

- Creating a new root folder
- Adding a sub-folder to a root folder
- Editing system monitoring checks parameters
- Deleting folders and monitoring checks

9.2.1 Creating a new root folder

To create a new root folder:

1. From **Configuration** tab > **System Monitoring** > **Common Tasks**, click **New root folder**.
2. Key in a name for the new root folder and an optional description.
3. Click **OK**.

9.2.2 Adding a sub-folder to a root folder

To add a new sub-folder:

1. From **Configuration** tab > **System Monitoring** > **Monitors**, right-click the root folder/folder that is going to contain the new folder and click **Add folder**.
2. Key in a name for the new folder and an optional description.
3. Click **OK**.

9.2.3 Editing system monitoring checks parameters

To edit monitoring checks parameters:

1. From **Configuration** tab > **System Monitoring** > **Monitors**, right-click the check you want to edit and select **Properties**.

2. Edit the required parameters from the **General**, **Custom properties** and **Action events** tabs and click **OK**.

9.2.4 Deleting folders and monitoring checks

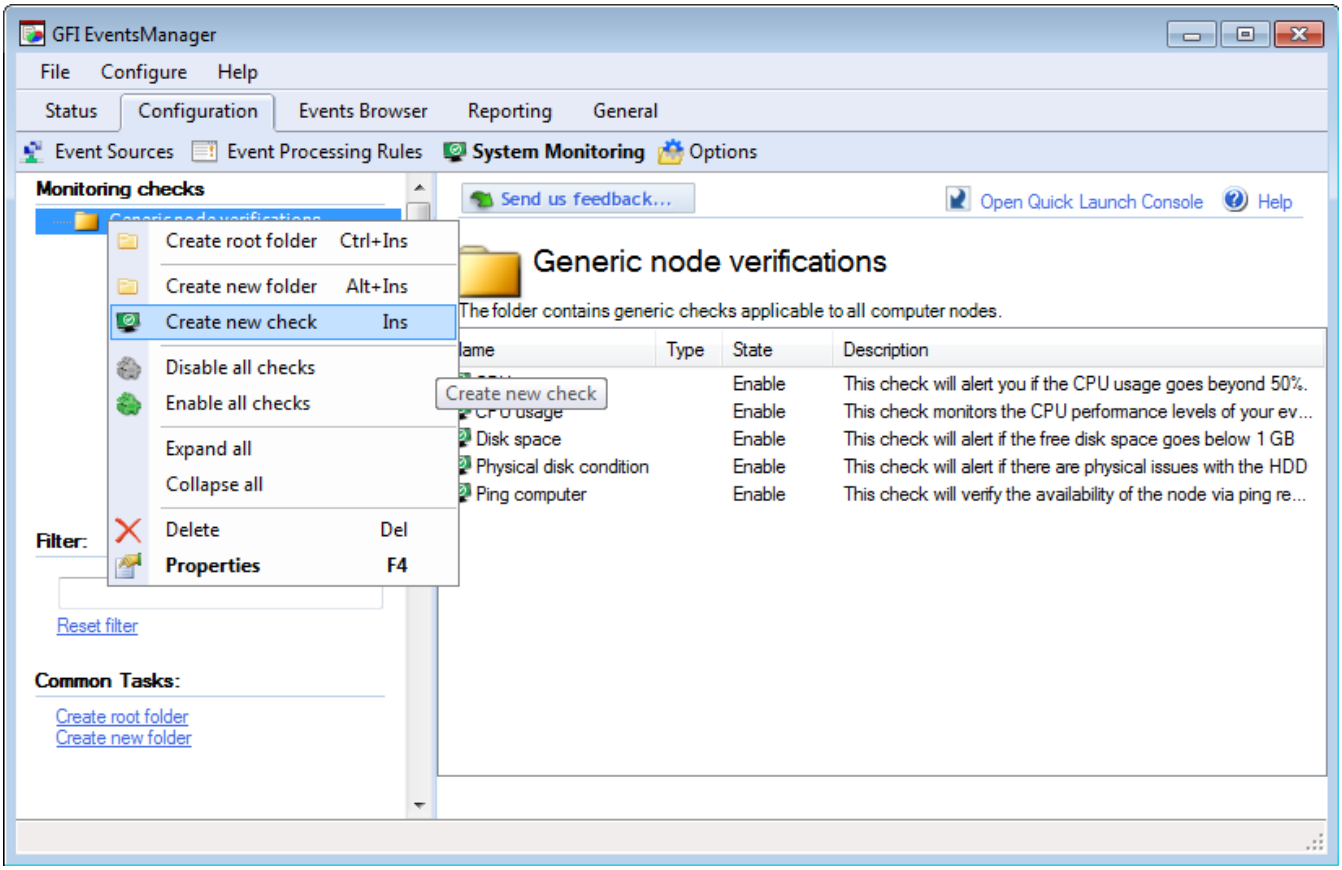
To delete a folder/monitoring check:

1. From **Configuration** tab > **System Monitoring** > **Monitors**, right-click the folder/check you want to edit and select **Delete**.

> **Important**
>
> Deleting a root folder (top-level folder), deletes all the contents as well. Make sure that you delete unwanted items only.

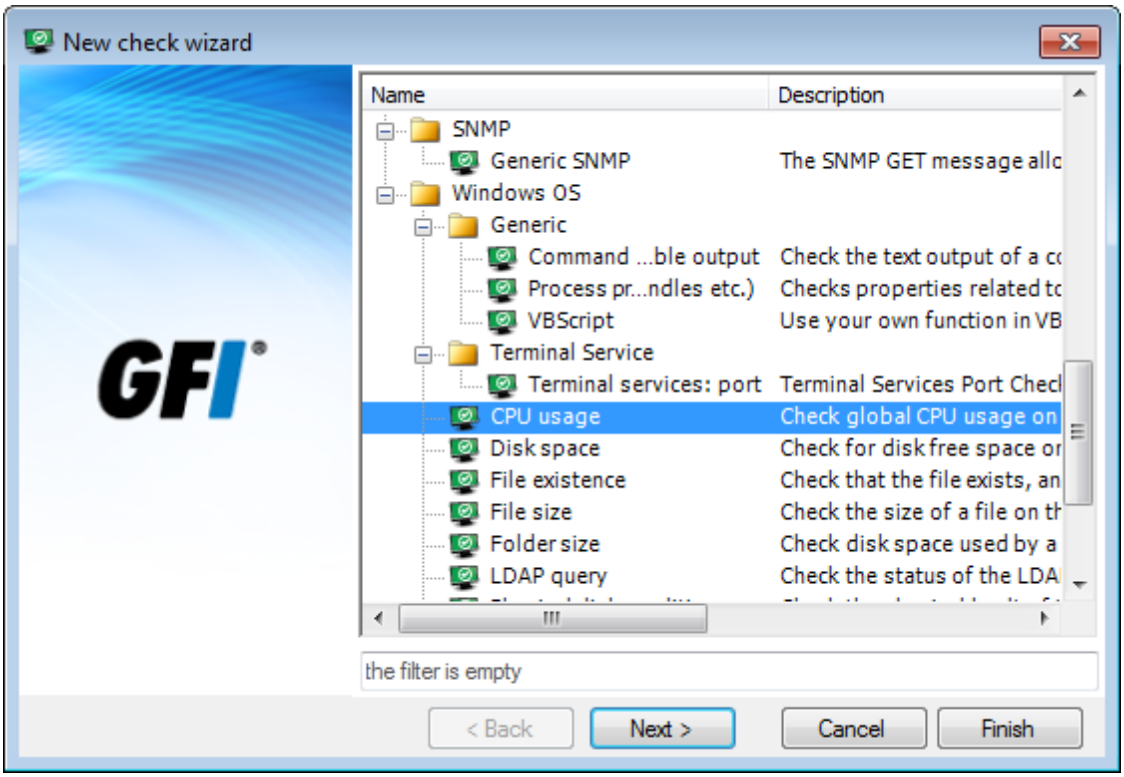
9.3 Creating a new monitoring check

To create a new system monitoring check:



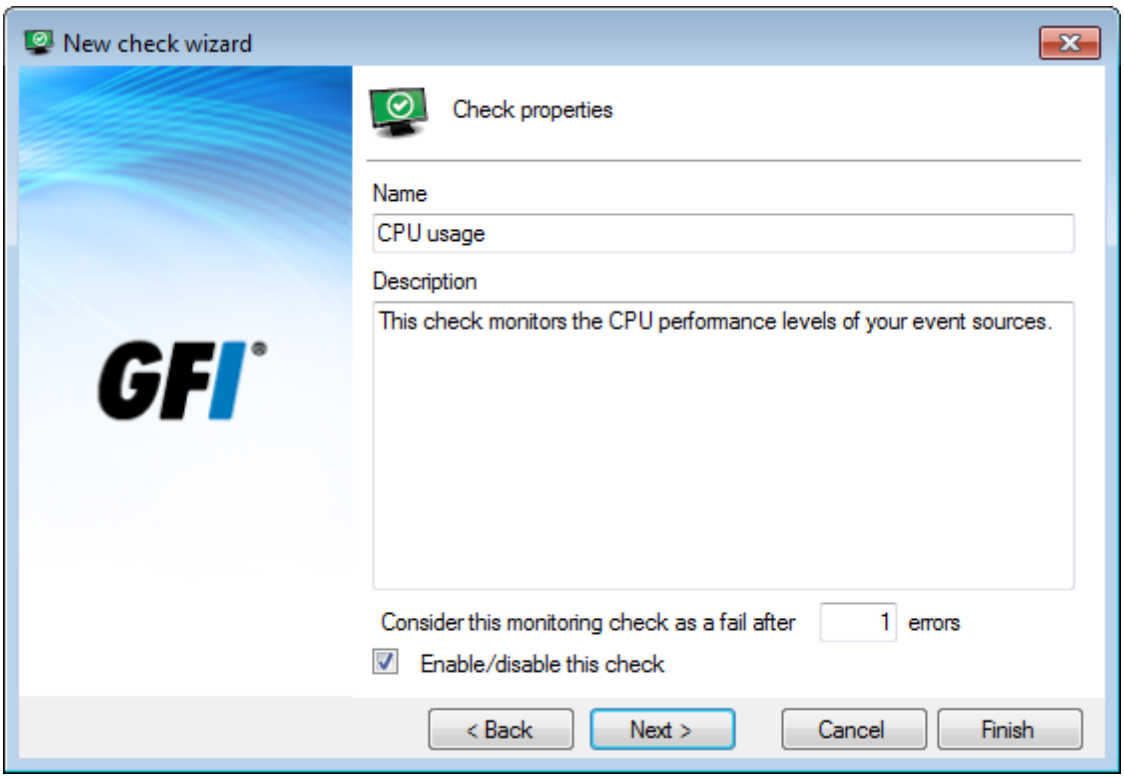
Screenshot 122: Creating a new system monitoring check

1. From **Configuration** tab > **System Monitoring** > **Actions**, click **Create new check**. Alternatively, right-click the folder where you want to add a check and select **Create new check**.



Screenshot 123: New monitoring check - Select check type

2. Select the type of check you want to create and click **Next**. For this example, the **CPU usage** monitoring check is selected.

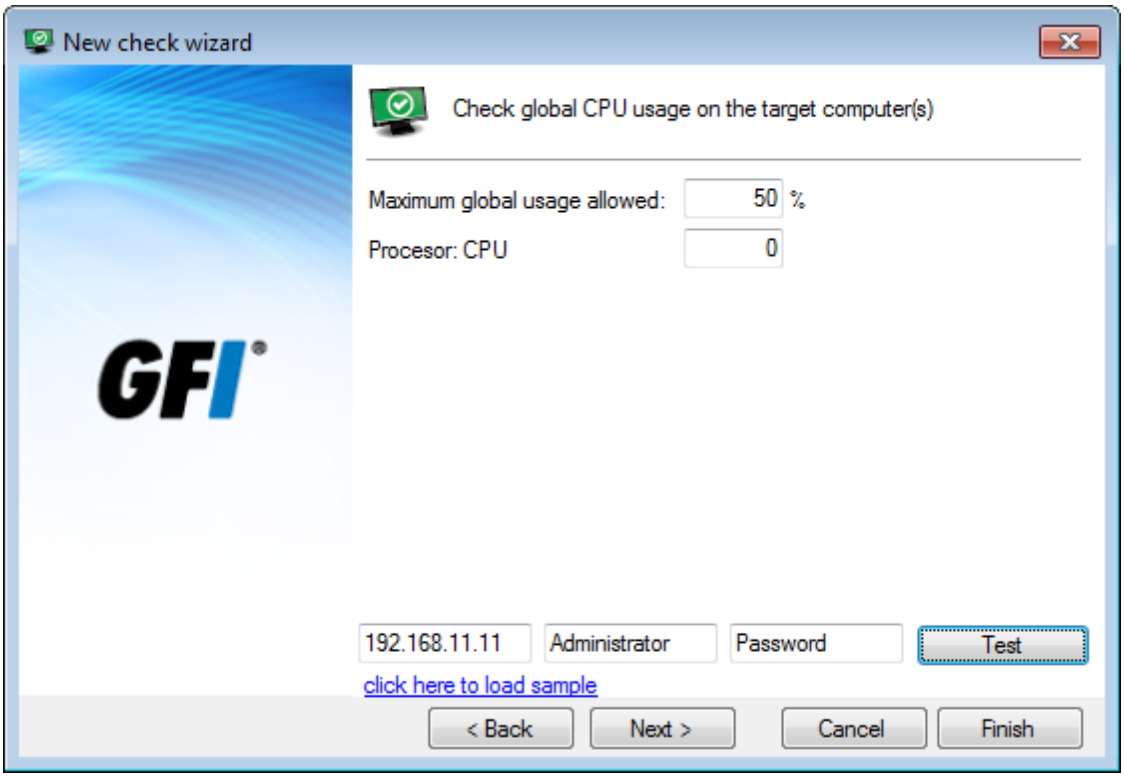


Screenshot 124: New monitoring check - Configure general properties

3. Specify a unique name and an optional description for the new monitoring check.

4. Specify the number of errors that have to occur before the check is considered as failed. Key in the number in the **Consider this monitoring check as a fail after {X} errors** text box.

5. Select/unselect **Enable/disable this check** to turn on/off the monitoring check. Click **Next**.



Screenshot 125: New monitoring check - Configure check conditions

4. Configure the monitoring check conditions. For the CPU Usage check, configure the **Maximum global usage allowed** and the **Processor: CPU** that has to be monitored. This step is different for each monitoring check selected in step 1.

5. (Optional) Specify alternative logon credentials and click **Test** to test the supplied details. To load a sample, click **Click here to load a sample**. Click **Next**.

Screenshot 126: New monitoring check - Configure action events

6. Configure the actions to execute when the events generate. Available options described below:

Table 69: Monitoring checks - Action events

Options	Description
Generate an audit event from this machine/device when the check	Select when an event log is generated upon completion of the check. Select from: » **Fails and succeeds** - An event log is generated whether the check fails or succeeds (recommended so that events processing rules can be created for each result) » **Fails** - An event log is generated only when the check fails » **Succeeds** - An event log is generated only when the check succeeds.
Only once after the failure	Generates an audit once after the monitoring check fails.
Once every {X} minutes as long as the check continues failing	Specify the time interval at which the event log is generated when a monitoring check repeatedly fails. Select this option to avoid generating noise (duplicate/unwanted) events.
When the check recovers from a failed state, generate an audit event from this machine/device	Generate an event log when the check succeeds after a number of fails.
Failed severity	Select the classification level of the generated event when the monitoring check fails.
Success severity	Select the classification level of the generated event when the monitoring check succeeds.

7. Click **Finish**.

> **Note**
>
> When the check is created, you can assign it to your event sources. For more information, refer to Configuring event source monitoring (page 51).

10 Users, Groups and Console Security

This chapter provides you with information related to creating and managing users and groups. Through the Users and Groups node, users and groups can be created and specific alerts, working hours and other properties can be assigned to each user and group; while different console access rights can be assigned to each user from the Console Security and Audit Options node.

Topics in this chapter:

10.1 Configuring the administrator account

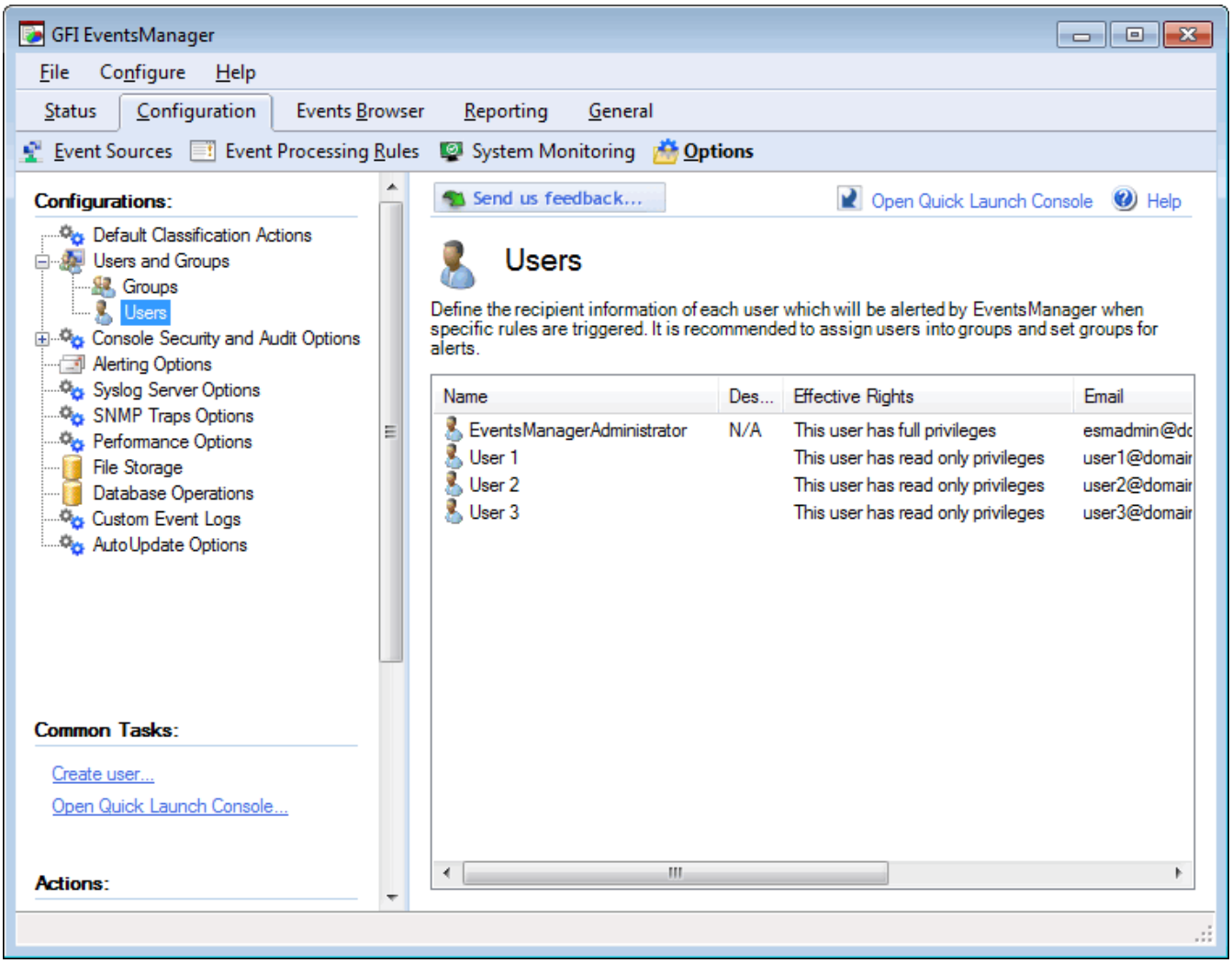
GFI EventsManager automatically creates an **EventsManagerAdministrator** account. However, you must still configure some properties such as the notification addresses and account security.

Note

GFI EventsManager requires a valid administrator email address in order to distribute automatic alerts when particular events are discovered.

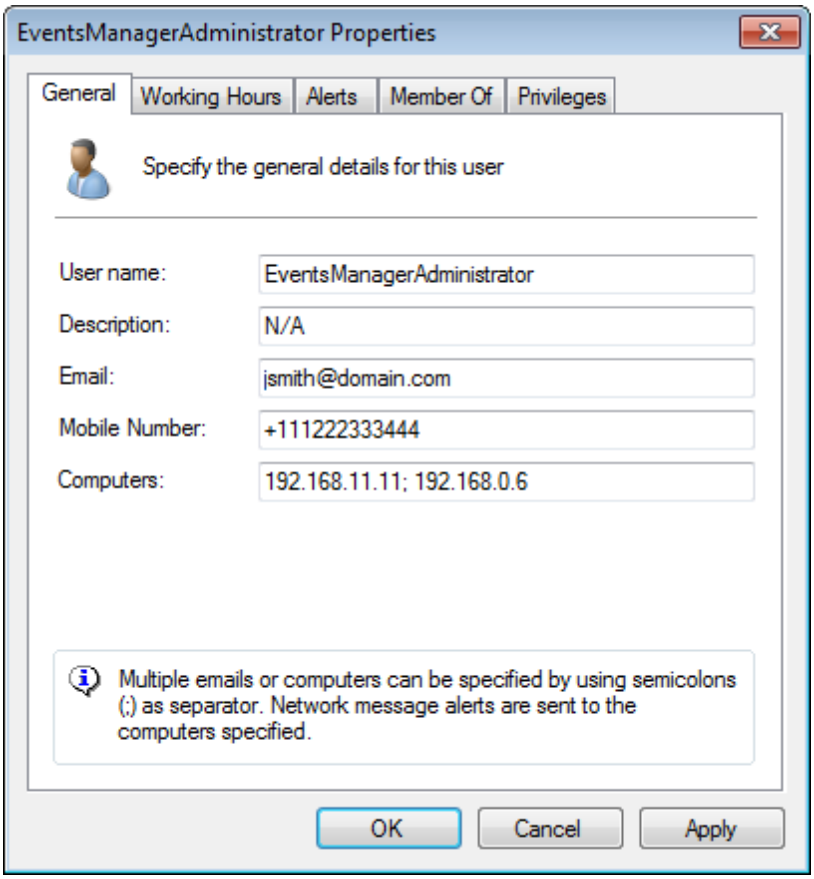
To configure the GFI EventsManagerAdministrator account:

1. From **Configuration** tab **>** **Options**, expand **Users and Groups > Users**.



Screenshot 127: Configuring EventsManagerAdministrator account

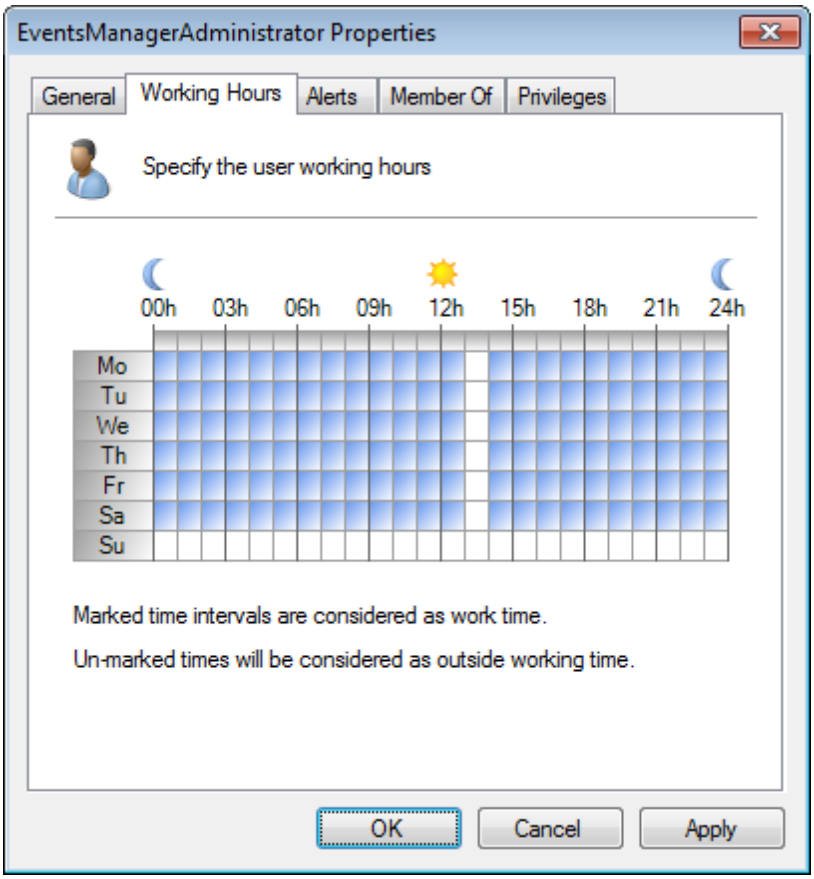
2. From the right pane, right-click **EventsManagerAdministrator** and click **Properties.**



Screenshot 128: EventsManagerAdministrator properties

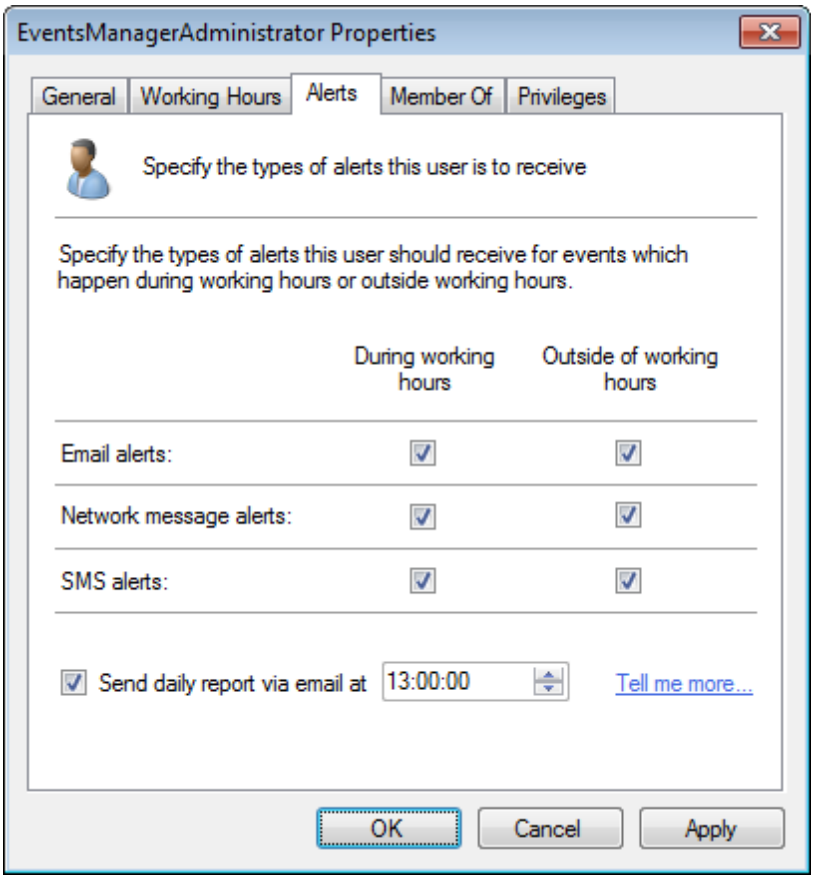
3. From the **General** tab specify:

- A username for GFI EventsManager administrator account
- (Optional) A description for the account
- A valid email address for email alerts distribution
- A valid mobile number for SMS alerts distribution
- Valid computer names/IPs for network alerts distribution.



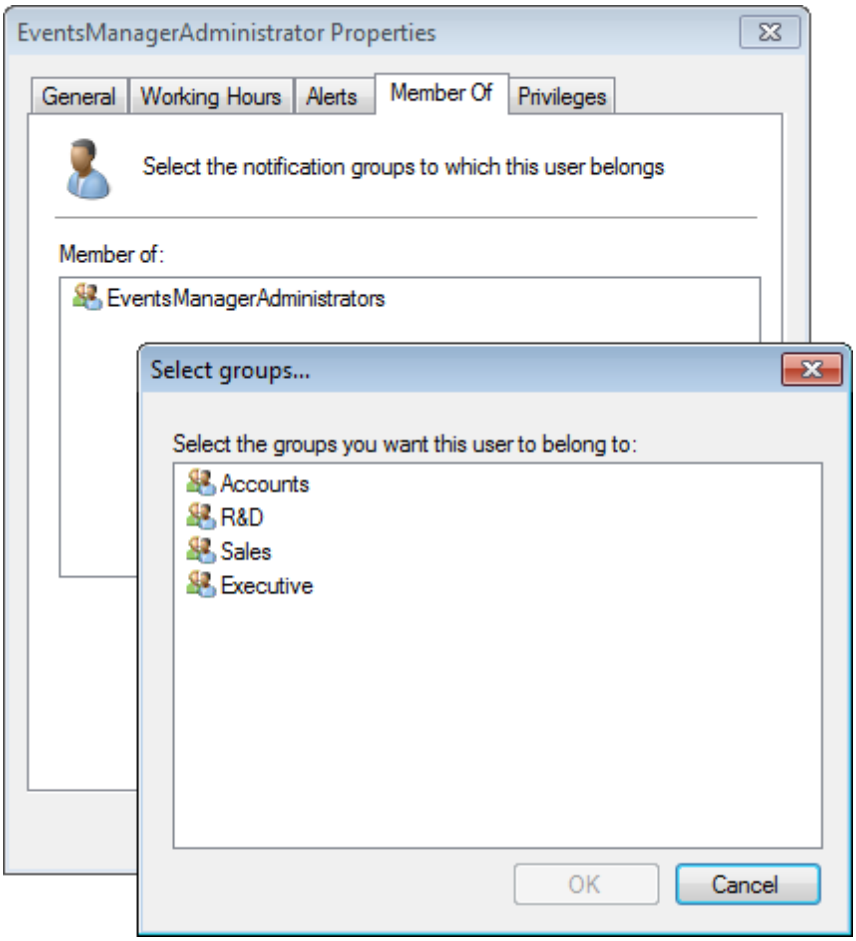
Screenshot 129: Configuring user typical working hours

4. Click **Working Hours** tab and specify the typical working hours of the administrator. Marked time intervals are considered as working hours.



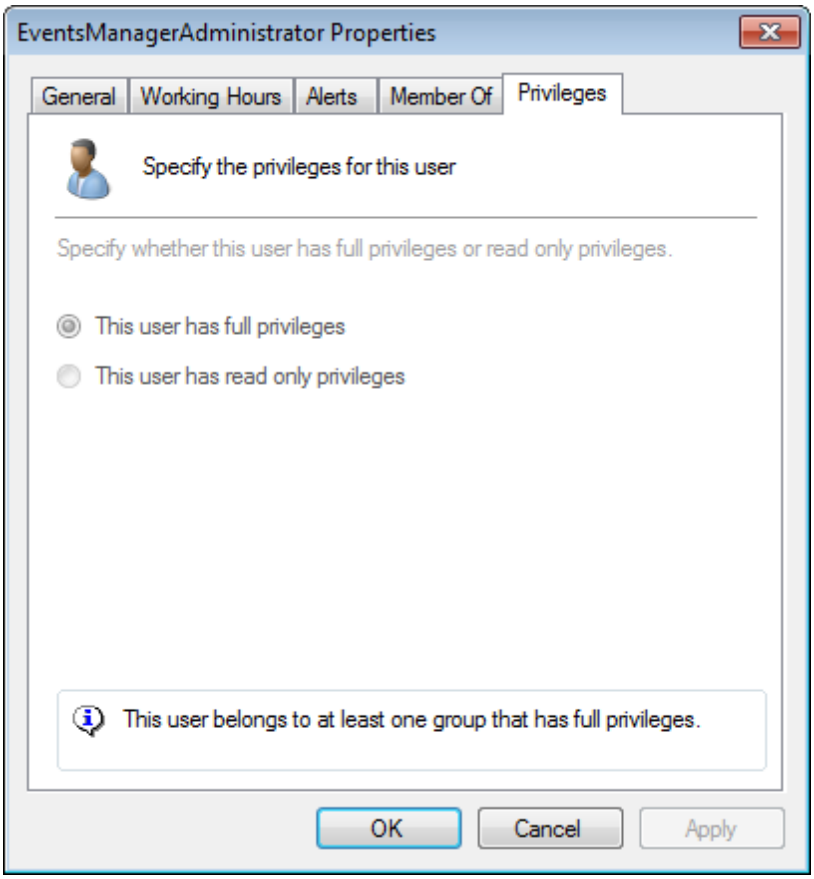
Screenshot 130: Configure alerts outside working hours

5. Click **Alerts** tab and select the alerts sent during and outside working hours. Optionally, select **Send daily report via email at** and specify the time to send an email containing daily activity.



Screenshot 131: Select the group which the user account is a member of

6. Click **Member Of** tab and select the notification groups to which the user belongs. By default the administrator is a member of the **EventsManagerAdministrators** notification group.



Screenshot 132: Configuring user account privileges

7. Click **Privileges** tab to edit the user privileges. By default the EventsManagerAdministrator account has full privileges and cannot be modified.

8. Click **Apply** and **OK**.

10.2 Managing user accounts

GFI EventsManager allows you to create a custom list of users which you can organize into groups to speed up administrative tasks.

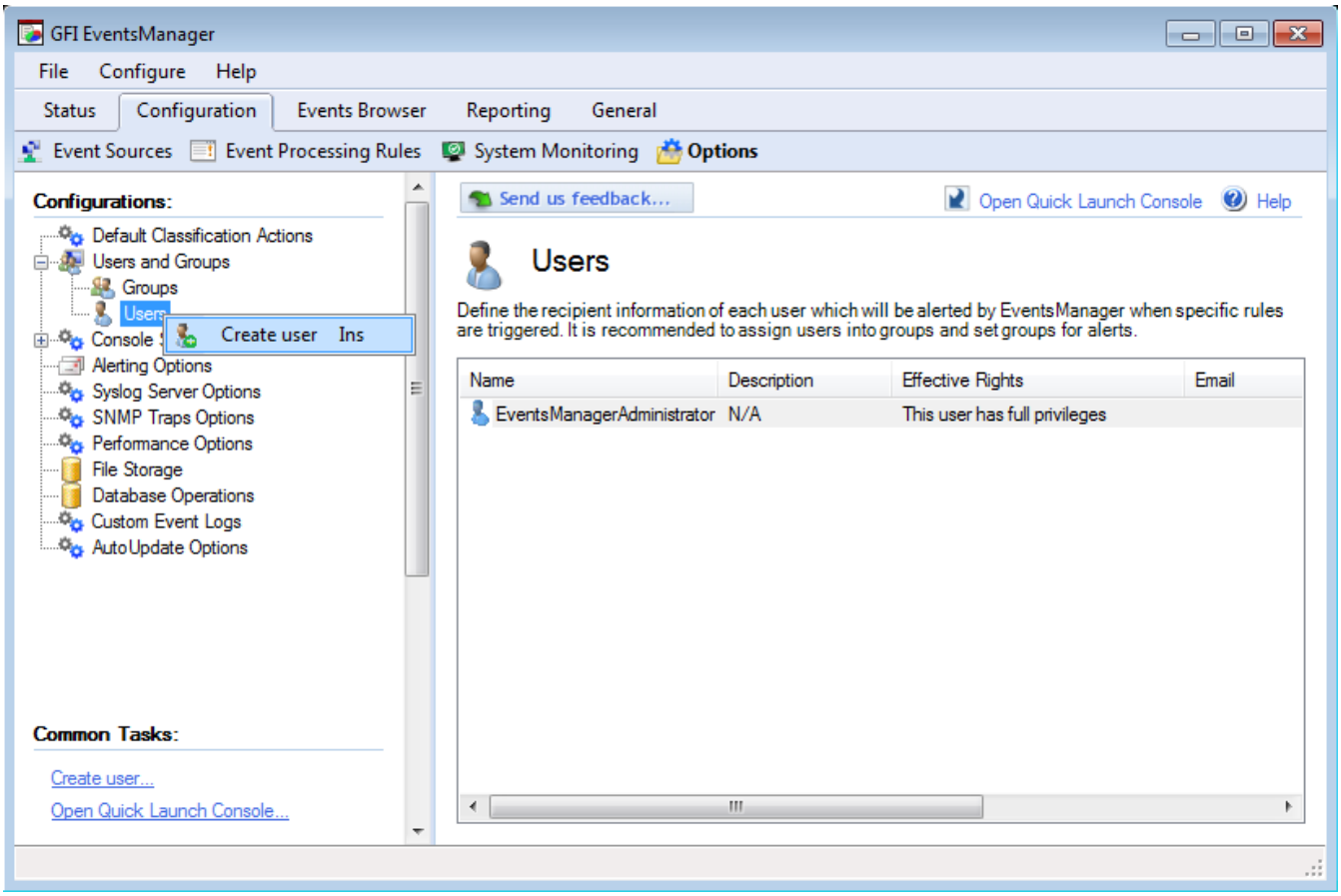
This section contains information about:

- Creating a new user account
- Changing user account properties
- Deleting a user account

10.2.1 Creating a new user account

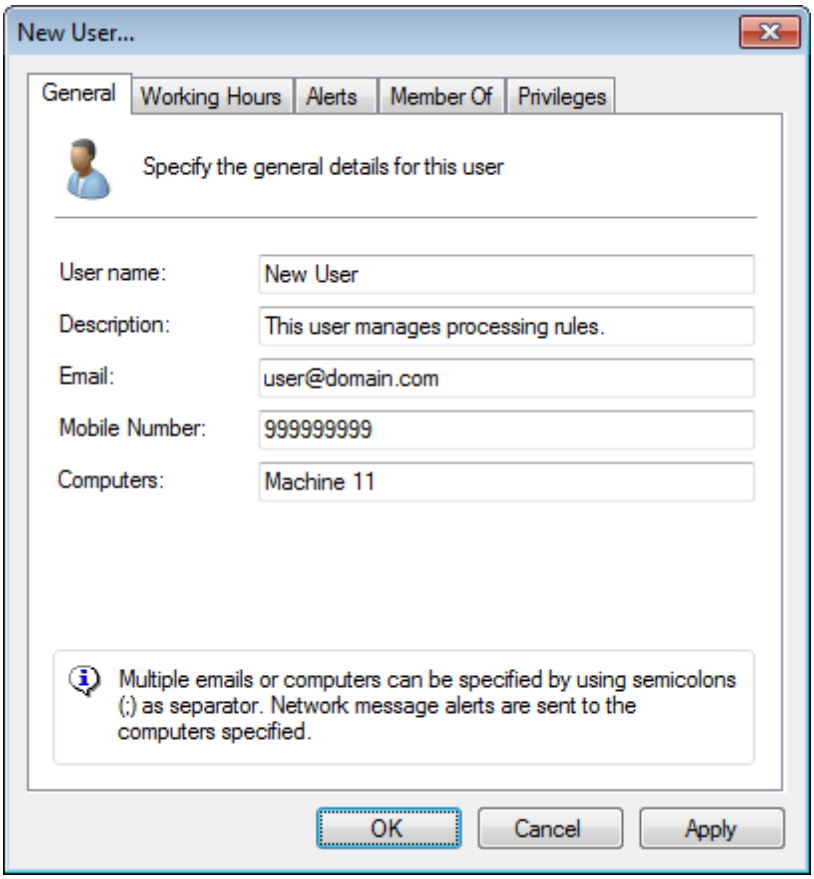
To create a new user:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node.



Screenshot 133: Creating a new user

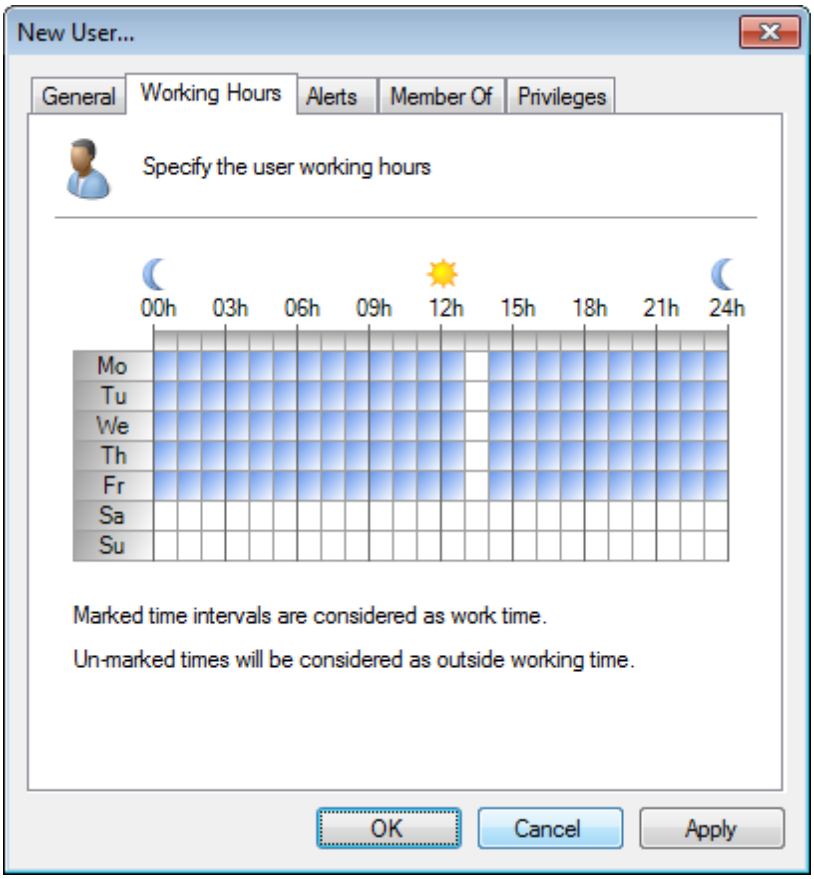
2. Right-click **Users** sub-node and select **Create user…**



Screenshot 134: Creating a new user - General properties

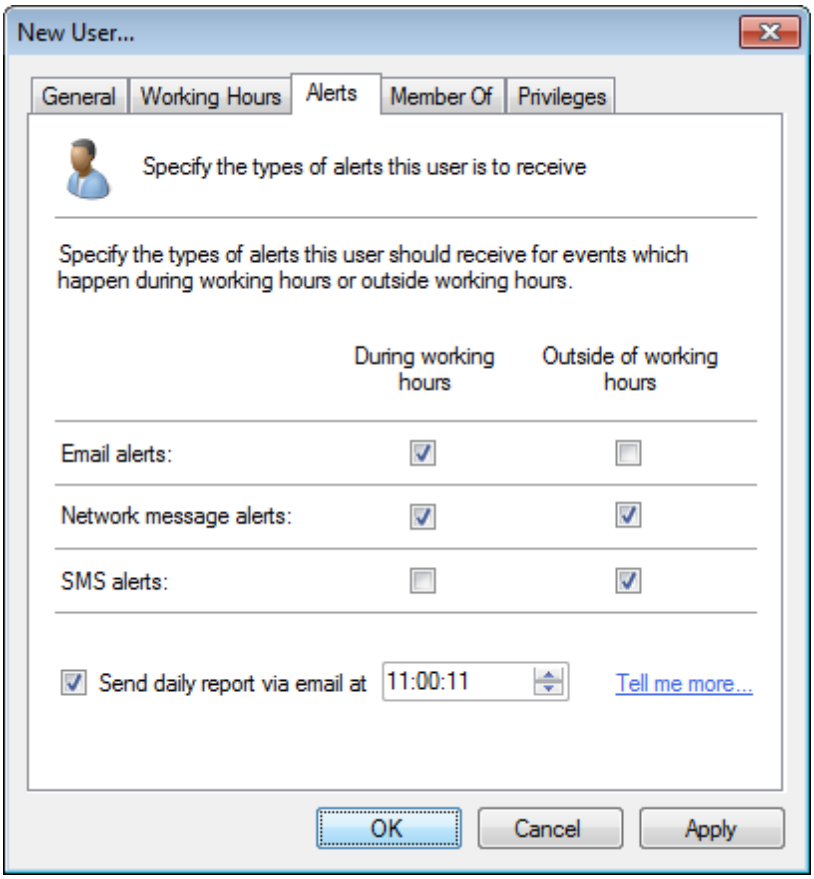
3. From the **General** tab specify:

- A username for the user account
- (Optional) A description for the account
- A valid email address for email alerts distribution
- A valid mobile number for SMS alerts distribution
- Valid computer names/IPs for network alerts distribution.



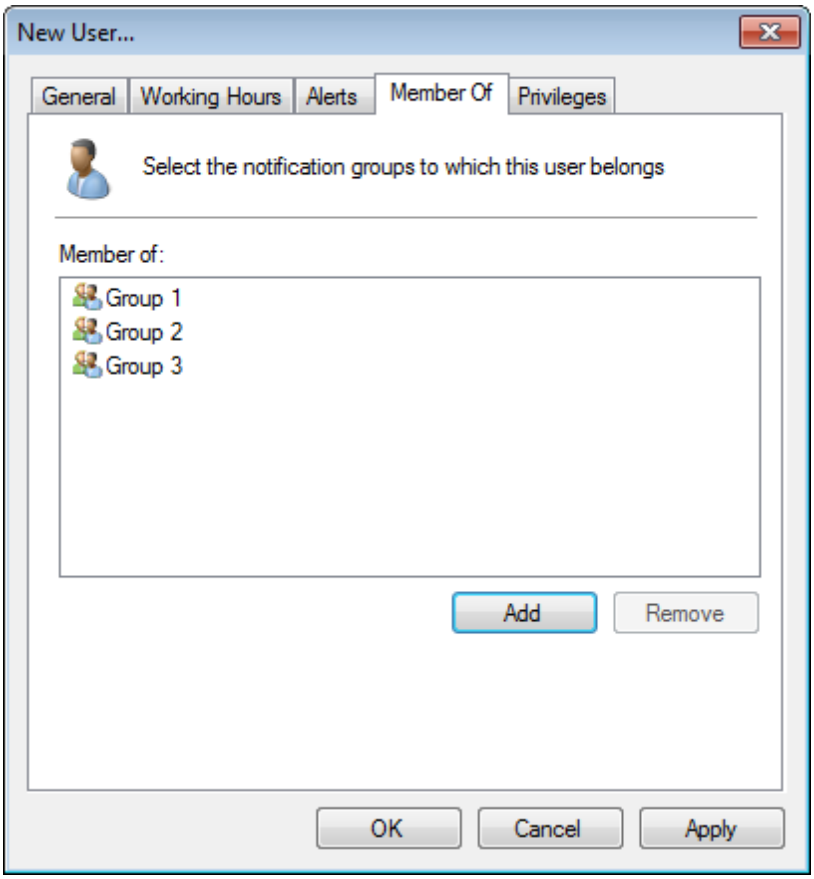
Screenshot 135: Creating a new user - Working hours

4. Click **Working Hours** tab and specify the typical working hours of the new user. Marked time intervals are considered as working hours.



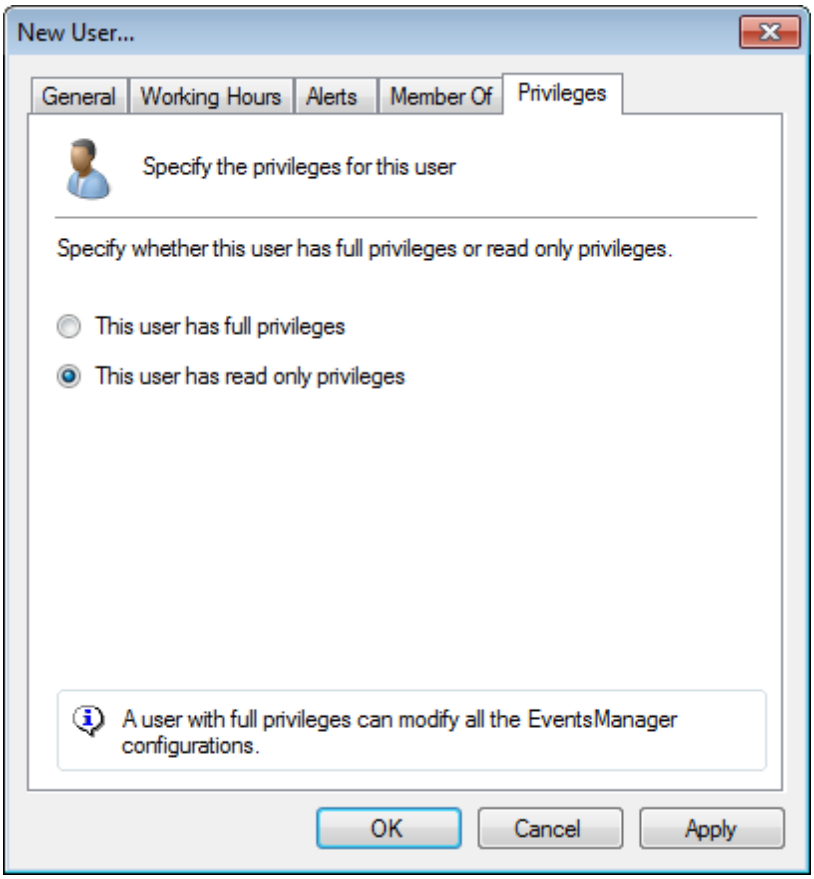
Screenshot 136: Creating a new user - Alerting options

5. Click **Alerts** tab and select the alerts sent during and outside working hours. Optionally, select **Send daily report via email at** and specify the time to send an email containing daily activity.



Screenshot 137: Creating a new user - Select notification group(s)

6. Click **Member Of** tab and click **Add**. Select the notification groups to which the user belongs and click **OK**.



Screenshot 138: Creating a new user - Privileges

7. Click **Privileges** tab to configure user privileges. By default, new user accounts have read only privileges.

8. Click **Apply** and **OK**.

10.2.2 Changing user account properties

To edit user properties:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node.

2. From **Users** sub-node, right-click a user and select **Properties**.

3. Make the required changes in the tabs available and click **OK**.

10.2.3 Deleting a user account

To delete a user:

1. From **Configuration** tab > **Options**, expand the **Users and Groups** node and select **Users**.

2. From right pane, right-click a user and select **Delete**.

10.3 Managing user groups

GFI EventsManager enables you to assign users to a group. Once the group properties have been configured, every member of the group inherits the same settings.

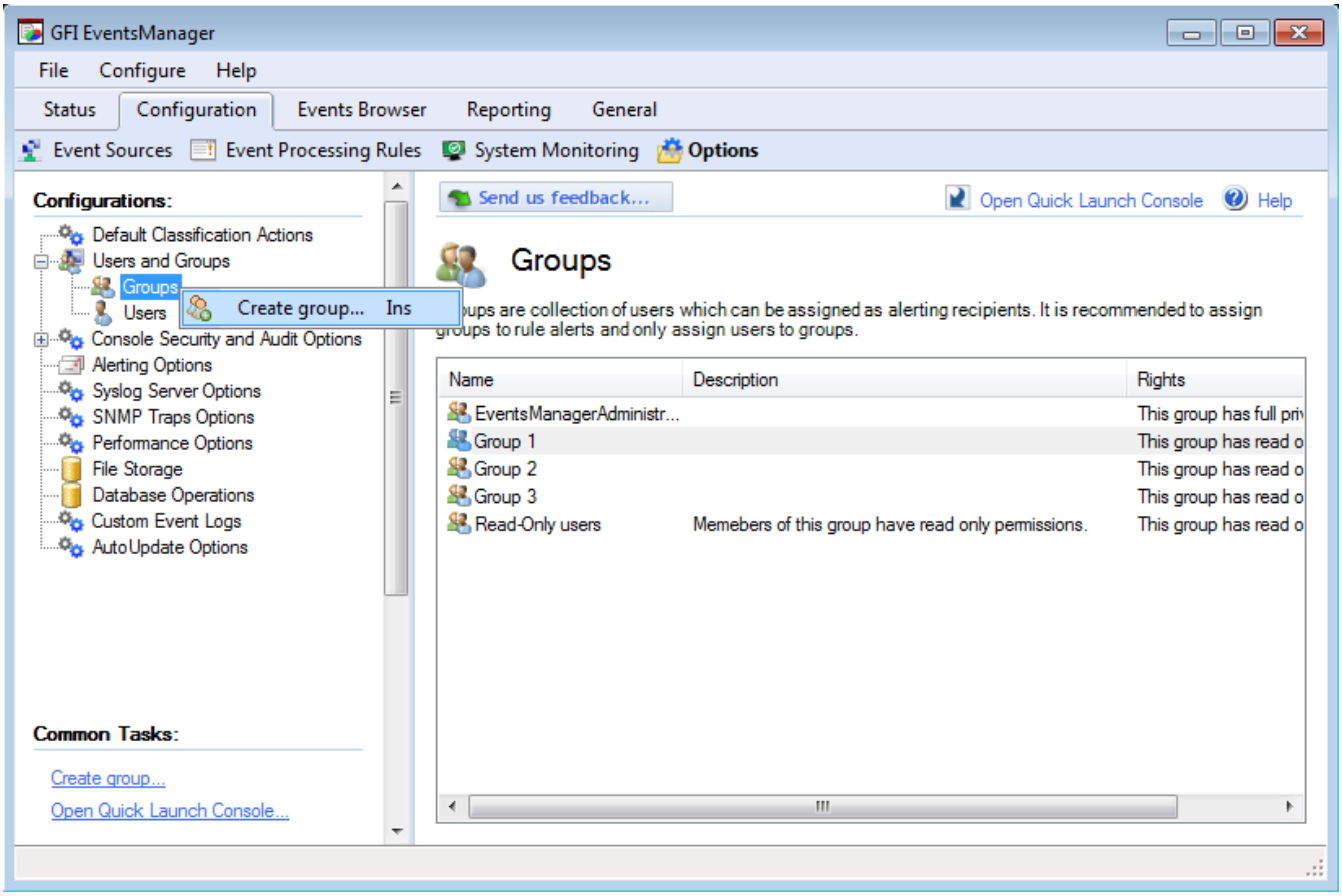
This section contains information about:

- Creating a new group
- Changing group properties
- Deleting a group

10.3.1 Creating a new group

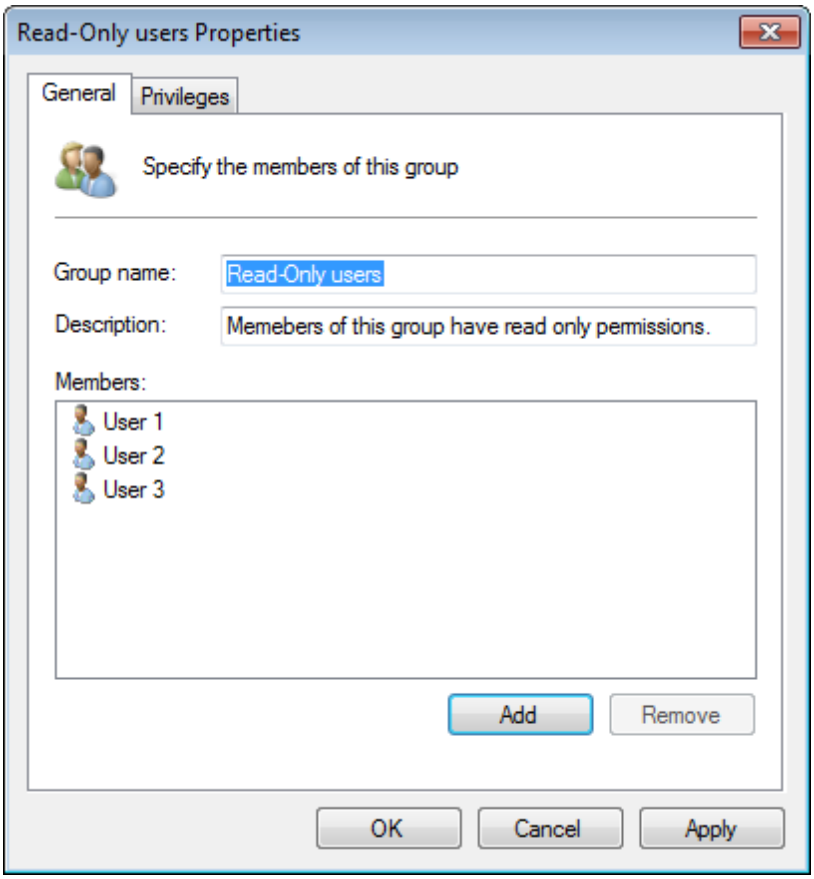
To create a new user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.



Screenshot 139: Creating a new user group

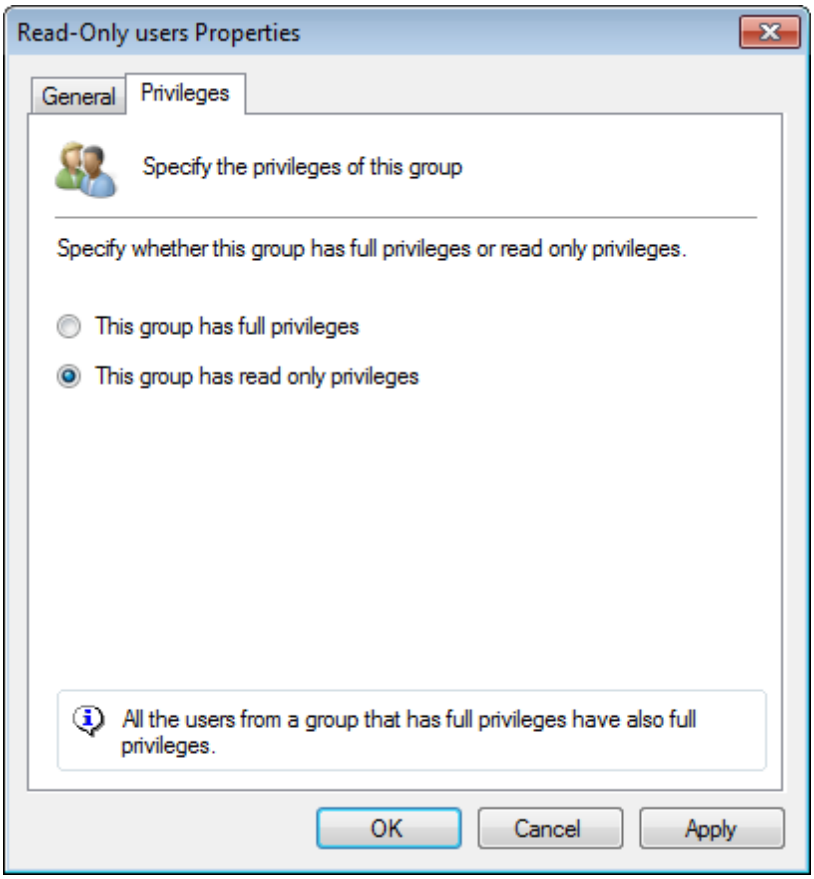
2. Right-click **Groups** sub-node and select **Create group…**



Screenshot 140: Creating a new user group - General properties

3. Specify the name and an optional description for the new group.

4. Click **Add** to add users to the group.



Screenshot 141: Creating a new user group - General properties

5. From the **Privileges** tab, select if the group has **Full** or **Read Only** permissions.

6. Click **Apply** and **OK**.

10.3.2 Changing group properties

To edit the settings of a user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.

2. From the right pane, right-click on the group to be configured and select **Properties**.

3. Perform the required changes in the tabs available and click **OK**.

10.3.3 Deleting a group

To delete a user group:

1. From **Configuration** tab > **Options**, expand **Users and Groups** node.

2. Right-click on the group to be deleted and select **Delete**.

10.4 Managing console security and audit options

Console security and audit options enable you to protect GFI EventsManager from unauthorized access and malicious intent. The provided audit options enable you to accurately monitor GFI EventsManager activity.

This section contains information about:

- Enabling the login system
- Password recovery

- Anonymization
- Audit console activity
- Auto-discovery credentials

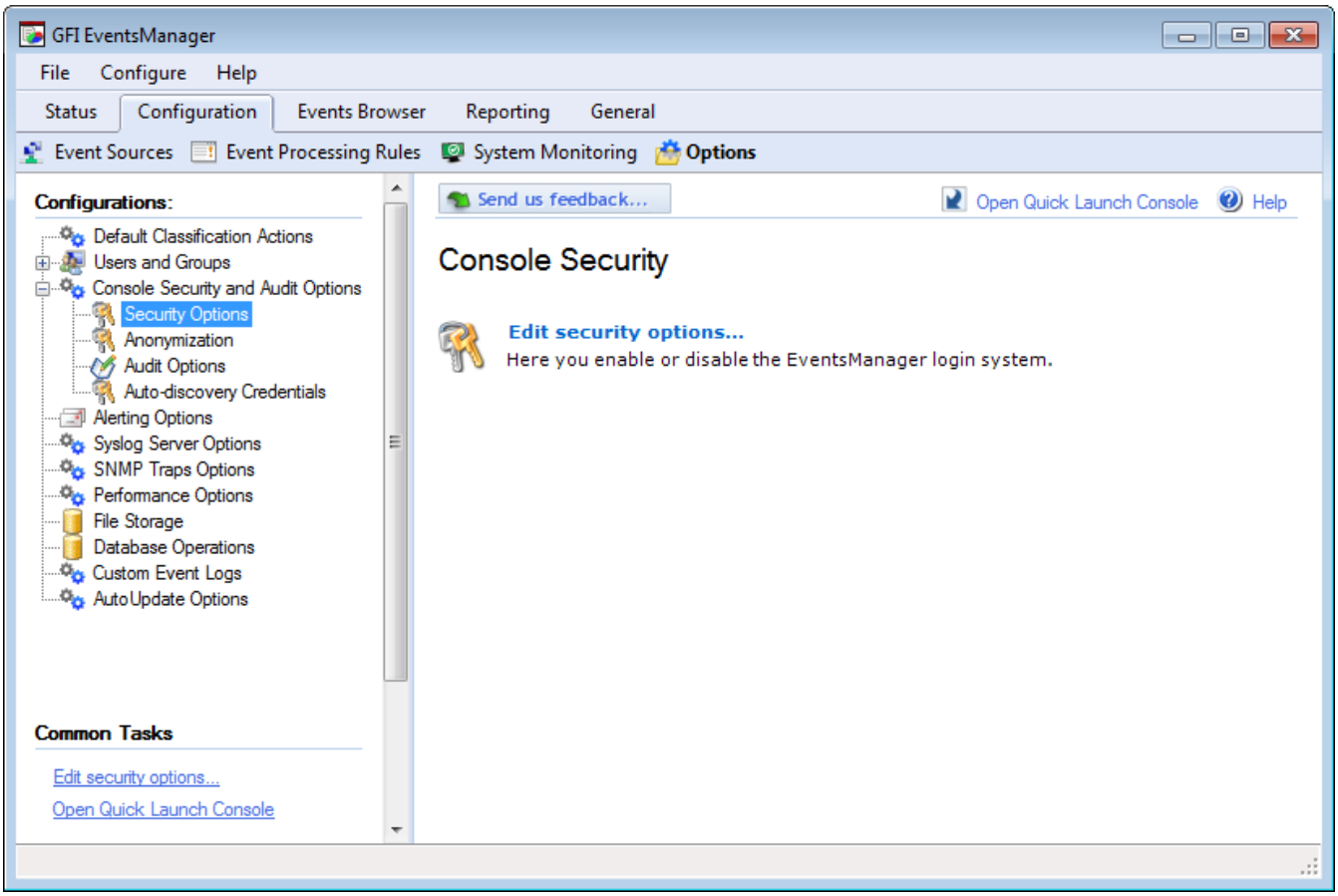
10.4.1 Enabling login system

When the login system is enabled all users will be asked to specify their credentials every time they launch the GFI EventsManager management console.

> **Note**
>
> Before you enable the login system, you must configure your mail server settings. For more information, refer to Configuring Alerting Options (page 187).

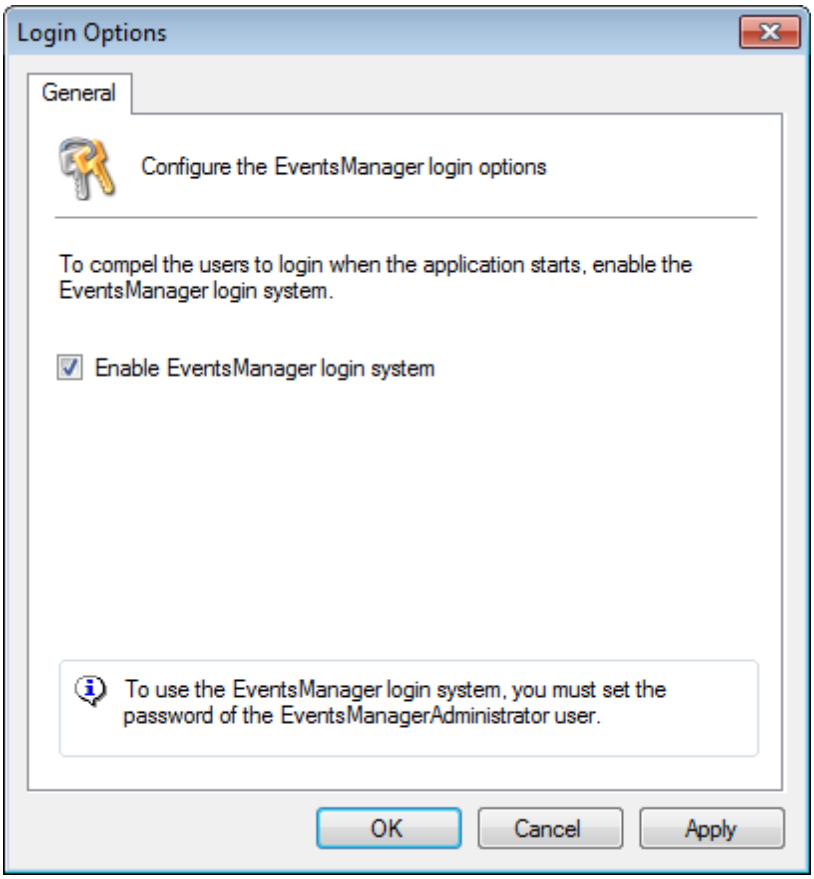
To enable the log-in system:

1. From **Configuration** tab > **Options** expand **Console Security and Audit Options** node.



Screenshot 142: Editing console security options

2. Expand **Console Security and Audit Options** node, right-click **Security Options** node and select **Edit security options...**.



Screenshot 143: Enabling EventsManager login system

3. Select **Enable EventsManager login system** to enable login.

4. Click **Apply** and **OK**.

Note

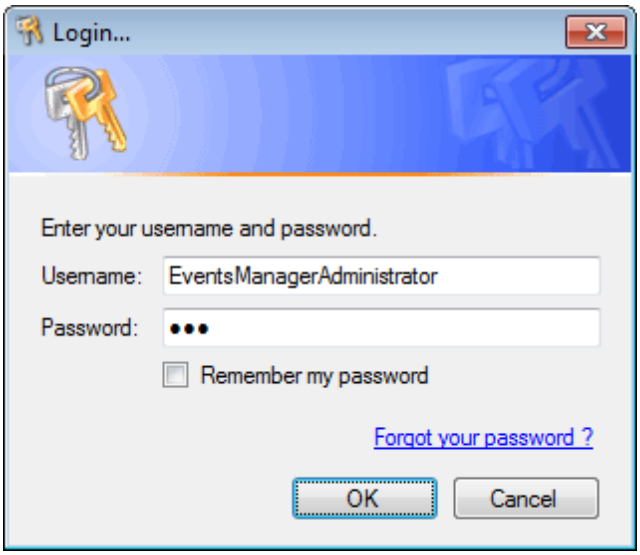
To configure or edit user passwords go to **Configuration** tab > **Users and Groups** > **Users**, right-click the user account and select **Change Password**.

Important

Once the login system is enabled, users must login to the console by specifying their username and password and must have a valid email configured to be able to retrieve lost passwords. For more information, refer to Managing user accounts (page 169).

10.4.2 Password recovery

When GFI EventsManager login system is enabled, all users are requested to enter a valid user name and password to access the management console.



Screenshot 144: Login credentials prompt

If a password is forgotten or lost:

1. Key in your username.

2. Click **Forgot your password?** link. GFI EventsManager will send an email containing your login password on the email address supplied during the user account setup.

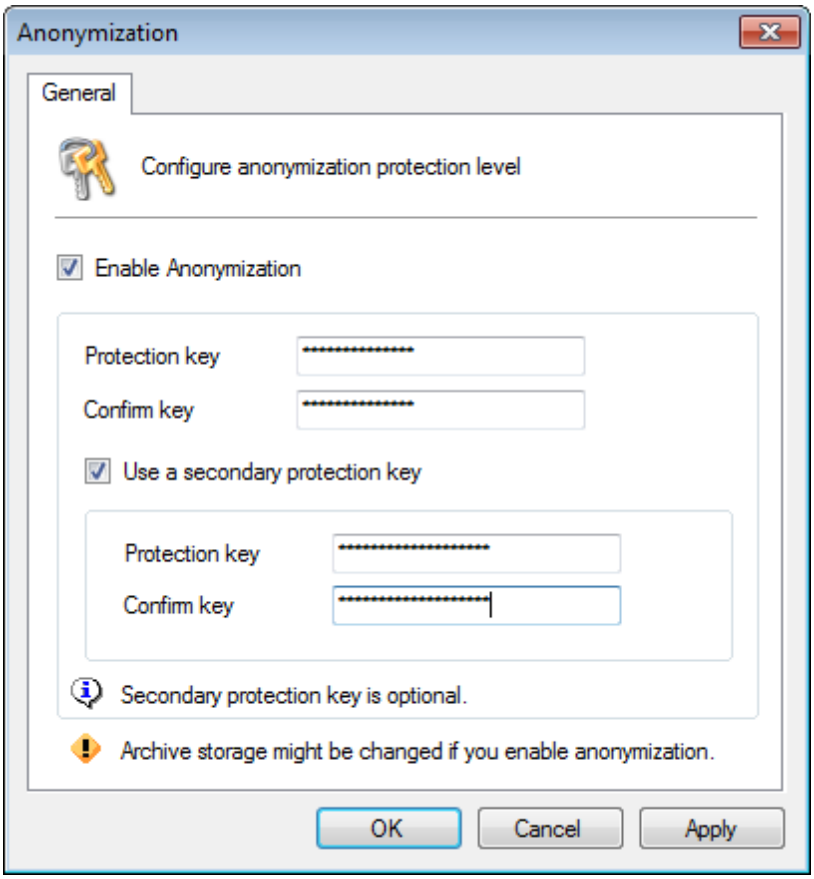
10.4.3 Anonymization

In some countries privacy laws state that it is against the law not to encrypt personal information retrieved by monitoring applications for privacy protection. GFI EventsManager enables you to encrypt personal information when exporting and/or viewing event logs.

Enable anonymization to encrypt all personal information. The Events Browser and Dashboard can recognize such information and do not display it. Instead, they display **<encrypted>** or **Anonymized data** messages instead.

To configure anonymization:

1. From **Configuration** tab **>** **Options**, expand **Console Security and Audit Options** node, right-click **Anonymization** and click **Edit anonymization options…**



Screenshot 145: Anonymization options

2. Select **Enable Anonymization** and enter the encryption password.

3. (Optional) Select **Use a secondary protection key** to use two passwords for event log encryption. Event logs can only be decrypted by providing two decryption passwords.

4. Click **Apply** and **OK**.

Note

Once anonymization is enabled, personal data is hidden in:

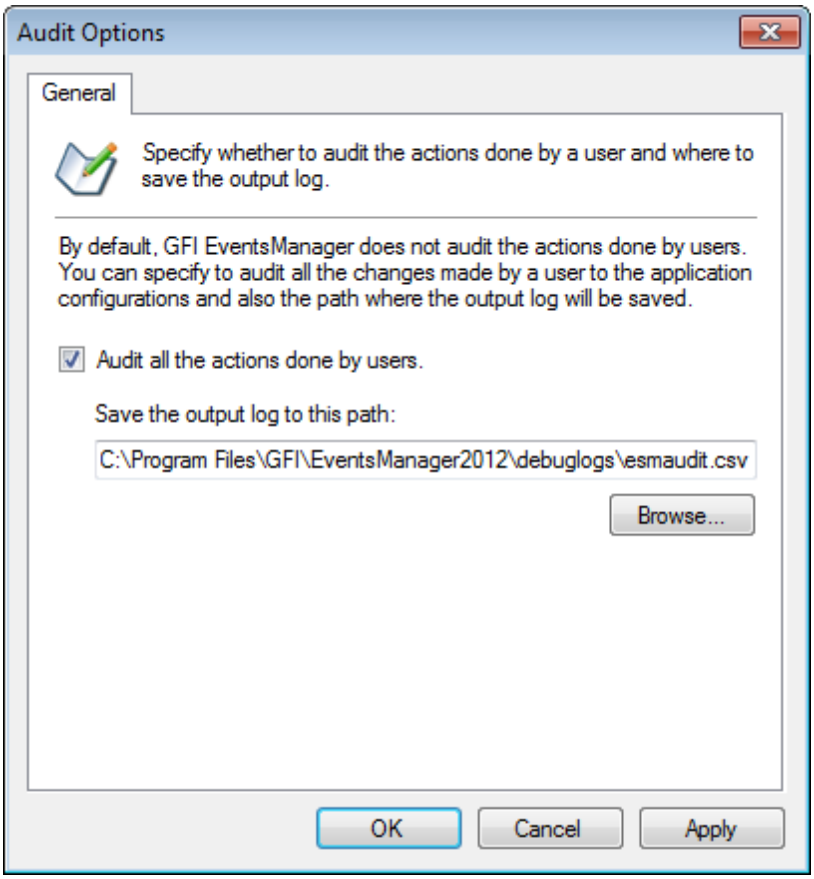
- Any of the Status views (General, Job Activity and Statistics)
- Events Browser
- Reports, and
- Exported/archived event logs (you can remove anonymization when importing the exported logs).

10.4.4 Auditing console activity

GFI EventsManager can save console activity to external logs. To configure console activity auditing:

1. From **Configuration** tab > **Options**, expand **Console Security and Audit Options** node.

2. Right-click **Audit Options** and select **Edit audit options…**.



Screenshot 146: Audit Options dialog

3. Select **Audit all the actions done by users** option and specify the location where the output log file will be saved.

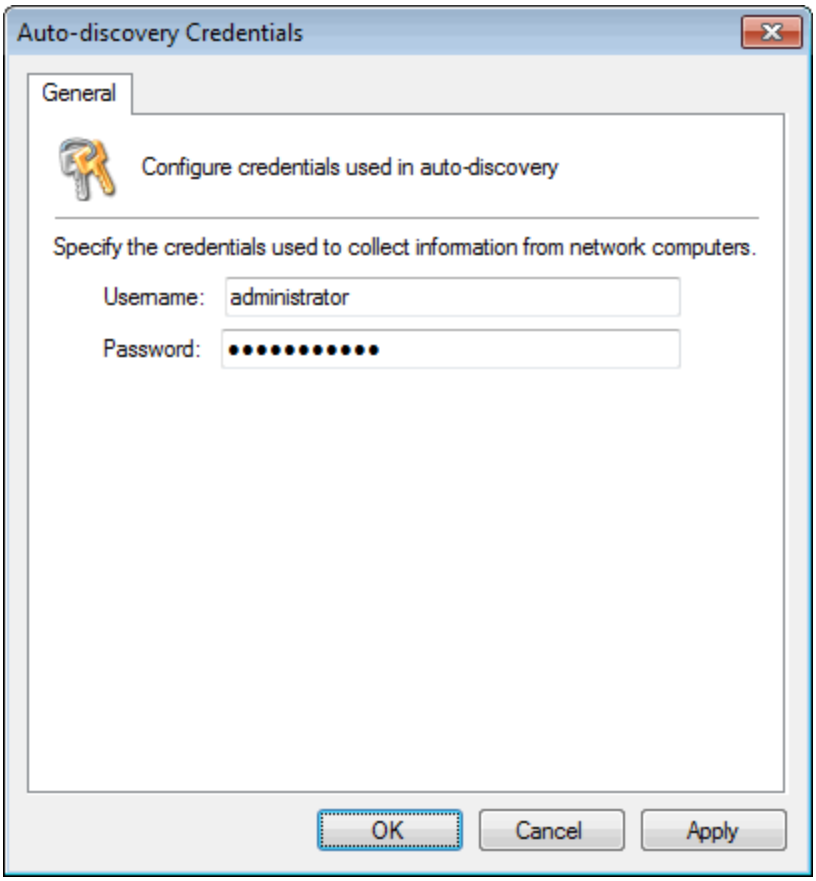
4. Click **Apply** and **OK**.

10.4.5 Auto-discovery credentials

Auto-discovery credentials are used by GFI EventsManager to login target machines and collect information when performing an automatic search for event sources. To configure the auto-discovery credentials:

1. From **Configuration** tab > **Options**, expand **Console Security and Audit Options** node.

2. Right-click **Auto-discovery credentials** and select **Edit auto-discovery credentials**.



Screenshot 147: Specify Auto-discovery credentials

3. Key in a valid username and password.

4. Click **Apply** and **OK**.

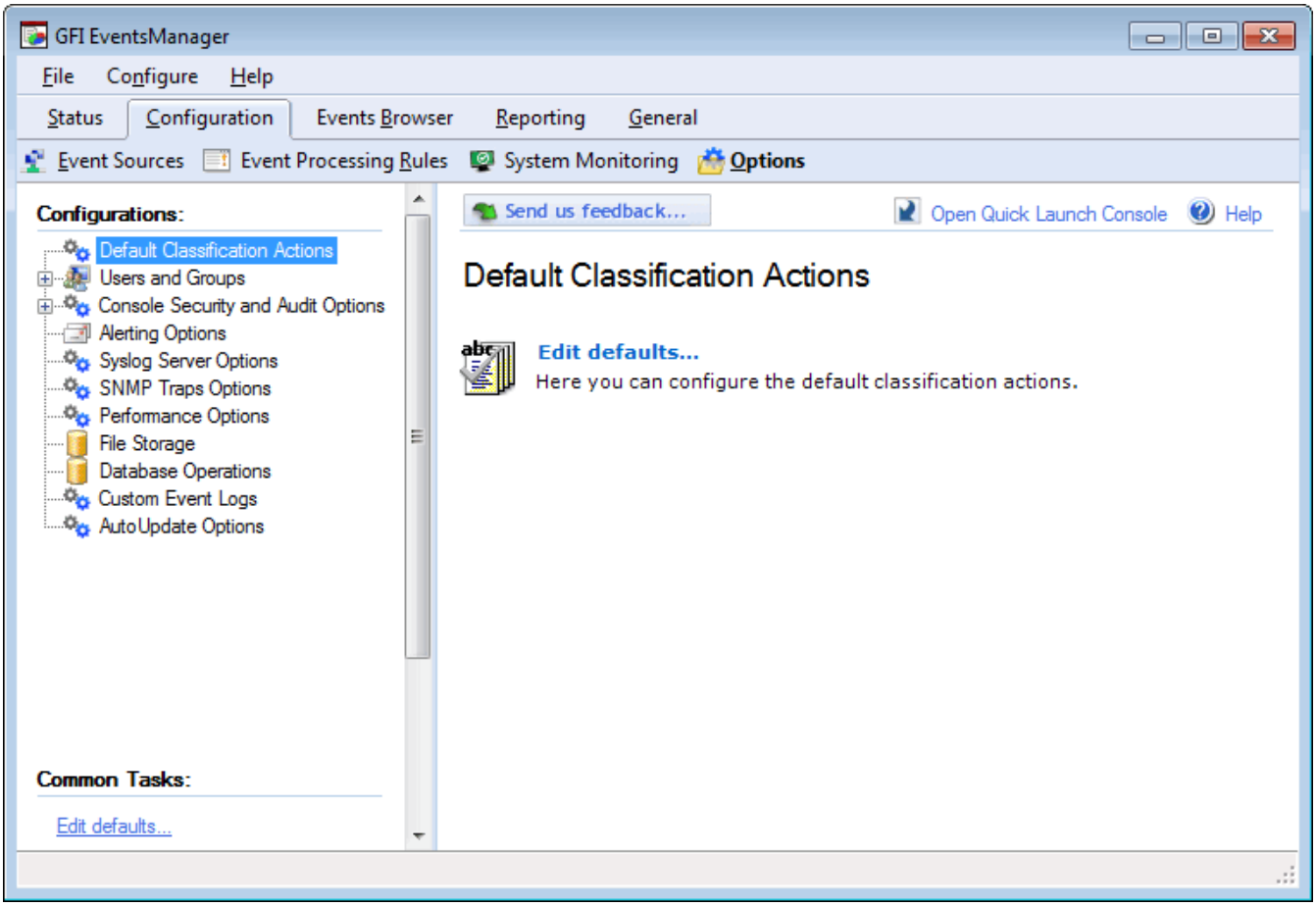
11 Alerts and Default Actions

This chapter provides you with information about the available alerting methods and how to configure each according to your requirements. During event processing, GFI EventsManager automatically executes actions and triggers alerts whenever particular events are encountered.

Topics in this chapter:

11.1 Configuring Default Classification Actions

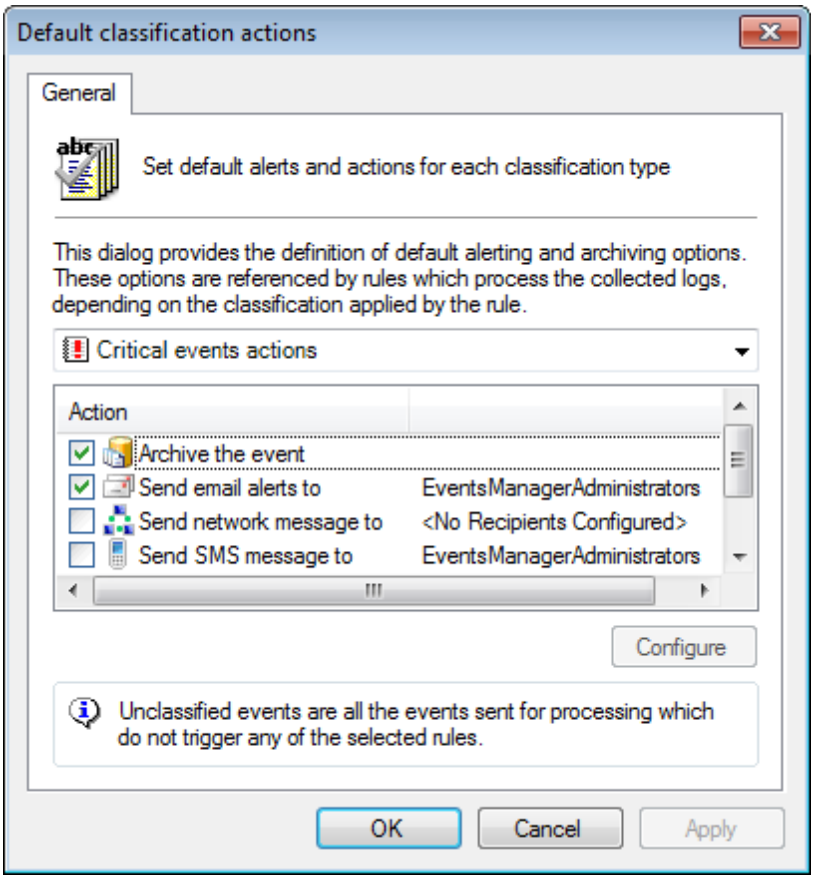
Through the configuration parameters provided in the default classification actions, you can trigger alerts and actions based only on event classification. Example: default classification parameters can be configured to trigger email alerts for all classified events (critical, high, medium and low) but archive only critical events.



Screenshot 148: Configuring default classification actions

To configure Default Classification Actions:

1. From **Configuration** tab > **Options**, right-click **Default Classification Actions** node and **Edit defaults...**



Screenshot 149: Default Classification Actions dialog

2. From the drop-down menu, select the event classification to be configured.

3. From **Action** list, select actions to be triggered and click **Configure**. The available actions are:

Table 70: Default Classification Actions

Action	Description
Archive the event	Archives events without further processing.
Send email alerts to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid email address configured. For more information, refer to Managing user accounts (page 169).
Send network messages to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid computer name/IP configured. For more information, refer to Managing user accounts (page 169).
Send SMS message to	Click **Configure** and select the recipients. **NOTE** Ensure that users have a valid mobile number configured. For more information, refer to Managing user accounts (page 169).

Action	Description
Run file	Click **Configure** and select the file to execute and specify any command-line parameters you want to pass to the file. Supported files include: » VB Scripts - *.VBS » Batch Files - *.BAT » Executables - *.EXE
Send SNMP Message	Click **Configure** and select the recipients.
Run checks on computer	Click **Configure**, select the monitoring checks you want to apply and click **OK**.

4. Click **Apply** and **OK**.

> **Note**
>
> Running default actions on events classified as **Low**, may cause a lot of network traffic when email, SMS, network or SNMP alerts are enabled. This may also be problematic when archiving is enabled on Low importance events.

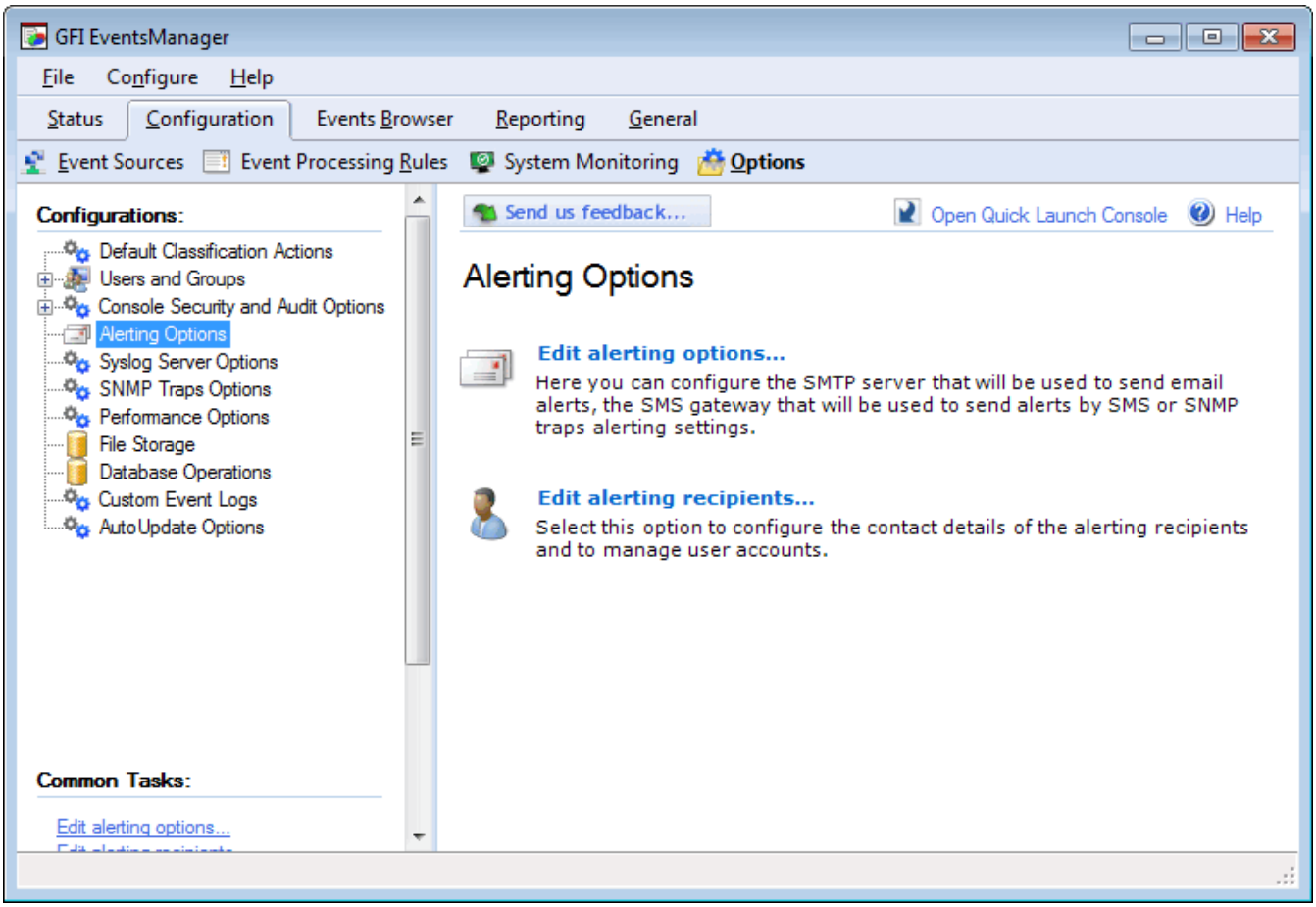
11.2 Configuring Alerting Options

Alerting options enable you to configure what alerts are triggered when particular event(s) are collected. For example, you can configure GFI EventsManager to send an email and SMS alert to one or more recipients when a Critical event is processed.

This section contains information about:

- Configuring email alerts
- Configuring network alerts
- Configuring SMS alerts
- Configuring SNMP Traps alerts
- Configuring general settings

To configure Alerting Options:



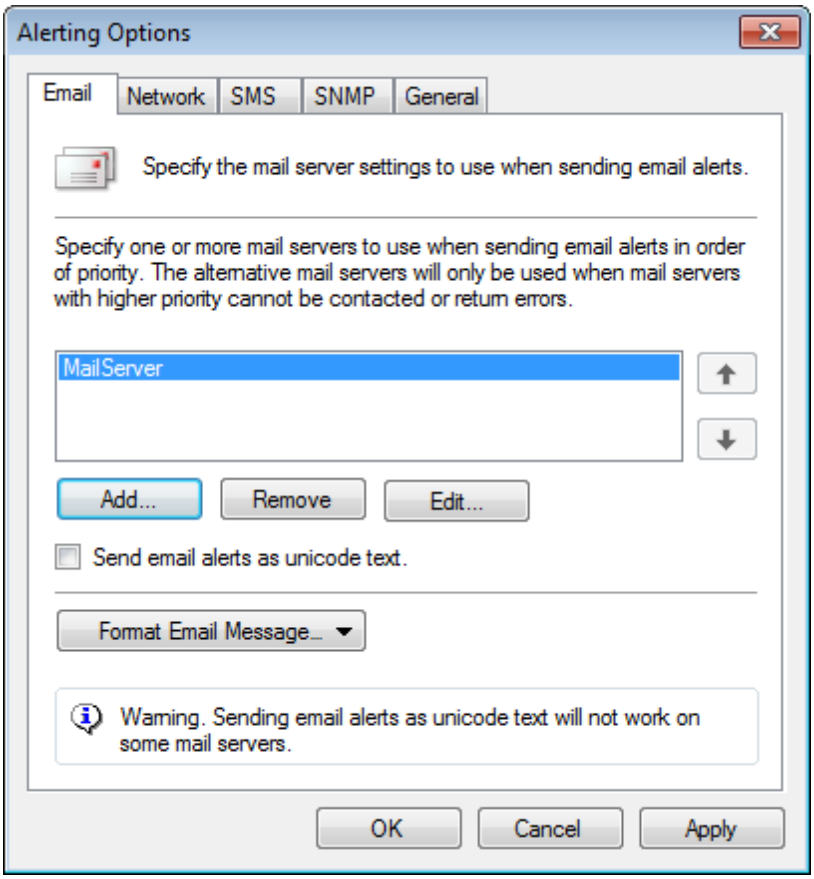
Screenshot 150: Configuring Alerting Options

1. Click **Configuration** tab > **Options**, right-click **Alerting Options** and select **Edit alerting options...**

> **Note**
>
> Select Edit alert recipients to configure the contact details of the alerting recipients and to manage user accounts. For more information, refer to Managing user accounts (page 169).

2. Configure the alerting method of your choice. The following sections describe how to configure:

11.2.1 Email alerts



Screenshot 151: Configuring Email options

To configure email alerts:

1. From the Alerting Options dialog, click **Email** tab.

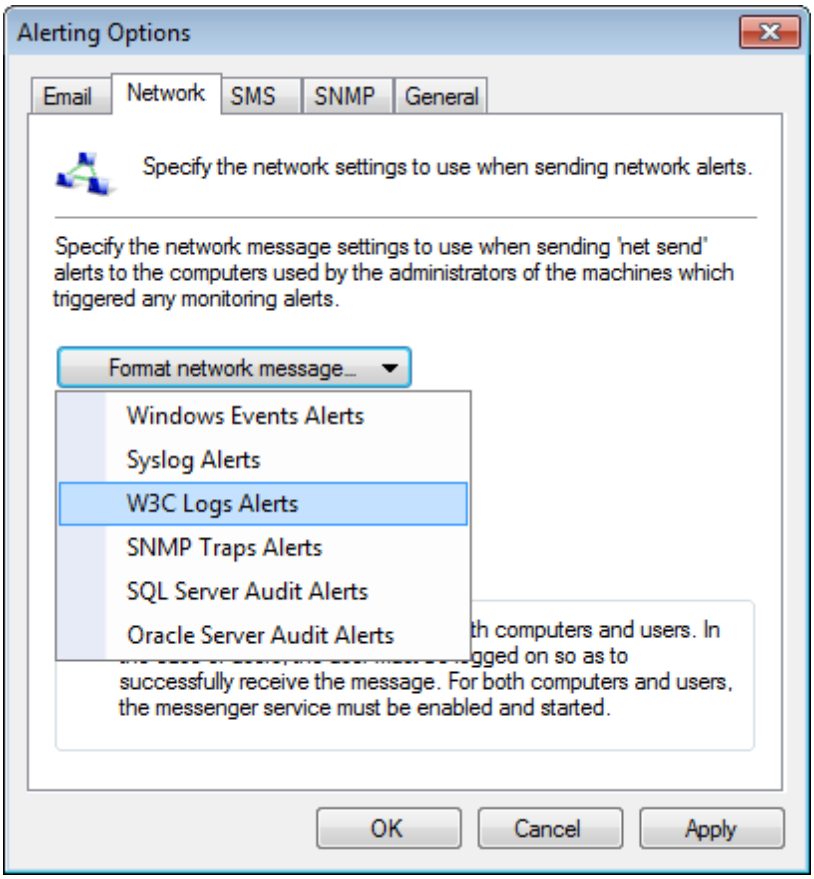
2. Configure the options described below:

Table 71: Alerting Options dialog - Email alerts

Option	Description
Add/Remove/Edit	Click **Add...** to specify the mail server details including the server name /IP, logon credentials and recipient email address. Use the **Remove** or **Edit** button to remove a selected server or edit details.
Up/Down arrow buttons	Use the arrow buttons to change the position of the selected mail server. GFI EventsManager attempts to deliver email alerts via the first mail server. If unsuccessful, it recursively checks the following mail servers.
Send email alerts as Unicode text	Select this option to send emails as Unicode text as opposed to HTML or RTF format.
Format Email Message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.2 Network alerts

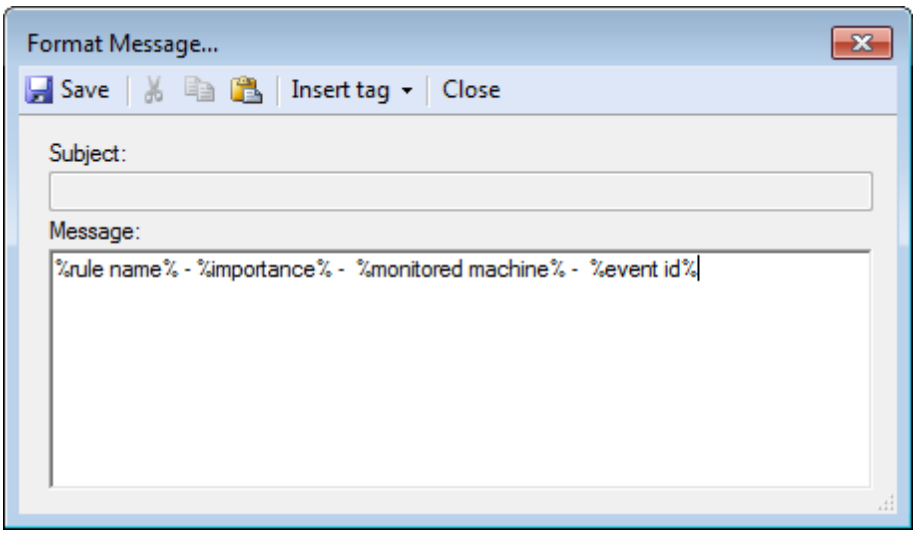


Screenshot 152: Configuring Network options

To configure network alerts:

1. From the Alerting Options dialog, click **Network** tab.

2. From **Format network message…** drop-down menu, select the log type and customize the format of the message.

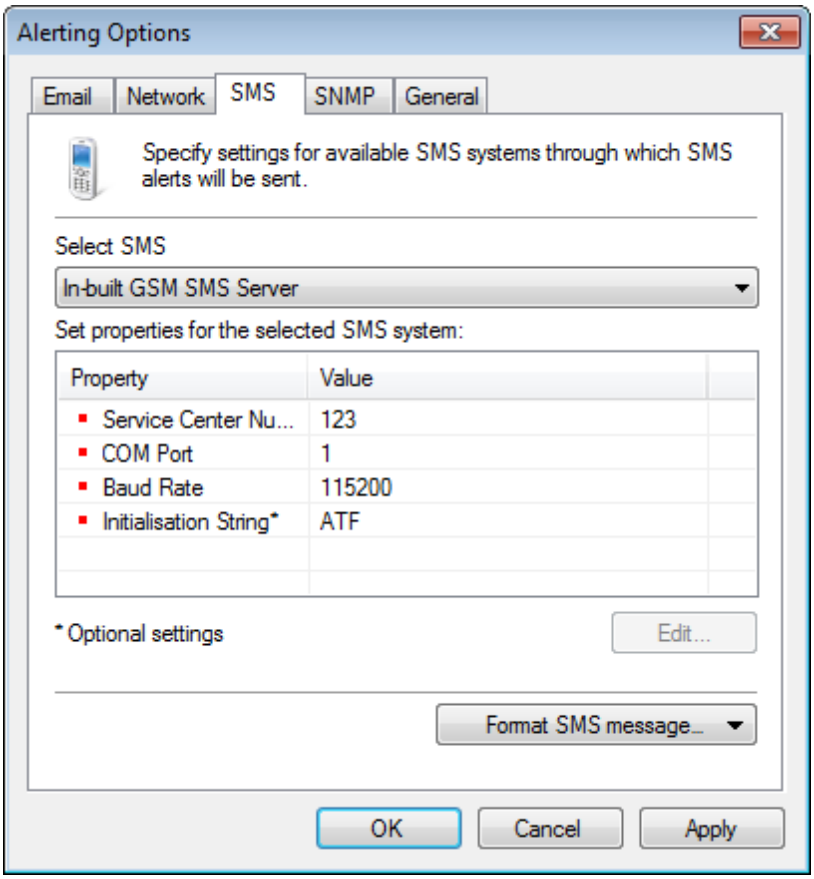


Screenshot 153: Configuring Network alerts: Format message

3. Click **Insert tag** to select from a list of tags to include in the message.

4. Click **Save** and **OK**.

11.2.3 SMS alerts



Screenshot 154: Configuring SMS options

To configure SMS alerts:

1. From the Alerting Options dialog, click **SMS** tab.

2. Configure the options described below:

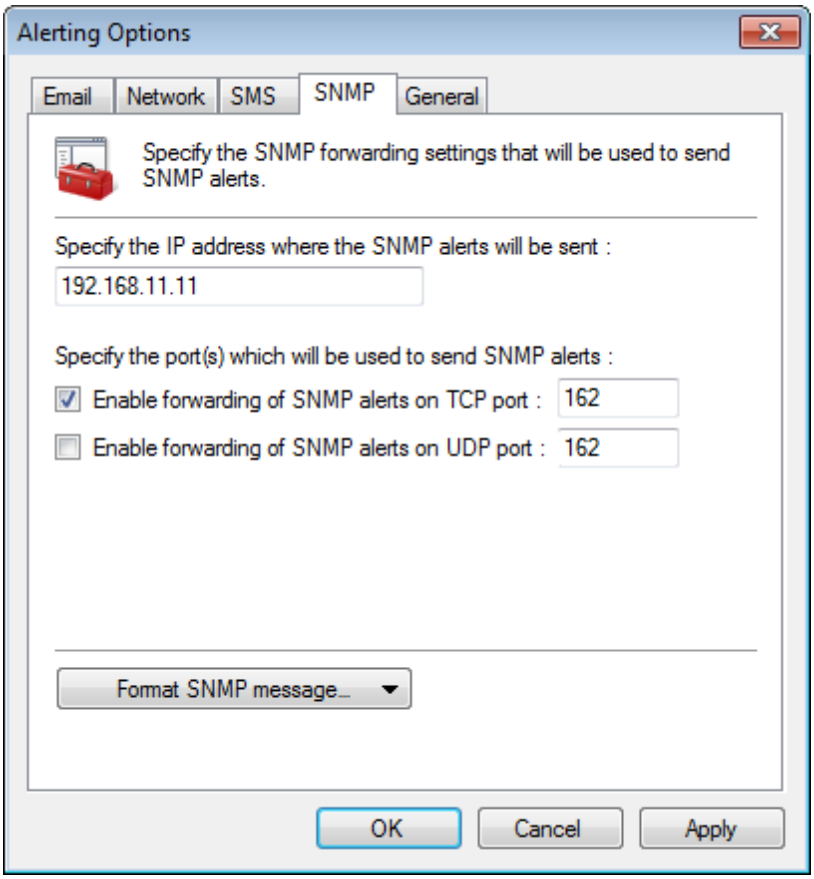
Table 72: Alerting Options dialog: SMS

Option	Description
Select SMS	Select the SMS service used to send SMS alerts. Available services include: » In-built GSM SMS Server » FaxMaker SMS service provider template » Clickatell Email2SMS Service » Generic SMS service provider template.
Set properties for the selected SMS system	Configure the properties for the selected SMS service type. Amongst others, property settings include: » Service center number » COM Port » Baud Rate » SMTP Server » SMTP Port. Click **Edit...** to configure the selected property.
Format SMS message	Optionally, from the **Format Email Message** drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.4 SNMP alerts

To configure SNMP alerts:



Screenshot 155: Configuring SNMP alerts

1. From the **Alerting Options** dialog, click **SNMP** tab.
2. Configure the options described below:

Table 73: Alerting Options: SNMP Traps

Option	Description
Specify the IP address where the SNMP alerts will be sent	Enter the IP address of the recipient.
Specify the port(s) which will be used to send SNMP alerts	Specify TCP/UDP communication port. By default, the assigned port is 162.
Format SNMP message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **Apply** and **OK**.

11.2.5 General settings

To configure general alerts settings:

1. From the **Alerting Options** dialog, click **General** tab.
2. Configure the options described below:

Table 74: Alerting Options: General settings

Option	Description
Send email alerts on database errors	Email alerts are sent upon database errors such as backup failure, data corruption, size exceeds maximum size specified and other database operation errors.

3. Click **Apply** and **OK**.

12 Database Maintenance

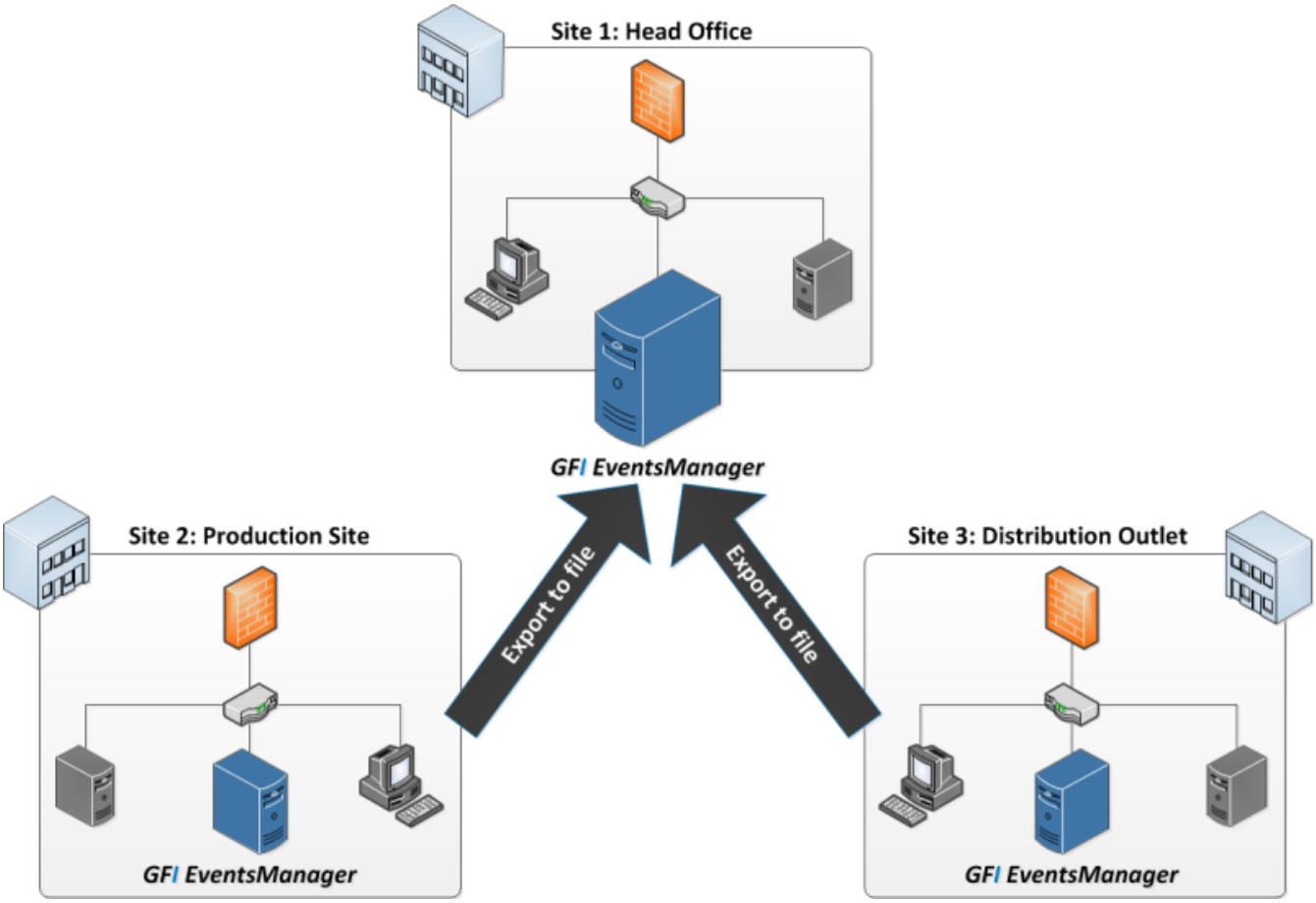
This chapter provides information about the storage system that GFI EventsManager uses to store processed events. This system allows great scalability with its fast read/write capabilities; even when processing high volumes of data. To help you maintain your database backend, GFI EventsManager provides you with dedicated maintenance job options.

Database maintenance jobs provide advanced functionality to administrators, allowing them to:

- Centralize events collected by other remote GFI EventsManager instances into one database back-end
- Optimize GFI EventsManager performance by actively controlling database backend growth hence keeping it in good shape
- Import and export data to and from older versions of GFI EventsManager without data inconsistencies.
- Import and export events to and from a storage folder minimizing data loads from the database.

Topics in this chapter:

12.1 Consolidation of events in a WAN environment



Screenshot 156: Export data from remote sites to the main instance of GFI EventsManager

In the case of organizations with remote geographical sites, Database Operations can be used to consolidate all or part of the events data collected in remote sites on to one central database. This is achieved using the Export to file feature through which GFI EventsManager compresses and encrypts the file as well as export the file to be processed to a central location. The Import to file job is executed at the central location, importing the events from the remote site into the central database.

Events for the remote site can then be viewed through the Events Browser. Reports with information relevant to the remote site can also be generated using data from the central database.

12.2 Managing the database backend

This section describes how you can easily manage your backend database through GFI EventsManager Management Console.

This section contains information about:

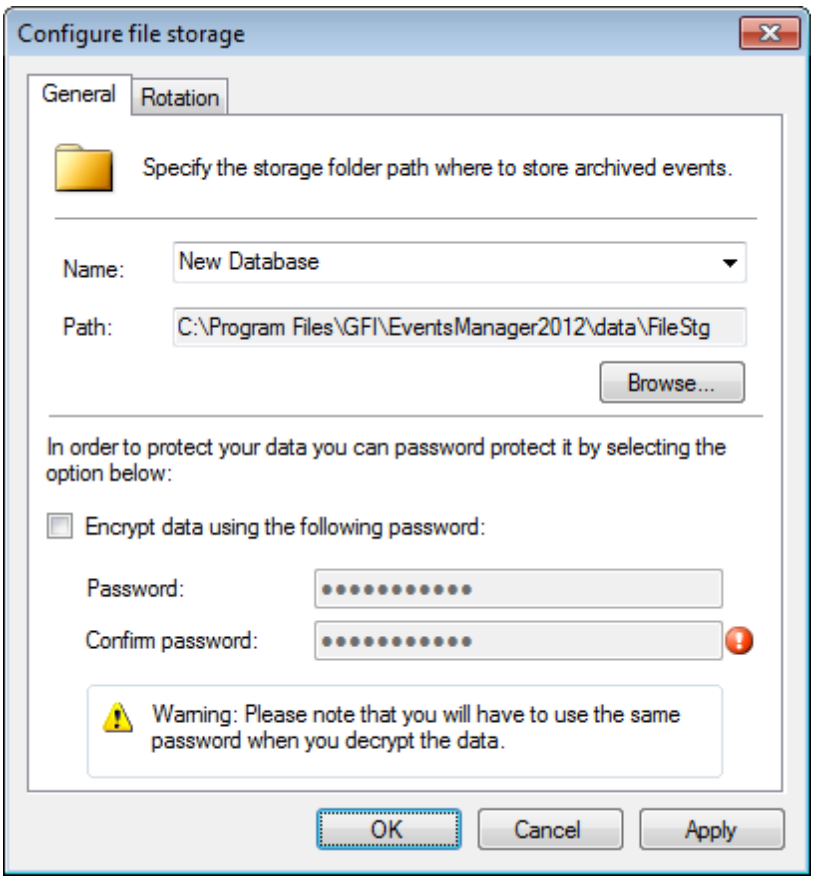
- Creating a new database
- Protecting your database
- Enabling database record hashing
- Switching databases
- Configuring database rotation options

12.2.1 Creating a new database

GFI EventsManager enables you to have multiple databases to store processed event logs. Through the Events Browser, Reporting tab and other locations, you can easily switch from one database to another, allowing you to view events or generate reports from multiple databases. Databases can be further secured by encrypting them with a password.

To create a new database:

1. From **Configuration** tab > **Options** > **Configurations**, right-click **File Storage** and select **Configure file storage…**.



Screenshot 157: File storage system dialog

3. Specify the name for the new database in the **Name** text box.

4. From **Path**, specify or browse for the path of the new database.

5. (Optional) Select **Encrypt data using the following password** and specify an encryption password.

6. Click **Apply** and **OK**.

Note

Indicates that the specified passwords do not match.

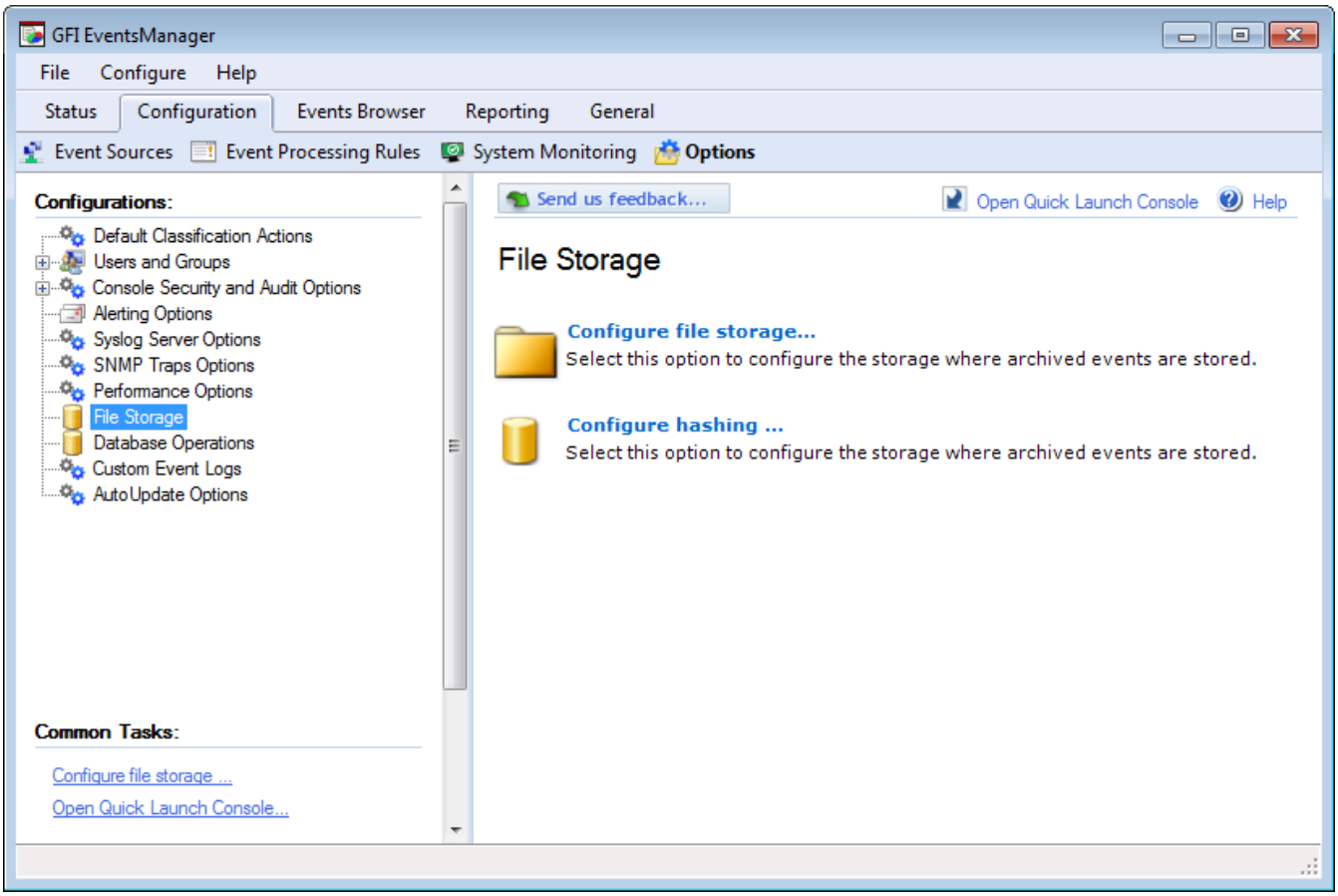
12.2.2 Protecting your database

GFI EventsManager enables you protect your database with an encryption key. Encrypting the database will prevent unauthorized personnel from viewing or accessing event logs.

Important

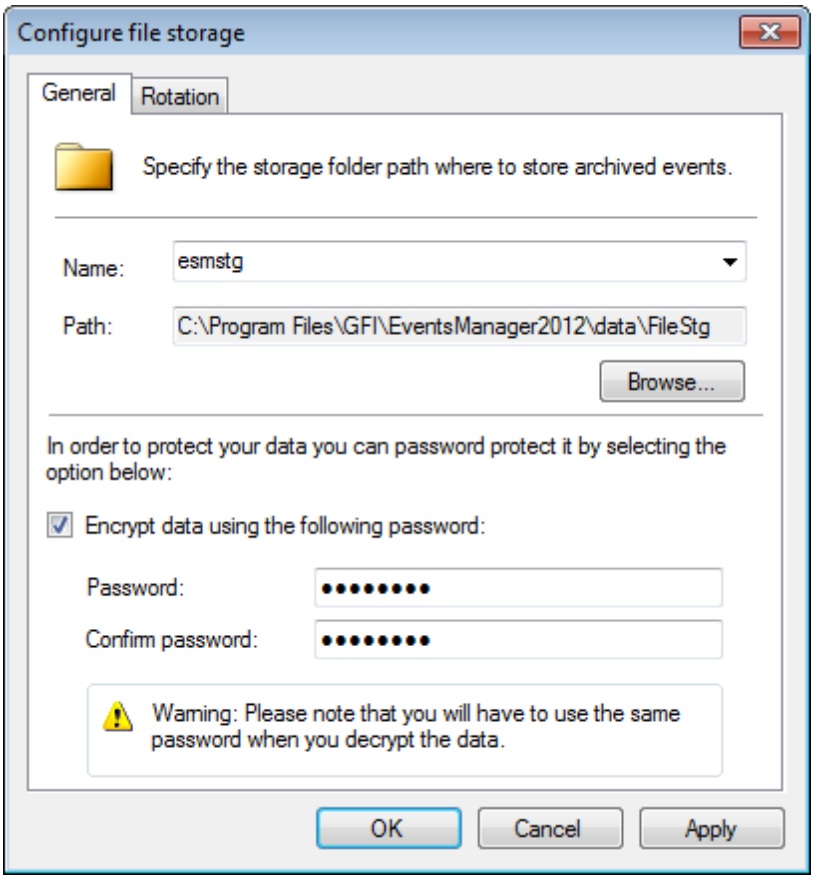
Encrypting the database will cause the **Status Monitor** and **Events Browser** to stop viewing sensitive information.

To encrypt the database backend:



Screenshot 158: Editing file storage settings

1. Click **Configuration** tab > **Options**, right-click **File Storage** and select **Configure file storage...**.



Screenshot 159: Enabling encryption

2. From **General** tab, select **Encrypt data using the following password** to enable encryption.
3. Specify the password and confirmation password.
4. Click **Apply** and **OK**.

> **Note**
>
> The live database (the database you are currently using) cannot be encrypted from this dialog. Only new or offline databases can be encrypted from here. To encrypt the live database, use the provided CMD tool: **esmdlibm.exe**. For more information, refer to Using Esmdlibm.exe (page 237).

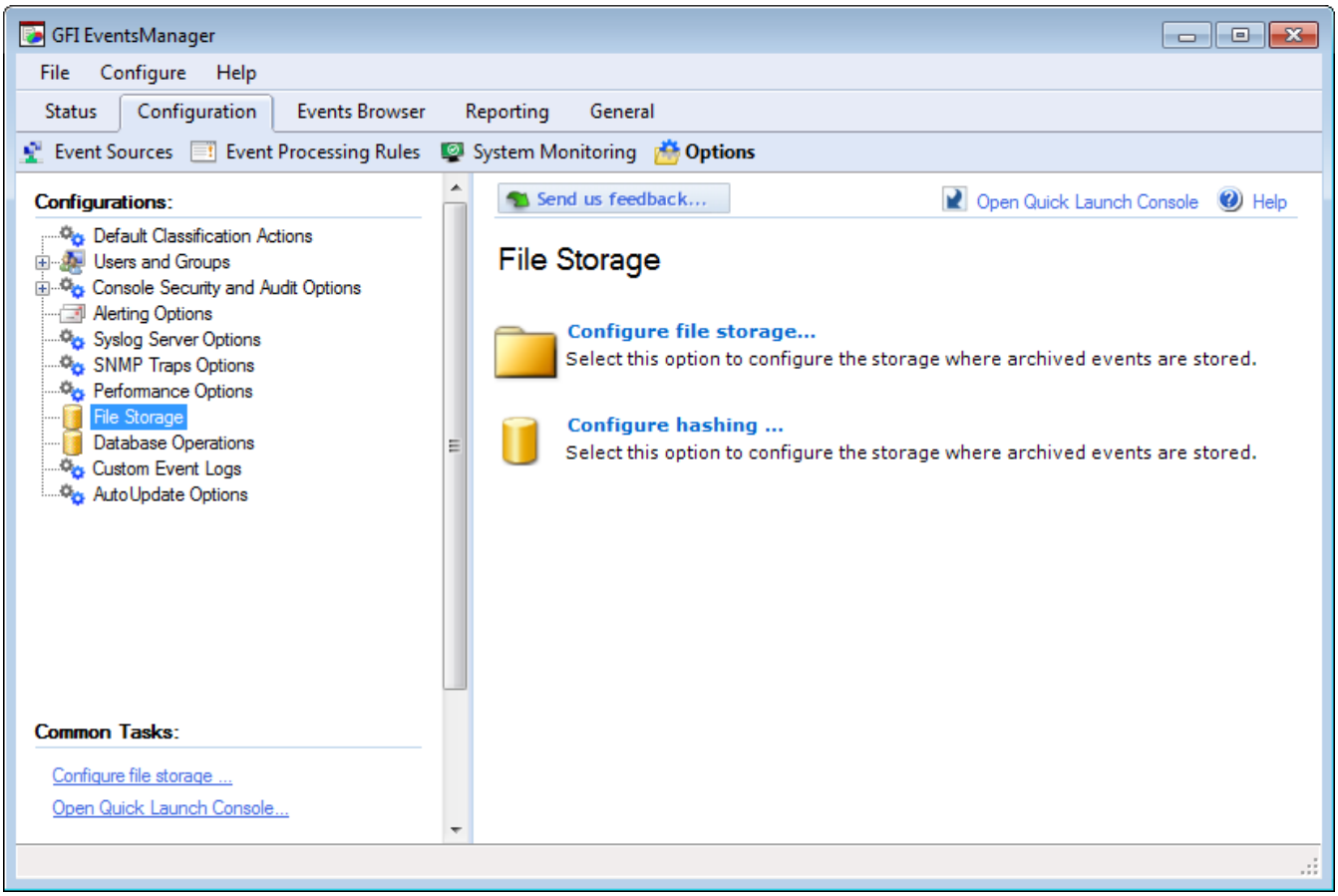
12.2.3 Database record hashing

To further protect your data, GFI EventsManager provides you with record hashing capabilities. Hashing new records is a method used to ensure that data in your databases remains unmodified. When record hashing is enabled, a hash is created for every collected log, at collection time. The hash is built based on the data contained in the event log itself and created as soon as the event log is collected to ensure that it is the original version. When data of a hashed record is modified (even a character from a word), the hash value changes, indicating that someone could be tampering with stored records.

Important

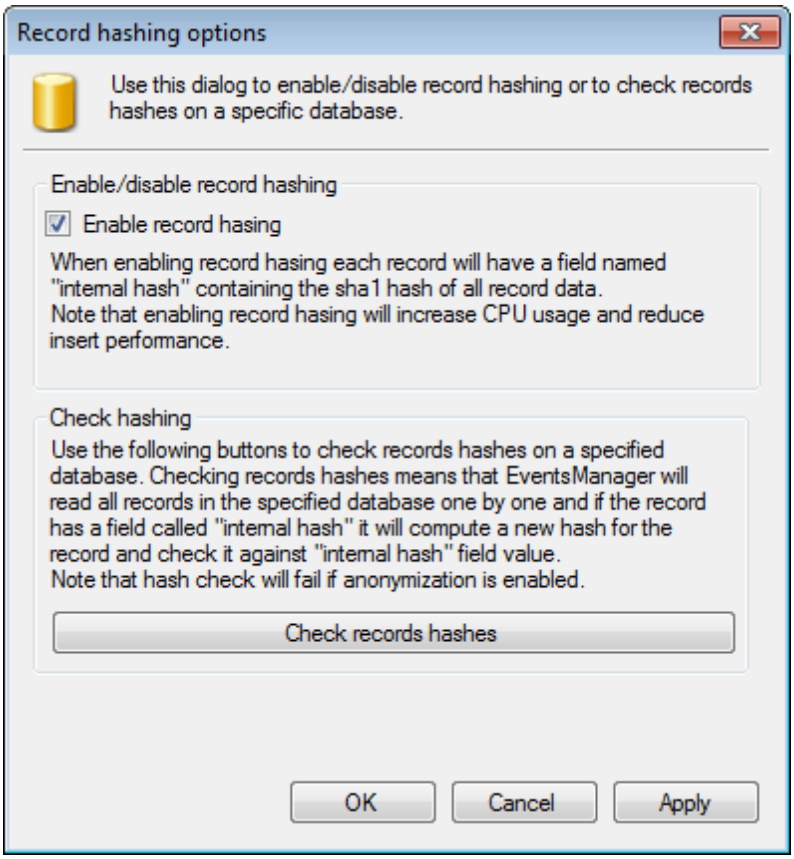
Hashing will fail if anonymization is enabled.

To configure hashing:



Screenshot 160: Enabling / disabling record hashing

1. From **Configuration** tab > **Options** > **Configurations**, click **File Storage** > **Configure hashing...**.



Screenshot 161: Record hashing dialog

2. Select/unselect **Enable record hashing** to turn on/off hashing features.

3. Click **Check records hashes** to run hash checks on the selected database. Select a database from the list and click **OK** to start the check.

4. Click **Apply** and **OK**.

12.2.4 Switching database

To switch from one database to another:

1. From **Configure file storage** dialog, click **Browse** or specify the path to the database you want to load.

2. From **Name** drop-down menu, select the database.

3. (Optional) Enable/Disable encryption. GFI EventsManager supports encryption of offline databases through the Management Console.

4. Click **Apply** and **OK**.

12.2.5 Configuring database rotation options

When processing events from a large number of event sources, it is important to configure database rotation options. These options instruct GFI EventsManager to automatically switch to a new database when a certain condition is met. Doing so helps you maintain a pool of fixed size databases which enable GFI EventsManager to perform better.

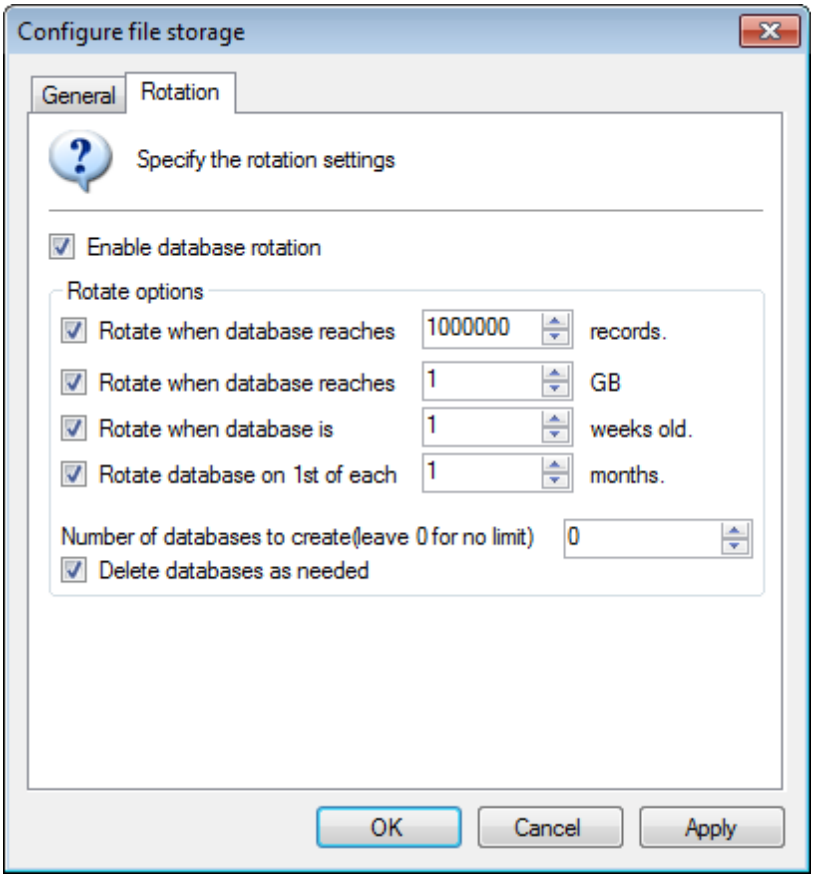
When a database becomes too large in size, queries take longer to complete so therefore, GFI EventsManager performance is affected negatively. For example, if you are monitoring a network where a lot of small size events are being generated, enable database rotation for when a specified

number of events are collected. On the other hand, if you have large size event logs being generated, enable database rotation for when the database exceeds a specified size.

To configure database rotation options:

1. Click **Configuration** tab > **Options**.

2. From **Configurations**, click **File storage** > **Configure file storage...**



Screenshot 162: Configuring database rotation options

3. Click **Enable database rotation**.

4. Configure the options described below:

Table 75: Database rotation options

Option	Description
Rotate when database reaches - Records	Specify the number of records that the database has to contain before rotating to a new one. Minimum value = 1,000,000 records.
Rotate when database reaches - GB	Rotate to a new database when the current one reaches the specified size in Giga Bytes (GB) Minimum value = 1GB.
Rotate when database is	Rotate database when the current one is older than the specified number of weeks. Minimum value = 1 week.
Rotate database on 1st of each	Select this option to rotate databases on the 1st of each number of specified months. Example, rotate database on the 1st of every month, 1st of every two months or 1st of every six months.
Number of databases to create	Specify the maximum number of databases that GFI EventsManager is able to create. Leave the value at **0** so that an unlimited number of databases can be created.
Delete database as needed	Select this option so that when the maximum number of databases is reached, GFI EventsManager automatically deletes the oldest database to free space for new ones.

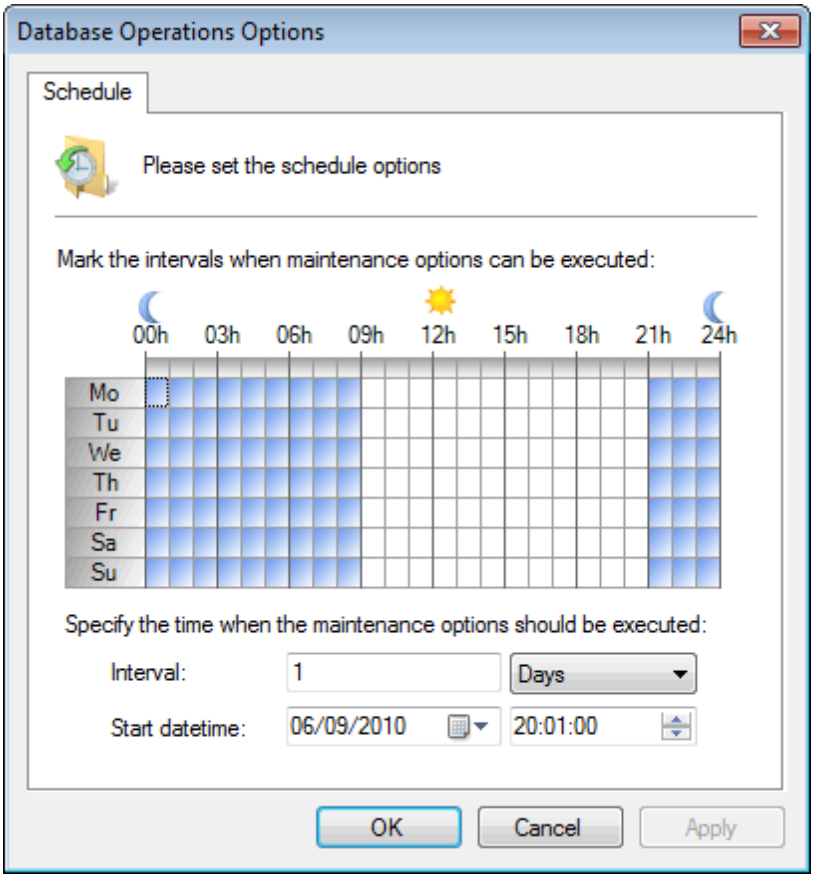
5. Click **Apply** and **OK**.

12.2.6 Configuring Database Operations

To configure Database Operations:

1. Click **Configuration** tab > **Options**.

2. From **Configurations**, right-click **Database Operations** and select **Properties**.



Screenshot 163: Database Operations Options dialog

3. Configure the options from the tabs described below:

Table 76: Configuring database operations

Tab	Description
General	Specify the unique identifier by which this instance of GFI EventsManager will be identified on the network. This identifier is used as part of the export file-name during Export to file operations.
Schedule	Through the Schedule tab, specify: » Hours of the day during which maintenance jobs can be executed » The interval in hours/days with which maintenance jobs will be executed » The scheduled date/time when maintenance jobs will start being executed.

4. Click **Apply** and **OK**.

> **Note**
>
> Schedule options can also be modified from **Configuration** tab > **Options** > **Actions** and click **Edit schedule options...**.

12.3 Creating maintenance jobs

With GFI EventsManager you can schedule maintenance jobs to be executed on a specific day, at a specific time and at specific intervals. Database maintenance operations may require high utilization of resources. This can degrade server and GFI EventsManager performance. Schedule maintenance jobs to be executed after office hours to maximize the availability of your system resources and avoid any possible disruptions to workflow.

GFI EventsManager supports two types of maintenance jobs as described below:

Table 77: Maintenance jobs types

Job type	Description
Import\Export Job	Import/export data from/to other instances of GFI EventsManager. Export data and import them in other instances as part of the data centralization process.
Legacy Import Job	Import data from older versions of the product. Import data from Microsoft SQL Server databases, legacy files and legacy file storage. The import jobs supported by this job type are all based on the database backend types of older versions of GFI EventsManager.

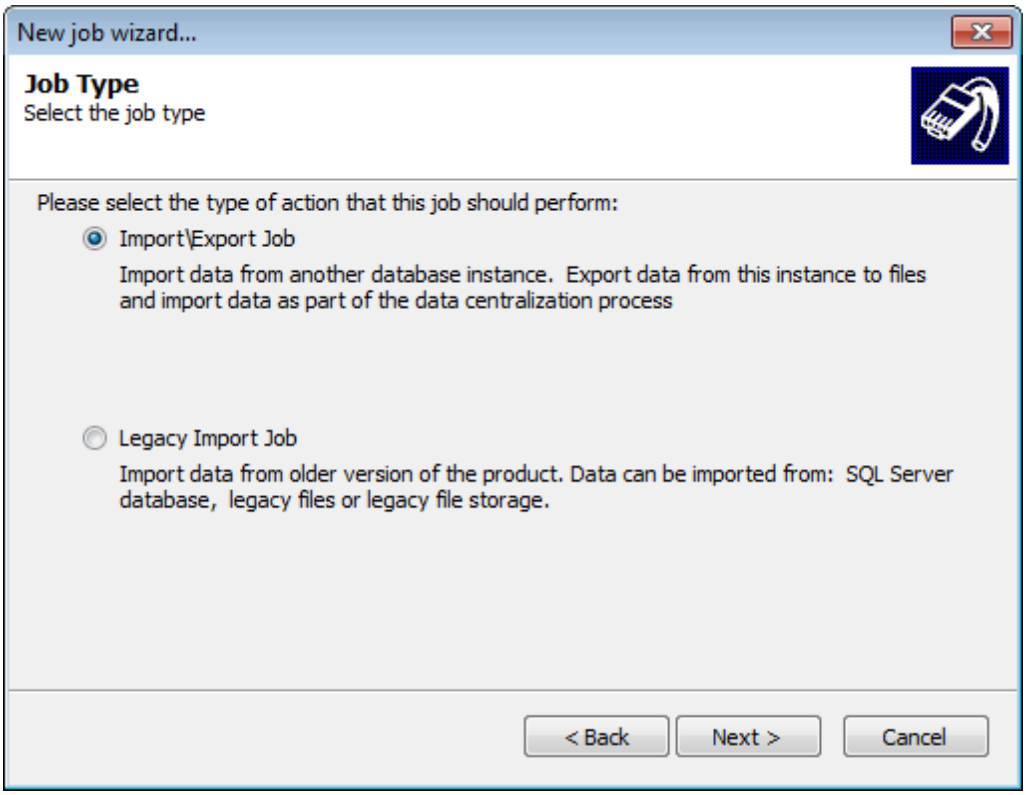
Read the following sections for information about creating the following maintenance jobs:

- Import from file
- Export to file
- Copy data
- Commit deletions
- Import from SQL Server databases
- Import from legacy files
- Import from legacy file storage

12.3.1 Import from file

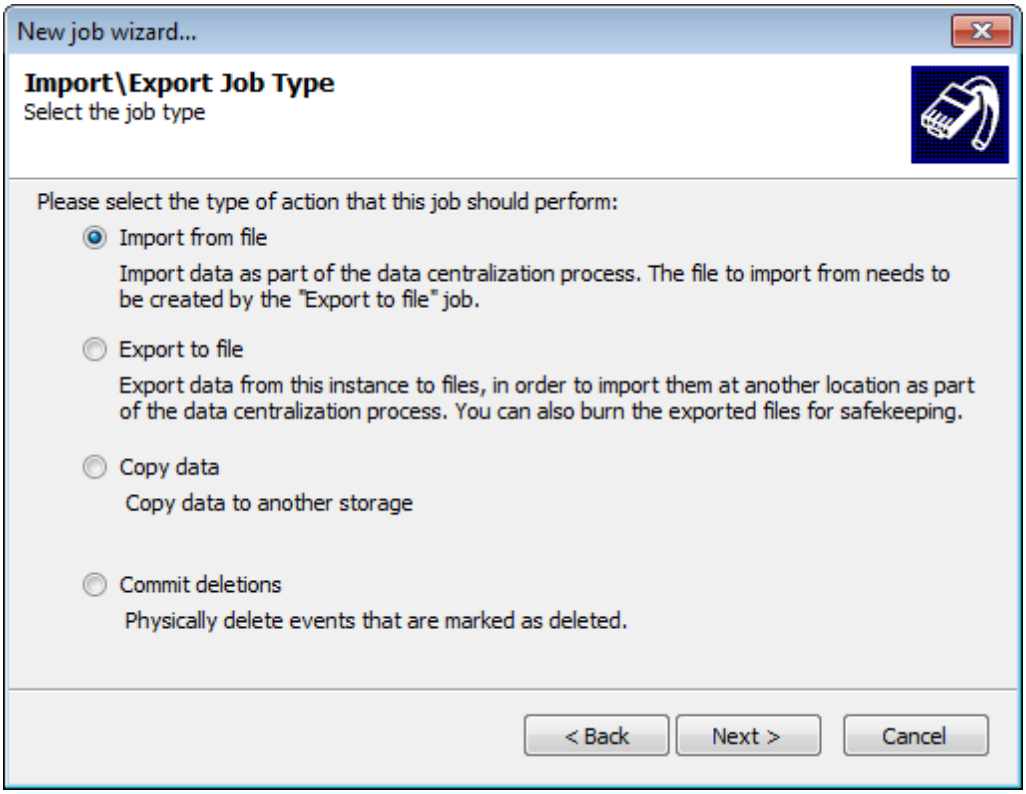
To create an Import from file job:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



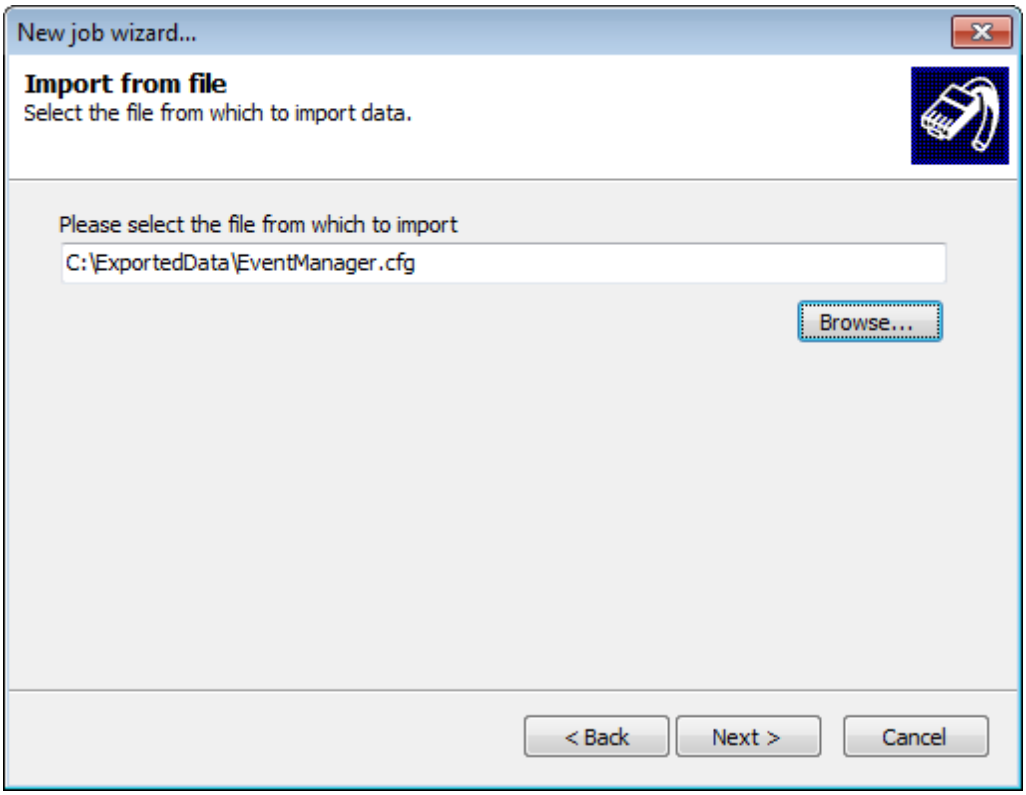
Screenshot 164: Creating Import\Export jobs

4. Select **Import\Export Job** and click **Next**.



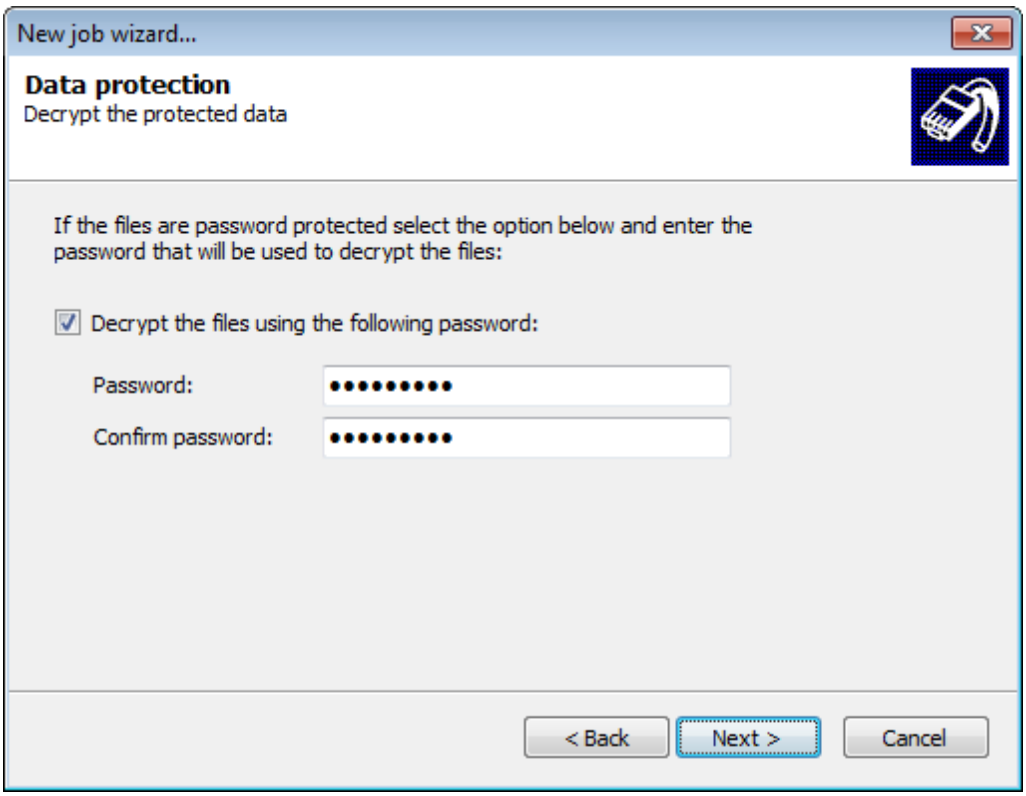
Screenshot 165: Import from file

5. Select **Import from file** and click **Next**.



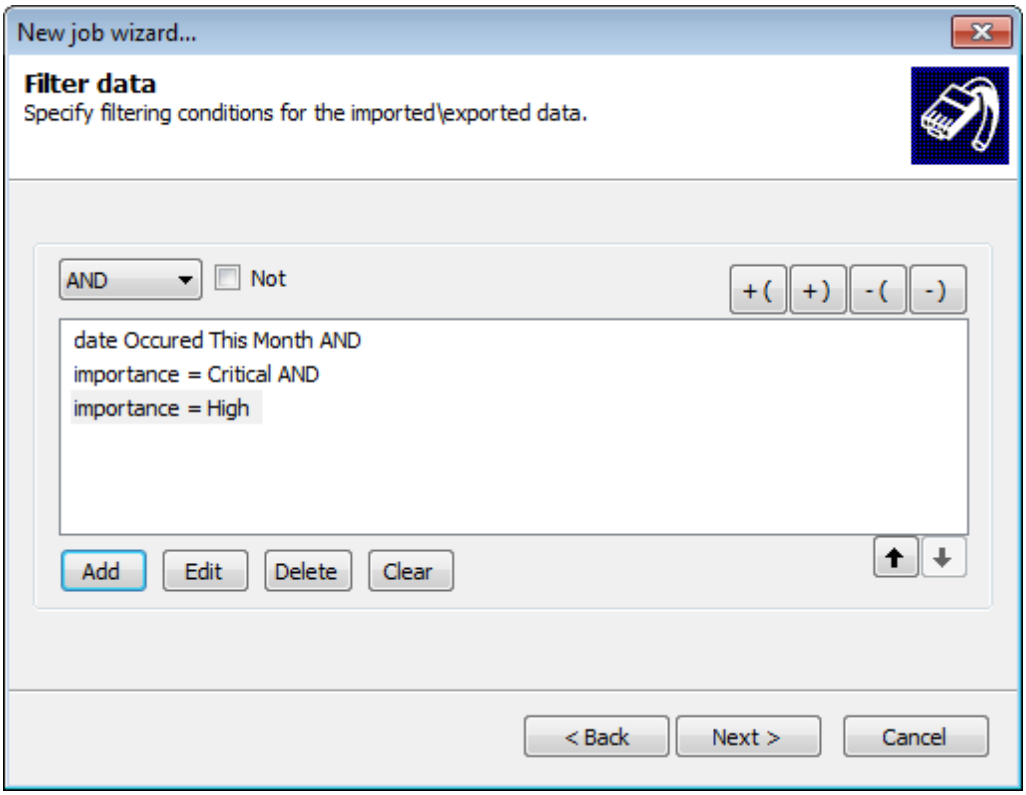
Screenshot 166: Import from file - Specify import file path

6. Specify the path to the file from which to import data, or click **Browse** to look for the location. Click **Next**.



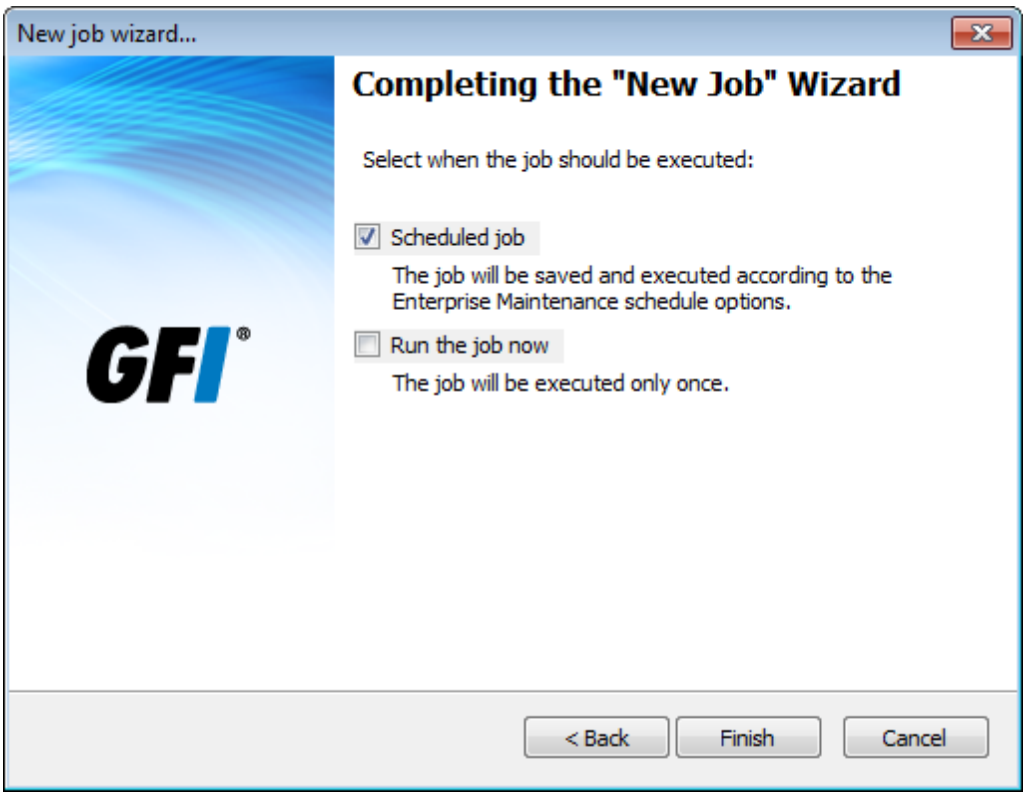
Screenshot 167: Decrypt secure import files

7. (Optional) If the file you are importing is encrypted, select **Decrypt the files using the following password** and specify the password used to encrypt the file. Click **Next**.



Screenshot 168: Add filtering conditions

8. Add filtering conditions to filter out unwanted data from the file. Leave blank to import all the event logs from the file. For more information, refer to Defining Restrictions. Click **Next**.



Screenshot 169: Specify when the job is executed

Select when the job is executed. The table below describes the available options:

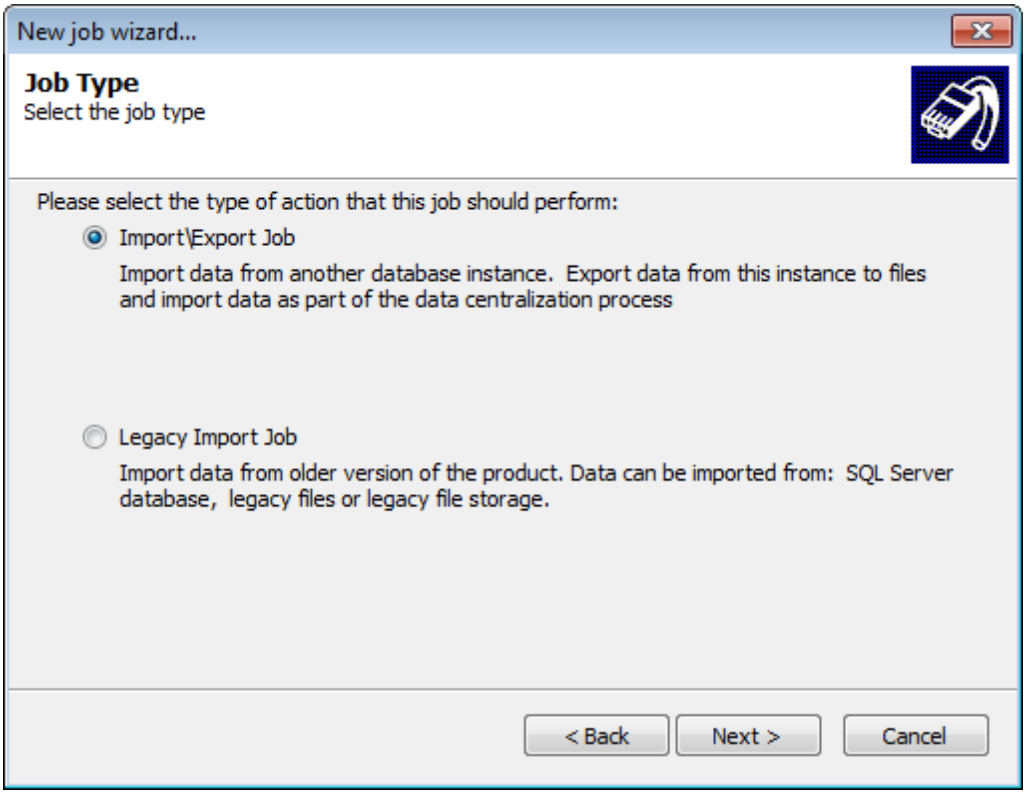
Table 78: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

9. Click **Finish**.

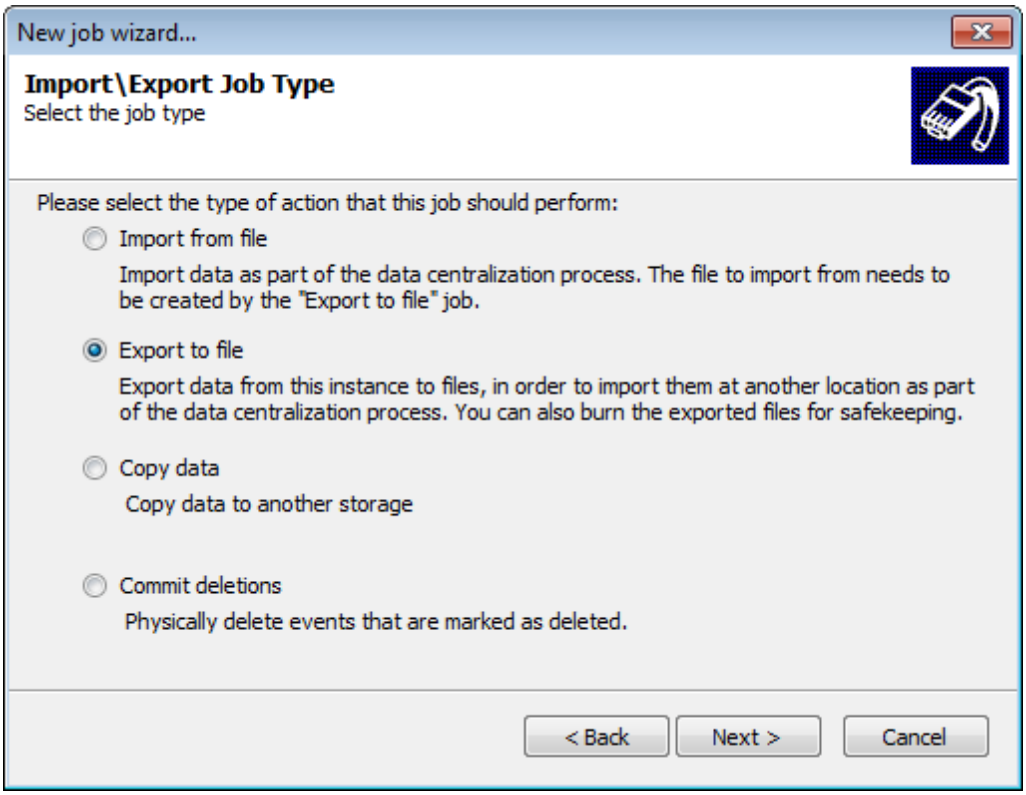
12.3.2 Export to file

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



Screenshot 170: Creating Import\Export jobs

4. Select **Import\Export Job** and click **Next**.

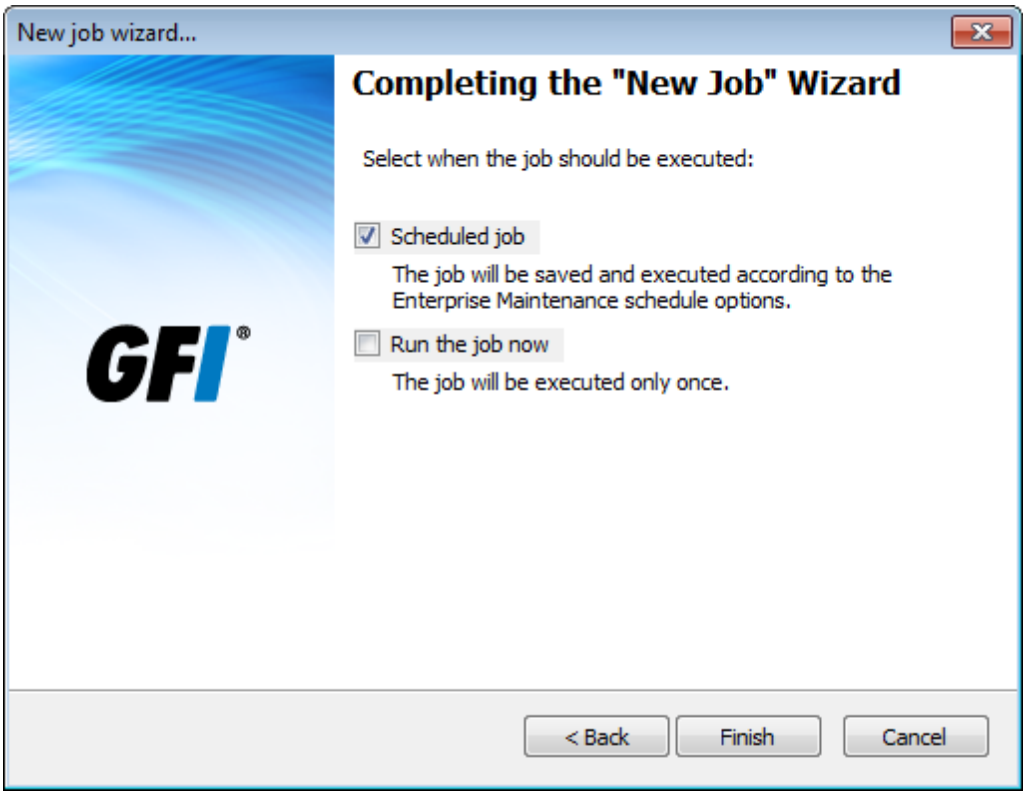


5. Select **Export to file** and click **Next**.

6. Specify the location where the exported files are saved to. Alternatively, click **Browse** to look for the location. Click **Next**.

7. (Optional) Select **Encrypt exported data using the following password** to secure the data you are exporting. Specify the encryption password and click **Next**.

8. (Optional) Add filtering conditions to export wanted events only by clicking **Add**. Leave blank to export every event log. For more information, refer to Defining Restrictions. Click **Next**.



Screenshot 171: Specify when the job is executed

Select when the job is executed. The table below describes the available options:

Table 79: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

9. Click **Finish**.

Export filename

The convention used by GFI EventsManager to name the export file is shown and described below:

```
[ESM ID]_[Job ID]_[Date From]_[Date To].EXP
```

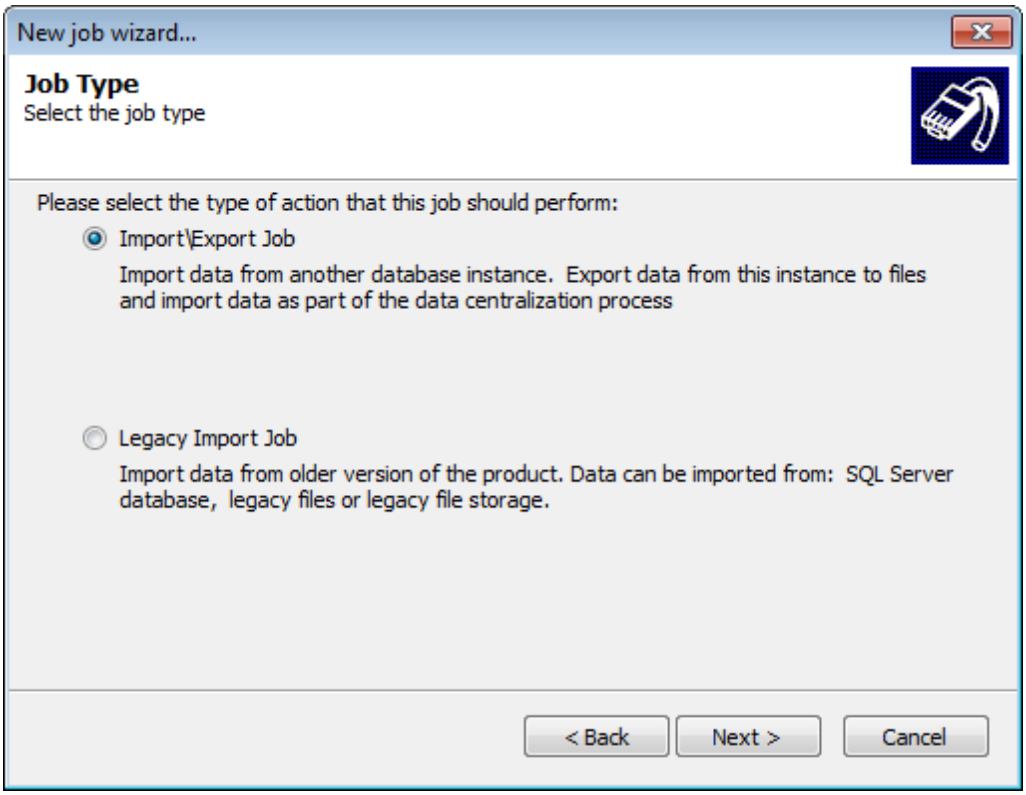
Table 80: Database operations: Export file name structure

Name Section	Description
ESM ID	Refers to the unique identifier given to each GFI EventsManager instance running in the organization.
Job ID	Refers to the unique identifier given to each maintenance job created.
Date From	Refers to the date of the earliest event exported.
Date To	Refers to the date of the latest event exported.
.EXP	This is the file extension given to all export files.

12.3.3 Copy data

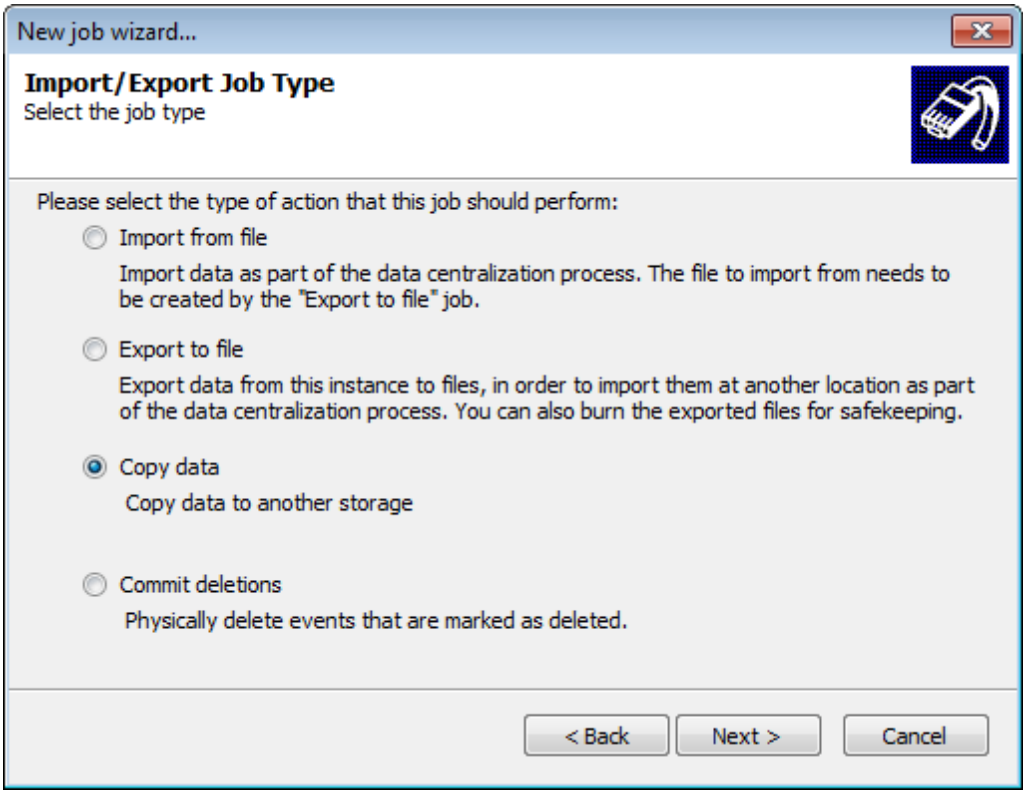
To create Copy data jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job**...
3. Click **Next** at the wizard welcome screen.



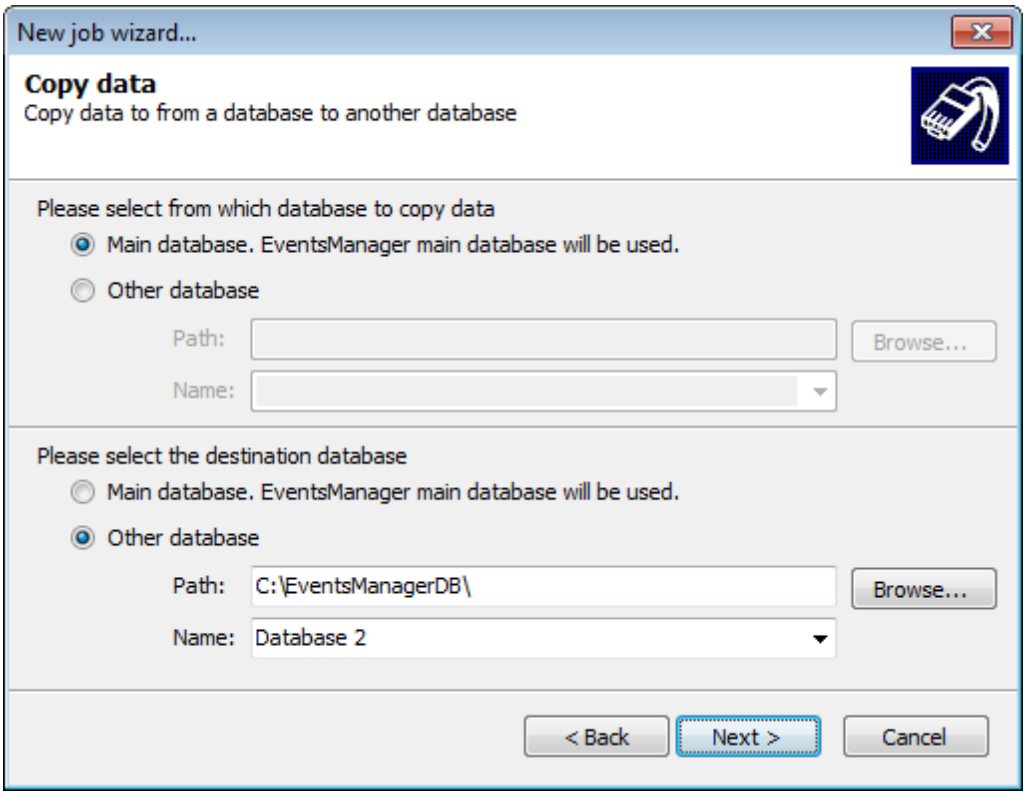
Screenshot 172: Creating Import\Export jobs

4. Select **Import\Export Job** and click **Next**.



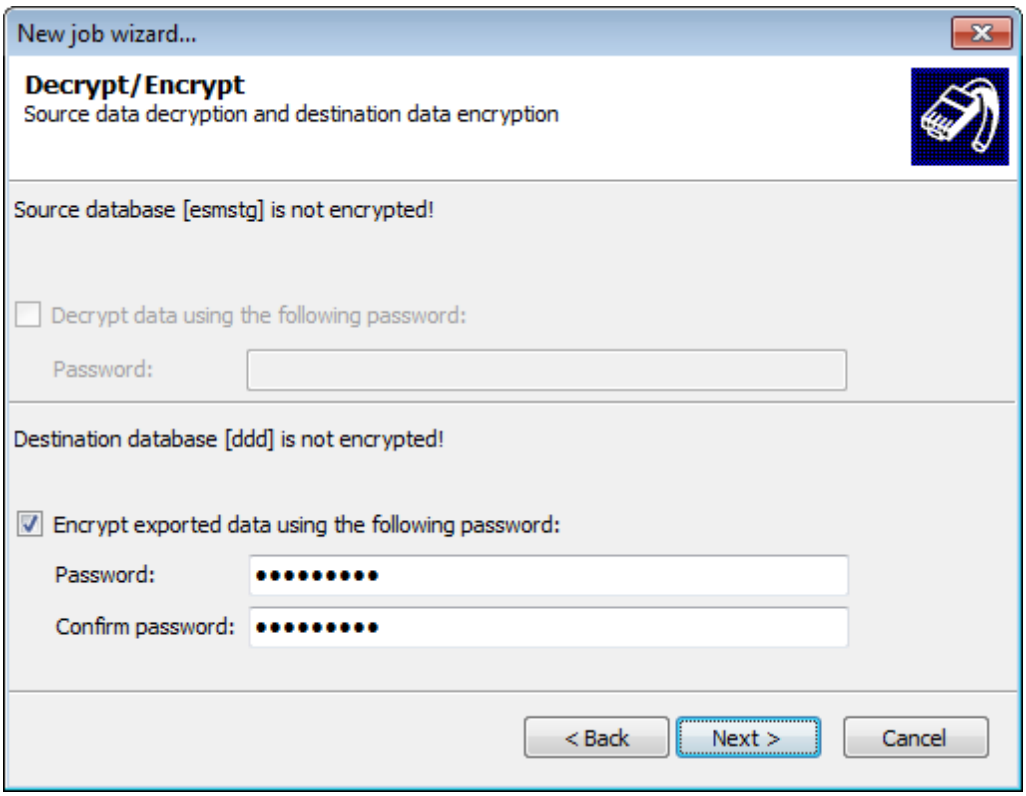
Screenshot 173: Select Copy data job

5. Select **Copy data** and click **Next**.



Screenshot 174: Specify source and destination databases

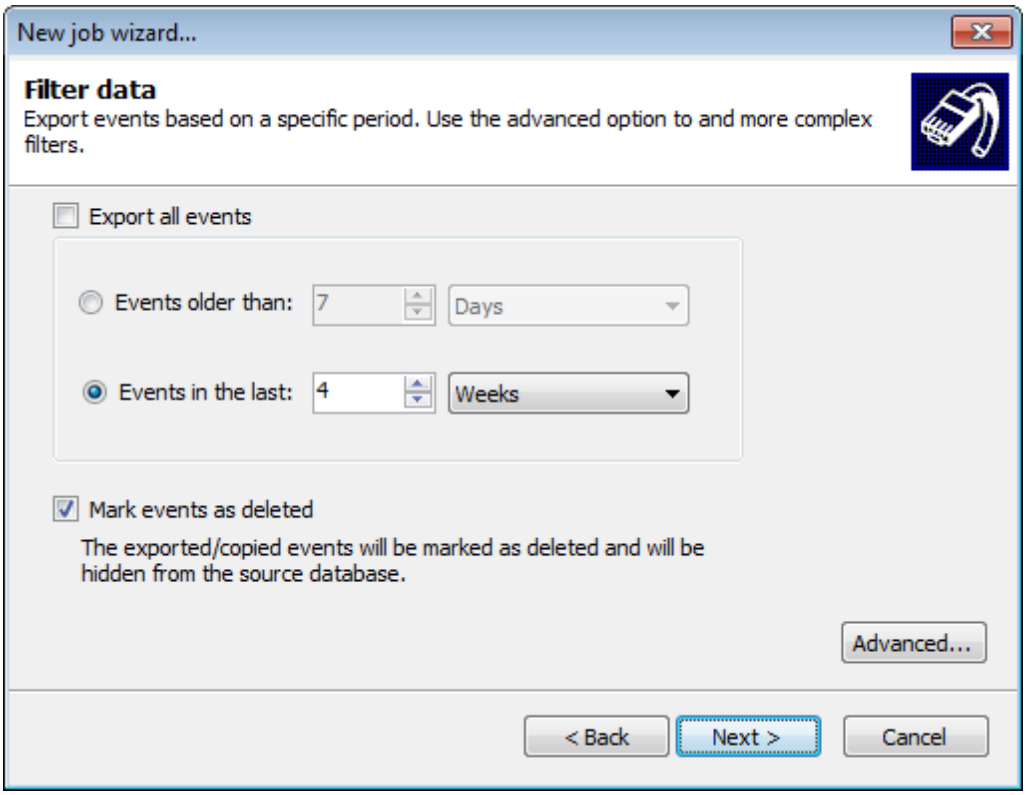
6. Select the source and destination databases. Click **Next**.



Screenshot 175: Decrypt source and encrypt destination databases

7. If the source database is encrypted, select **Decrypt data using the following password** and specify the password used to encrypt the database.

8. If you want to encrypt the source data, select **Encrypt exported data using the following password**. Specify the encryption password and click **Next**.

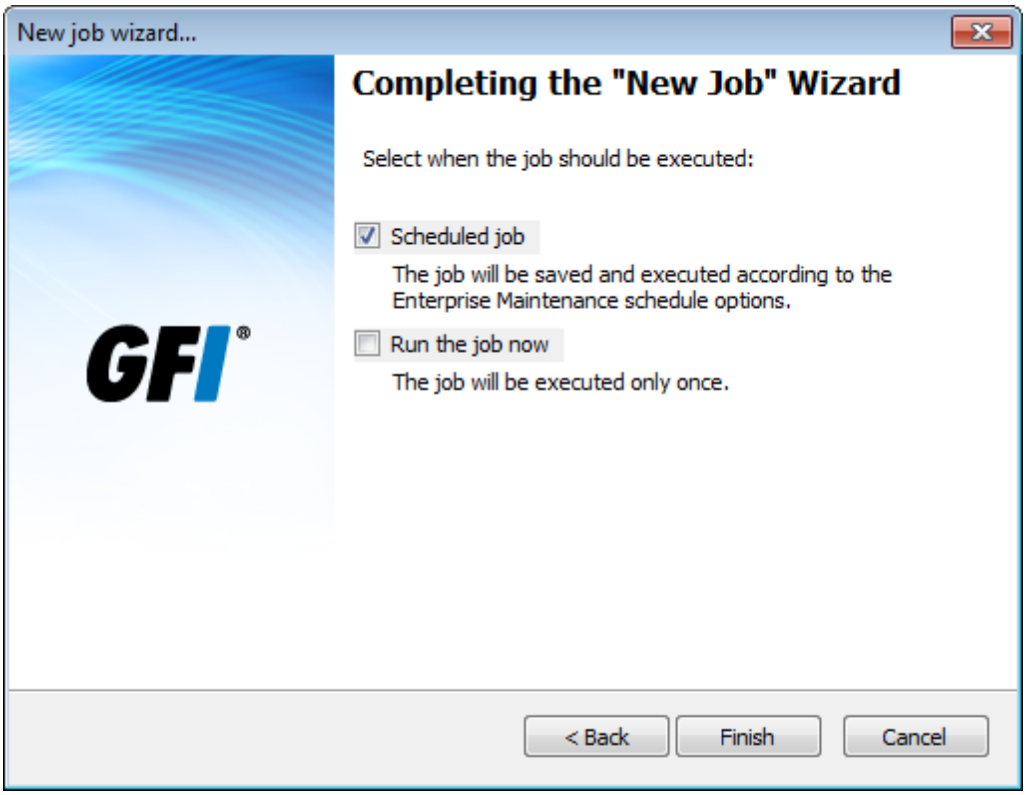


Screenshot 176: Filter exported logs

9. (Optional) Unselect **Export all events**, configure the options described below and click **Next**:

Table 81: Copy data - Export options

Option	Description
Events older than	Select this option to export only events older than the specified number of days, weeks or months.
Events in the last	Select this option to export only events that occurred in the last number of specified days, weeks or months.
Mark events as deleted	Select Mark events as deleted to flag the as deleted from the source database. **NOTE** By doing so, you will only hide exported events from the database. To commit deletions, run a **Commit deletions** job on the source database. For more information, refer to Commit deletions (page 213).
Advanced...	Click **Advanced...** to launch the filtering conditions dialog. For more information, refer to Defining restrictions (page 126).



Screenshot 177: Specify when the job is executed

Select when the job is executed. The table below describes the available options:

Table 82: Creating maintenance jobs - Schedule options

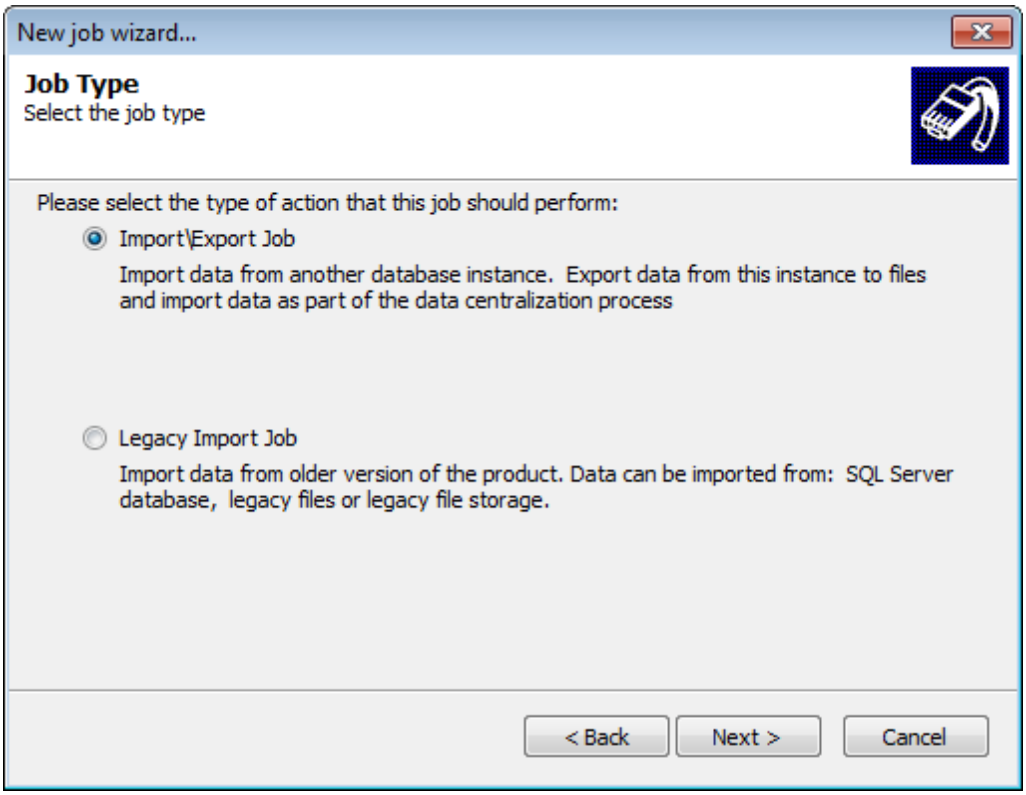
Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

10. Click **Finish**.

12.3.4 Commit deletions

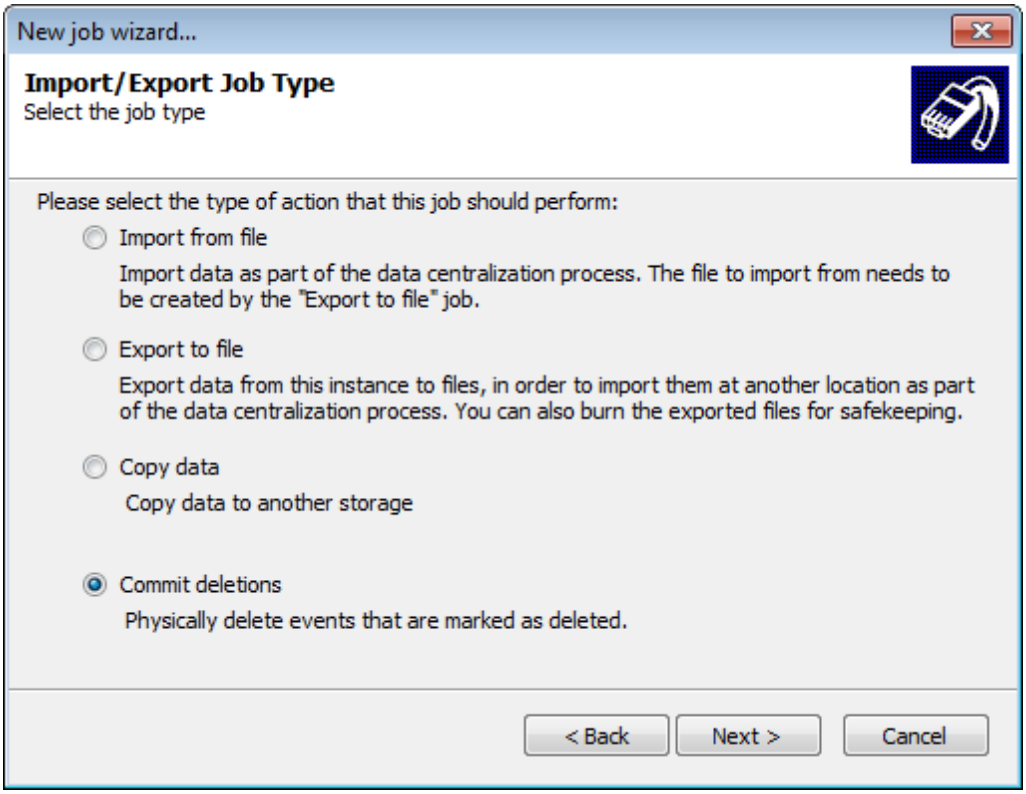
To create Commit deletions jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



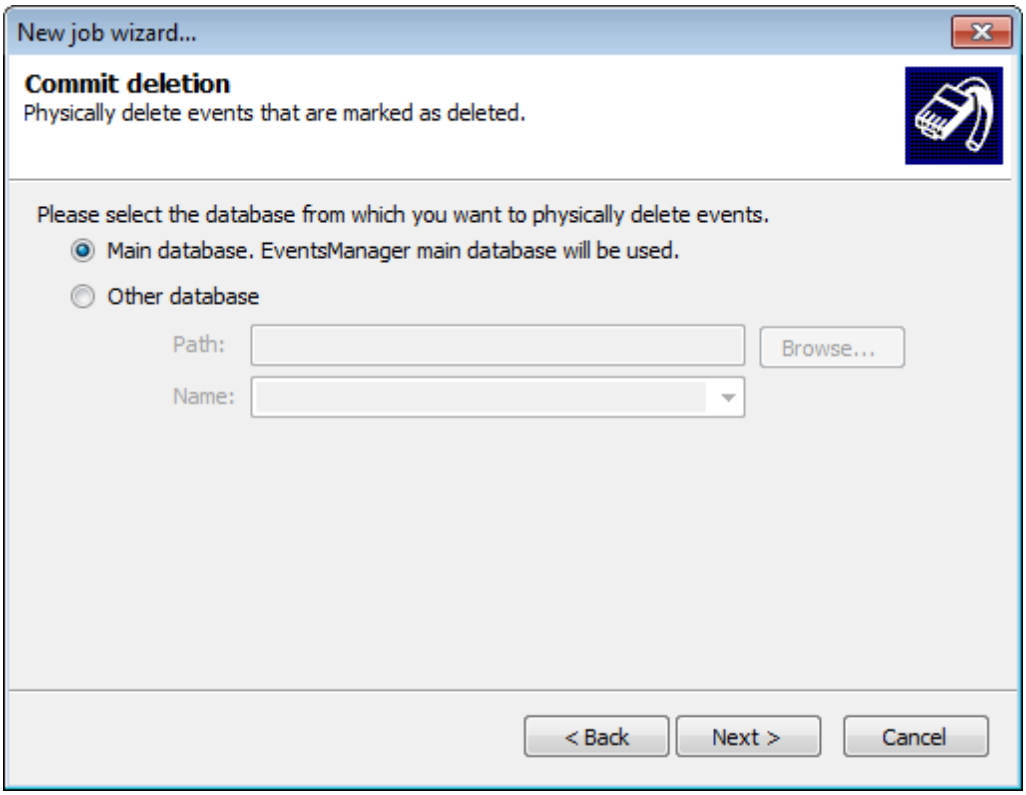
Screenshot 178: Creating Import\Export jobs

4. Select **Import\Export Job** and click **Next**.



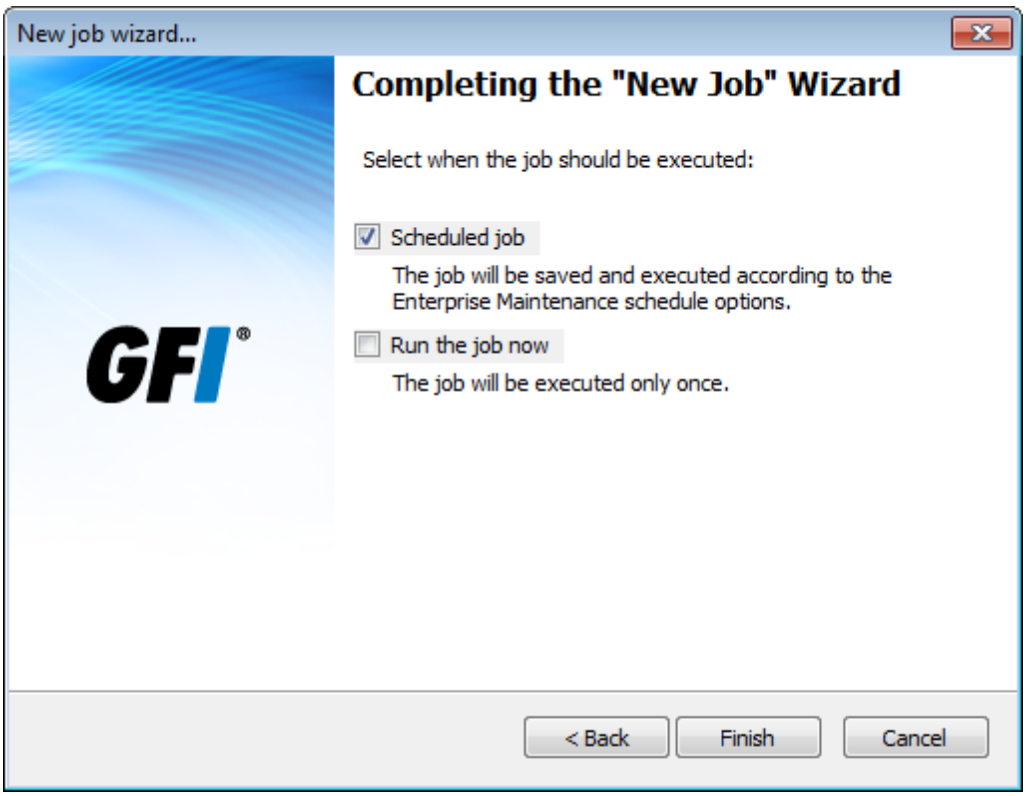
Screenshot 179: Create commit deletion jobs

5. Select **Commit deletions** and click **Next**.



Screenshot 180: Select database to delete records from

6. Select the database to delete records from. Click **Next**.



Screenshot 181: Specify when the job is executed

Select when the job is executed. The table below describes the available options:

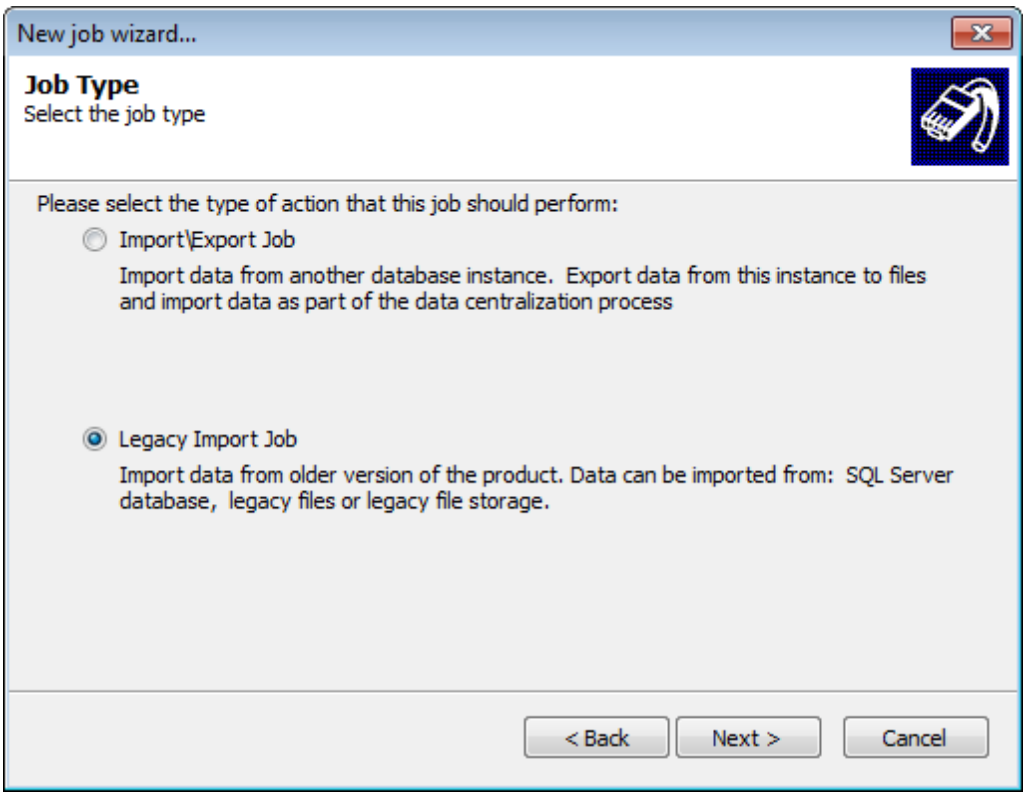
Table 83: Creating maintenance jobs - Schedule options

Options	Description
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

7. Click **Finish**.

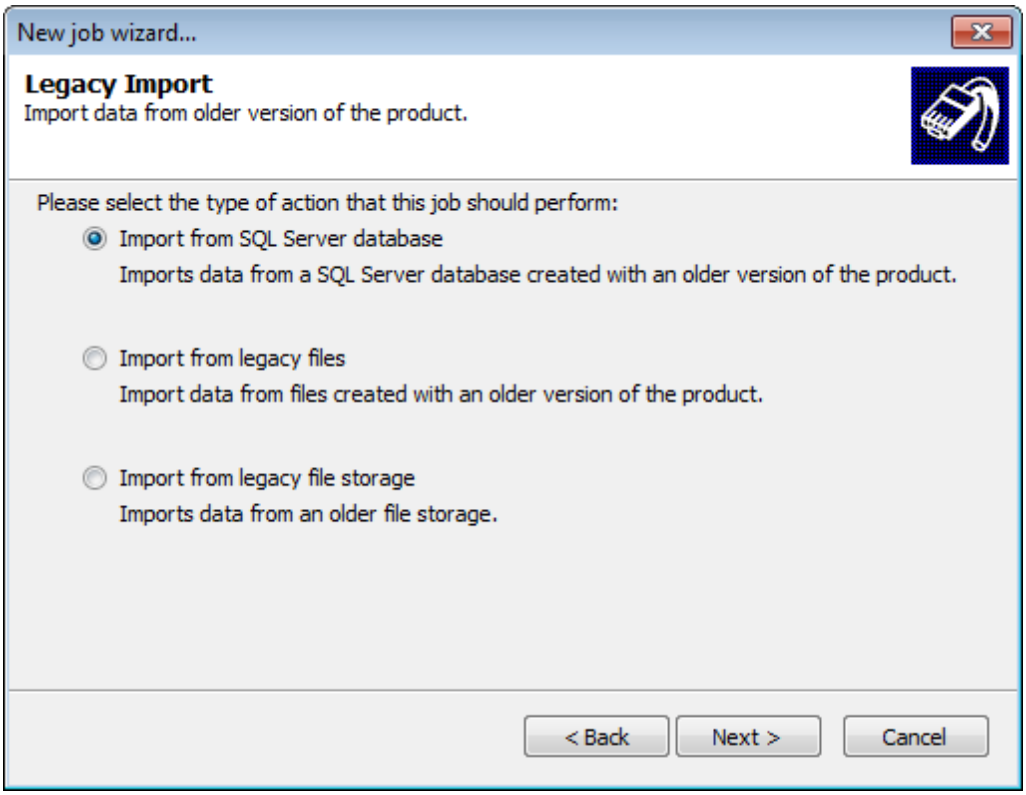
12.3.5 Import from SQL Server Database

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



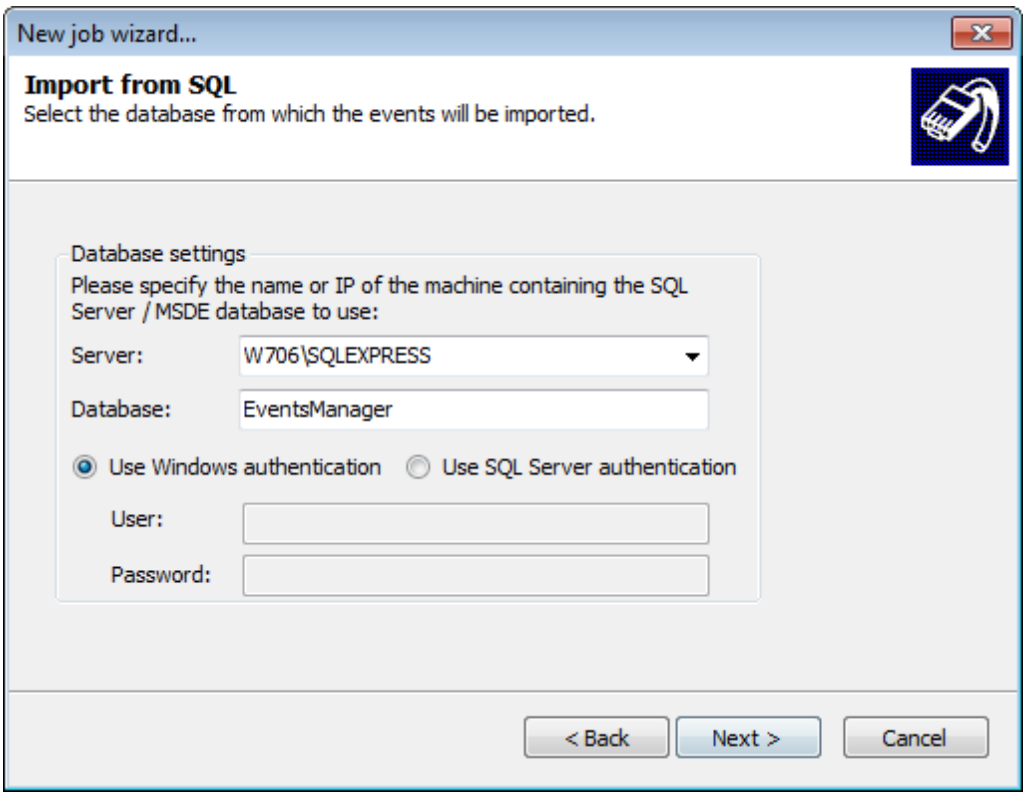
Screenshot 182: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.



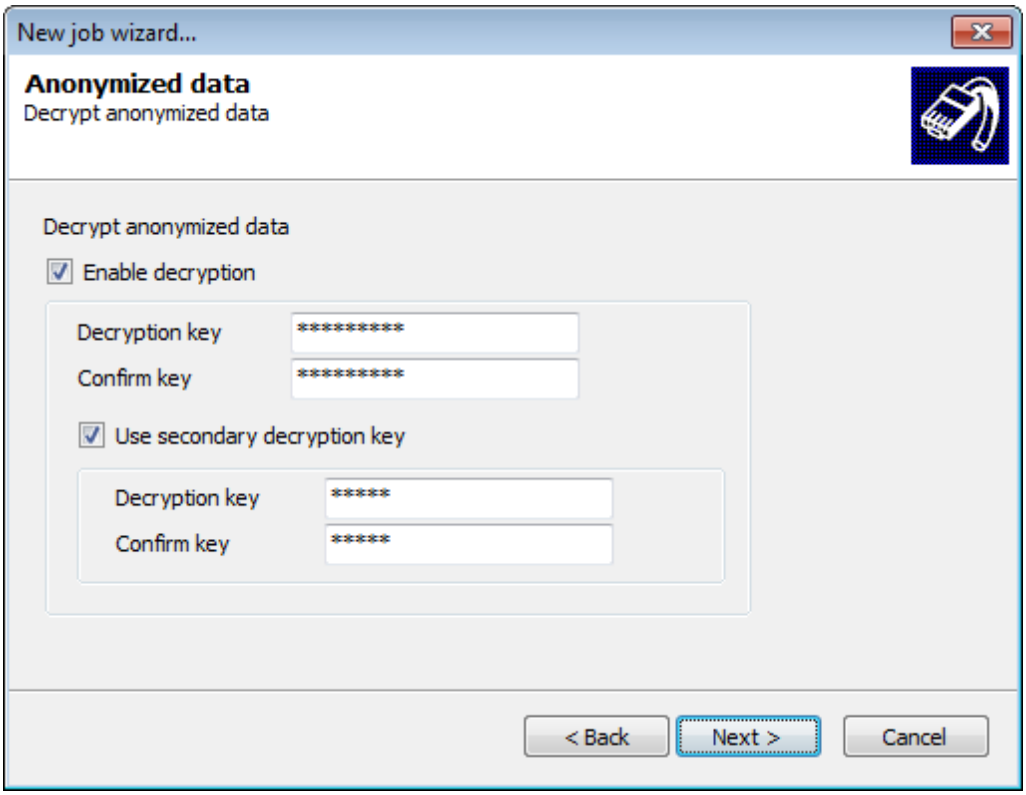
Screenshot 183: Select Import from SQL Server Database

5. Select **Import from SQL Server database** and click **Next**.



Screenshot 184: Specify SQL Server address and login details

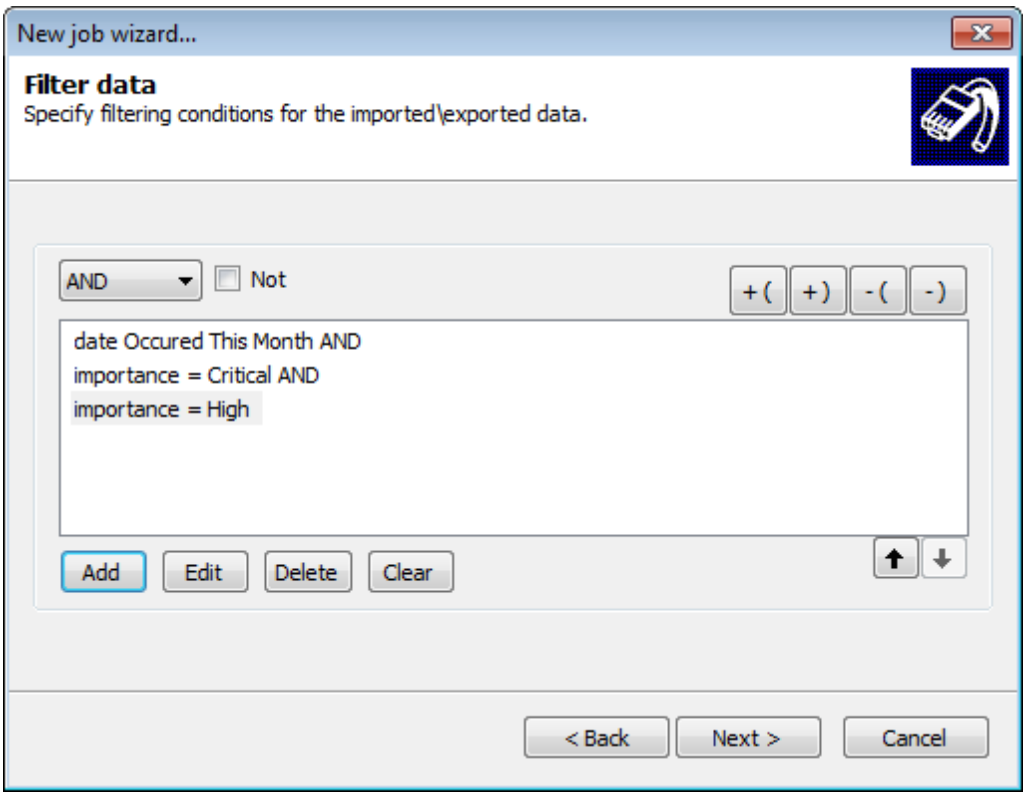
6. Specify the database settings including server address, database name and authentication mode. Click **Next**.



Screenshot 185: Decrypt anonymized databases

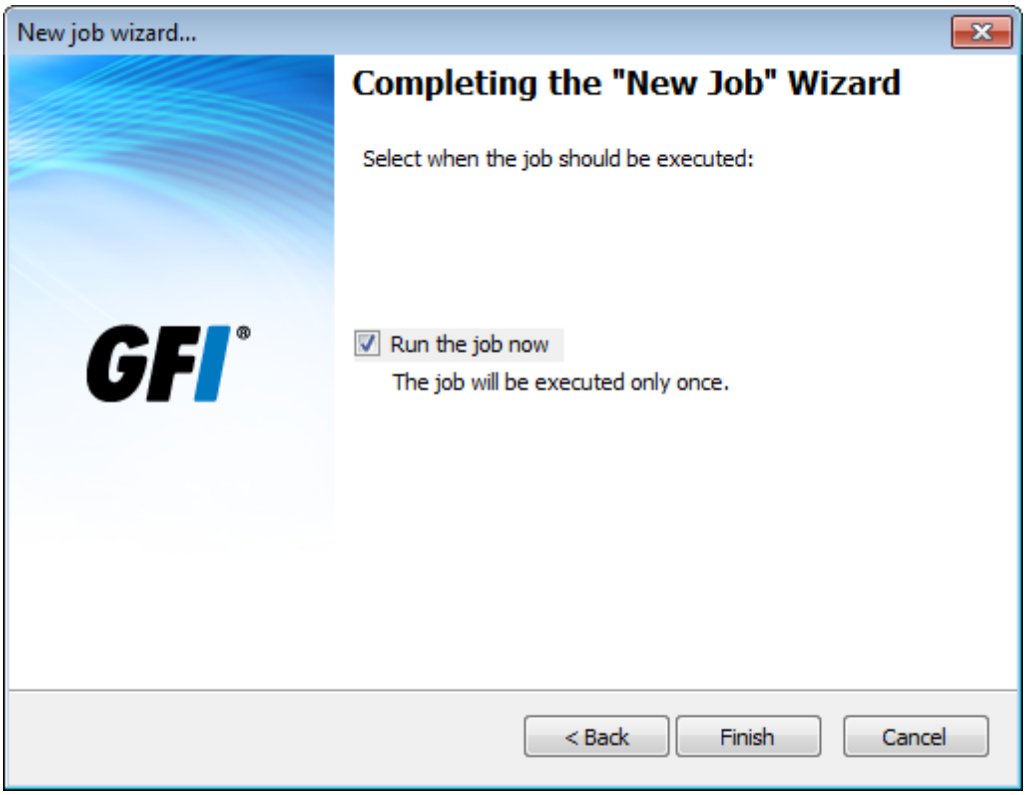
7. (Optional) If the SQL Server database is anonymized, select **Enable decryption** and specify the password used to anonymize the database.

8. (Optional) If the SQL Server database was anonymized using two password, select **Use secondary decryption key** and specify the second security password used to anonymize the database. Click **Next**.



Screenshot 186: Add filtering conditions to filter unwanted data

9. (Optional) Add filtering conditions to import wanted data only. Leave blank to import every event log in the database. For more information, refer to Defining Restrictions. Click **Next**.



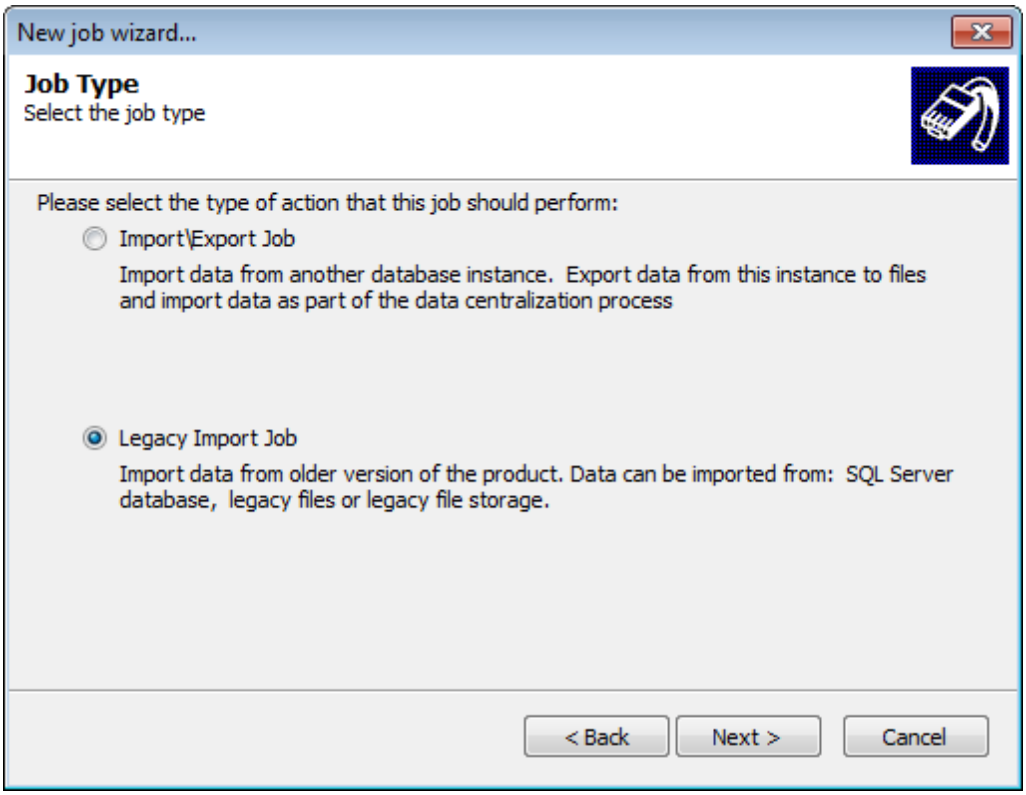
Screenshot 187: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

12.3.6 Import from legacy files

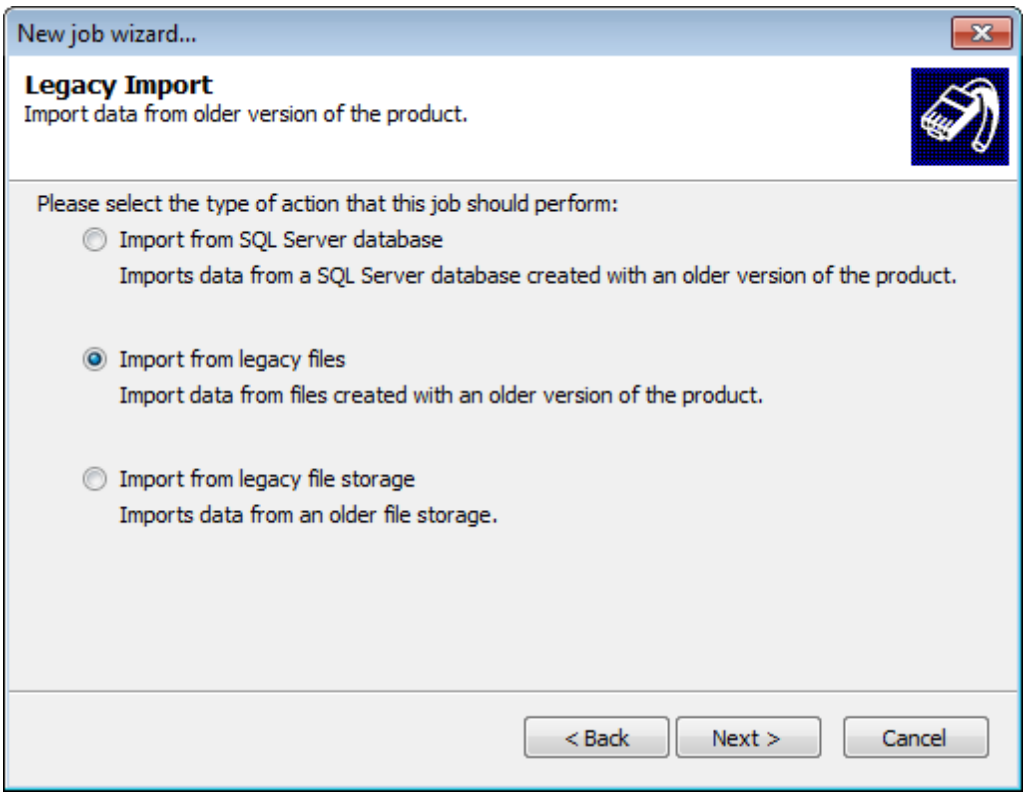
To create Import from legacy files jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



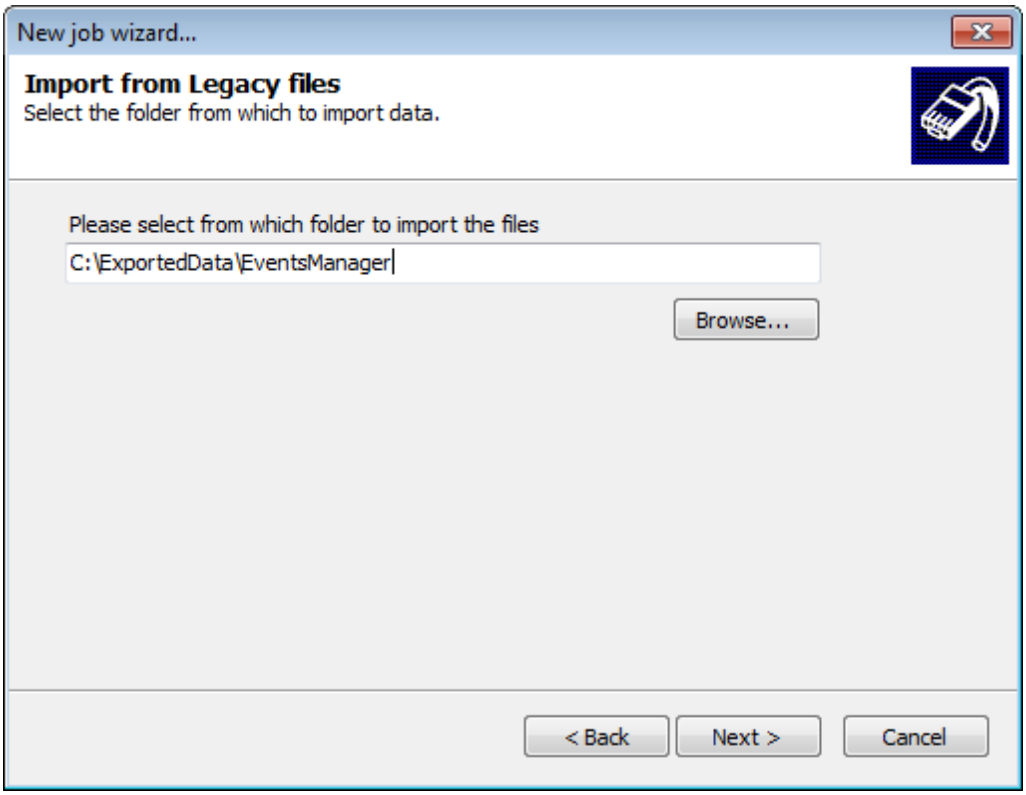
Screenshot 188: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.



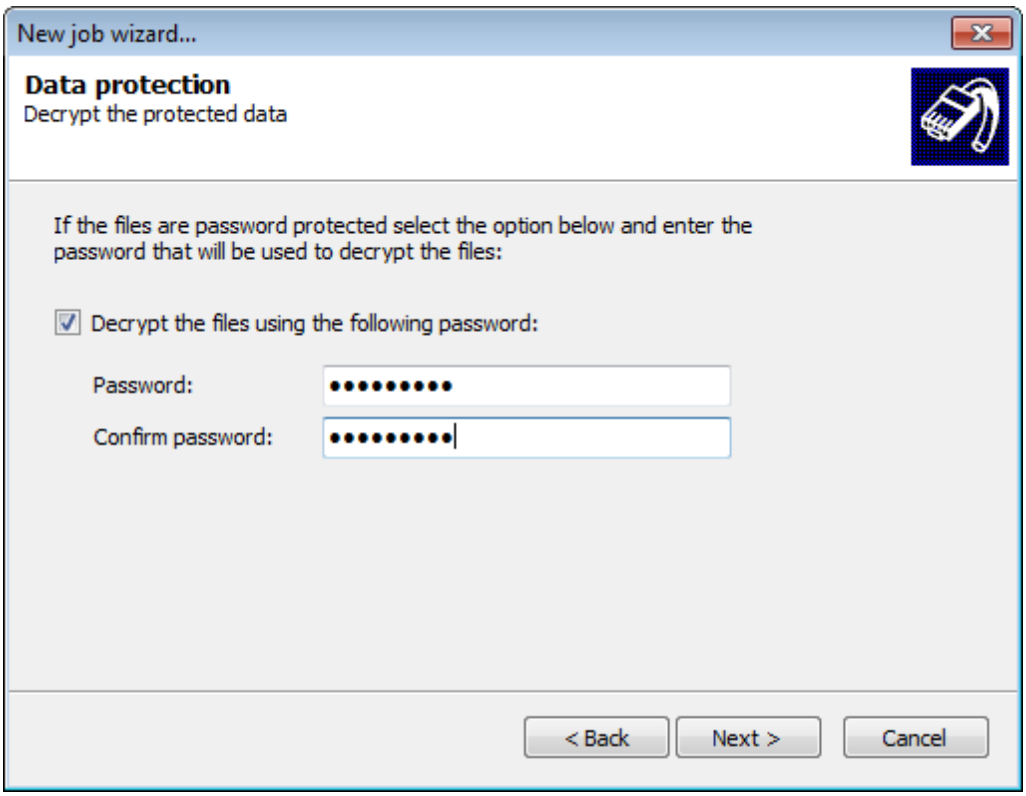
Screenshot 189: Import from legacy files

5. Select **Import from legacy files** and click **Next**.



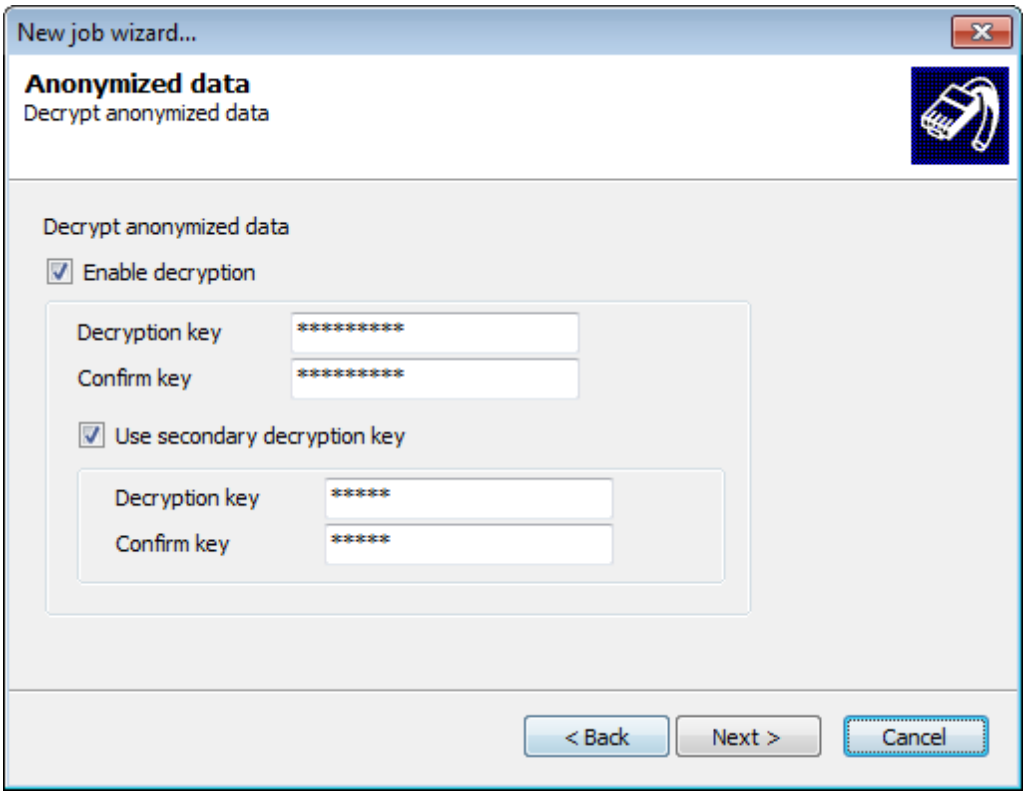
Screenshot 190: Specify import file location

6. Specify the path to the file from which to import data, or click **Browse** to look for the location. Click **Next**.



Screenshot 191: Decrypt the information in the import file

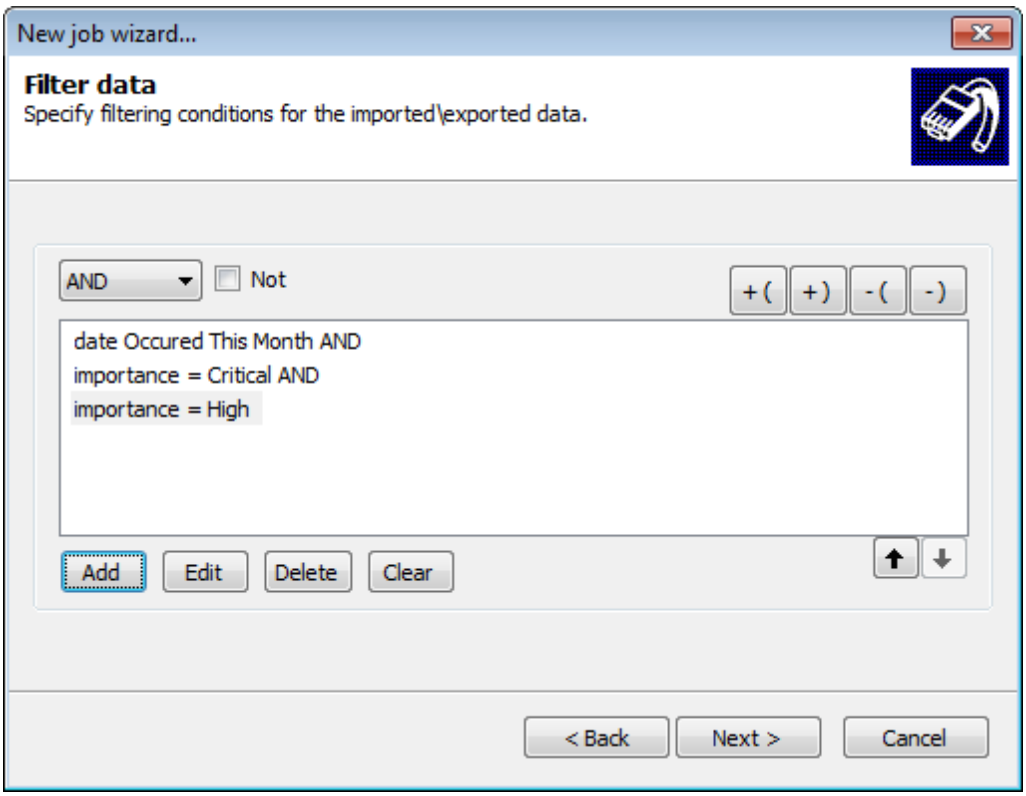
7. (Optional) If the file was encrypted, select **Decrypt the files using the following password** and specify the password used to encrypt the file. Click **Next**.



Screenshot 192: Remove anonymization

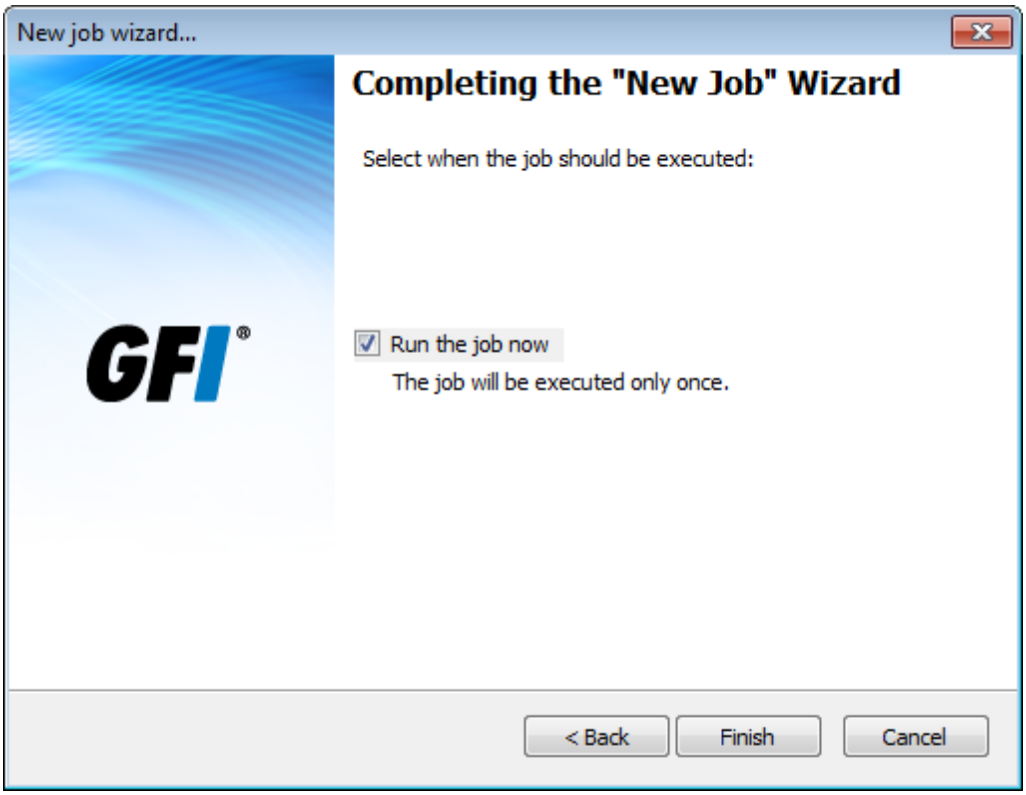
8. (Optional) If the file is anonymized, select **Enable decryption** and specify the password used to anonymize the data.

9. (Optional) If the file was anonymized using two passwords, select **Use secondary decryption key** and specify the second key used to anonymize the data within the file. Click **Next**.



Screenshot 193: Filter unwanted events through filtering conditions

10. (Optional) Add filtering conditions to filter unwanted events. Leave blank to import every event log from the file. For more information, refer to Defining Restrictions.



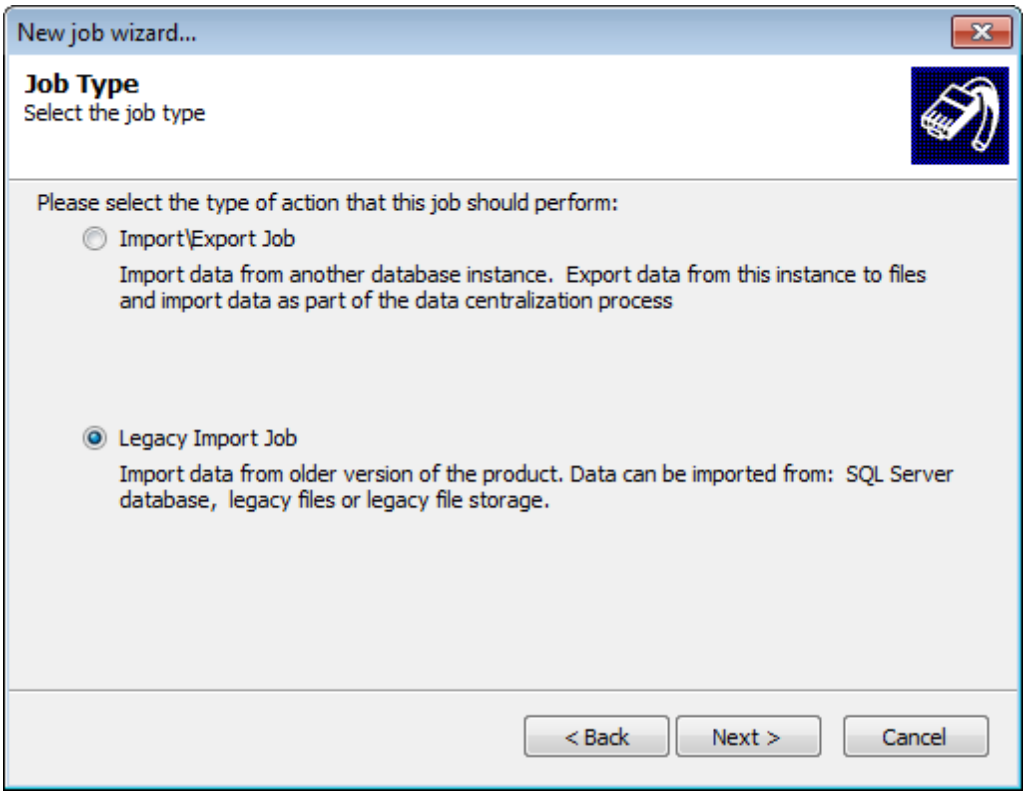
Screenshot 194: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

12.3.7 Import from legacy file storage

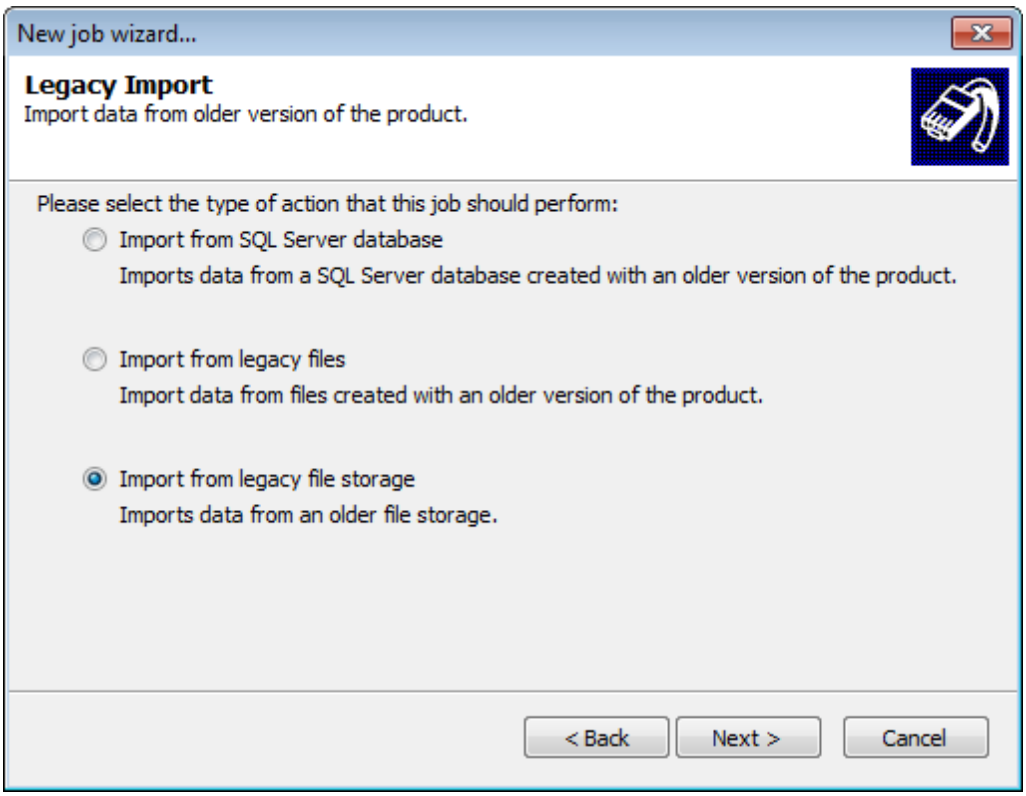
To create Import from legacy files jobs:

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click **Database Operations** node and select **Create new job…**
3. Click **Next** at the wizard welcome screen.



Screenshot 195: Creating Import\Export jobs

4. Select **Legacy Import Job** and click **Next**.



Screenshot 196: Import legacy file storage data

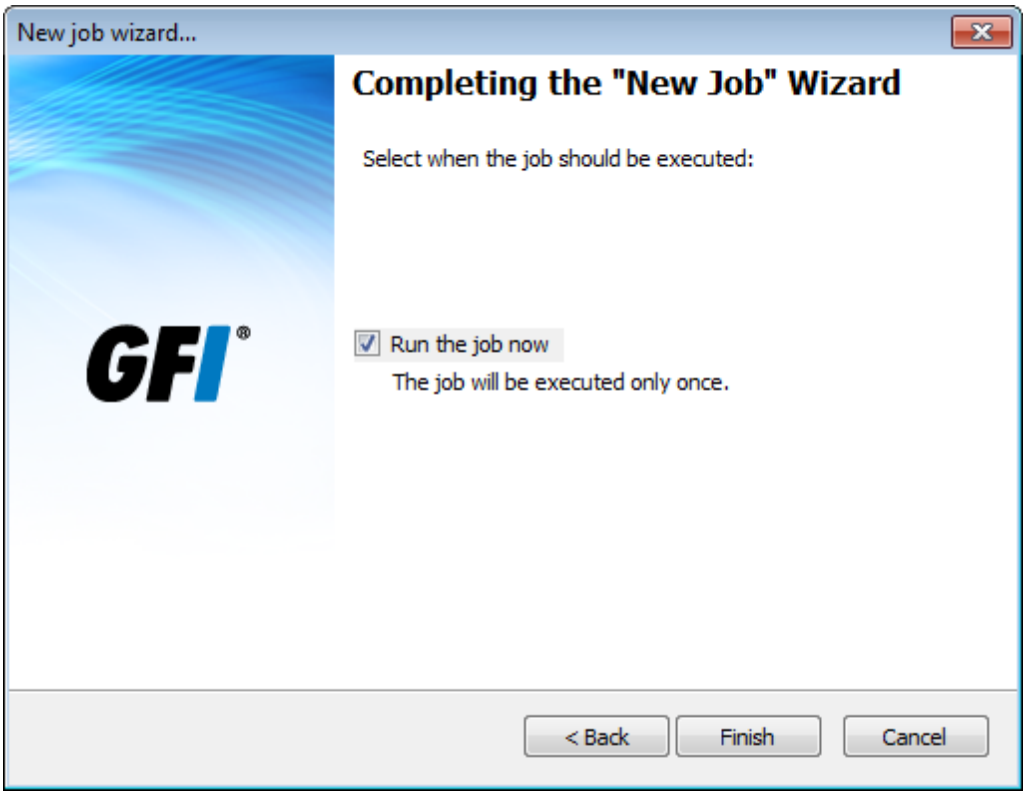
5. Select **Import from legacy file storage** and click **Next**.

6. Specify the path to where the import file is located. Alternatively, click **Browse** and look for the location.

7. (Optional) If the data is anonymized, select **Enable decryption** and specify the password used to encrypt the data.

8. (Optional) If the data is encrypted by two passwords, select **Use secondary decryption** key and key in the secondary password. Click **Next**.

9. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. For more information, refer to Defining Restrictions. Click **Next**.



Screenshot 197: Specify when the maintenance job is executed

Select **Run the job now** and click **Finish**.

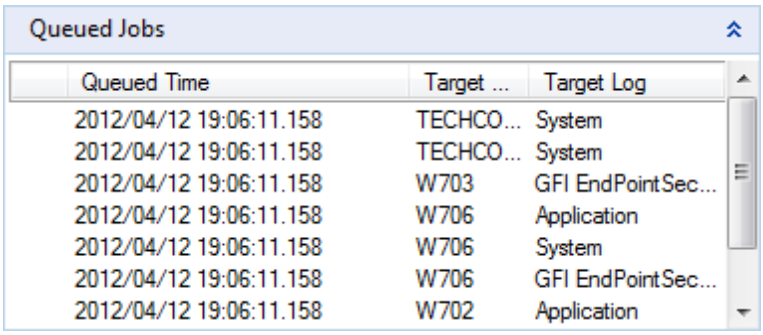
12.4 Editing maintenance jobs

This section contains information about:

- Viewing scheduled maintenance jobs
- Editing maintenance job properties
- Changing maintenance jobs priority
- Deleting a maintenance job

12.4.1 Viewing scheduled maintenance jobs

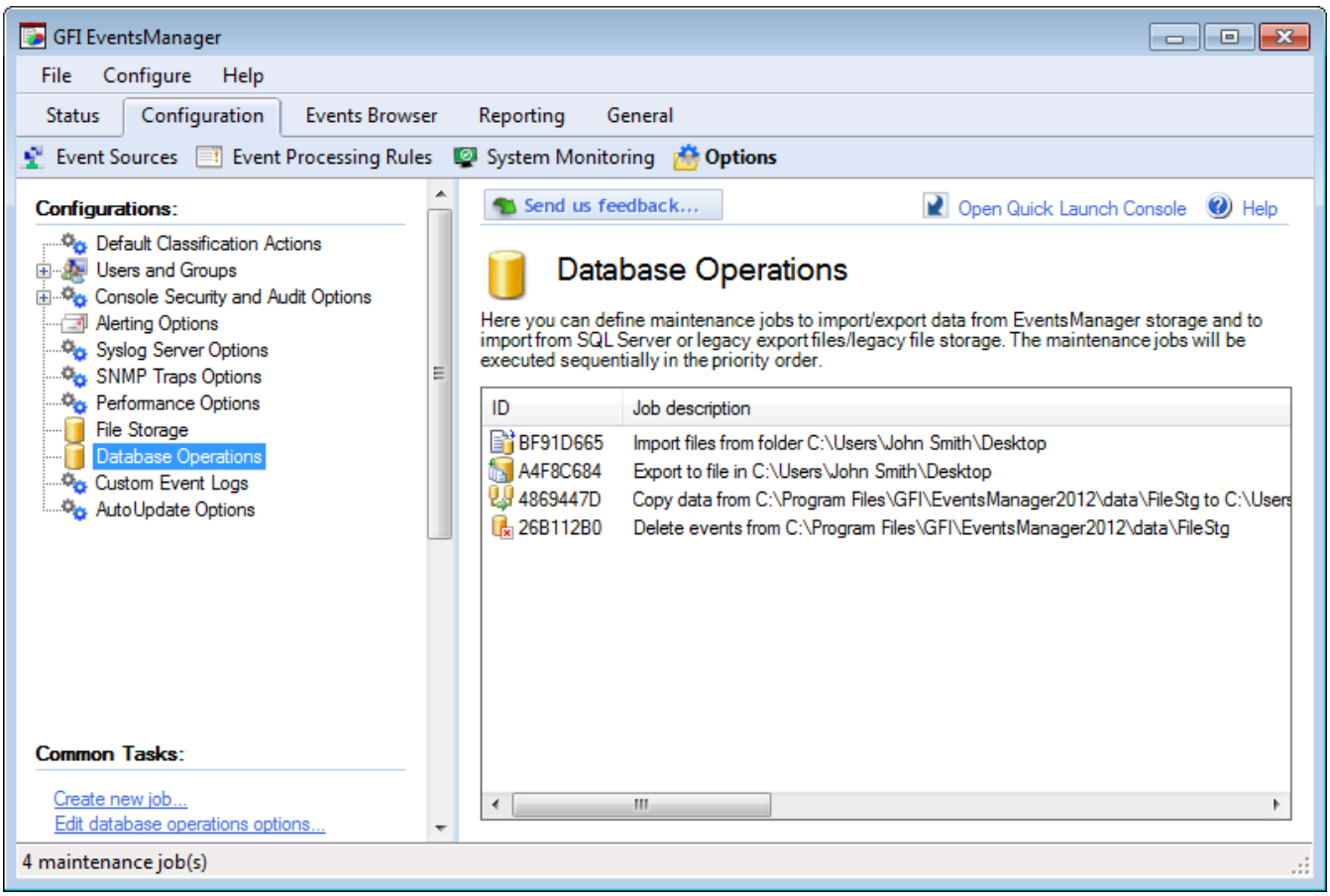
To view the progress of scheduled maintenance jobs:



Screenshot 198: Maintenance job activity

Click **Status** tab > **Job Activity**. The status of all maintenance jobs will be displayed in the **Queued Jobs** section.

To view created maintenance jobs:



Screenshot 199: Viewing scheduled maintenance jobs

1. Click **Configuration** tab and select **Options**.

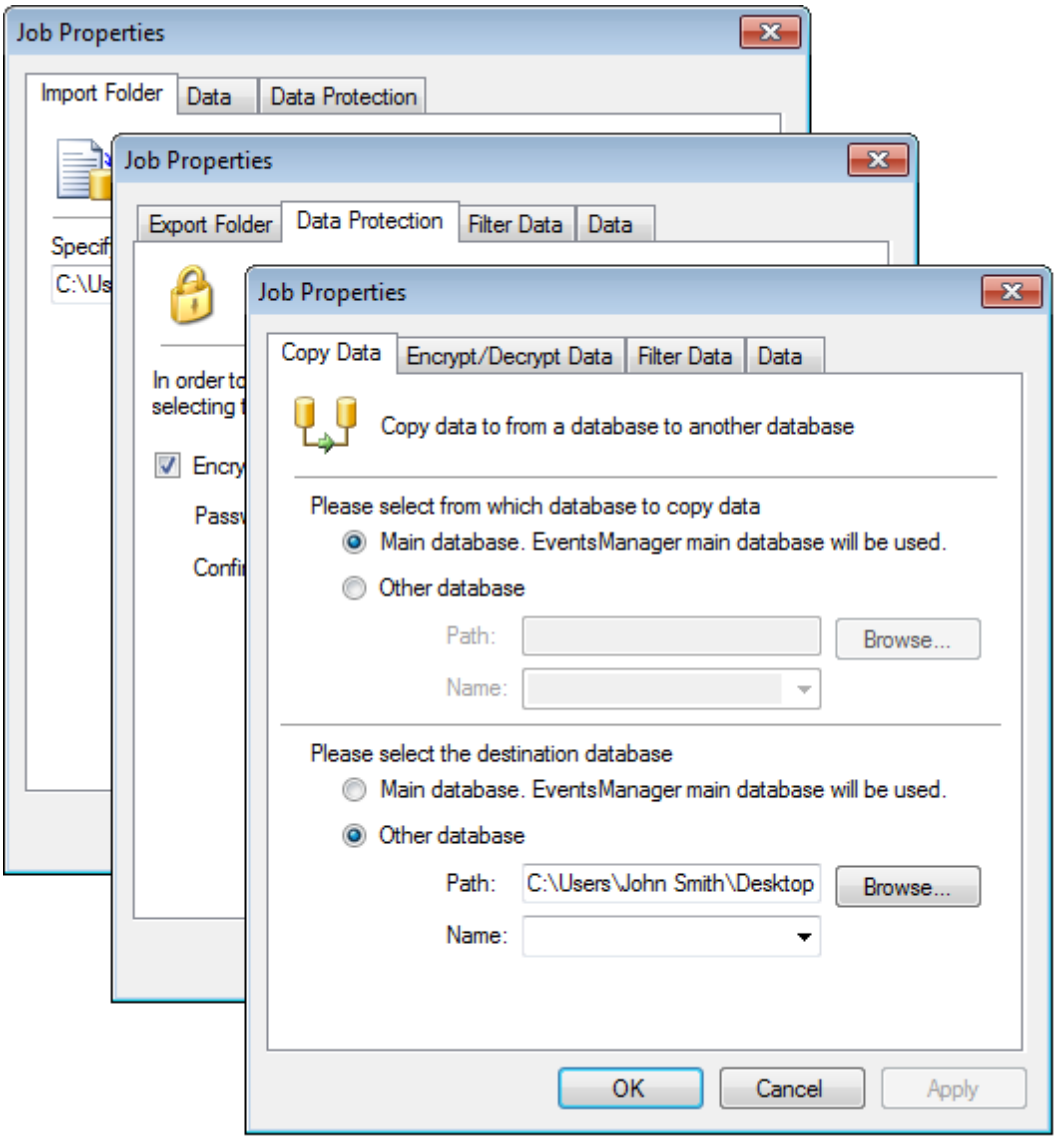
2. From **Configurations**, select the **Database Operations** node. Scheduled maintenance jobs are displayed in the right pane.

12.4.2 Editing maintenance job properties

To edit maintenance jobs properties:

1. From **Configuration** tab > **Options** > **Configurations**, click **Database Operations**.

2. From the right pane, right-click on a maintenance job and select **Properties**.



Screenshot 200: Maintenance job properties dialog

3. From the Job Properties dialog, you can modify the settings you configured while creating the job; such as:

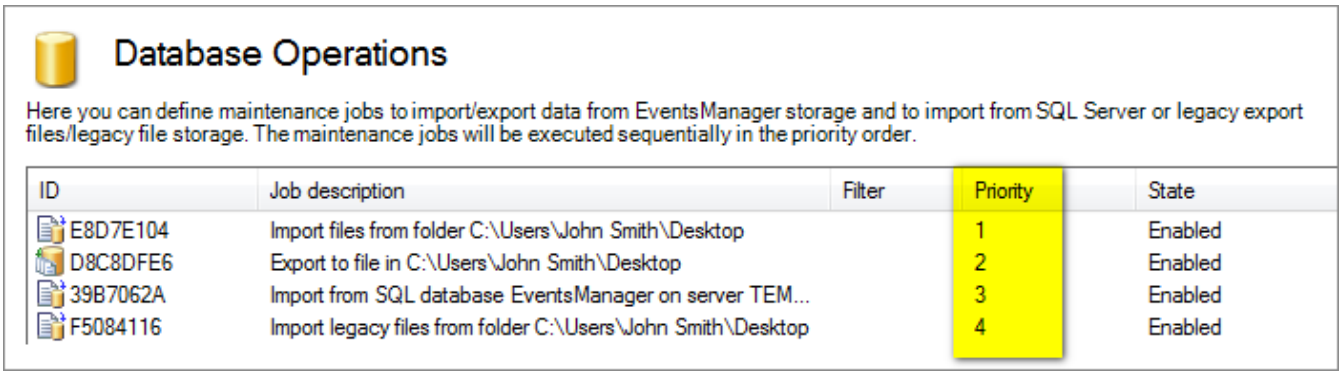
- Encryption/decryption passwords
- Database names and addresses
- Source/destination paths
- General job details.

4. Click **Apply** and **OK**.

Note

For more information, refer to Creating maintenance jobs (page 203).

12.4.3 Changing maintenance jobs priority



Screenshot 201: Maintenance job priorities

By default maintenance jobs are executed according to the sequence with which the jobs are created (First-in-First-out). Thus the priority of maintenance jobs is determined by the sequence in which jobs are executed.

To increase or decrease the priority of a maintenance job:

1. Click **Configuration** tab and select **Options**.

2. From **Configurations**, select **Database Operations** node.

3. From the right pane, right-click the maintenance job and select **Increase Priority** or **Decrease Priority** accordingly.

12.4.4 Deleting a maintenance job

To delete maintenance jobs:

1. Click **Configuration** tab and select **Options**.

2. From **Configurations**, select **Database Operations** node.

3. From the right pane, right-click on the maintenance job to delete and select **Delete**.

> **Note**
>
> Before deleting maintenance jobs ensure that all data is backed up.

13 Configuring the Management Console

This chapter provides you with information about configuring general settings of GFI EventsManager, such as product licensing, performance options and product updates.

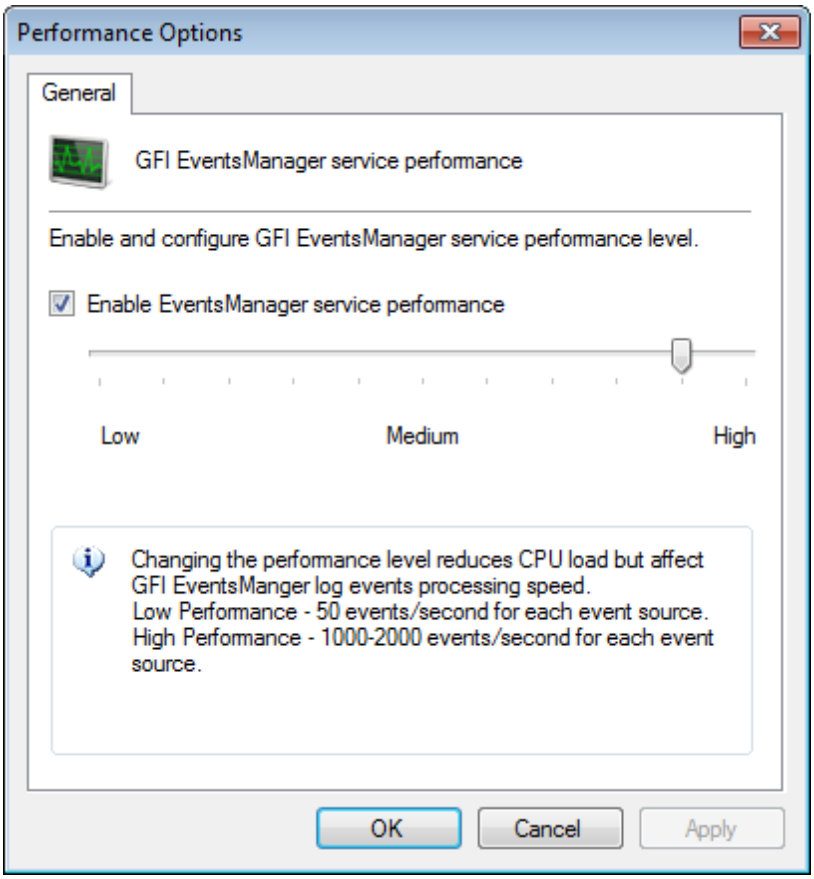
Topics in this chapter:

13.1 Performance options

GFI EventsManager provides you with options which enable you to set the performance level of the GFI EventsManager service.

To configure the performance level:

1. From **Configuration** tab **> Options > Configurations**, right-click **Performance Options** and select **Edit Performance Options**.



Screenshot 202: GFI EventsManager Performance Options

2. Select/Unselect **Enable EventsManager service performance** to enable/disable service performance options.

3. Move the slider left (low) to right (high) until you reach the required performance level.

4. Click **Apply** and **OK**.

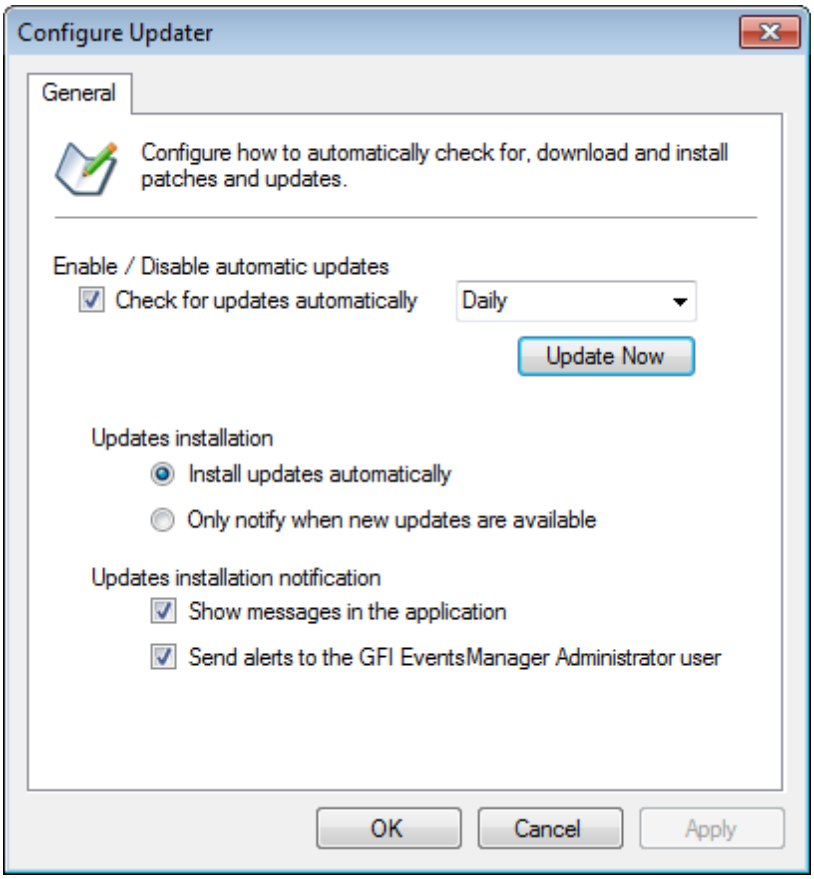
> **Note**
>
> Setting the performance level on **low** is estimated to process **50 events per second per event source**, while setting the bar on **high** processes **1,000 - 2,000 events per second per event source**.

13.2 Product updates

GFI EventsManager enables users to configure how to automatically check for, download and install product updates.

To configure Auto Update options:

1. From **Configuration** tab **>** **Options** **>** **Configurations**, right-click **Auto Update Options** and select **Edit updater options...**



Screenshot 203: Configure auto update

3. Configure the options described below:

Table 84: Auto update options

Options	Description
Check for updates automatically	If selected, GFI EventsManager will check for updates automatically on a daily or weekly basis.
Update Now	If **Check for updates automatically** is not selected, use this option to manually check for updates and install missing updates.
Install updates automatically	Installs downloaded updates automatically.
Only notify me when updates are available	Available updates are shown in the **Missing Updates** section but are not installed.
Show messages in the application	Shows a message at the bottom of the application page. Click on the displayed message to action the updates.
Send alerts on GFI EventsManager Administrator user	Sends an email alert on the configured GFI EventsManagerAdministrator account. For more information, refer to Configuring the administrator account (page 163).

4. Click **Apply** and **OK**.

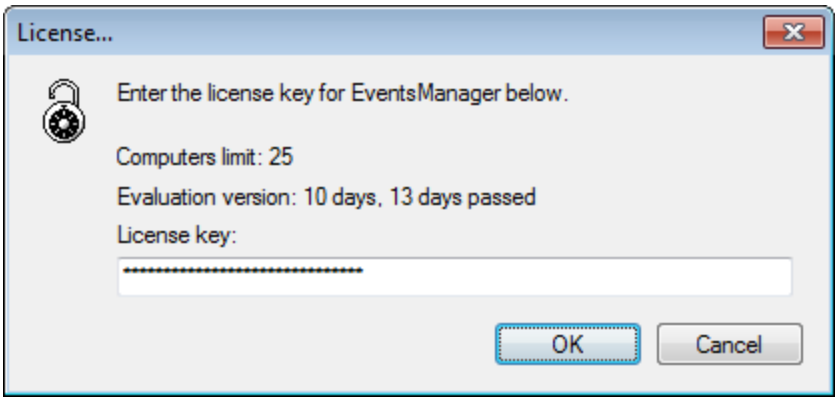
13.3 Product licensing

GFI EventsManager is licensed by event source/computer. All devices that generate a log are considered to be an event source. Refer to the sections below for more information about GFI EventsManager licensing options.

Updating license key

To update your current license key:

1. From **General** tab > **General**, right-click **Licensing** and select **Update key...**



Screenshot 204: Update license key dialog

3. Specify your license key and click **OK**.

Obtaining a free 30-day trial license key

GFI EventsManager allows you to register your version of the product and receive a free 30-day trial. Once the trial period is expired, all event log monitoring and management services are disabled and a full license key is required.

To register and receive a 30-day trial license key:

1. From **General** tab > **General**, click **Licensing**.

2. Click the provided link. This will take you to GFI website where you are able to enter you details and receive the license key by email. The email address you provide in the registration form is where your free 30-day trial key will be sent. If you have a spam filtering system, make sure the email is not blocked as spam.

Viewing license details

License details provide you with license distribution details. To view licensing details:

1. From **General** tab > **General**, click **Licensing**.

2. From the right pane, click **Show details** to expand the details section. This will show the number of event sources configured and respective license type (such as Workstation or Server).

Purchasing a license key

To purchase a license key:

1. From **General** tab > **General**, click **Licensing**.

Screenshot 205: Buy now! Button

2. From the right pane, click **Buy now!**. This takes you to GFI website where you can view further information about licensing and purchase a valid key.

Note

For more information, refer to:

- Licensing Information - http://www.gfi.com/page/13789/products/gfi-events-manager/pricing/licensing/licensing
- Pricing Information - http://www.gfi.com/products/gfi-eventsmanager/pricing

13.4 Product version information

Checking your GFI EventsManager version

To check your version information details:

1. From **General** tab > **General**, click **Version Information**.

2. View version information details from the right pane.

Checking for newer versions

To check for newer builds of GFI EventsManager:

1. From **General** tab > **General**, right-click **Version Information** and select **Check for newer builds...**

2. From the left pane, right-click Version Information and select Check for newer builds...

Note

Select **Automatically check for a newer version at startup** to automate this process. By default, this option is selected.

13.5 Export configuration to a file

To export you GFI EventsManager configurations:

1. Click **File > Import and Export Configurations....**

2. Select **Export the desired configurations to a file** and click **Next**.

3. Specify the location where the exported file will be saved or click **Browse...** to look for the location. Click **Next**.

4. Select the configurations you want to export and click **Next**.

5. Wait for GFI EventsManager to export the configuration and click **OK**.

13.6 Import configuration from a file

To import configurations from a file:

1. Click **File > Import and Export Configurations....**

2. Select **Import the desired configurations from a file** and click **Next**.

3. Specify the path where the import file is stored or click **Browse...** to look for it. Click **Next**.

4. Select the configurations you want to import and click **Next**.

5. Wait for GFI EventsManager to import the configurations and click **OK**.

Note

If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

13.7 Import configuration from another instance

To import configurations from another instance of GFI EventsManager:

1. Click **File > Import and Export Configurations...**

2. Select **Import the configurations from another instance** and click **Next**.

3. Specify the installation folder path of the instance you want to import configurations from. Alternatively, click **Browse...** to look for it. Click **Next**.

4. Select the configurations you want to import and click **Next**.

5. Wait for the configurations to import and click **OK**.

Note

If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

14 Miscellaneous

This chapter provides you with information related to configuring Third-Party components required for GFI EventsManager auditing operations. Learn how to configure and run GFI EventsManager actions through the provided command line tools.

Topics in this chapter:

14.1 GFI EventsManager Command Line Tools

GFI EventsManager provides you with command line tools through which you can perform various functions without accessing the Management Console. These tools are located in the GFI EventsManager installation folder. GFI EventsManager command line tools include:

Table 85: GFI EventsManager CMD tools

Tool	Description
ESMCmdConfig.exe	This tool enables you to configure general settings for GFI EventsManager; such as: » GFI EventsManager logon credentials » License key » Mail server settings » Administrator account » Create/Remove Group shortcuts » Get computer names. For more information, refer to Using ESMCmdConfig.exe (page 235).
Esmdlibm.exe	Use this CMD tool to run operations against the file storage system where processed events are stored (database backend). Such operations include Importing or Exporting data. For more information, refer to Using Esmdlibm.exe (page 237).
Esmreport.exe	Generates in-product reports such as configuration and job activity reports. For more information, refer to Using Esmreport.exe (page 239).
ExportHTML2PDF.exe	Export generated reports (HTML) to Portable Document Format (PDF). For more information, refer to Using ExportHTML2PDF.exe (page 241).
Importsettings.exe	Imports configuration from a data folder or from a configuration export file and is used when preserving configuration. For more information, refer to Using ImportSettings.exe (page 241).
ExportSettings.exe	Exports configuration settings from GFI EventsManager installation to a configuration file. For more information, refer to Using ExportSettings.exe (page 242).
SyncComputers.exe	Use this tool to manually sync all event sources with GFI EventsManager.

14.1.1 Using ESMCmdConfig.exe

To use ESMCmdConfig.exe:

1. Click **Start** > **Run** and key in **CMD**.

2. Click **Ctrl** + **Shift** + **Enter** to run CMD with elevated privileges.

3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **ESMCmdConfig.exe** followed by any of the following functions:

Table 86: CMD: ESMCmdConfig.exe functions

Function	Description
Register Services	This function registers GFI EventsManager services using an administrator account. It is made up of: » /op:registerService - parameter name » /user:<username> - specify username » /pass:<password> - specify password. **Example:** `ESMCmdConfig.exe /op:registerService /user:Administrator /pass:1234`
Enable services	This function enables events log management features. **Example:** `ESMCmdConfig.exe /op:enable`
Disable services	Disables GGFI EventsManager and prompts the user with a custom message. It is made up of: » /opdisable - function name » /message:<message> - specify the message to show. **Example:** `ESMCmdCOnfig.exe /op:disable /message:Feature is going to be disabled in one minute.`
Set license key	This function is used to specify a license key for GFI EventsManager. It is made up of: » /op:setLicense - function name » /licenseKey:<key> - specify the license key. **Example:** `ESMCmdCOnfig.exe / op:setLicense /licenseKey:XXXXXXXXX`
Configure alerting	Enable and configure alerting options. Function is made up of: » /op:configureAlerting - function name » /Server:<server> - specify server IP » /SenderEmail:<email> - specify senders' email address » /Port:<port> - specify the SMTP port (i.e. 25) » /RequiresAuthentication<true|false> - specify a True or False value » /User:<username> - specify a username for the email account » /Pass:<password> - specify a password for the email account. **Example:** `ESMCmdCOnfig.exe /op:configureAlerting /Server:192.168.11.11 /SenderEmail:name@domain.com /Port:25 /RequiresAuthentication:True /User:Administrator /Pass:1234`

Function	Description
Set administrator's email	Enables you to configure the Administartor's email address. This function is made up of: » /op:setAdminEmail - function name » /email:<email> - specify email. **Example:** `ESMCmdCOnfig.exe /op:setAdminEmail /email:administrator@domain.com`
Create program group shortcuts	Enables you to create group shortcuts. **Example:** `ESMCmdCOnfig.exe /op:CreateProgramGroupShortcuts`
Remove program group shortcuts	Enables you to remove group shortcuts. **Example:** `ESMCmdCOnfig.exe /op:RemoveProgramGroupShortcuts`
Get computers	Enables you to get computer names by specifying a filename where the data is exported. **Example:** `ESMCmdCOnfig.exe /op:GetComputers /filename:ExportedNames`

5. Press **Enter** to run the command.

14.1.2 Using Esmdlibm.exe

To use Esmdlibm.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **Esmdlibm.exe** followed by any of the following functions:

Table 87: CMD: Esmdlibm.exe functions

Function	Description
Import from SQL	The Import from SQL function is used to import data from previous versions of GFI EventsManager backend database. It is made up of the following parameters: » /importFromSql - function name » /logTypes:<application, custom, directory, security, dns, filereplication, syslog, system, snmp, oracle, sql, w3c> - specify the log typs to import » /server:<serverName> - specify the SQL Server IP » /database:<maindb |backupdb> - specify the database to import events from » /dbauth:<SQL|WIN> - specify the authentication mode » /username:<username> - specify the SQL Server username » /password:<password> - specify the SQL Server password » /jobId:<id> - optionally, specify a unique job ID. **Example:** `Esmdlibm.exe /importFromSql /logTypes:application,w3c /server:192.168.11.11 /database:main /dbauth:SQL /username:sa /password:1234 /jobId:987`
Import from Dlib database	This function enables you to import exported data from GFI EventsManager. It is made up of the following parameters: » /importFromDlib - function name » /path:<path> - specify the path of the import file » /name:<name> - specify the name of the import file » /anonpass1:<password> - optionally, specify the primary decryption password » /anonpass2:<password> - optionally, specify the secondary encryption password » /jobId:<id> - optionally, specify a unique job ID. **Example:** `Esmdlibm.exe /importFromDlib /path:C:\Events /name:importFile.txt /anonpass1:1234 /jobId: 987`
Import from Legacy File	This function enables you to import data exported or archived from an older version of GFI EventsManager. It is made up of the following parameters: » /importFromLegacyFile - function name » /path:<path> - specify the path of the import file » /logTypes:<application, custom, directory, security, dns, filereplication, syslog, system, snmp, oracle, sql, w3c> - specify the log type to import » /password:<password> - optionally, specify the password » /anonpass1:<password> - optionally, specify the primary decryption password » /anonpass2:<password> - optionally, specify the secondary encryption password » /jobId:<id> - optionally, specify a unique job ID. **Example:** `Esmdlibm.exe /importFromLegacyFile / path:C:\Events /logTypes: dns,security, w3c /password:1234 /jobId:987`

Function	Description
Export to file	This function enables you to export data to a file. It is made up of the following parameters: » /exportToFile - function name » /path:<path> - specify the path where the exported file is saved » /password:<password> - specify a password to protect the exported file » /olderThenXDays:<number of days> - specify what data is exported based on the number of days passed since the event was generated » /olderThenXHours:<number of hours> - specify what data is exported based on the amount of hours passed since the event was generated » /jobId:<id> - optionally, specify a unique job ID. **Example:** `Esmdlibm.exe /exportToFile /path:C:\Events /password:1234 /olderThenXDays:7 /jobId:987`
Encrypt database	This function enables you to encrypt any database which stores exported/archived event logs. It is made up of the following parameters: » /encryptDatabase - function name » /dbPath:<path> - specify the path for the location of the database you want to encrypt » /dbName:<name> - specify the database name you want to encrypt » /password:<password> - specify the encryption password used to encrypt the database. **Example:** `esmdlibm.exe /encryptDatabase /dbPath:C:\Events /dbName:Database1 /password:pa$$word`
Decrypt database	This function enables you to decrypt any encrypted database which stores exported/archived event logs. It is made up of the following parameters: » /decryptDatabase - function name » /dbPath:<path> - specify the path for the location of the database you want to decrypt » /dbName:<name> - specify the database name you want to decrypt » /password:<password> - specify the encryption password used to encrypt the database to be able to decrypt it. **Example** `esmdlibm.exe /decryptDatabase /dbPath:C:\Events /dbName:Database1 /password:pa$$word`

5. Press **Enter** to run the command.

14.1.3 Using Esmreport.exe

To use Esmreport.exe:

1. Click **Start > Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **Esmreport.exe** followed by any of the following functions:

Table 88: CMD: Esmreport.exe functions

Function	Description
Generate Configuration/Status/Events Report	Enables you to generate reports based on GFI EventsManager configuration. It is made up of the following parameters: » /type:<CONFIGURATION|STATUS|EVENTS> - specify report type » /target:<path> - specify destination folder » /format:<HTML|CSV> - specify report format. **Example:** `Esmreport.exe /type:STATUS /target:C:\Events /format:HTML`
Event source configuration report	Enables you to generate reports on event sources configuration. It is made up of the following parameters: » /type:configuration - specify report type » /source:<name> - specify a single event source name Or » /group:<name> - specify a group name to report on multiple event sources. **Example:** `Esmreport.exe /type:configuration /group:Servers`

Status report	This function is made up of the following parameters:
	» /type:status - specify report type
	» /subtype:<MESSAGES|STATS> - specify the report sub type
	» /period:<CURRENT|"date"> - specify the period for MESSAGES sub type
	» /period:<"ALL TIME"|date> - specify the period of STATS sub type
	» /options:<"ERROR MESSAGES"|"ONLY WITH ISSUES"> - specify options for STATS sub type.
	
	Example 1:
	`Esmreport.exe /type:STATUS /subtype:MESSAGES /period:CURRENT`
	
	Example 2:
	`Esmreport.exe /type:STATUS /subtype:STATS/period:”ALLTIME” /options:”ERROR MESSAGES”`

Events report	This function is made up of the following parameters: » /type:events - specify report type » /repid:<report ID> - specify report ID » /target:<path> - specify destination folder » /format:<HTML|PDF> - specify report format » /scheduled - specify report schedule. This enables schedule and uses the default settings configured in GFI EventsManager. **Example:** `Esmreport.exe /type:events /repid:11 /target:C:\Events /format:PDF`

5. Press **Enter** to run the command.

14.1.4 Using ExportHTML2PDF.exe

To use ExportHTML2PDF.exe:

1. Click **Start > Run** and key in **CMD**.

2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.

3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **ExportHTML2PDF.exe** followed by any of the following functions:

Table 89: CMD: Esmreport.exe functions

Functions	Description
Export HTML reports to PDF	This function enables you to export pre-generated HTML reports to a Portable Document Format file. It is made up of the following parameters: » /source:<path to HTML files> - specify the source folder path which contains the HTML reports » /target:<path to PDF file> - specify the PDF destination folder. **Example**: `ExportHTML2PDF.exe /source:C:\Program Files\EventsManager 2012 /target:C:\PDFReports\EventsManager`

5. Press **Enter** to run the command.

14.1.5 Using ImportSettings.exe

Use this tool to import GFI EventsManager configurations exported from previous installations.

To use ImportSettings.exe:

1. Click **Start > Run** and key in **CMD**.

2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.

3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **ImportSettings.exe** followed by the parameters described below:

Table 90: CMD: ImportSettings.exe parameters

Parameter	Description
/operation:<operation>	Defines the operation to perform, either import folder or import file.
/destination:<destination path>	Defines the destination folder where the configuration is imported.
/sourceFile:<filename>	Defines the name of the file that contains the exported GFI EventsManager configuration.
/sourceFolder:<folder name/path>	Defines the name of the folder that contains the exported GFI EventsManager configuration.

Important

Any parameter that contains spaces must be enclosed in double quotes (“).

5. Press **Enter** to run the command.

Example:

```
importsettings.exe /operation:importfolder /destination:
c:\esm\data /sourcefolder: c:\esm\old
```

14.1.6 Using ExportSettings.exe

Use this tool to export GFI EventsManager configuration.

To use ExportSettings.exe:

1. Click **Start > Run** and key in **CMD**.

2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.

3. Change the directory to the GFI EventsManager install directory:

```
CD <C:\Program Files\GFI\EventsManager 2012>
```

4. Key in **ExportSettings.exe** followed by the parameters described below:

Table 91: CMD: ExportSettings.exe parameters

Parameter	Description
/destination:<filename>	Defines the file where the configuration will be exported.
/folder:<folder>	Specify a path to export from an alternative folder.

Important

Any parameter that contains spaces must be enclosed in double quotes (“).

5. Press **Enter** to run the command.

Example:

```
exportsettings.exe /destination:”c:\export”
```

14.2 Enabling event source permissions manually

This section describes how to configure permissions that are required by GFI EventsManager to audit systems and process the necessary events. This process has to be done on each machine to scan.

This section contains information about:

- Enabling permissions on Microsoft Windows XP
- Enabling permissions on Microsoft Windows Vista
- Enabling permissions on Microsoft Windows 7
- Enabling permissions on Microsoft Windows Server 2003
- Enabling permissions on Microsoft Windows Server 2008 (including R2)

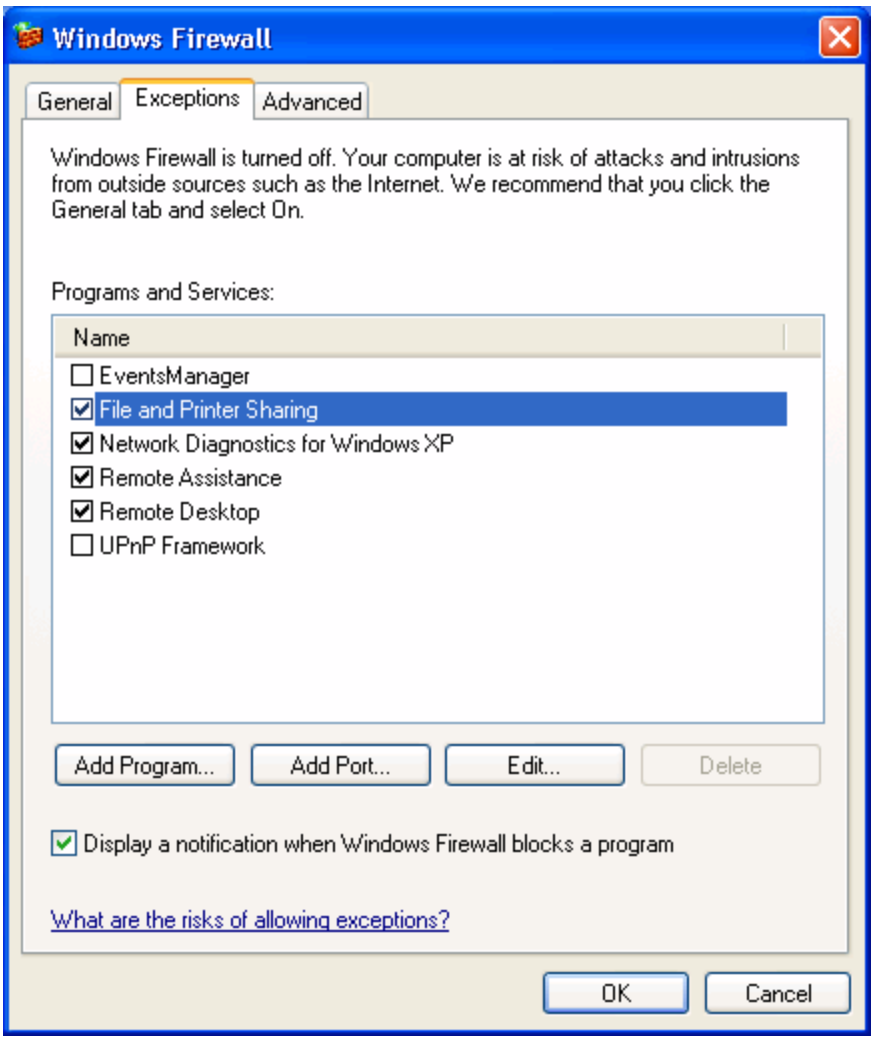
Note

In an active directory environment, permissions can be set automatically via Group Policy Object (GPO). For more information, refer to Enabling event source permissions automatically (page 249).

14.2.1 Enabling permissions on Microsoft Windows XP

To enable permissions Microsoft Windows event sources:

1. Click **Start > Control Panel > Windows Firewall > Exceptions** tab.



Screenshot 206: Firewall rules on Microsoft Windows XP

2. From **Programs and Services** list, enable **File and Printer Sharing**.

3. Click **OK**.

14.2.2 Enabling permissions on Microsoft Windows Vista

This process contains two steps outlined below:

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows Vista:

1. Click **Start > Control Panel > Security** and click **Allow a program through Windows Firewall** from the left panel.

2. Select **Exceptions** tab and from **Allowed programs and features** list, enable the following rules:

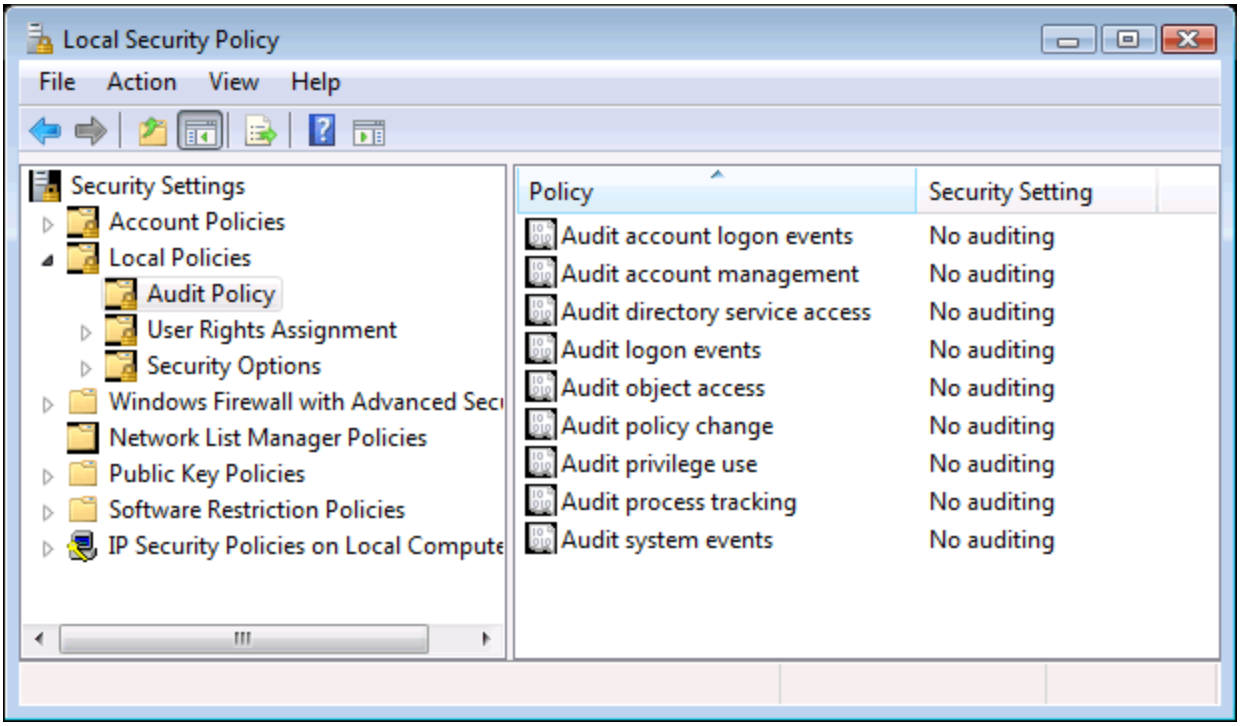
- Remote Event Log Management
- File and Printer Sharing
- Network Discovery.

3. Click **Apply**.

Step 2: Enable additional auditing features

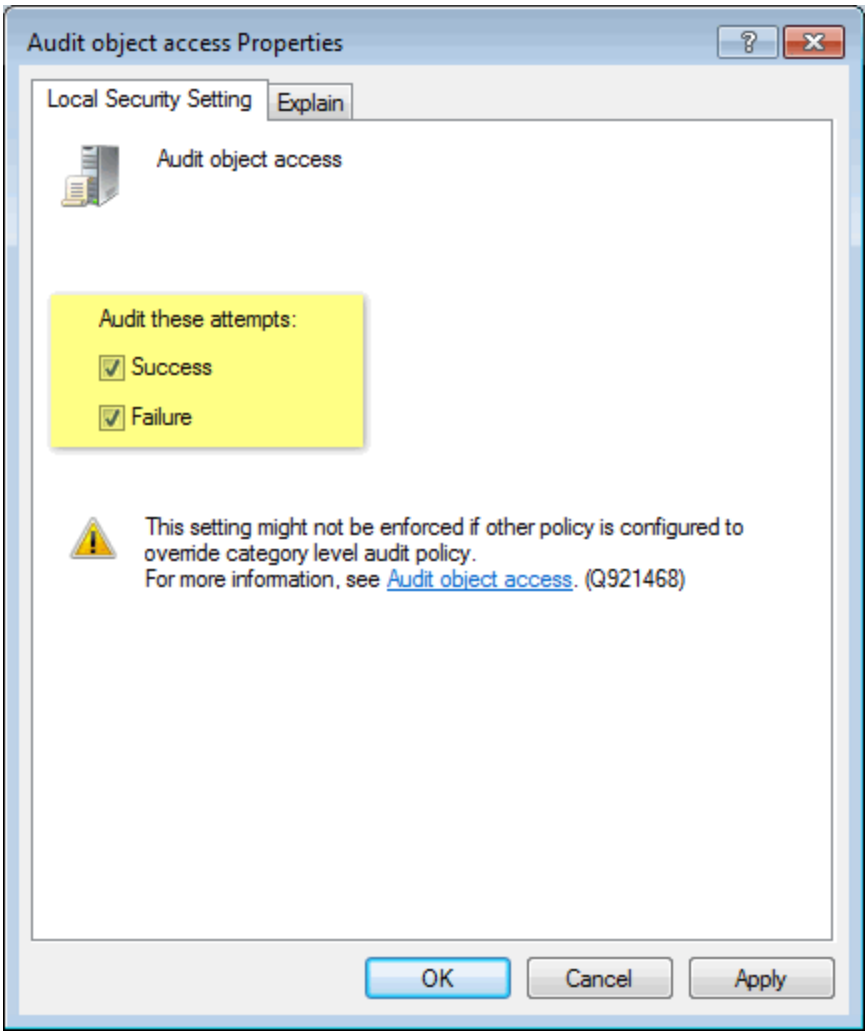
1. Click **Start > Run** and key in **secpol.msc**. Press **Enter**.

2. From the **Security Settings** node, expand **Local Policies > Audit Policy**.



Screenshot 207: Local security policy window

3. From the right panel, double-click **Audit object access**.



Screenshot 208: Audit object access properties

4. From the **Audit object access Properties**, select **Success** and **Failure** and click **OK**.

5. From the right panel, double-click **Audit Process tracking**.

6. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.

7. From the right panel, double-click **Audit account management**.

8. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.

9. From the right panel, double-click **Audit system events**.

10. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.

11. Close the Local Security Policy window.

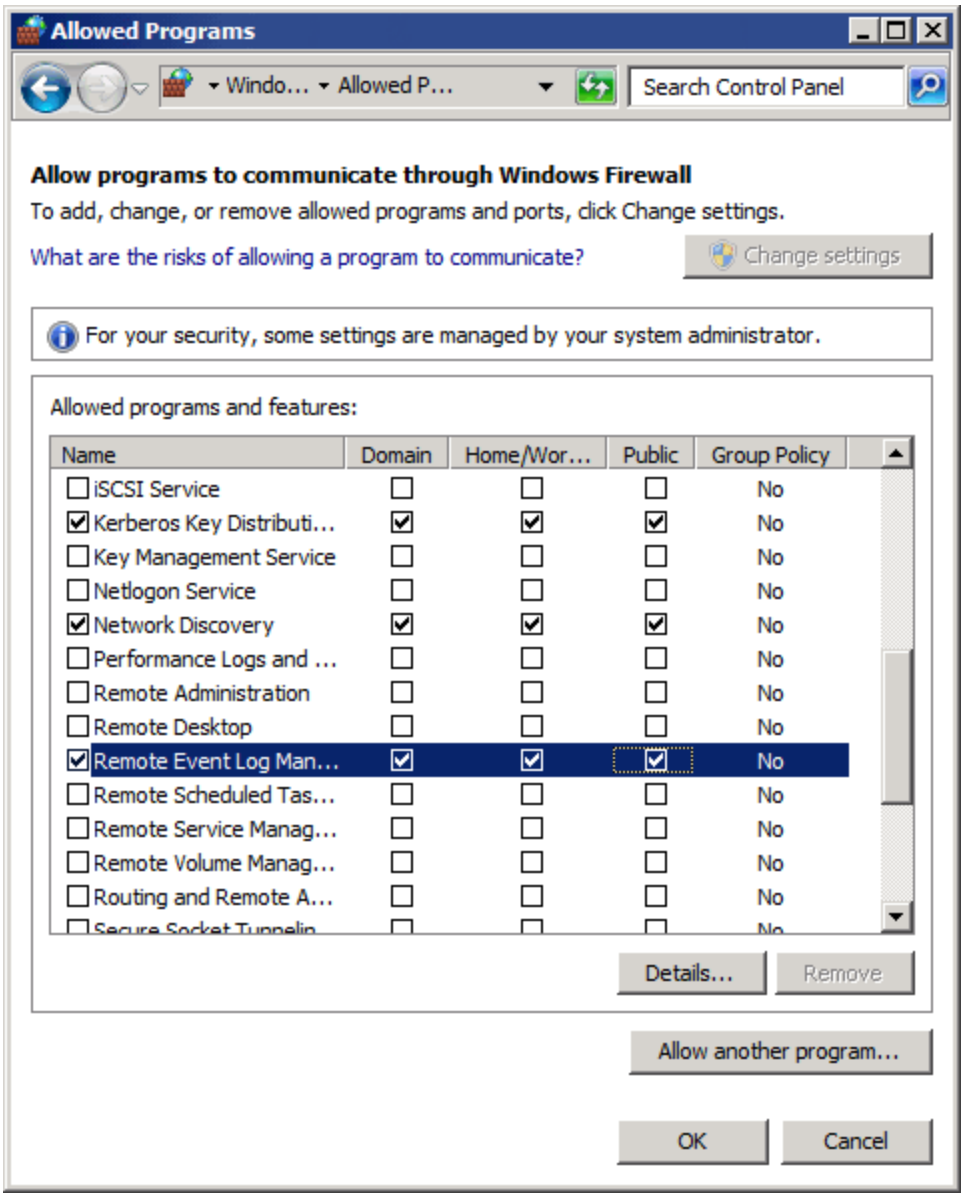
14.2.3 Enabling permissions on Microsoft Windows 7

This process contains two steps outlined below:

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows 7:

1. Click **Start > Control Panel > System and Security** and click **Allow a program through Windows Firewall**, under Windows Firewall category.



Screenshot 209: Allowed programs in Microsoft Windows Vista or later

2. From **Allowed programs and features** list, enable the following rules:

- Remote Event Log Management
- File and Printer Sharing
- Network Discovery.

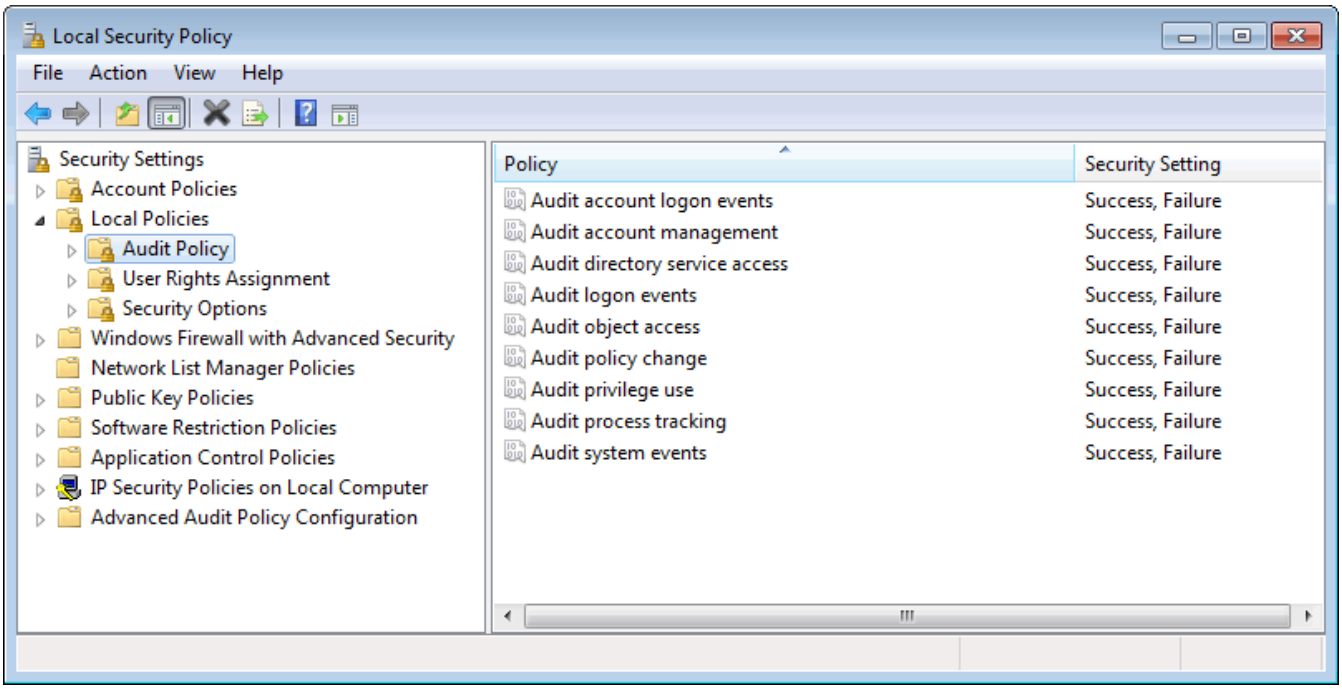
3. Select **Domain**, **Private** and **Public** for each rule mentioned above.

4. Click **OK**.

Step 2: Enable additional auditing features

1. Click **Start > Run** and key in **secpol.msc**. Press **Enter**.

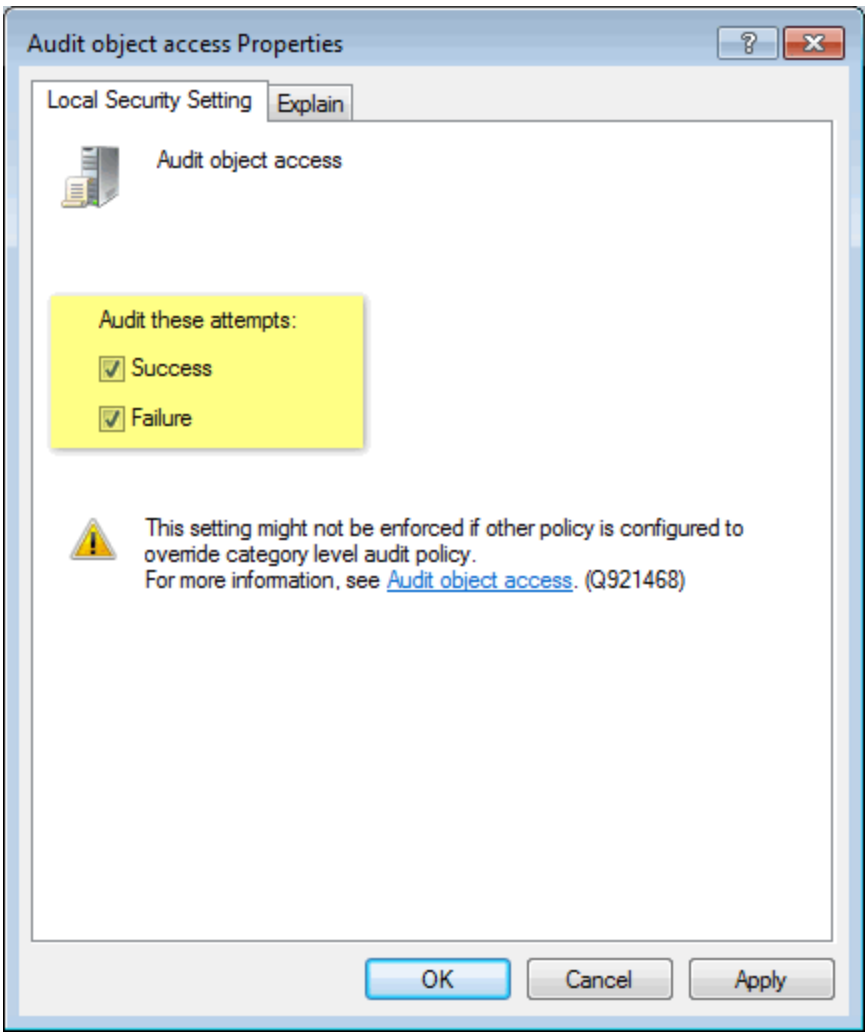
2. From the **Security Settings** node, expand **Local Policies > Audit Policy**.



Screenshot 210: Local security policy window

3. From the right panel, double-click **Audit object access**.

4. From **Audit object access Properties**, select **Success** and **Failure**. Click **OK**.



Screenshot 211: Audit object access Properties

5. From the right pane, double-click **Audit Process tracking**.

6. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.

7. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.

8. From the right panel, double-click **Audit account management**.

9. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.

10. From the right panel, double-click **Audit system events**.

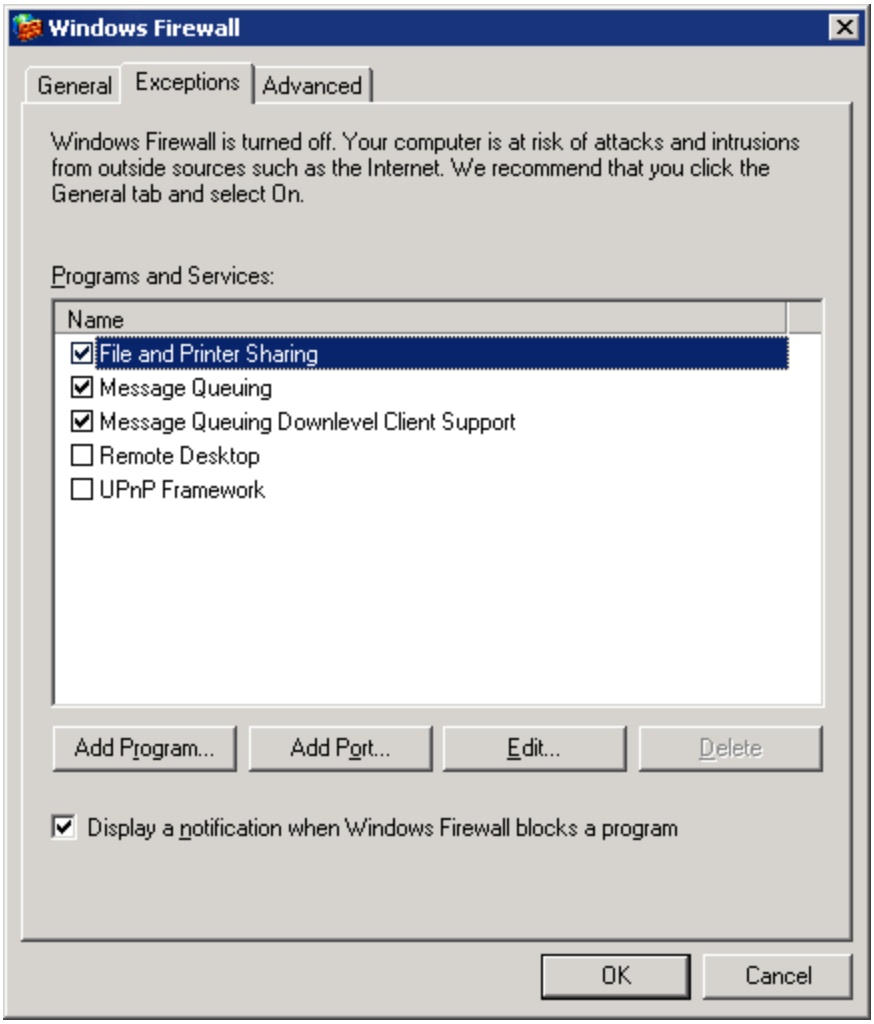
11. From **Audit process tracking Properties**, select **Success** and **Failure**. Click **OK**.

12. Close the local Security Policy window.

14.2.4 Enabling permissions on Microsoft Windows Server 2003

To manually enable firewall rules on Microsoft Windows Server 2003:

1. Click **Start > Control Panel > Windows Firewall** and select **Exceptions** tab.



Screenshot 212: Enable firewall rules in Microsoft Windows Server 2003

2. From **Programs and Services** list, enable **File and Printer Sharing**.

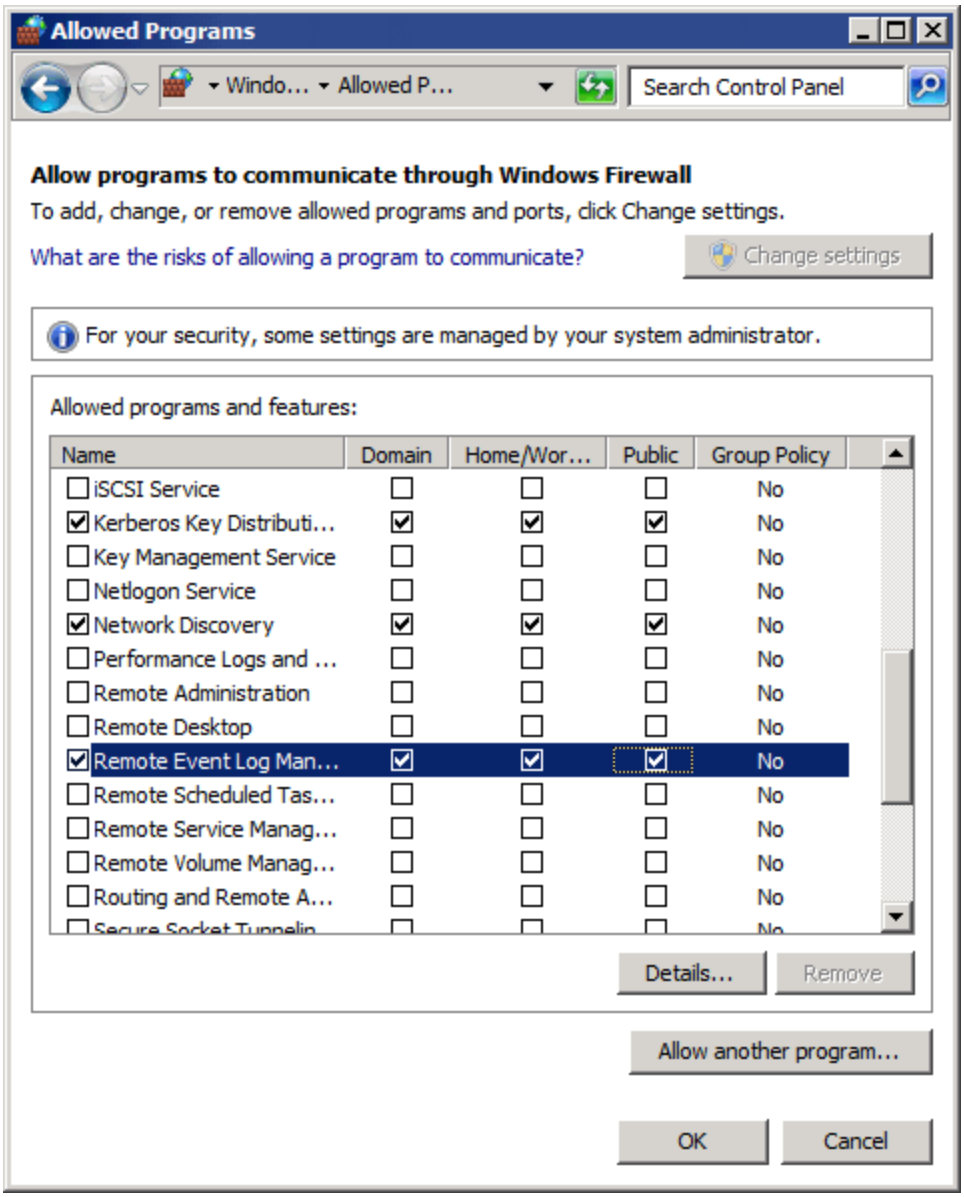
3. Click **OK**.

14.2.5 Enabling permissions on Microsoft Windows Server 2008 (including R2)

1. Click **Start > Control Panel > Security** and click **Allow a program through Windows Firewall** under **Windows Firewall** category.

2. In the list of programs, enable the following:

- File and Printer Sharing
- Network Discovery
- Remote Event Log Management.



Screenshot 213: Firewall rules on Microsoft Windows Server 2008

3. Click **OK**.

> **Note**
>
> In Windows Server 2008 R2, ensure to select **Domain**, **Private** and **Public** for each rule mentioned above.

14.3 Enabling event source permissions automatically

This section contains information about:

14.3.1 Enabling permissions on Windows Server 2003 via GPO

To open enable permissions on all domain clients using Microsoft Windows Server 2003 domain controller:

1. Click **Start > Run**, key in **mmc**. Press **Enter**.

2. Click **File > Add/Remove Snap-in** and click **Add**.

3. Locate and select **Group Policy Object Editor** and click **Add**.

4. Click **Browse**, select **Default Domain Policy** and click **OK**.

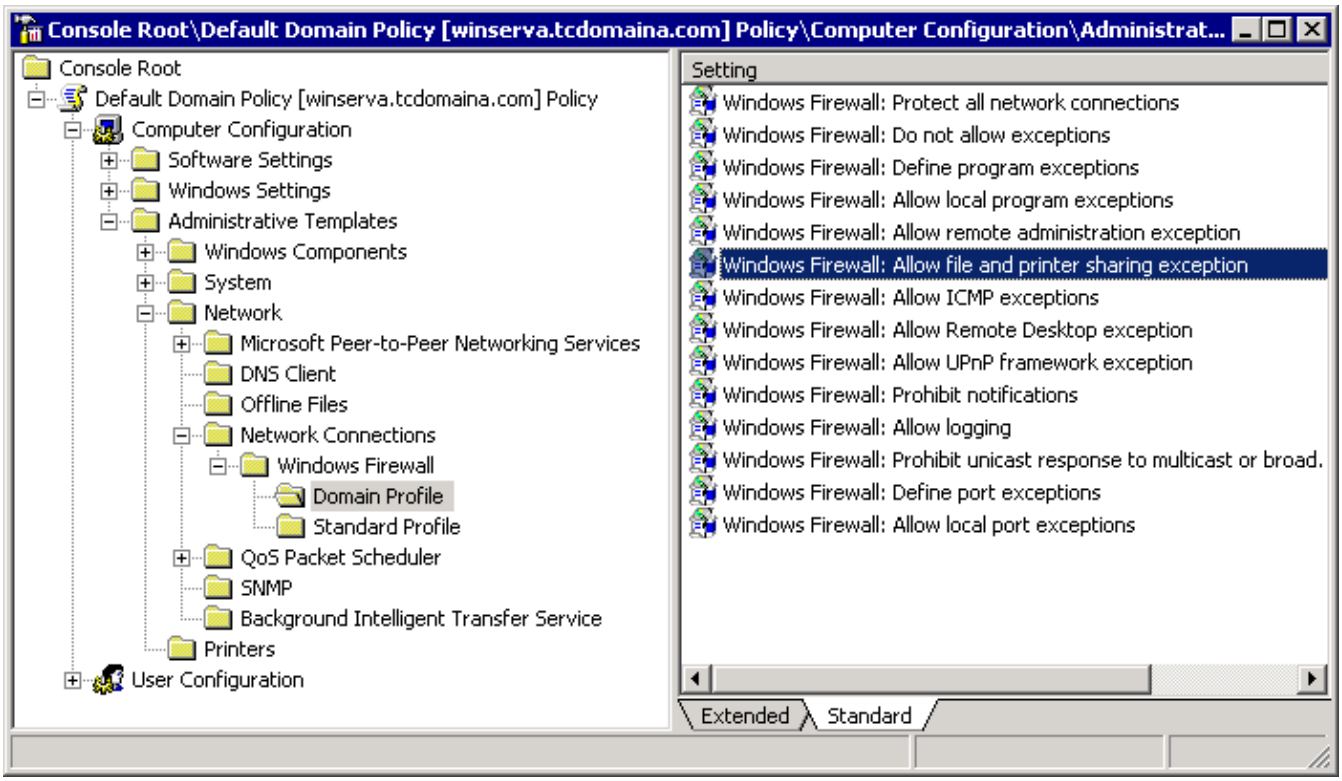
5. Click **Finish**.

6. Select **Group Policy Object Editor** again and click **Add**.

7. Click **Browse**, double-click **Domain Controllers** folder and select **Default Domain Controllers Policy**. Click **OK**.

8. Click **Finish** and **Close**.

9. From **Console Root**, expand **Default Domain Policy > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.



Screenshot 214: Domain Policy console in Microsoft Windows Server 2003

10. From **Setting** list, right-click **Windows Firewall: Allow file and printer sharing exception** and select **Properties**.

11. From the **Settings** tab, select **Enabled** and click **OK**.

12. Repeat steps 9 to 11 for **Default Domain Controllers Policy**.

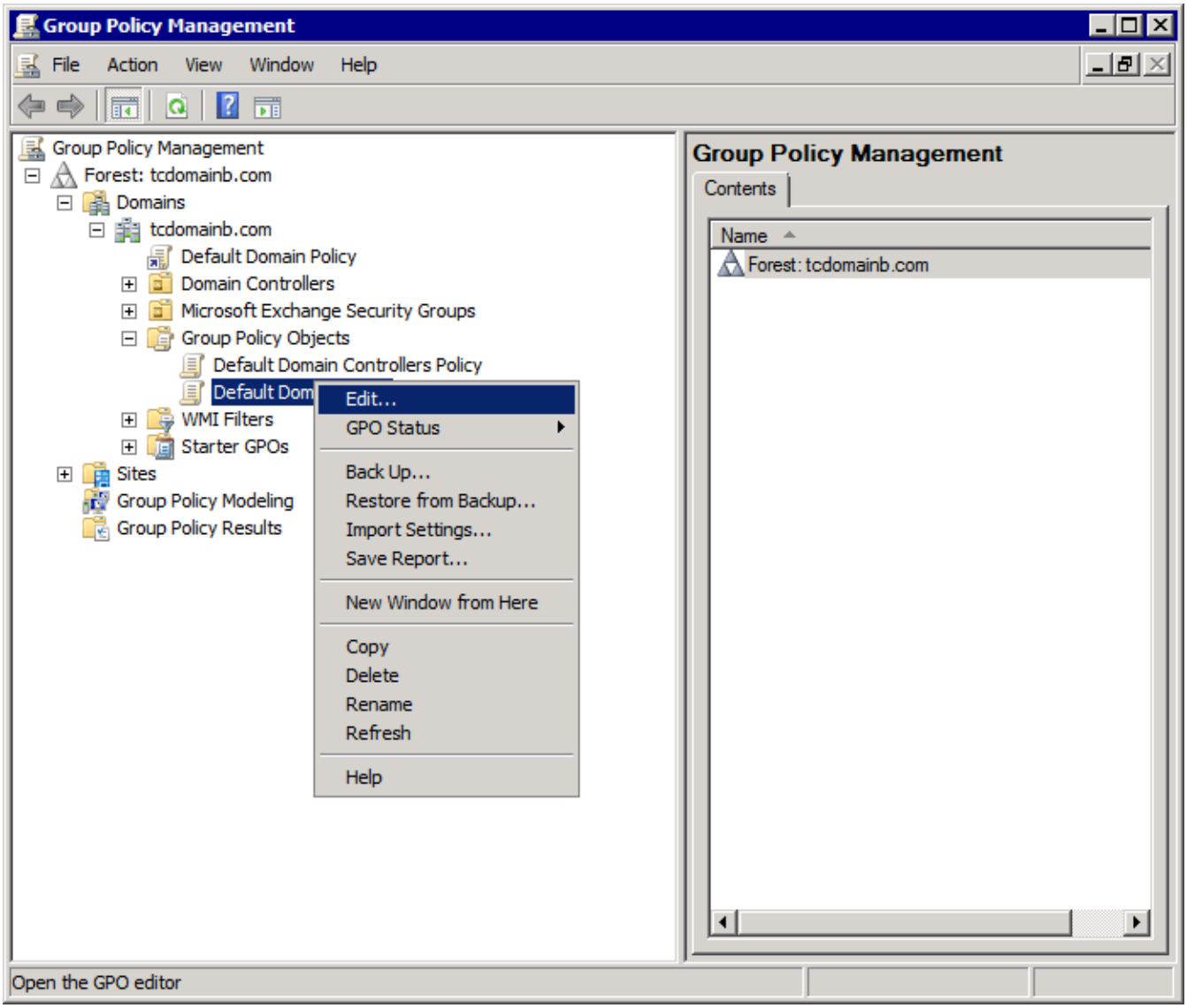
13. Click **File > Save** to save the management console. The group policy comes into effect the next time each machine is restarted.

14.3.2 Enabling permissions on Windows Server 2008 via GPO

To enable permissions on all domain clients:

1. Click **Start > Administrative Tools > Group Policy Management.**

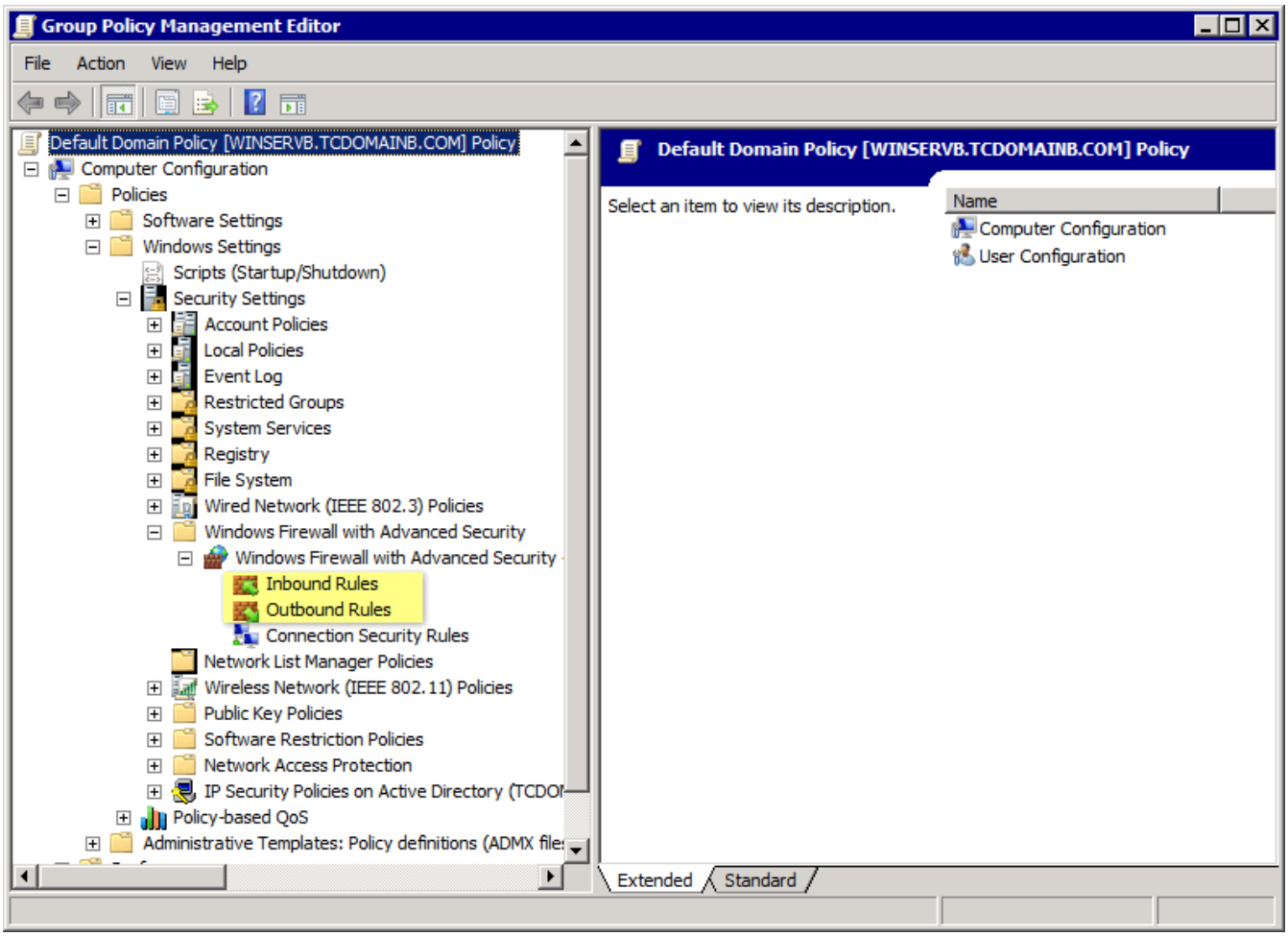
2. Expand **Group Policy Management > Forest > Domains > <*Domain name*> > Group Policy Objects.**



Screenshot 215: Group Policy Management in Microsoft Windows Server 2008 R2

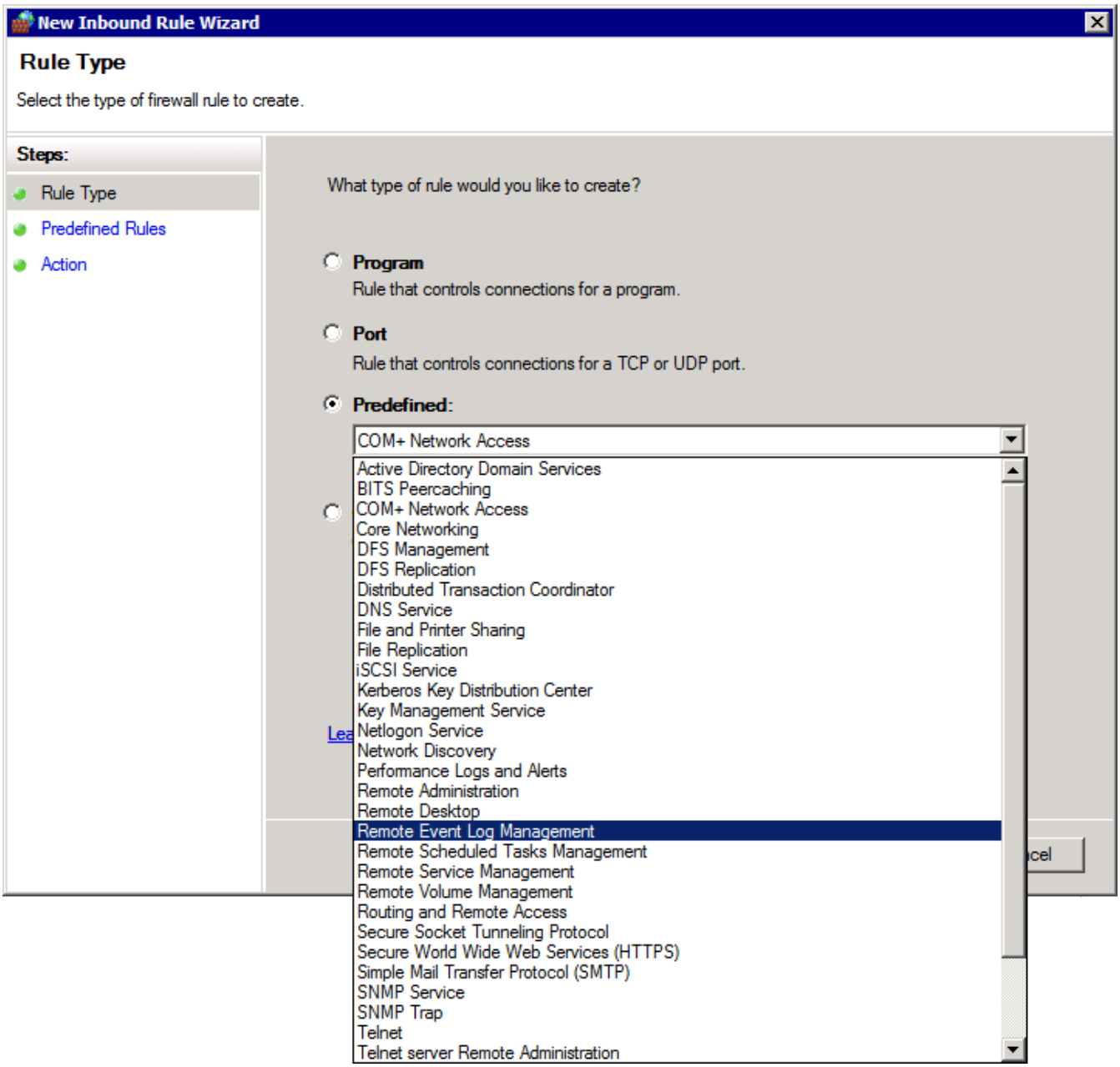
3. Right-click **Default Domain Policy** and select **Edit.**

4. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, right-click **Inbound Rules** and select **New Rule…**



Screenshot 216: Group Policy Management Editor

5. In the **New Inbound Rule** Wizard, select **Predefined** and select **File and Printer Sharing**.



Screenshot 217: Predefined rules

6. Click **Next**.

7. Select all rules and click **Next**.

8. Select **Allow the connection** and click **Finish**.

9. Repeat steps 5 to 8 for each of the following rules:

- Remote Event Log Management
- Network discovery.

10. From **Group Policy Management Editor**, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**, right click **Outbound Rules** and select **New Rule…**

11. Repeat Steps 5 to 9 while at step 9 enable only **Network Discovery**.

12. Close **Group Policy Management Editor**.

13. From **Group Policy Management**, expand **Group Policy Management > Forest > Domains > <*Domain name*> > Default Domain Controllers Policy**.

14. Repeat steps 4 to 13.

15. Click **File > Save** to save the management console. The group policy comes into effect the next time each machine is restarted.

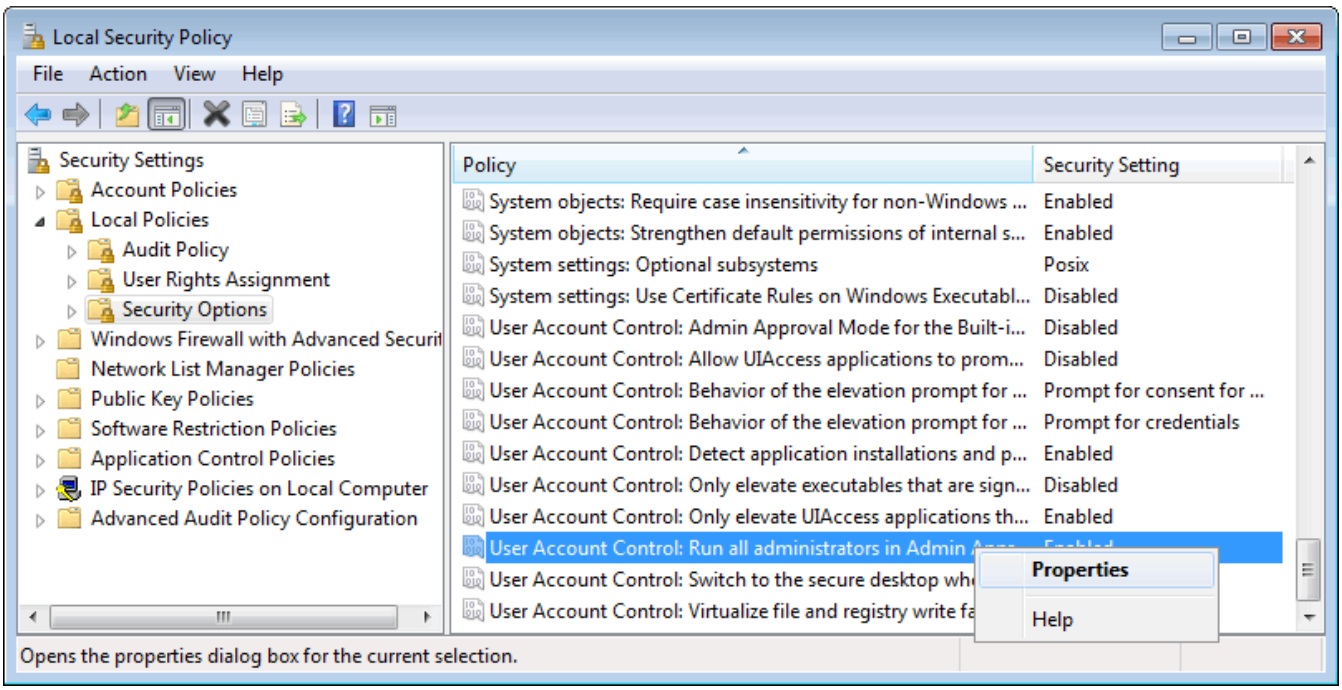
14.4 Disabling User Account Control (UAC)

When GFI EventsManager is configured to collect events using a local account target machines must have **User Account Control (UAC)** disabled. To disable UAC on Microsoft Windows Vista machines or later:

1. Click **Start > Run**, key in **secpol.msc** and press **Enter**.

2. From **Security Settings**, expand **Local Policies** and click **Security Options**.

3. Right-click **User Account Control: Run all administrators in Admin Approval Mode** and select **Properties**.



Screenshot 218: Disabling UAC

4. From the **Local Security Settings** tab, select **Enabled** and click **OK**.

5. Close the Local Security Policy window.

15 Troubleshooting

This chapter provides you with information about how to resolve any issues encountered while using GFI EventsManager. The main sources of information are:

Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

Using Trouble.exe

To use the troubleshooting tool:

1. Go to the install folder of GFI EventsManager.

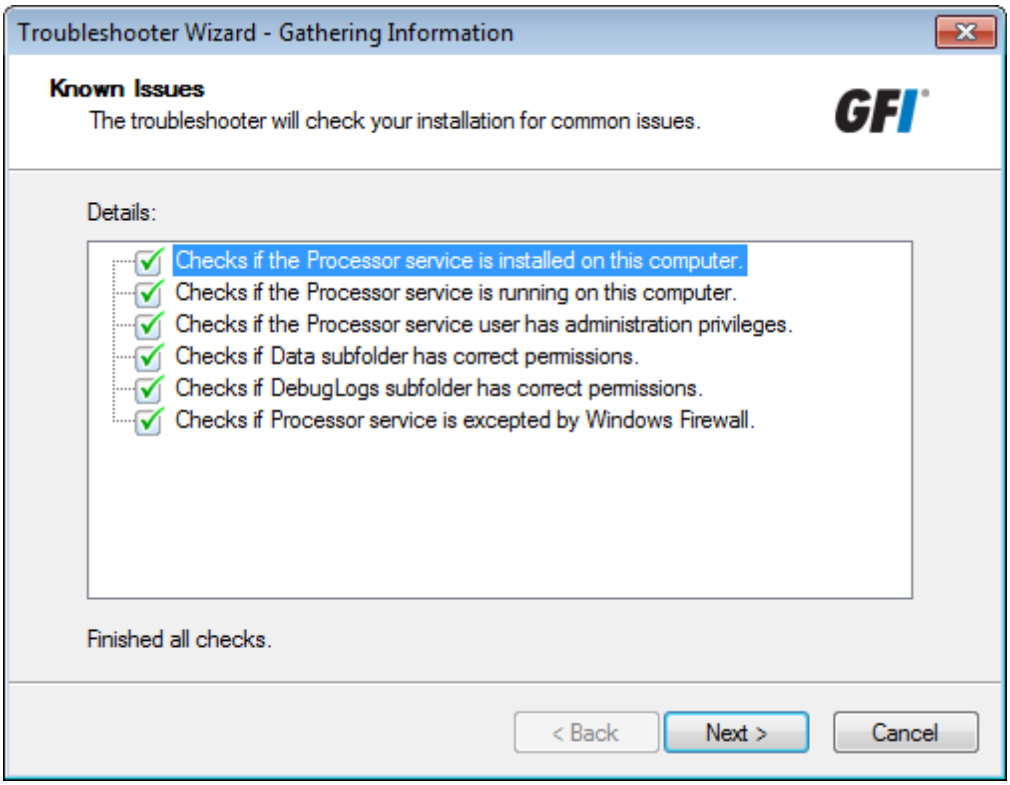
2. Locate and double-click **Trouble.exe**.

3. Click **Next** at the wizard welcome screen.

Screenshot 219: Select information gathering mode

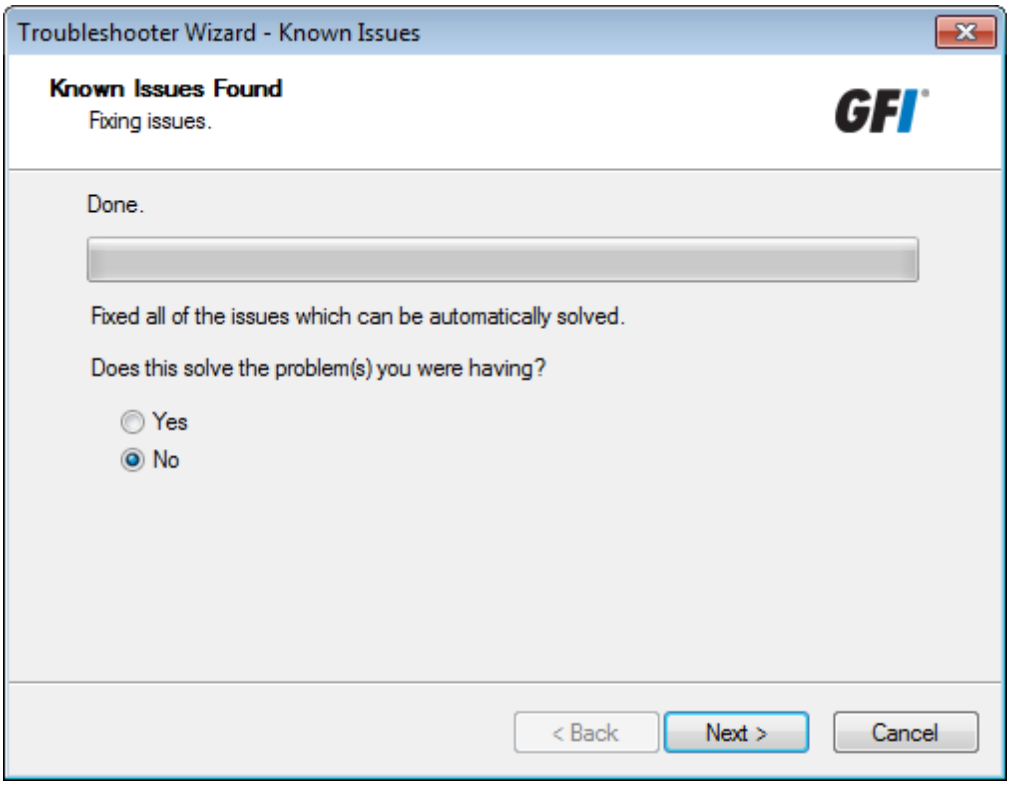
4. Select how the troubleshooter will collect information. Select from:

- **Automatically detect and fix known issues** - Select this option to allow GFI EventsManager to run a set of checks to determine what is wrong
- **Gather only application information and logs** - Specify your contact details, issue description and your system information to upload them to our support team. If you choose this option, skip to step **9**.



Screenshot 220: Troubleshooter automatic checks

5. Wait for the troubleshooter to run the required checks and click **Next**.



Screenshot 221: Troubleshooter automatically fixing detected issues

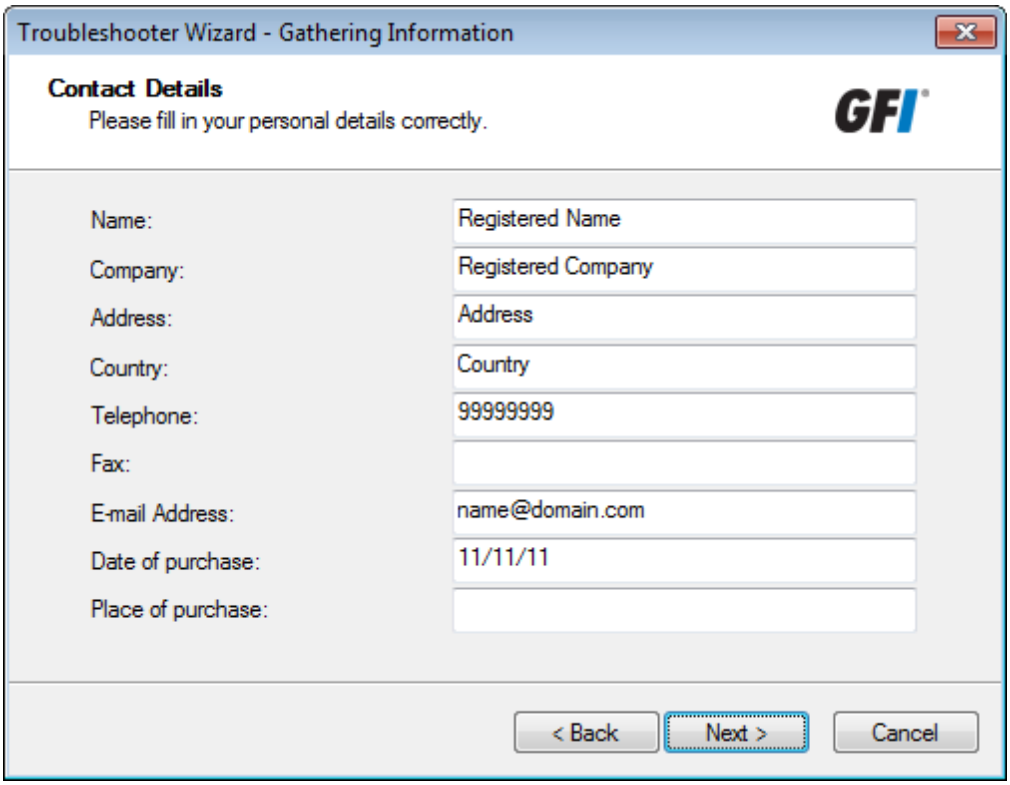
6. Wait for the troubleshooter to apply fixes for issues detected during the check. If this solves your problem, click **Yes** and **Finish**. If the problem remains, select **No** and click **Next**.

Screenshot 222: If the problem persists, search for articles on our knowledge base

7. Search our knowledge base archive for articles related to your problem. Key in the error your are encountering in the **Enter search items** text box and click **Search**. If this solves your problem, click **Yes** and **Finish**. If the problem remains, select **No** and click **Next**.

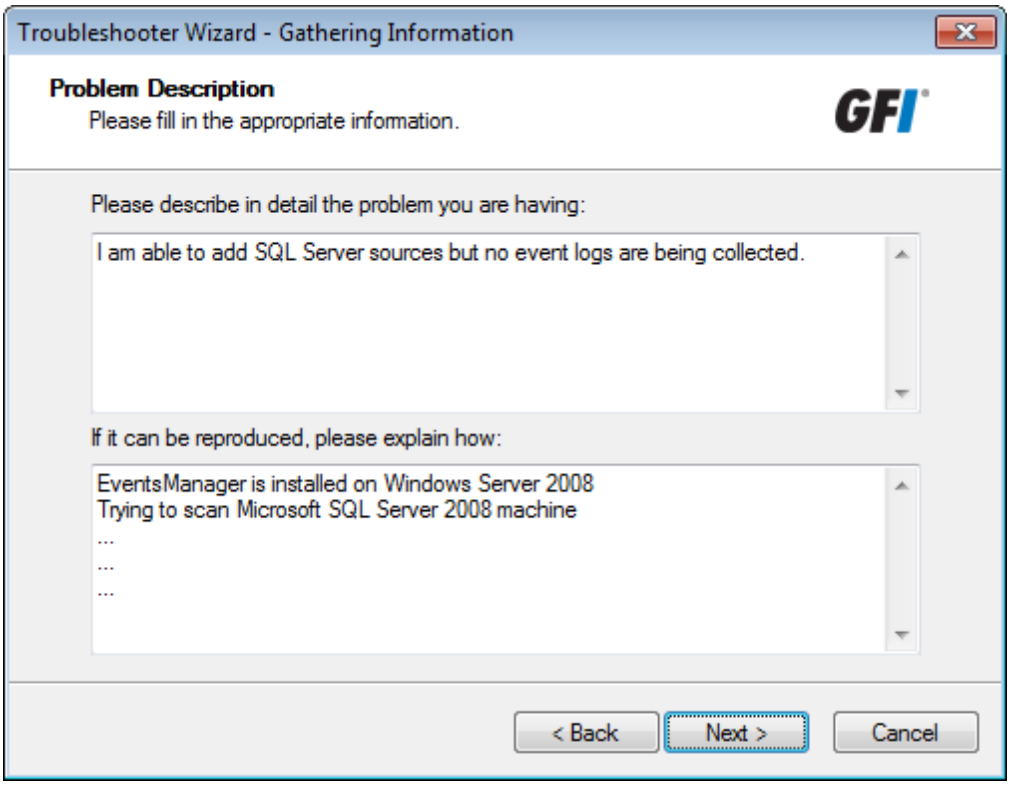
Screenshot 223: Manually checking for issues

8. Click **Next**.



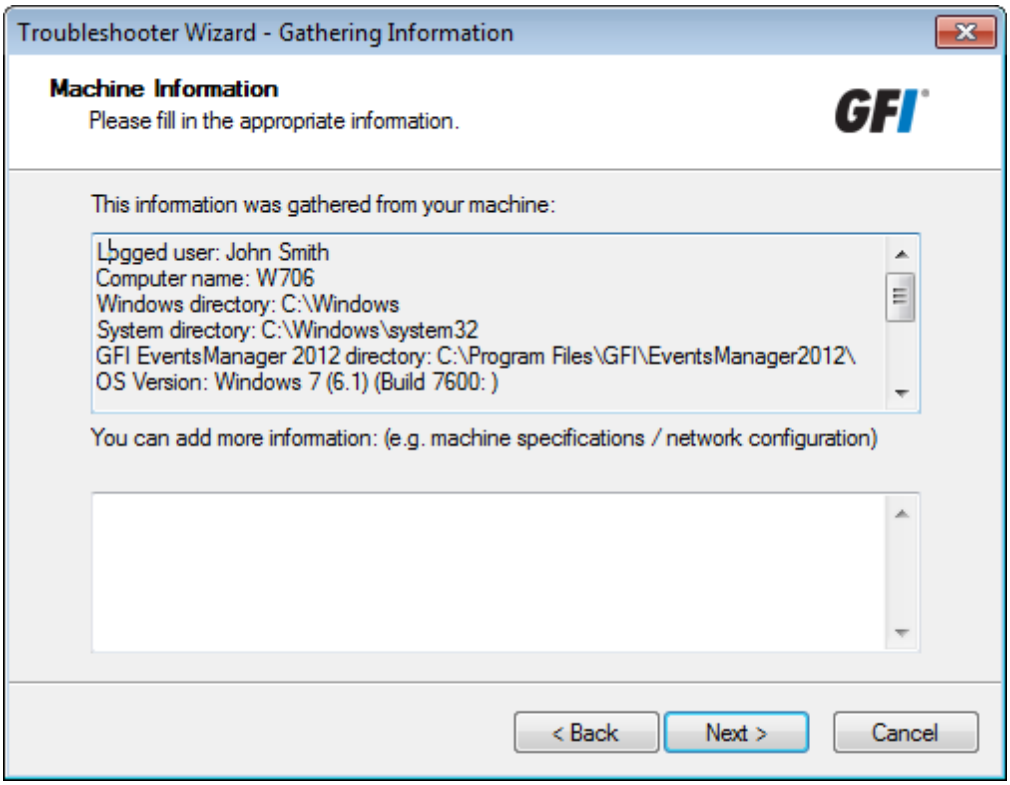
Screenshot 224: Specify contact details

9. Key in your contact details so that our support team would be able to contact you for further analysis information. Click **Next**.



Screenshot 225: Key in the problem description and other information

10. Specify the error you are getting and other information that would help our support team to recreate this issue. Click **Next**.



Screenshot 226: Gathering machine information

11. The troubleshooter scans your system to get hardware information. You can manually add more information in the space provided or click **Next**.

Screenshot 227: Finalizing the troubleshooting process

12. At this stage, the troubleshooter creates a package with the information gathered from the previous steps. Next, send this package to our support team so they can analyze and troubleshoot your problem. Select from:

- **FTP Upload Instructions** - Opens an article to give you instructions on how you can upload the troubleshooter package to our FTP server
- **Open Containing Folder** - Opens the folder containing the troubleshooter package so that you can send it via email
- **Go to GFI Support** - Opens the support page of GFI website.

13. Click **Finish**.

GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting: http://kb.gfi.com/.

Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com/.

Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **NOTE**
>
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

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

16 Glossary

A

Actions

The activity that will be carried out as a result to events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.

Alerts

Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.

Archive

A collection of events stored in the SQL Server based database backed of GFI EventsManager.

Audit account management

Generates events when account management operations are done such as create/delete a user account or group, enable/disable a user account and set/change a user password. For more information, refer to http://technet.microsoft.com/en-us/library/cc737542(WS.10).aspx

Audit process tracking

Generates events which track actions such as programs which are launched, closed, as well as other indirect object access information which contain important security information. For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx

Audit system events

Generates events when important system events happen such as user restarts or shuts down the target computer or when an event occurs that affects the security log. For more information, refer to http://technet.microsoft.com/en-us/library/cc782518(WS.10).aspx

C

COM+ Network Access

Enable this firewall permission to allow client machines to access applications or services that resides on the server. This allows GFI EventsManager to access resource from all servers. For more information about this permission, refer to http://technet.microsoft.com/en-us/library/cc731967.aspx

E

Email alerts

Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.

Event classification

The categorization of events as Critical, High Medium, Low or Noise.

Event logs

A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.

Event processing rules

A set of instructions which are applied against an event log.

F

File and Printer sharing

Enable this firewall permission to allow GFI EventsManager to access events definitions on target machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc779133(WS.10).aspx

I

Internet Protocol Security

A framework of open standards used to encrypt and authenticate network packets during a communication session between computers. Using cryptography services, IPsec ensures data integrity, authentication and confidentiality.

IPsec

Internet Protocol Security is a framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the Application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

M

Management Information Base

A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.

N

Network alerts

Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.

Network discovery

Enable this firewall permission to allow GFI EventsManager to gather information about connected machines on the network that can be scanned. For more information, refer to http://technet.microsoft.com/en-us/library/cc181373.aspx

Noise

Repeated log entries which report the same event.

O

Object auditing

Enable this auditing feature to audit events of users accessing objects (example, files, folder and printer). For more information, refer to http://technet.microsoft.com/en-us/library/cc976403.aspx

R

Remote Event Log Management

Required to allow GFI EventsManager to access and collect events from remote machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc766438.aspx

Rule-set folder

The folder which contains one or more rule-sets.

Rule-sets

A collection of event processing rules.

S

SMS alerts

SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.

SNMP Object Identifier (OID)

An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (Example: 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (Example: hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.

SNMP Traps

Notifications/alerts generated and transmitted by active network components (Example: hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.

Syslog messages

Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.

U

Unclassified events

Events that did not satisfy any of the event processing conditions configured in the event processing rules.

W

W3C logs

W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.

Windows Event Logs

A collection of entries which describe events that occurred on a computer system running Windows OS.

17 Index

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, 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, San Andrea Street, San Gwann, SGN 1612, 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

GFI®