GFI White Paper

How to configure IBM iSeries (formerly AS/400) event collection with Audit and GFI EventsManager™

This document explains how to configure and use GFI EventsManager to collect IBM iSeries (formerly AS/400) audit events through Audit, a software tool developed by Raz-Lee Security.

Contents

Overview

The solution works as follows:

- GFI EventsManager is installed on a machine in the network
- An instance of Audit is installed on each IBM iSeries logical partition that needs to be monitored
- GFI EventsManager is configured to process Syslog messages coming from all the IBM iSeries machines that need to be monitored
- Audit is configured to scan the iSeries logs and send them as Syslog messages to the machine on which GFI EventsManager is installed
- The newly generated IBM iSeries logs will be automatically forwarded by Audit to GFI EventsManager
- GFI EventsManager can be used to further archive, process, review and analyze those logs through Syslog processing rules, the Syslog event browser and generic Syslog reports from the GFI ReportPack

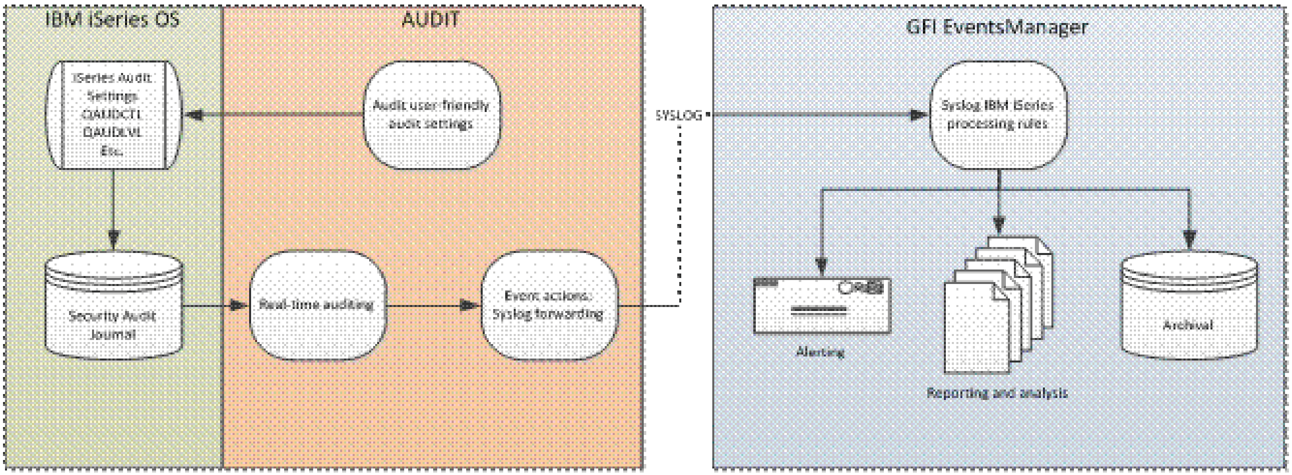

IBM iSeries OS
AUDIT
GFI EventsManager
iSeries Audit Settings QAUDCTL QAUDLVL Etc.
Audit user friendly audit settings
SYSLOG
Syslog IBM iSeries processing rules
Security Audit Journal
Real-time auditing
Event actions: Syslog forwarding
Alerting
Reporting and analysis
Archival

Figure 1

Note: GFI EventsManager does not include a license for Audit. You would need to purchase an Audit license from Raz-Lee Security for each IBM iSeries logical partition that you want to monitor.

For more information about Audit, contact Raz-Lee Security:
For general information: http://www.razlee.com/products/security/audit/audit_for_iseries_o.php
Raz-Lee Security Account Manager: http://www.razlee.com/contact_us/contact_us.php (1-888-RAZLEE-4)

Prerequisites

This procedure assumes that:

- GFI EventsManager 2011 and the GFI EventsManager ReportPack 2011 are installed on a machine in the network
- At least one functional installation of IBM iSeries logical partition is in place and Audit has been installed and configured on that iSeries logical partition

Summary of the main IBM iSeries event categories that can be processed

Through Audit and GFI EventsManager you can audit the following trails:

- **User activity**: This refers to tracking events initiated by a specific user or by a program run by that user; examples of such events include: unsuccessful sign-on attempts, program failures and attempts to use system, management tasks and so on
- **Object access auditing**: IBM iSeries systems allow auditing of all attempts to access certain critical objects, such as database files, source code files or key libraries

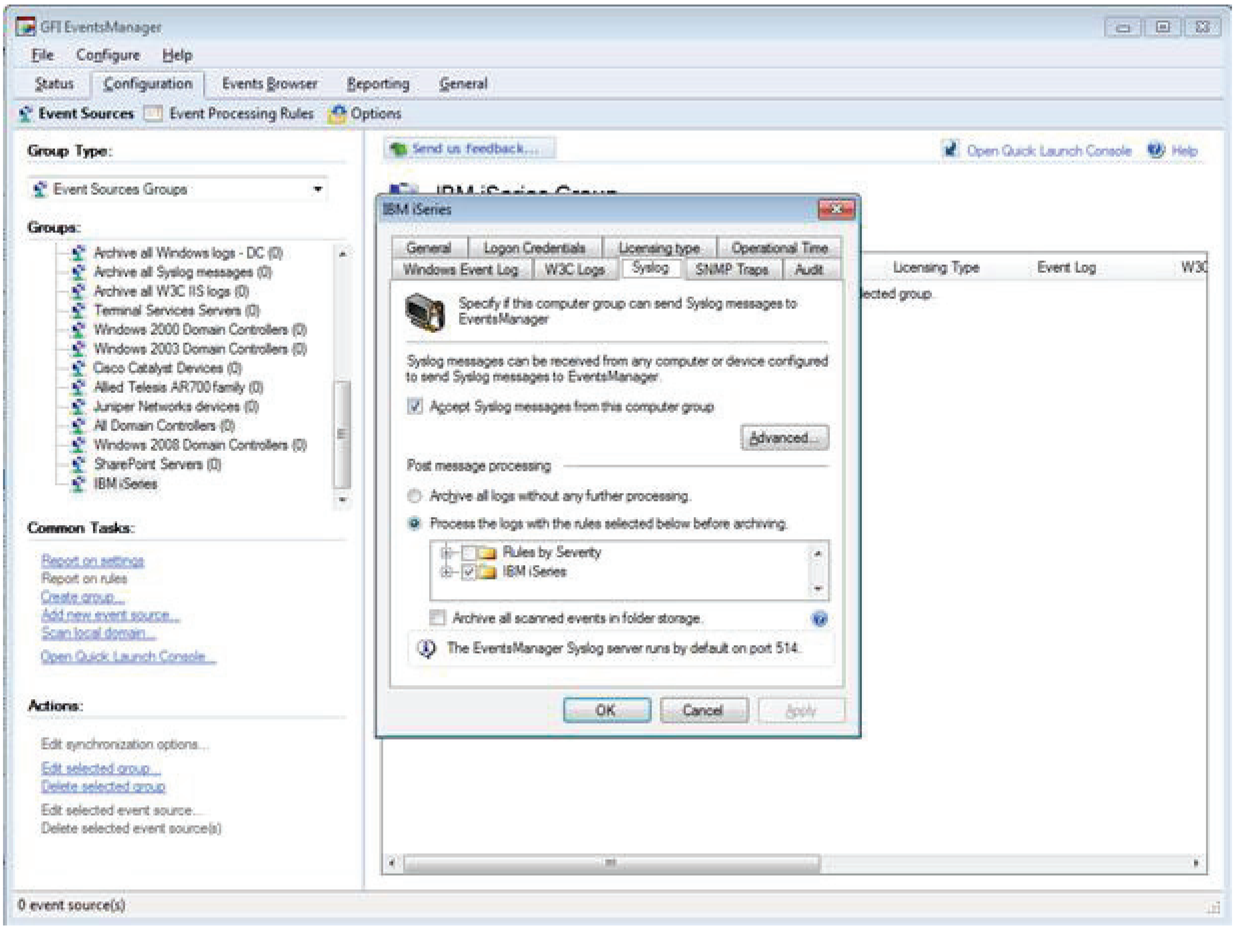
- **Security audit journal**: The security audit journal is the repository of historical security data on IBM iSeries systems.

Configuration

Configuring GFI EventsManager to accept Syslog messages from an Audit instance

Once Audit is installed on an IBM iSeries logical partition that needs to be monitored, GFI EventsManager must be setup to accept Syslog messages from that system as the logs will be sent in Syslog format. To do that, you need to:

- Open the GFI EventsManager main interface
- Go to the Configuration->Event Sources
- Select the event source group named IBM iSeries
- Right-click on the group, add a new source and enter the IP of the IBM system you wish to monitor


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Event Sources Event Processing Rules Options
Group Type:
Event Sources Groups
Groups:
Archive all Windows logs - DC (0)
Archive all Syslog messages (0)
Archive all W3C IIS logs (0)
Terminal Services Servers (0)
Windows 2000 Domain Controllers (0)
Windows 2003 Domain Controllers (0)
Cisco Catalyst Devices (0)
Allied Telesis AR700 family (0)
Juniper Networks devices (0)
All Domain Controllers (0)
Windows 2008 Domain Controllers (0)
SharePoint Servers (0)
IBM iSeries
Common Tasks:
Report on settings
Report on rules
Create group...
Add new event source...
Scan local domain...
Open Quick Launch Console...
Actions:
Edit synchronization options...
Edit selected group...
Delete selected group
Edit selected event source...
Delete selected event source(s)
0 event source(s)
Send us feedback...
Open Quick Launch Console
Help
IBM iSeries Group
Licensing Type
Event Log
W3C
lected group.
IBM iSeries
General
Logon Credentials
Licensing type
Operational Time
Windows Event Log
W3C Logs
Syslog
SNMP Traps
Audit
Advanced...
OK
Cancel
Apply

Specify if this computer group can send Syslog messages to EventsManager

Syslog messages can be received from any computer or device configured to send Syslog messages to EventsManager.

☑ Accept Syslog messages from this computer group

Post message processing

○ Archive all logs without any further processing.

● Process the logs with the rules selected below before archiving.

- □ Rules by Severity
- ☑ IBM iSeries

□ Archive all scanned events in folder storage.

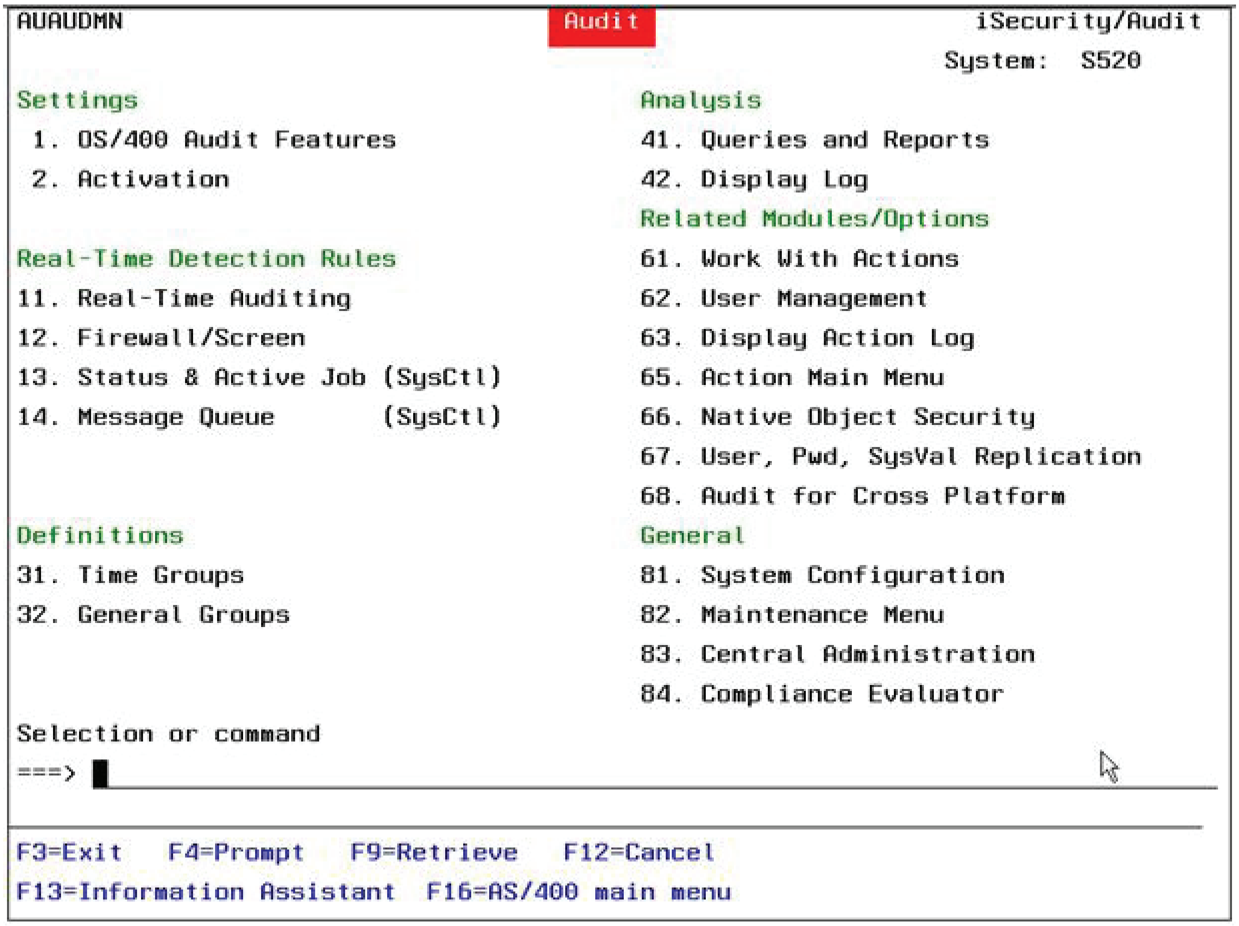
The EventsManager Syslog server runs by default on port 514.

Figure 2: IBM iSeries event sources

Now GFI EventsManager is ready to receive logs from the IBM system. By default, GFI EventsManager archives all the events and marks them as low importance events. You can change this behavior if you define your own processing rules as described later in this document.

Selecting the audit options in Audit

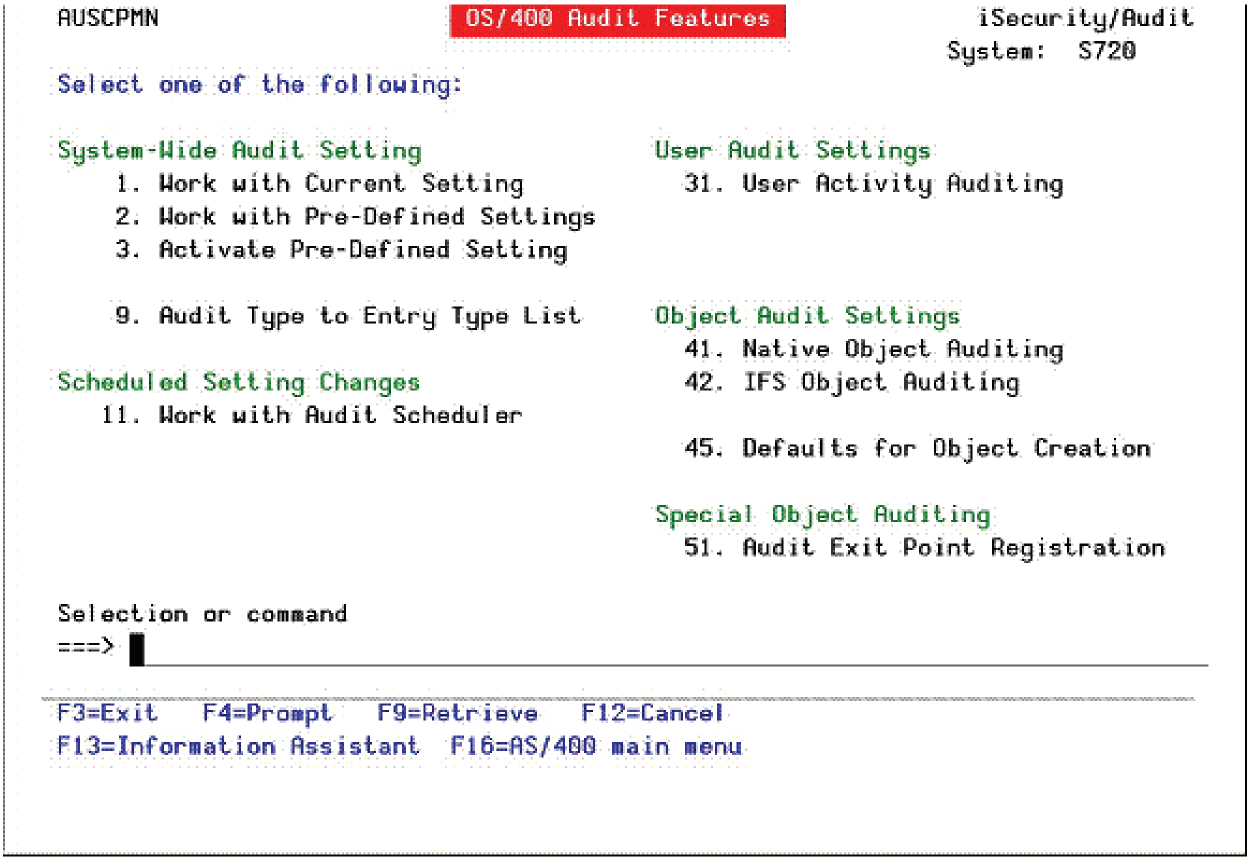
Before Audit starts to send IBM iSeries logs to GFI EventsManager, you can take a look and review the settings that control which logs you want to process from the IBM machine. To do that, you must open Audit's main interface, which allows you to perform different types of customizations.



```
AUAUDMN                          Audit                      iSecurity/Audit
                                                           System:   S520
Settings                                  Analysis
 1. OS/400 Audit Features                 41. Queries and Reports
 2. Activation                            42. Display Log
                                          Related Modules/Options
Real-Time Detection Rules                 61. Work With Actions
11. Real-Time Auditing                    62. User Management
12. Firewall/Screen                       63. Display Action Log
13. Status & Active Job (SysCtl)          65. Action Main Menu
14. Message Queue       (SysCtl)          66. Native Object Security
                                          67. User, Pwd, SysVal Replication
                                          68. Audit for Cross Platform
Definitions                               General
31. Time Groups                           81. System Configuration
32. General Groups                        82. Maintenance Menu
                                          83. Central Administration
                                          84. Compliance Evaluator

Selection or command
===> 

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

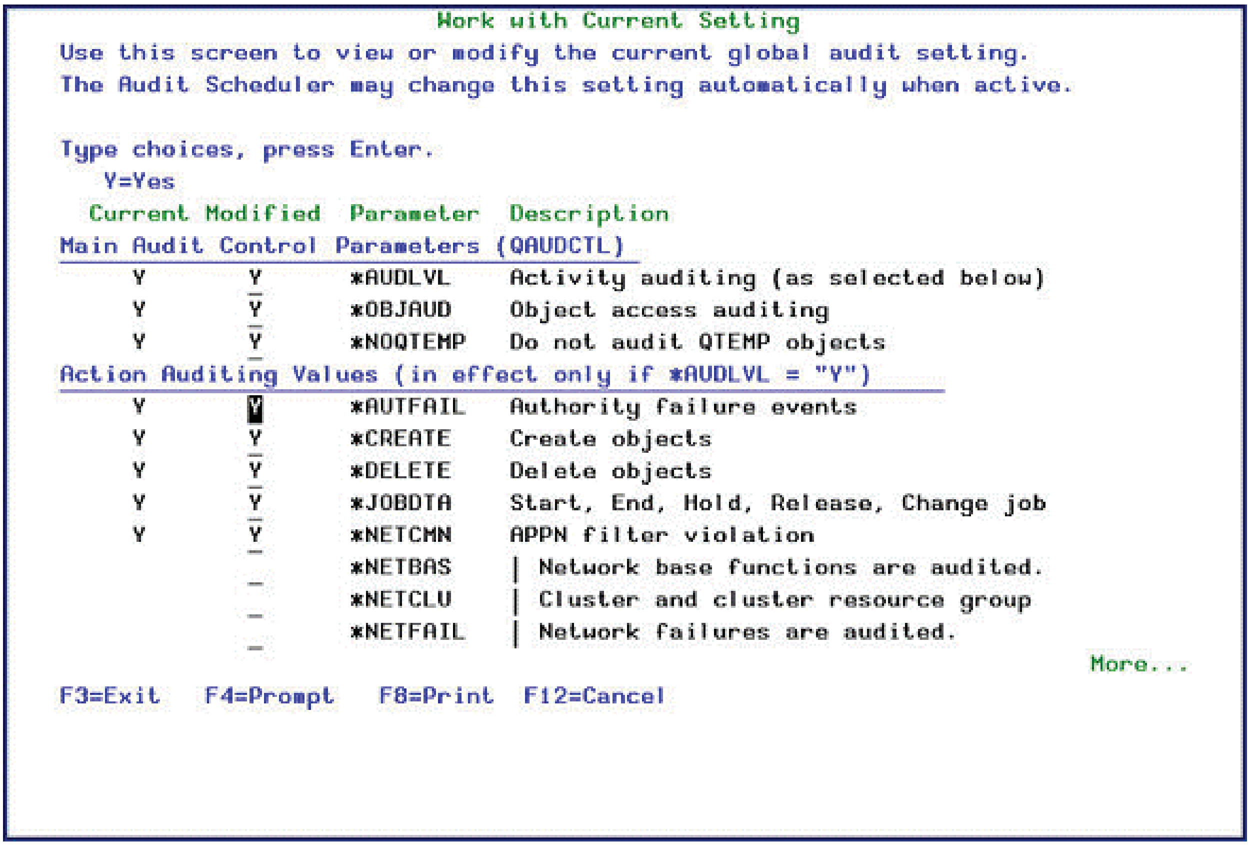
Figure 3: The main interface of Audit

Audit comes with predefined settings for auditing the most important events, but you can also customize the event categories you want to monitor if you choose option 1 and then again option 1, as per the following example depicted below:



```
AUSCPMN                   OS/400 Audit Features              iSecurity/Audit
                                                             System:   S720
Select one of the following:

System-Wide Audit Setting                User Audit Settings
    1. Work with Current Setting           31. User Activity Auditing
    2. Work with Pre-Defined Settings
    3. Activate Pre-Defined Setting

    9. Audit Type to Entry Type List     Object Audit Settings
                                           41. Native Object Auditing
Scheduled Setting Changes                  42. IFS Object Auditing
   11. Work with Audit Scheduler
                                           45. Defaults for Object Creation

                                         Special Object Auditing
                                           51. Audit Exit Point Registration

Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 4: OS/400 Audit features



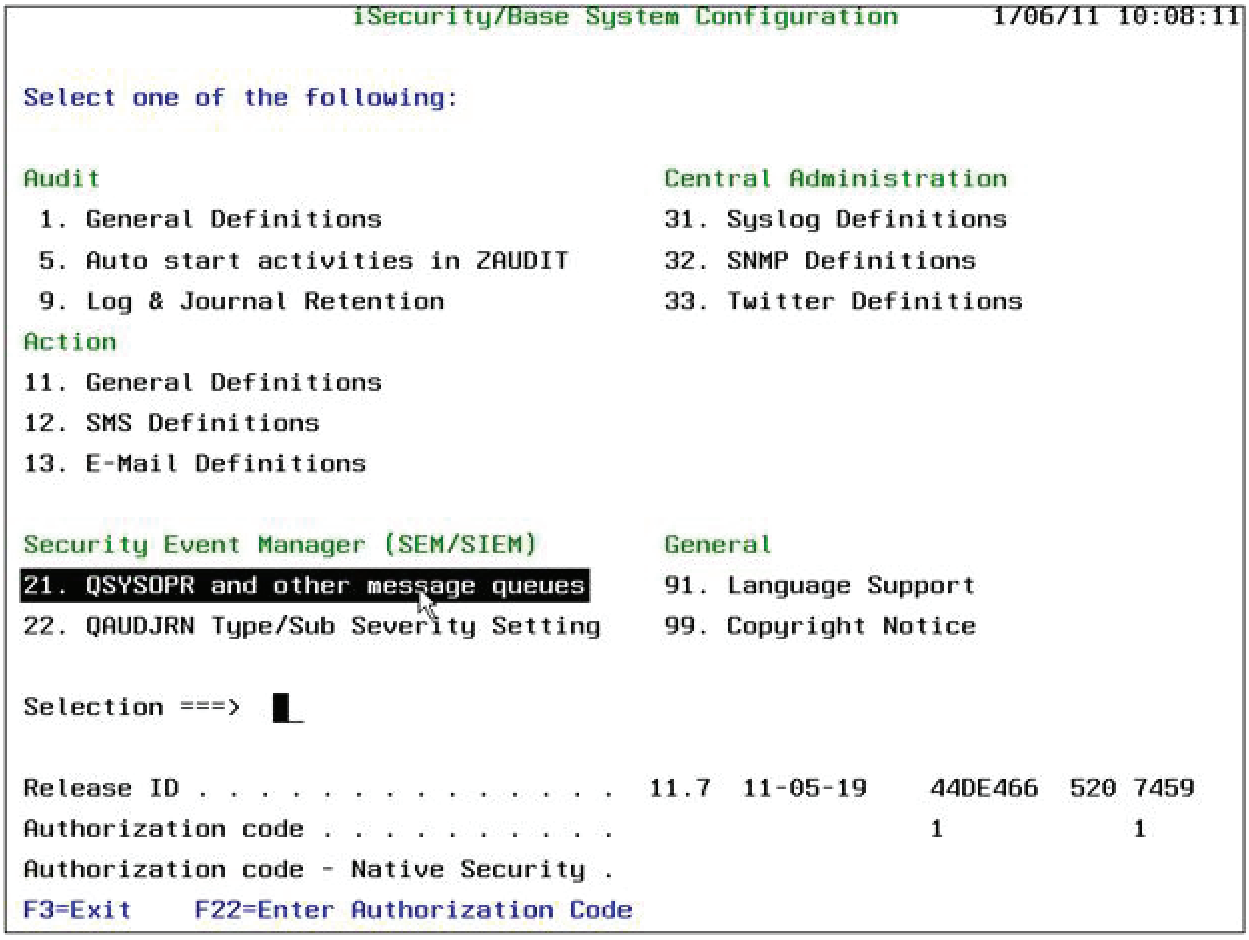
```
                          Work with Current Setting
Use this screen to view or modify the current global audit setting.
The Audit Scheduler may change this setting automatically when active.

Type choices, press Enter.
   Y=Yes
  Current Modified  Parameter  Description
Main Audit Control Parameters (QAUDCTL)
      Y        Y        *AUDLVL     Activity auditing (as selected below)
      Y        Y        *OBJAUD     Object access auditing
      Y        Y        *NOQTEMP    Do not audit QTEMP objects
Action Auditing Values (in effect only if *AUDLVL = "Y")
      Y        Y        *AUTFAIL    Authority failure events
      Y        Y        *CREATE     Create objects
      Y        Y        *DELETE     Delete objects
      Y        Y        *JOBDTA     Start, End, Hold, Release, Change job
      Y        Y        *NETCMN     APPN filter violation
               _        *NETBAS     | Network base functions are audited.
               _        *NETCLU     | Cluster and cluster resource group
               _        *NETFAIL    | Network failures are audited.
                                                                    More...
F3=Exit   F4=Prompt   F8=Print  F12=Cancel
```

Figure 5: Default IBM iSeries Audit settings

Configure Audit to forward the IBM iSeries logs as Syslog messages

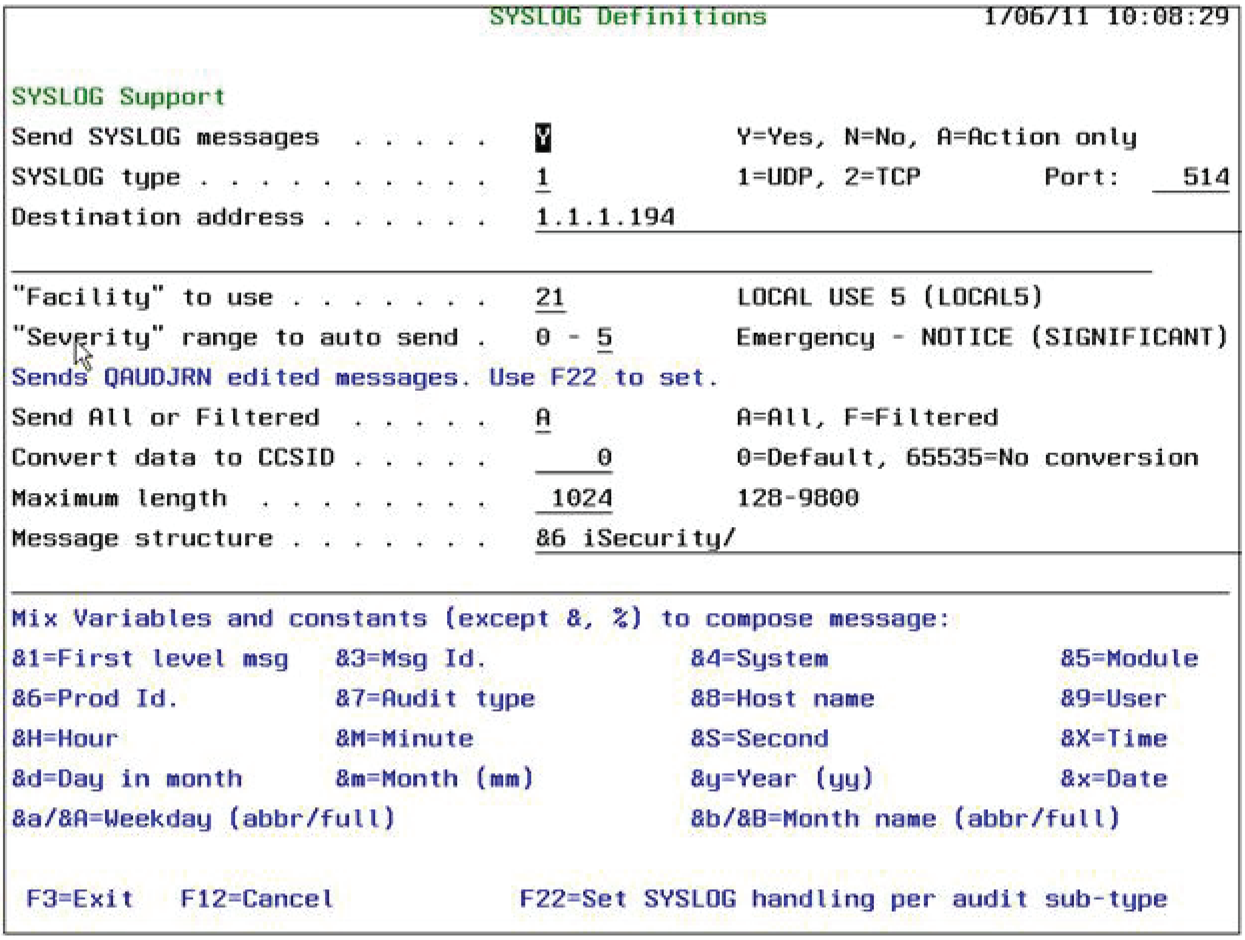
Once the audit settings are in place, you must enable the Syslog forwarder so that the new events generated on the IBM machine will be sent as Syslog messages to the machine on which GFI EventsManager is installed.

To do that, you need to know the IP address of the machine on which GFI EventsManager is installed and you must enter it in the Syslog configuration section of Audit. To get there, from the main menu you need to choose option 81, followed by option 31, as shown below.



```
                      iSecurity/Base System Configuration      1/06/11 10:08:11

 Select one of the following:

 Audit                                    Central Administration
  1. General Definitions                  31. Syslog Definitions
  5. Auto start activities in ZAUDIT      32. SNMP Definitions
  9. Log & Journal Retention              33. Twitter Definitions
 Action
 11. General Definitions
 12. SMS Definitions
 13. E-Mail Definitions

 Security Event Manager (SEM/SIEM)        General
 21. QSYSOPR and other message queues     91. Language Support
 22. QAUDJRN Type/Sub Severity Setting    99. Copyright Notice

 Selection ===>

 Release ID . . . . . . . . . . . . . .  11.7  11-05-19     44DE466   520 7459
 Authorization code . . . . . . . . . .                     1             1
 Authorization code - Native Security .
 F3=Exit    F22=Enter Authorization Code
```

Figure 6: Audit base system configuration



```
                              SYSLOG Definitions                1/06/11 10:08:29

SYSLOG Support
Send SYSLOG messages  . . . . . .   Y          Y=Yes, N=No, A=Action only
SYSLOG type . . . . . . . . . . .   1          1=UDP, 2=TCP          Port:    514
Destination address . . . . . . .   1.1.1.194


"Facility" to use . . . . . . . .   21         LOCAL USE 5 (LOCAL5)
"Severity" range to auto send .     0 - 5      Emergency - NOTICE (SIGNIFICANT)
Sends QAUDJRN edited messages. Use F22 to set.
Send All or Filtered  . . . . . .   A          A=All, F=Filtered
Convert data to CCSID . . . . . .       0      0=Default, 65535=No conversion
Maximum length  . . . . . . . . .    1024      128-9800
Message structure . . . . . . . .   &6 iSecurity/


Mix Variables and constants (except &, %) to compose message:
&1=First level msg   &3=Msg Id.             &4=System               &5=Module
&6=Prod Id.          &7=Audit type          &8=Host name            &9=User
&H=Hour              &M=Minute              &S=Second               &X=Time
&d=Day in month      &m=Month (mm)          &y=Year (yy)            &x=Date
&a/&A=Weekday (abbr/full)                   &b/&B=Month name (abbr/full)

 F3=Exit   F12=Cancel           F22=Set SYSLOG handling per audit sub-type
```

Figure 7: Configuring syslog settings in Audit

Apart from general Syslog settings like the destination IP address, common field values (e.g. facility , severity) and others, the Syslog configuration section also allows users to customize the format of the Syslog message in a very flexible manner. You can define your own Syslog message format by combining your text with values taken directly from iSeries events by using variables like: product id, date, time, event message , host name, user name and so on (as shown in the above image).

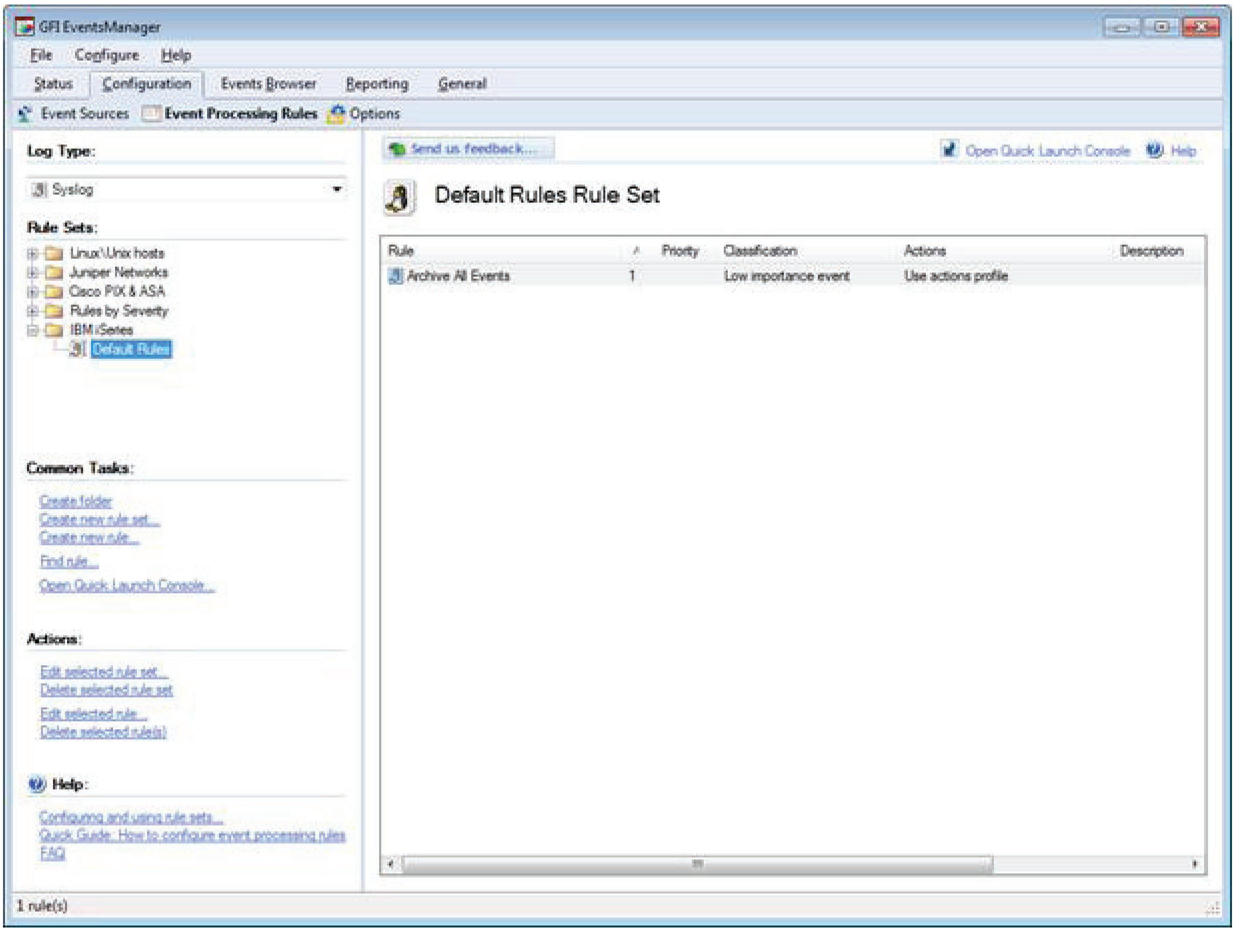
The format of the Syslog messages can also be customized based on the category of the events being audited.

Now the new events that are generated on the IBM system can be forwarded to the GFI EventsManager machine for further processing.

Processing IBM iSeries in GFI EventsManager

GFI EventsManager can process the IBM iSeries logs in the same way as it processes Syslog messages that come from different other sources. As such, depending on the format of the Syslog messages, you can define processing rules in GFI EventsManager to quickly identify and categorize the most important events, to send alerts and even to run certain applications or scripts in response to events.

GFI EventsManager ships with a predefined processing rule that archives all the IBM iSeries events into the database and marks them as low importance. Of course, you can change this behavior by defining your own rules.



Log Type: Syslog

Default Rules Rule Set

Rule	Priority	Classification	Actions	Description
Archive All Events	1	Low importance event	Use actions profile	

1 rule(s)

Figure 8: The default processing rule for IBM iSeries events

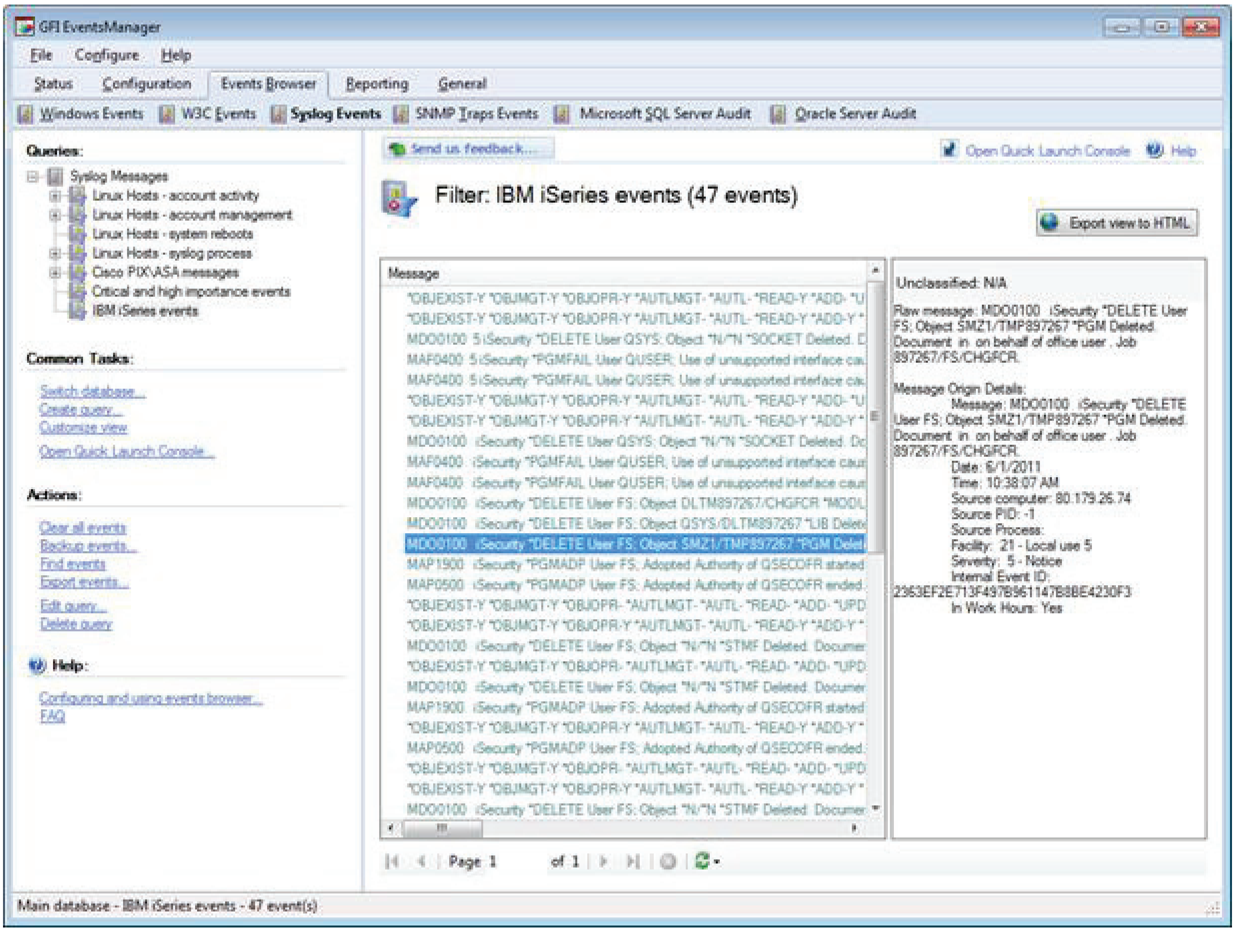
To create additional rules for IBM iSeries logs, follow these steps:

- Go to Configuration->Event Processing Rules
- Select Syslog from the Log Type combo from the top left side of the panel
- Select IBM iSeries->Default rules
- Right-click on the rules set to create new rules, making sure you assign rules a higher priority to the new rules than the default which is shipped with the product

For more information about creating processing rules click on the following link: http://support.gfi.com/manuals/en/esm2011/esm2011manual.1.47.html#9001941

GFI EventsManager also allows users to store the iSeries logs, for short or long term, into SQL Server databases, into storage files or into backup files that can be compressed and encrypted.

To review the IBM iSeries logs, you must open the Syslog events browser. GFI EventsManager ships with a predefined view for IBM iSeries which selects the iSeries events which contains "iSecurity" keyword inside the message. Of course, you can also define your own views to quickly sort and filter the events of interest.



Filter: IBM iSeries events (47 events)

```
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD- *U
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD-Y *
MDO0100  5 iSecurity *DELETE User QSYS: Object *N/*N *SOCKET Deleted. D
MAF0400  5 iSecurity *PGMFAIL User QUSER: Use of unsupported interface cau
MAF0400  5 iSecurity *PGMFAIL User QUSER: Use of unsupported interface cau
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD- *U
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD-Y *
MDO0100   iSecurity *DELETE User QSYS: Object *N/*N *SOCKET Deleted. Dc
MAF0400   iSecurity *PGMFAIL User QUSER: Use of unsupported interface caus
MAF0400   iSecurity *PGMFAIL User QUSER: Use of unsupported interface caus
MDO0100   iSecurity *DELETE User FS: Object DLTM897267/CHGFCR *MODU
MDO0100   iSecurity *DELETE User FS: Object QSYS/DLTM897267 *LIB Delete
MDO0100   iSecurity *DELETE User FS: Object SMZ1/TMP897267 *PGM Delet
MAP1900   iSecurity *PGMADP User FS: Adopted Authority of QSECOFR started
MAP0500   iSecurity *PGMADP User FS: Adopted Authority of QSECOFR ended.
*OBJEXIST-Y *OBJMGT-Y *OBJOPR- *AUTLMGT- *AUTL- *READ- *ADD- *UPD
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD-Y *
MDO0100   iSecurity *DELETE User FS: Object *N/*N *STMF Deleted. Documer
*OBJEXIST-Y *OBJMGT-Y *OBJOPR- *AUTLMGT- *AUTL- *READ- *ADD- *UPD
MDO0100   iSecurity *DELETE User FS: Object *N/*N *STMF Deleted. Documer
MAP1900   iSecurity *PGMADP User FS: Adopted Authority of QSECOFR started
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD-Y *
MAP0500   iSecurity *PGMADP User FS: Adopted Authority of QSECOFR ended.
*OBJEXIST-Y *OBJMGT-Y *OBJOPR- *AUTLMGT- *AUTL- *READ- *ADD- *UPD
*OBJEXIST-Y *OBJMGT-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y *ADD-Y *
MDO0100   iSecurity *DELETE User FS: Object *N/*N *STMF Deleted. Documer
```

```
Unclassified: N/A

Raw message: MDO0100  iSecurity *DELETE User
FS: Object SMZ1/TMP897267 *PGM Deleted.
Document  in  on behalf of office user . Job
897267/FS/CHGFCR.

Message Origin Details:
            Message: MDO0100  iSecurity *DELETE
User FS: Object SMZ1/TMP897267 *PGM Deleted.
Document  in  on behalf of office user . Job
897267/FS/CHGFCR.
            Date: 6/1/2011
            Time: 10:38:07 AM
            Source computer: 80.179.26.74
            Source PID: -1
            Source Process:
            Facility:  21 - Local use 5
            Severity:  5 - Notice
            Internal Event ID:
2363EF2E713F497B961147B8BE4230F3
            In Work Hours: Yes
```

Figure 9: IBM iSeries events in the GFI EventsManager browser

For more information about creating views, click on this link: http://support.gfi.com/manuals/en/esm2011/esm2011manual.1.21.html

For reporting purposes, there are two important features available in EventsManager:

- From the Syslog browser you can generate HTML reports based on the events shown in the current view (just click on the "Export view to HTML" button). You can also customize the layout of the HTML reports by selecting the columns of the report or the css section that corresponds to the template. For more information about HTML reports, click on the following link: http://support.gfi.com/manuals/en/esm2011/esm2011manual.1.24.html#9000759
- From the GFI ReportPack, users can select the generic Syslog report (Miscellaneous, Customizable Reports->Generic Syslog) to generate or schedule reports in PDF format using a predefined layout.

Technical difficulties and support

In case of technical difficulties with any of the components involved in the process described in this document, it is important to first evaluate which part of the process is failing in order to contact the appropriate support personnel.

- GFI EventsManager is not receiving any event coming from the IBM iSeries machine.
  - To see which part of the solution is failing, you need to check the following items:
    - Check if the IP of the IBM iSeries system is correctly configured in GFI EventsManager; check the properties of the event group and the machine to make sure Syslog scanning is enabled on the desired protocol and port
    - Check your firewall settings and make sure they allow incoming Syslog traffic from the IBM machine

    - If the previous points do not help you fix the problem, go to the Status->Job Activity->Server Message History panel and check for any information about incoming messages from the IBM system.
        - If you can see that messages are incoming, then it is likely that your processing rules are not properly configured. You should review the definition and priority of the rules which are used to process the IBM events or contact the GFI support team (http://support.gfi.com)
        - If there are no incoming messages, then most probably Audit is unable to send those messages from the IBM machine. You should contact the Raz-Lee Security support team by email (support@razlee.com) or phone (1-888-RAZLEE-2).

- GFI EventsManager is receiving IBM iSeries events, but some events of interest seem to be missing.
    - This part of the process is related to Audit. You should review the settings of Audit or contact the Raz-Lee Security support team via email (support@razlee.com). In emergency situations, send an e-mail and also call 1-888-RAZLEE-4).
- Events are being generated on the IBM iSeries server but GFI EventsManager is unable to process them according to the configured processing rules.
    - This part of the process is related to GFI EventsManager and will be handled by the GFI support team which can be contacted via http://support.gfi.com.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small and medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

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, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

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

Disclaimer

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

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