iSecurity SIEM

User Guide
Version 14.12

www.razlee.com

Contents

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The SIEM User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Native IBM i (OS/400) User Interface

SIEM is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

COMMAND **> 81 > 32**

meaning: Syslog definitions activated by typing ***COMMAND***and selecting option: **81** then option: **32**.

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. *To* select a menu option, simply type the option number and press **Enter**. The command line is

available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1**: **Help** Display context-sensitive help
- **F3**: **Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4**: **Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6**: **Add New** Create a new record or data item
- **F8**: **Print** Print the current report or data item
- **F9**: **Retrieve** Retrieve the previously-entered command
- **F12**: **Cancel** Return to the previous screen or menu without updating

Legal Notice

Contacts

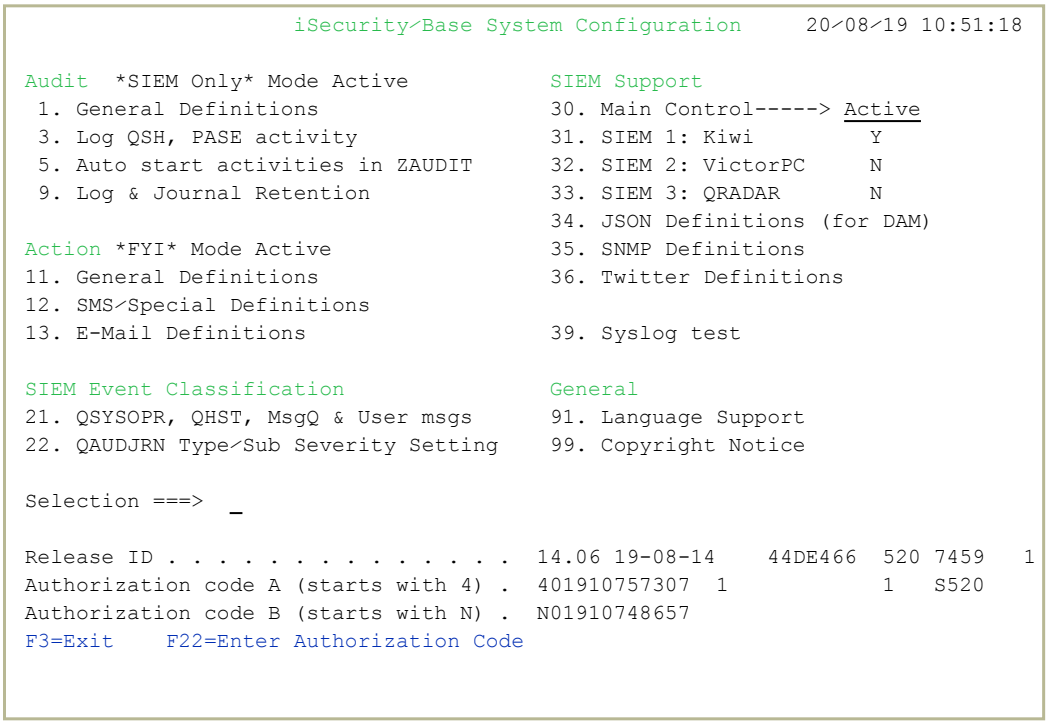
Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

SIEM Support

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems. Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, malicious network access to the Series i, and more.

System Configuration

This section shows you how to set general configuration for Audit. To access configuration features, select **81. System Configuration** in the Main menu (*STRAUD* > **81**). The **iSecurity/Base System Configuration** menu appears.



QAUDJRN Type/Sub Severity Setting

You can set the range of severities for each Audit type to control when to send entries to SIEM reporting.

1. Select **22. QAUDJRN Type/Sub Severity Setting** from the iSecurity/Base System Configuration screen (*STRAUD* **> 81 > 22**). The **QAUDJRN Type/Sub Severity Setting** screen appears.

```
                          SIEM Severity Setting
                                              Subset by type. .  _________
                                                    by entry .  __
Type options, press Enter.                          by text. .  ______________
  blank=Do not send   0=Emergency   1=Alert   2=Critical   3=Error
  4=Warning   5=Notice   6=Info   7=Debug   I=Use IBM standard
SIEM   IBM  Audit            Pink represents additions
1 2 3  STD  Type  Type       to types not covered by IBM
6 6 6   6   @1 A  *ACTIVE    Message queue (Group Id 1)
6 6 6   6   @2 A             Message queue (Group Id 2)
6 6 6   6   @3 A             Message queue (Group Id 3)
6 6 6   6   @4 A             Message queue (Group Id 4)
6 6 6   6   @5 A             Message queue (Group Id 5)
6 6 6   6   @6 A             Message queue (Group Id 6)
6 6 6   6   @7 A             Message queue (Group Id 7)
6 6 6   6   @8 A             Message queue (Group Id 8)
I I I   I   @9 A             QHST messages. Set I for IBM standard severety.
5 5 5   5   AD D  *SECURITY  Auditing of a DLO was changed with CHGDLOAUD
                             command.
5 5 5   5   AD G             Get user from identity token successful
                                                                      More...
F3=Exit  F19=Info  F21=Set 1 as IBM  F22=Set 2 as IBM  F23=Set 3 as IBM
```

Each line on the body of the screen represents a single IBM audit type. (If the description field of the type is longer than will fit on a single line, it wraps onto a second.)

Enter the required severity level for each SIEM in the first three fields for each line. All events of this Audit Type/ Subtype that have this severity level or higher are sent to SIEM. The higher the level, the fewer events that are sent.

Possible values include:

- Blank = Do not send
- **0** = Emergency
- **1** = Alert
- **2** = Critical

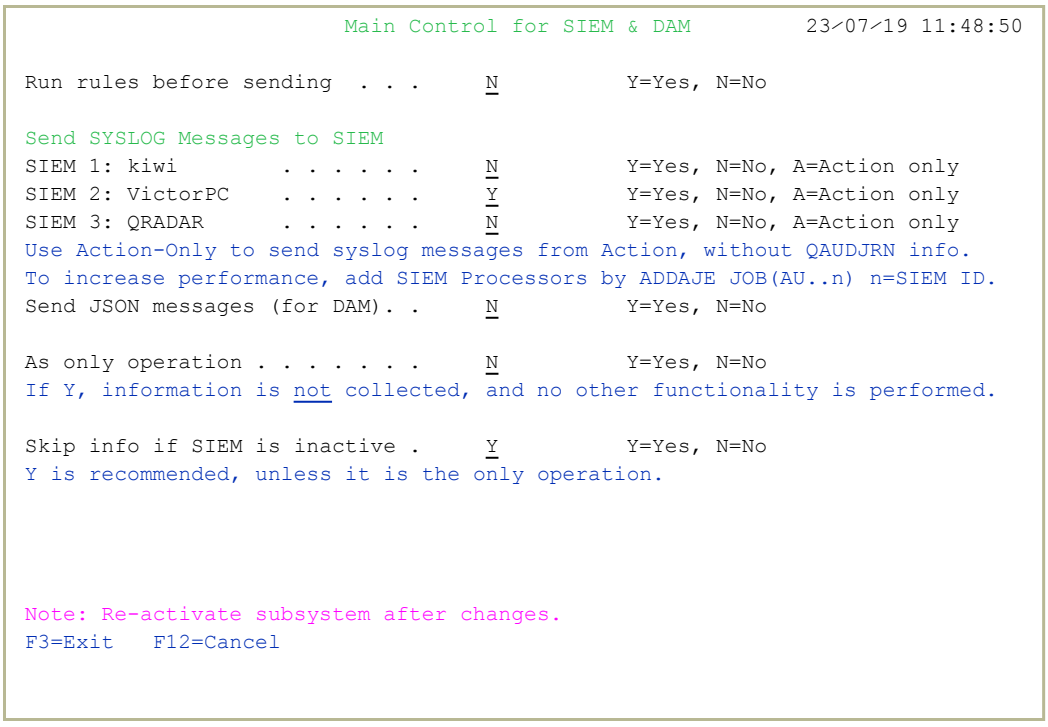
- **3** = Error
- **4** = Warning
- **5** = Notice
- **6** = Info
- **7** = Debug

Syslog Parameters

The syslog standards, LEEF and CEF, send data in Field mode enabling pairs of data to be displayed, i.e. Field name and Field value. QHST, QSYSOPR and others in the message queue are supported in LEED and CEF field mode. UDP, TCP and TLS (encrypted) protocols are supported and once the settings are turned on, the SIEM can intercept the message and make it legible for the Syslog Admin. Standard message support for edited messages and replacement values exist, enabling sending information in any free format as well as LEEF and CEF.

To send syslog messages for SIEM:

1. Select **30. Main Control** from the **iSecurity/Base System Configuration** screen (*STRAUD* **> 81 > 30**). The **Main Control for SIEM & DAM** screen appears.



The body of the screen includes these fields:

Run rules before sending

Y = Yes

N = No

Send SYSLOG messages to SIEM

Y = Yes

N = No

A = Action only; Use Action-Only to send syslog messages from Action, without QAUDJRN info.

Send JSON messages (for DAM)

Y = Yes; Y is recommended, unless it is the only operation.

N = No

As only operation

Y = Yes; If Y, information is not collected, and no other functionality is performed.

N = No

Skip info if SIEM is inactive

Y = Yes; Y is recommended, unless it is the only operation.

N = No

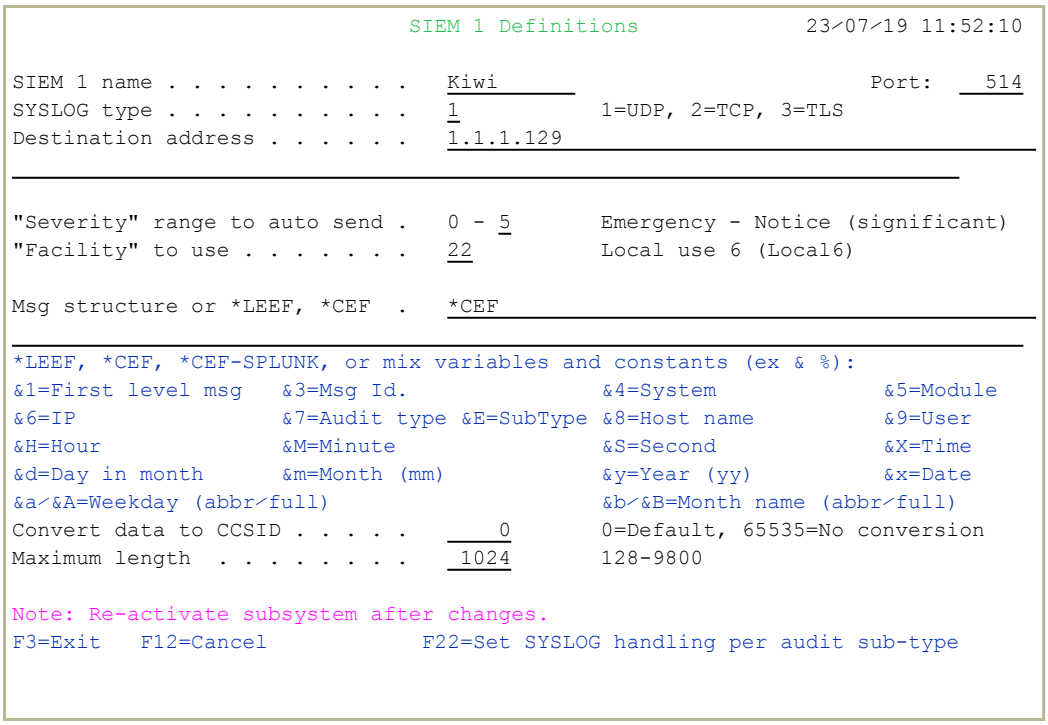
Triple Syslog Definitions (#1-#3)

Events from IBM i and different Audit entry types are sent to a remote SYSLOG server according to a range of severities such as Emergency, Alert, Critical, Error, and Warning. When **Send SYSLOG messages (for SIEM)** is set to `Yes` in the Main Control for SIEM & DAM definitions, the product will automatically send all events according to the Severity range to auto send for the message structure selected, as described in the table below.

The option to use more than one SIEM is implemented on a separate job per SIEM. This is enabled by an intermediate buffer which assists SIEM in overcoming communication problems or SIEM downtime, while sending a message to QSYSOPR when the buffer is full or processes are delayed. For this purpose Triple Syslog definitions are required, which are described in this section.

To configure SIEM message structure:

1. Select the SIEM system from the iSecurity/Base System Configuration menu (*STRAUD* **> 81**).
    - For SIEM 1, Select **31. SIEM 1** (*STRAUD* **> 81 > 31**).
    - For SIEM 2, Select **32. SIEM 2** (*STRAUD* **> 81 > 32**).
    - For SIEM 3, Select **33. SIEM 3** (*STRAUD* **> 81 > 33**).
2. The selected SIEM Definitions screen appears.



The body of the screen includes these fields:

SIEM name

The name of the SIEM system.

Port

The port to which the Syslog is listening, according to the SYSLOG type. SYSLOG type 3 uses port 6514.

SYSLOG type

The type of SYSLOG for this SIEM. Possible values are:

- **1**: UDP
- **2**: TCP
- **3**: TLS

Destination address

The IP address of the SIEM

Severity range to auto send

Send SYSLOG messages for event with a severity from 0 through this value:

- **0**: EMERGENCY - EMERGENCY
- **1**: EMERGENCY - ALERT

- **2**: EMERGENCY - CRITICAL
- **3**: EMERGENCY - ERROR
- **4**: EMERGENCY - WARNING
- **5**: EMERGENCY - NOTICE (SIGNIFICANT)
- **6**: EMERGENCY - INFORMATIONAL
- **7**: EMERGENCY - DEBUG

Facility to use

The facility that sends SYSLOG messages to this SIEM:

- **1**: USER-LEVEL MESSAGES
- **2**: MAIL SYSTEM
- **3**: SYSTEM DAEMONS
- **4**: SECURITY/AUTHORIZATION MESSAGES
- **5**: SYSLOGD INTERNAL
- **6**: LINE PRINTER SUBSYSTEM
- **7**: NETWORK NEWS SUBSYSTEM
- **8**: UUCP SUBSYSTEM
- **9**: CLOCK DAEMON
- **10**: SECURITY/AUTHORIZATION MESSAGES
- **11**: FTP DAEMON
- **12**: NTP SUBSYSTEM
- **13**: LOG AUDIT
- **14**: LOG ALERT
- **15**: CLOCK DAEMON
- **16**: LOCAL USE 0 (LOCAL0)
- **17**: LOCAL USE 1 (LOCAL1)
- **18**: LOCAL USE 2 (LOCAL2)
- **19**: LOCAL USE 3 (LOCAL3)
- **20**: LOCAL USE 4 (LOCAL4)
- **21**: LOCAL USE 5 (LOCAL5)
- **22**: LOCAL USE 6 (LOCAL6)
- **23**: LOCAL USE 7 (LOCAL7)

Message Structure

Messages can be in two predefined formats or constructed freely from a wide variety of constants and variables.

The predefined formats are:

- **CEF** – Common Event Format, an open standard that passes messages over to the communications module that handles the transmission of the messages to the waiting log collection server using either UDP, TCP or TLS protocol.
- **LEEF** – Log Event Extended Format, another open standard for log management and interoperability of security related information from different devices, network components and applications. The LEEF format is a customized event format for IBM security Qradar that contains readable and easily processed events.

Free definitions can use these elements:

- **&a**: Abbreviated name of the day of the week (Sun, Mon, and so on).
- **&A**: Full name of the day of the week (Sunday, Monday, and so on).
- **&b**: Abbreviated month name (Jan, Feb, and so on).
- **&B**: Full month name (January, February, and so on).
- **&c**: Date/Time in the format of the locale.
- **&C**: Century number [00-99], the year divided by 100 and truncated to an integer.
- **&d**: Day of the month [01-31].
- **&D**: Date Format, same as **&m/&d/&y**.
- **&e**: Same as **&d**, except single digit is preceded by a space [1-31].
- **&g**: 2 digit year portion of ISO week date [00,99].
- **&G**: 4 digit year portion of ISO week date. Can be negative.
- **&h**: Same as **&b**.
- **&H**: Hour in 24-hour format [00-23].
- **&I**: Hour in 12-hour format [01-12].
- **&j**: Day of the year [001-366].
- **&L**: Three digit milliseconds part of event time
- **&m**: Month [01-12].
- **&M**: Minute [00-59].
- **&n**: Newline character.

- **&O**: UTC offset. Output is a string with format **+HH:MM** or **–HH:MM**, where **+** indicates east of GMT, **–** indicates west of GMT, **HH** indicates the number of hours from GMT, and **MM** indicates the number of minutes from GMT.
- **&p**: AM or PM string.
- **&r**: Time in AM/PM format of the locale. If not available in the locale time format, defaults to the POSIX time AM/PM format: **&I:&M:&S&p**.
- **&R**: 24-hour time format without seconds, same as **&H:&M**.
- **&S**: Second [00-61]. The range for seconds allows for a leap second and a double leap second.
- **&t**: Tab character.
- **&T**: 24-hour time format with seconds, same as **&H:&M:&S**.
- **&u**: Weekday [1,7]. Monday is 1 and Sunday is 7.
- **&U**: Week number of the year [00-53]. Sunday is the first day of the week.
- **&V**: ISO week number of the year [01-53]. Monday is the first day of the week. If the week containing January 1st has four or more days in the new year then it is considered week 1. Otherwise, it is the last week of the previous year, and the next year is week 1 of the new year.
- **&w**: Weekday [0,6], Sunday is 0.
- **&W**: Week number of the year [00-53]. Monday is the first day of the week.
- **&x**: Date in the format of the locale.
- **&X**: Time in the format of the locale.
- **&y**: 2 digit year [00,99].
- **&Y**: 4-digit year. Can be negative.
- **&z**: UTC offset. Output is a string with format **+HHMM** or **–HHMM**, where **+** indicates east of GMT, **–** indicates west of GMT, **HH** indicates the number of hours from GMT, and **MM** indicates the number of minutes from GMT.
- **&Z**: Time zone name.
- **&0**: Bytes 1-9800 in USRDATA (9800 bytes). This can only be used as the last parameter.
- **&1**: The first level message

- **&2**: Bytes 1101-9800 in USRDATA (8700 bytes). This can only be used as the last parameter.
- **&3**: The ID of the first level message
- **&4**: The name of the system where the event took place
- **&5**: The full name of the RazLee product
- **&6**: The IP address of the system where the event took place
- **&7**: The two character Audit type of the transaction
- **&8**: The Host name of the system where the event took place
- **&9**: The user ID for the event

Convert data to CCSID

Whether to convert data to CCSID. Possible values include **0**, to use the system default, or **66535** for no conversion.

Maximum length

The maximum length of the string. This can be an integer between **128** and **9800**.

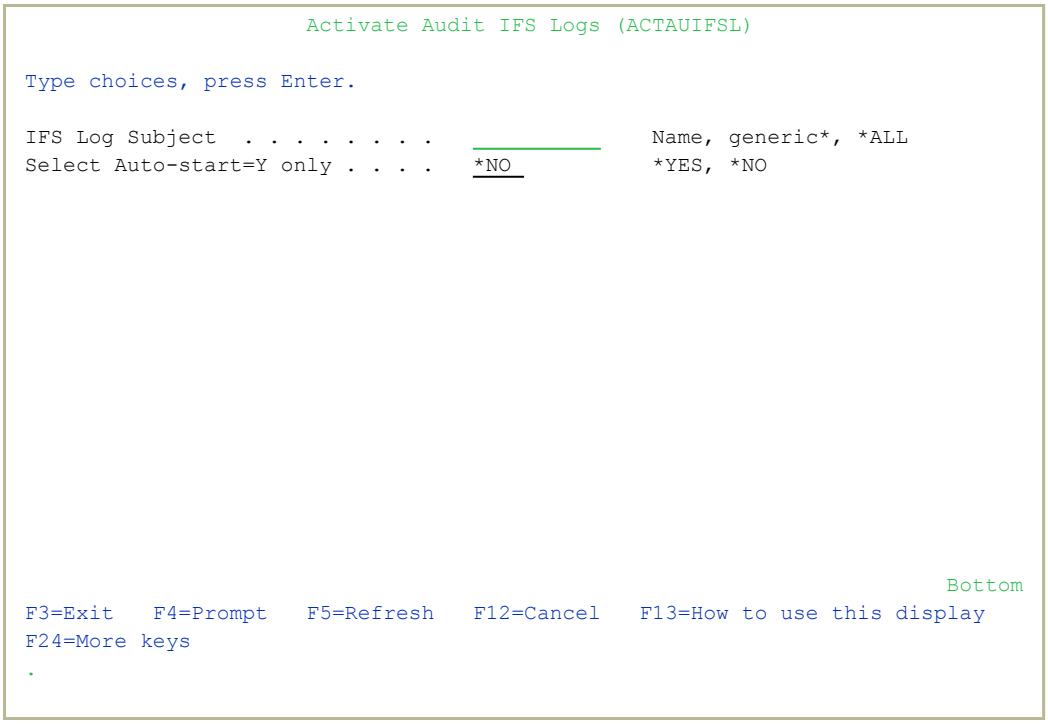
NOTES:

- These fields are not converted to ASCII.
- SYSLOG manager must set maximum message length from default (1024) to expected size (10000).
- SYSLOG manager must take care of non-printable characters option.

Activate /Deactivate IFS Log Detection

Once the administrator has added and configured all of the desired servers to participate in the SIEM message handling, you can proceed to the **`Activate IFS Log Detect`** section in order to Activate/Deactivate them for transmitting the information to the SIEM system. Use this section in order to activate the servers that were configured at the **Work with IFS logs Auditing** menu page.

To **activate Audit IFS Logs** (ACTAUIFSL), select **`21. Activate`** from the **IFS Logs** screen (*STRAUD* **`> 15 > 21`**). The **Activate Audit IFS Logs** screen appears:



The body of the screen includes these fields:

`IFS Log Subject`

Choose which servers should send their messages to the SIEM system. The administrator can choose between a specific server (Name) and all enabled servers (*ALL).

`Select Auto-start=Y only`

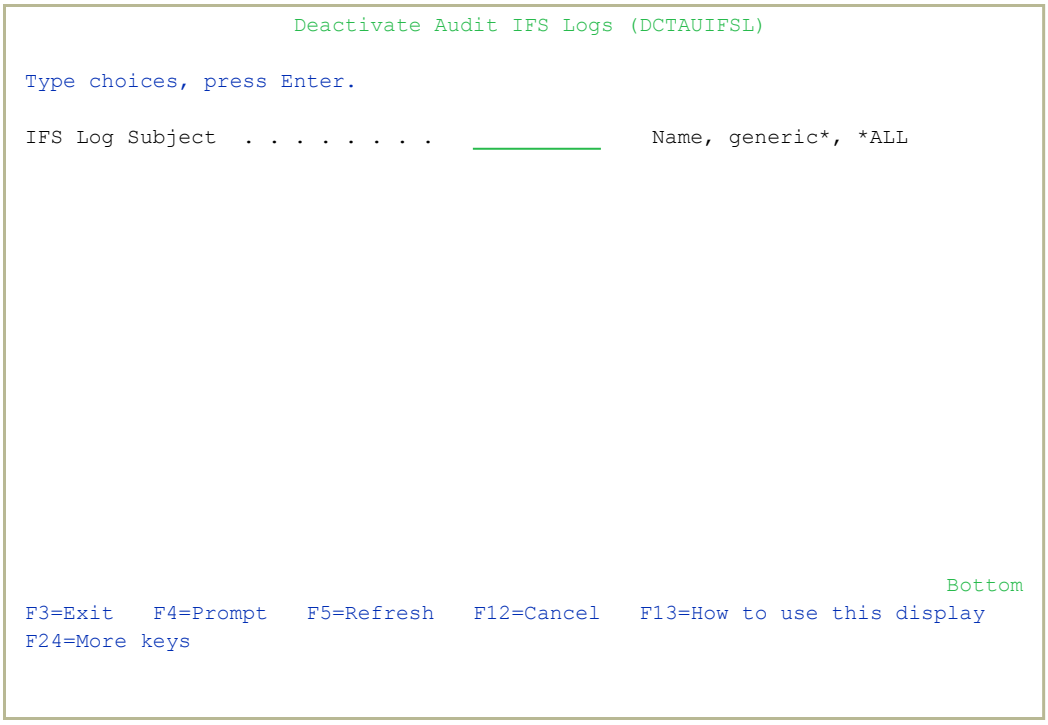
If set to `*YES`, activate only the servers with that IFS Log Subject for which the Auto-Start field was set to "`Y`" on the **Work with IFS Logs**

Definition screen.

NOTE: Only the enabled subject at the **Control IFS Logs** menu will be activated.

To deactivate Audit IFS Logs (DCTAUIFSL):

1. Select **22. Deactivate** from the **IFS Logs** screen (*STRAUD* **> 15 > 22**).



2. Enter the log subject to deactivate or `*ALL` to deactivate all of them, then press **Enter**.

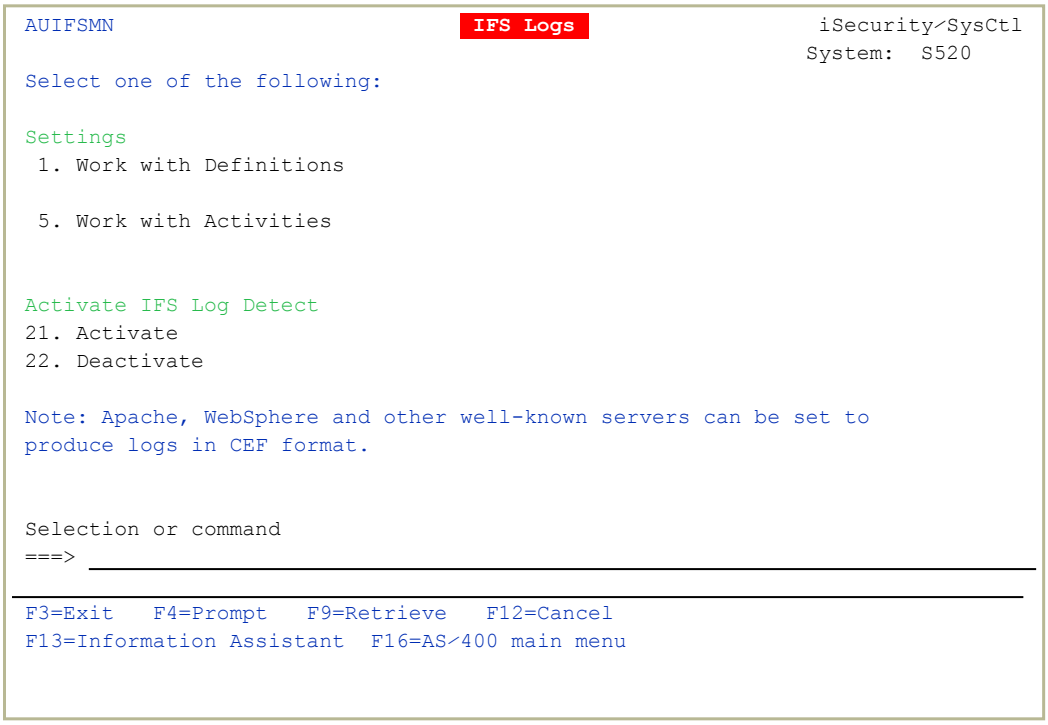
Working with IFS logs

When an organization is using a Security Information and Event Management (SIEM) system, Raz-Lee Security provides the administrator with an easy and effective tool for sending messages and events to those systems. With special capabilities and advanced features, Raz-Lee allows configuring up to three unique SIEM systems to be handled using the IFS logs mechanism.

NOTE: For more information about SIEM integration and configuration, see SIEM Support.

To access the IFS Logs:

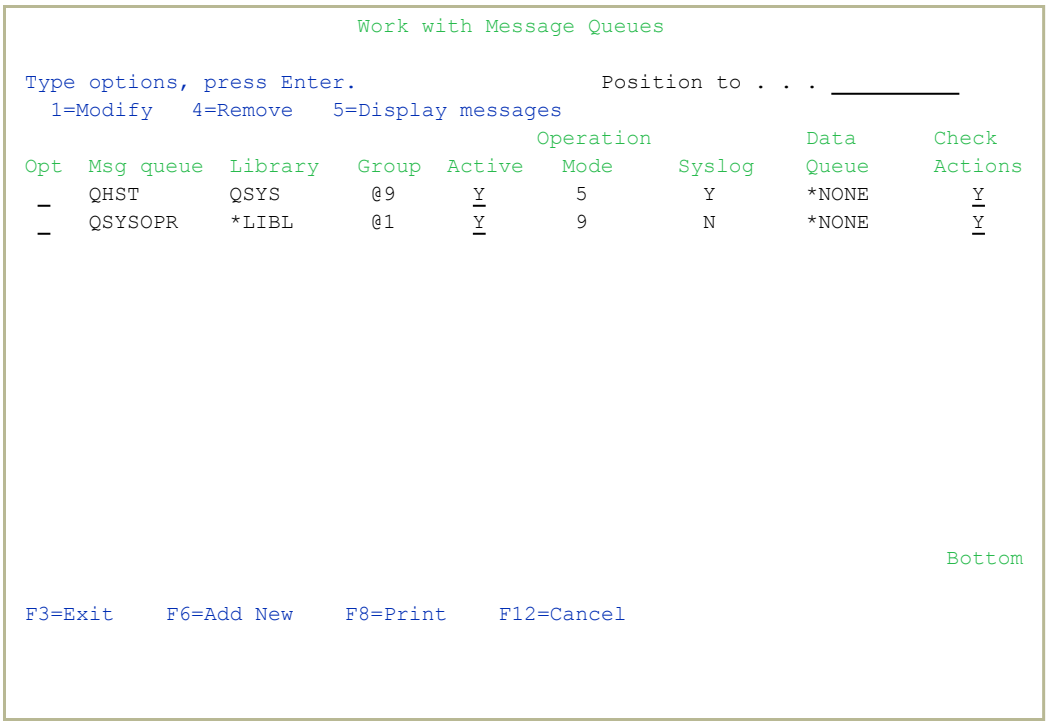
- Select **15. IFS Logs** from the Audit main menu screen (*STRAUD* **> 15)**.



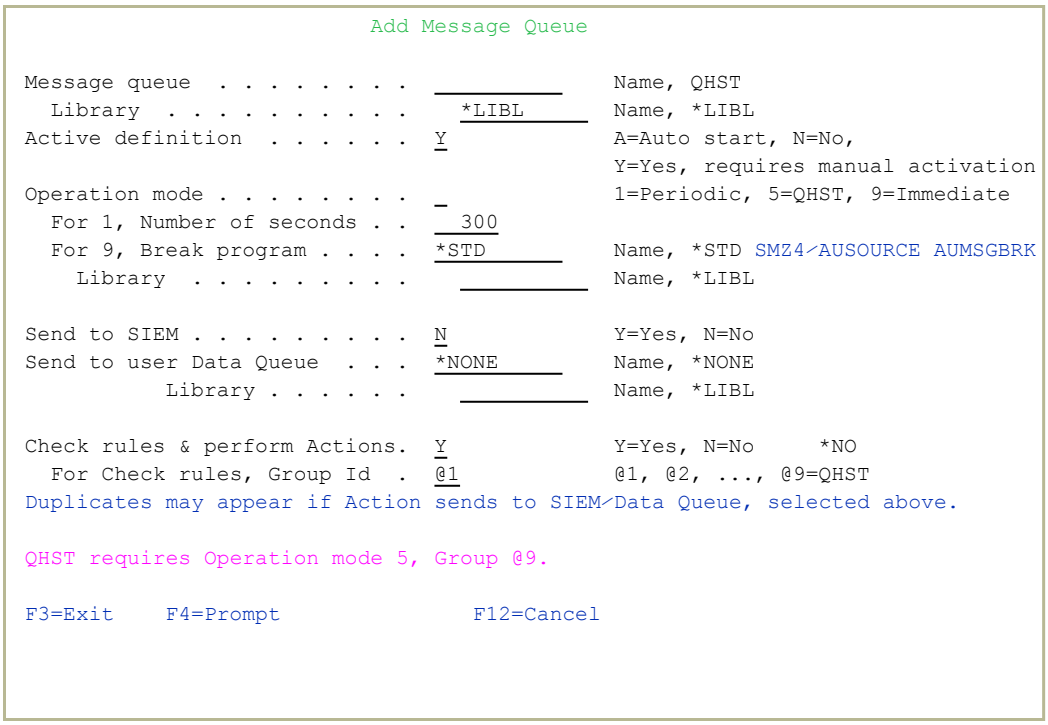
The **IFS Logs** menu allows the administrator to set and configure various types of message sources to be forwarded to SIEM systems such as Apache web server, IBM's WebSphere Application Server (WAS), and various database tools.

Create Message Queue Audit Rules

1. To define a message queue to monitor, select **`1. Control Message Queues/QHST`** from the Message Queue menu (*STRAUD*> **`14 > 1`**). The **`Work with Message Queues`** screen appears.



2. Select **`1=Modify`** to modify an existing message queue or **F6** to create a new message queue. The **`Add Message Queue`** screen appears.



The body of the screen includes these fields:

Message queue/library

The name of message queue being created or modified and the library where it exists.

Active Definition

A = Automatic start at IPL or restart. You can only choose this if the Message Queues (set to start at *IPL) parameter in the Auto Start Activities screen is set to Yes.

Y = Yes. After activating ZAUDIT, you will need to manually restart the Message Queue.

N = No

Operation mode

1 = Periodic

5 = Watch. You must use 5 if you are monitoring QHST.

9 = Immediate

Number of seconds

If Operation Mode is set to **1**, the number of seconds to wait between each application of the rule.

Break program/library

If Operation Mode is set to **9**, the name and library of the program to use for break handling.

The program source for ***STD** is *SMZ4/AUSOURCE AUMSGBRK*.

Send to SIEM

Define how to send the break information to SIEM:

1 = Syslog

2 = SNMP

N = No

Send to user data queue/library

Define the name and library of the data queue to use for break handling.

Check rules & perform Actions

Y = Yes

N = No

For check rules, Group Id

The Group ID for the rule definitions. Use option **11. Message Queue** rules to create/modify the rule definitions. Use the Group ID to group message queues with similar handling together to reduce the number of rules needed.

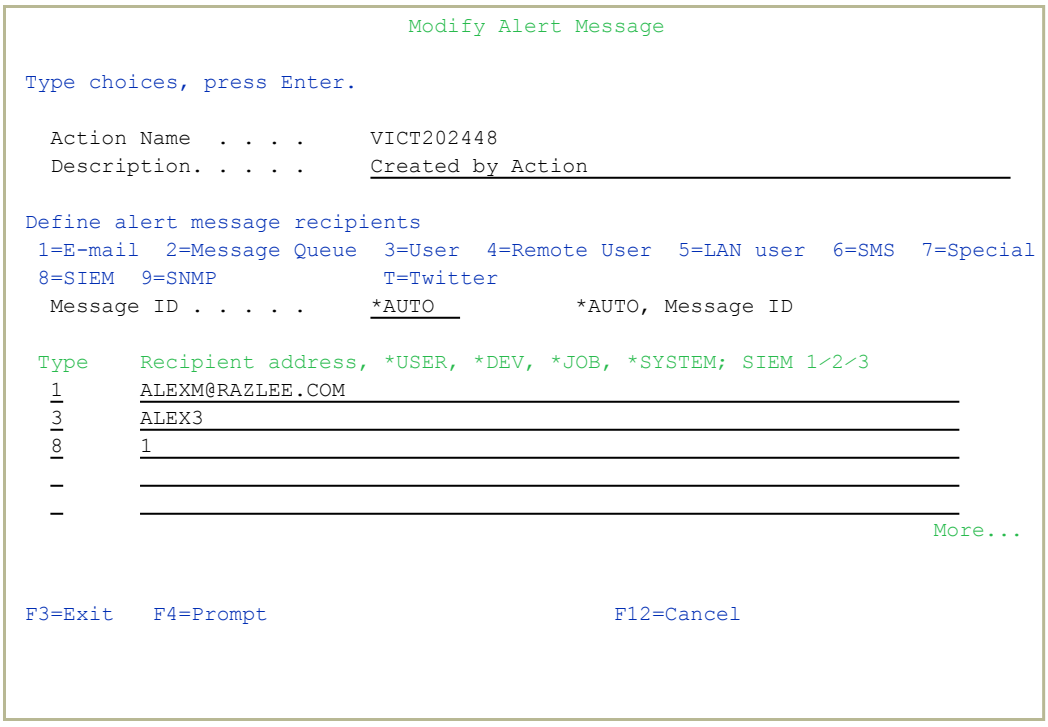
3. Enter parameters and data as described in the table, then press Enter. The Filter Conditions screen appears. Filter criteria allow you to limit application of real-time detection rules to certain specific conditions.

Defining Alert Messages

Your rule can send alert messages to designated personnel via one or more of the following methods:

- Email over the Internet
- Local workstation message queue using the ***SNDMSG MSG (MSGTEXT) TOMSGQ (MSGQNAME)*** command
- Local user message queue using the ***SNDMSG MSG (MSGTEXT) TOUSER (USERNAME)*** command
- Remote user on another IBM i system over the SNADS network using the ***SNDNETMSG*** command
- SMS service to a cellular telephone
- Syslog and SNMP

The message definition consists of predefined message text and one or more recipient addresses. You can opt to have the system send a default message or you can select a predefined message.



The body of the Modify Alert Message screen includes the following fields:

Description

A free-form text description of the action.

Message ID

A predefined message to be sent. Options include:

- ***AUTO** = Use the default message text
- **Msg ID** = name of a predefined alert message
- **F4** = Select a predefined message from the list or create a new message

Type

The type of message to be sent. Options include:

- **1** = E-mail
- **2** = Any specific message queue (SNDMSG TOMSGQ)
- **3** = User message queue (SNDMSG TOUSR)
- **4** = Remote system user (SNDNETMSG)
- **5** = Users or workstations on a LAN (SNDNWSGMSG)
- **6** = SMS message to a cellular telephone
- **7** = Message to beeper or pager
- **8** = Syslog
- **9** = SNMP

Recipient Address

Recipient address formatted according to the recipient type:

- **1** – E-mail: Email address in standard email format (recipient@address)
- **2** – Message Queue: Fully qualified name of the message queue or *SYSOPR
- **3** – User profile or IBM i group profile
- **4** – Network user profile and SNA address separated by a space (for example, USER SYSTEM)
- **5** – LAN User: Valid network user name or *DOMAIN for all users on your domain
- **6** – SMS: Phone number including country code and area code as necessary
- **7** – Special: Phone number and access codes for the pager service

Display Authorization Status

You can display the current authorization status of all installed iSecurity products on the local system.

1. Select **`22. Display Authorization Status`** from the **BASE Support** menu (*COMMAND* **`> 89 > 22`**). The **Status of iSecurity Authorization** screen appears.

```
 44DE466  520 7459    Status of iSecurity Authorization      LPAR Id 1 S520
Type choices, press Enter.                 Subset by . . . . . _____________
 1=Select                                  Warning days before expiration . 14

Opt Lib.   Status      Release ID      Product
 _  SMZ4-A Demo 19-08  14.04 19-06-27  *BASE, Audit, Action, SIEM, MSys, CmpEvl
     Auth code: 499999999999 1           Valid until 2019-08-31
 _  SMZ4-B Demo 19-08  14.04 19-06-27  Compliance (User,Native,IFS), Replicate
     Auth code: 499999999999 1           Valid until 2019-08-31
 _  SMZ8   Demo 19-08  18.06 19-07-14  Firewall, Screen, Command, Password
     Auth code: 899999999999 1           Valid until 2019-08-31
 _  SMZJ   Demo 19-08  09.05 19-07-16  AP-Journal, Update-Control
     Auth code: J99999999999             Valid until 2019-08-31
 _  SMZO   Demo 19-08  05.09 19-05-21  Authority on Demand,Pwd-Reset
     Auth code: O99999999999             Valid until 2019-08-31
 _  SMZC   Demo 19-08  05.00 18-10-08  Capture, w/BI
     Auth code: C99999999999 123         Valid until 2019-08-31
 _  SMZT   Demo 19-08  01.35 19-07-10  Change Tracker
     Auth code: T99999999999 *ALL        Valid until 2019-08-31
 _  SMZV   Demo 19-08  06.98 18-03-20  Antivirus, Anti-Ransomware, ICAP
     Auth code: V99999999999 1           Valid until 2019-08-31
                                                                   More...
F3=Exit    F10=Authority Code
```

2. Select a specific line and type **`1`** in the **`Opt`** field to see the authority details of one specific product.
   NOTE: Codes that will expire in less than 14 days appear in pink. Permanent codes have deliberately been hidden in this screenshot.

Global Installation Defaults

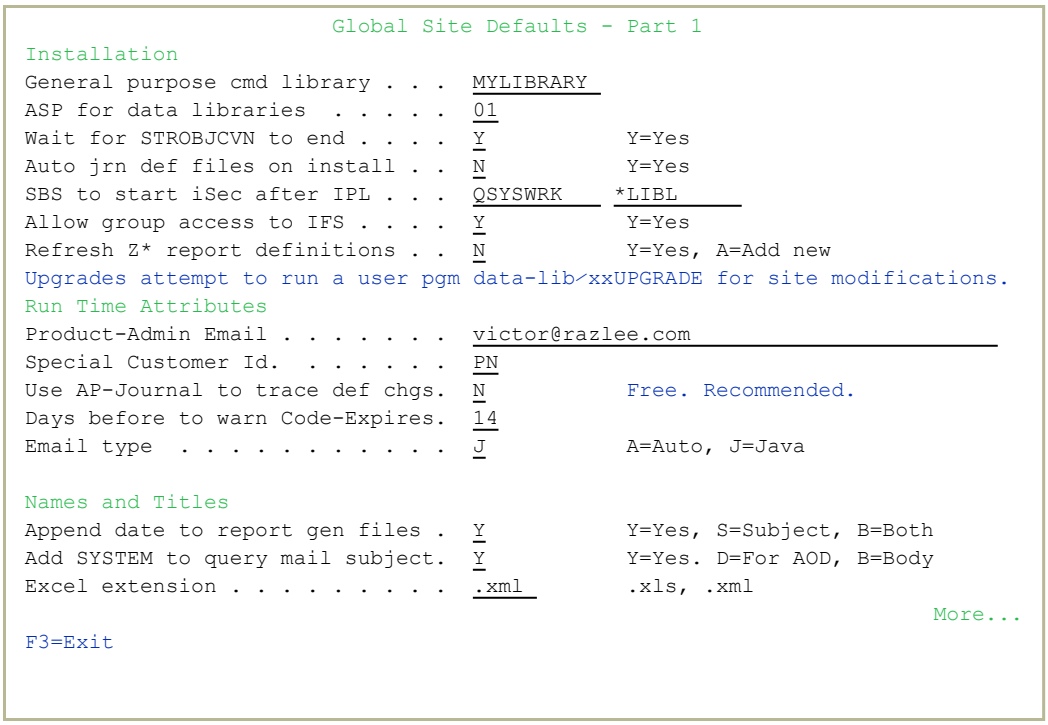
Global installation configuration now includes access to the Raz-Lee Support Menu. Customers should not use it without guidance. It includes:

- Adding a system to enter field help and possible values for all fields in Query Generator and Logs in all products
- Setting of Default Report Summaries

You can set the parameters that iSecurity uses to control the Installation and upgrade processes. The option includes a Product-Admin Email and SYSTEM was added to the query mail subject line.

NOTE: Consult Raz-Lee support staff at support@razlee.com before changing any of the values on this form.

Select **`59. Global Installation Defaults`** from the **BASE Support** menu (*COMMAND* **`> 89 > 59`**). The **Global Installation Defaults** screen appears.



```
                        Global Site Defaults - Part 1
Installation
General purpose cmd library . . .  MYLIBRARY
ASP for data libraries  . . . . .  01
Wait for STROBJCVN to end . . . .  Y            Y=Yes
Auto jrn def files on install . .  N            Y=Yes
SBS to start iSec after IPL . . .  QSYSWRK     *LIBL
Allow group access to IFS . . . .  Y            Y=Yes
Refresh Z* report definitions . .  N            Y=Yes, A=Add new
Upgrades attempt to run a user pgm data-lib/xxUPGRADE for site modifications.
Run Time Attributes
Product-Admin Email . . . . . .  victor@razlee.com
Special Customer Id.  . . . . .  PN
Use AP-Journal to trace def chgs.  N            Free. Recommended.
Days before to warn Code-Expires.  14
Email type  . . . . . . . . . .  J            A=Auto, J=Java

Names and Titles
Append date to report gen files .  Y            Y=Yes, S=Subject, B=Both
Add SYSTEM to query mail subject.  Y            Y=Yes. D=For AOD, B=Body
Excel extension . . . . . . . .  .xml          .xls, .xml
                                                                    More...
F3=Exit
```

```
                        Global Site Defaults - Part 2
Syslog (SIEM) Support      Leave blank for default.
Syslog source Port/IP 1 .  _____  ________________________________________
              Port/IP 2 .  _____  ________________________________________
              Port/IP 3 .  _____  ________________________________________

TLS Application ID SIEM 1  ________________________________________
                   SIEM 2  ________________________________________
                   SIEM 3  ________________________________________

Std CEF Ext. fld. names .  Y           Y=Yes
Include QAUDJRN Seq. Num.  N           Y=Yes
*AUTO Level of message  .  1           1=1st-*AUTO1, 2=2nd-*AUTO2

Product behaviour
GUI must run in SSL . . .  N           Y=Yes
Use IBM std auto disable.  E           Y=Yes (IBM), E=Extended (iSec, generic*)
                                       On change, Set ANZPRFACT accordingly.
Mask UsrPrf with dft pwd.  ?%%%%%%%%%  ?=Display, %=Display, random if blank
Share Item/Time Groups  .  Y           Y=Yes (AP-Journal shares Audit)

                                                                      Bottom
F3=Exit    F12=Cancel
```

Enter values in the following fields

Installation

General purpose cmd library

An alternative library to QGPL from which all ***STR****, ***RUN****, and ****INIT*** commands will be run.

ASP for data libraries

Products which are installed for the first time will be installed to this ASP. This refers to the product library and data library (for example, SMZ4, SMZ4DTA)

In some products such as APJournal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number.

Change the current ASP of the library. All future upgrades will use this ASP.

All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.

Wait for STROBJCVN to end

Y: Yes

N: No

When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work in parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to **Y**.

The default value, which Raz-Lee recommends, is **N**.

Auto jrn def files on install

Y: Yes

N: No

SBS to start iSec after IPL

The Subsystem name and library to use for the Autostart Job.

Allow group access to IFS

Allow access to IFS from group profiles.

Y: Yes

N: No

Refresh Z* report definitions

Y: Yes

A: Replace all

Product-Admin Email

The email of the product admin to send automated messages to.

Run Time Attributes

Use AP-Journal to trace def changes

Y: Yes

N: No

Days before code expir. to warn

All products whose authorization expires in less than this number of days are reported as an exception.

Enter a number between 01 and 99. The default is 14 days.

Name and Titles

Append date to report gen files

Y: Yes

N: No

Add SYSTEM to query mail subject

Y: Yes

N: No

Excel extension

The extension to be used when creating Excel files

Syslog (SIEM) Support

Syslog source Port/IP

Syslog port source IP

TLS Application ID SIEM

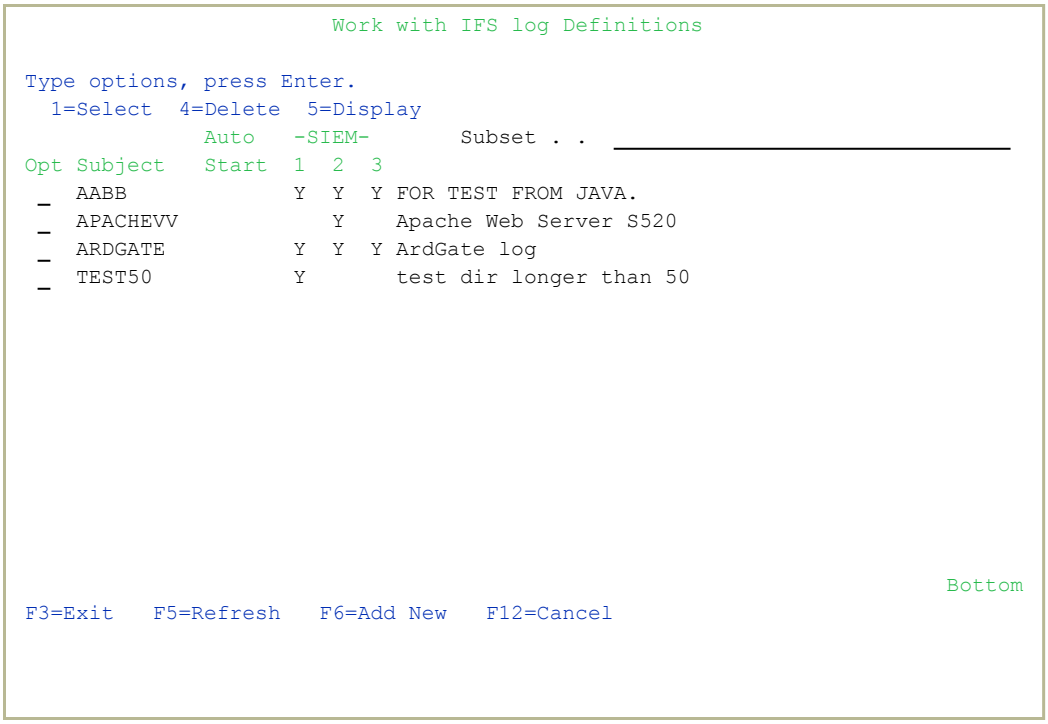
TLS ID for SIEM application

Enter your required parameters and press **Enter**.

Settings

In the settings section, you can configure IFS logging, including defining which files are logged.

To **work with Definitions**, adding, removing, displaying and modifying the desired application messages to communicate with the SIEM, select *STRAUD* **> 15 > 1. Work with Definitions**. The **Work with IFS log Definitions** screen appears:

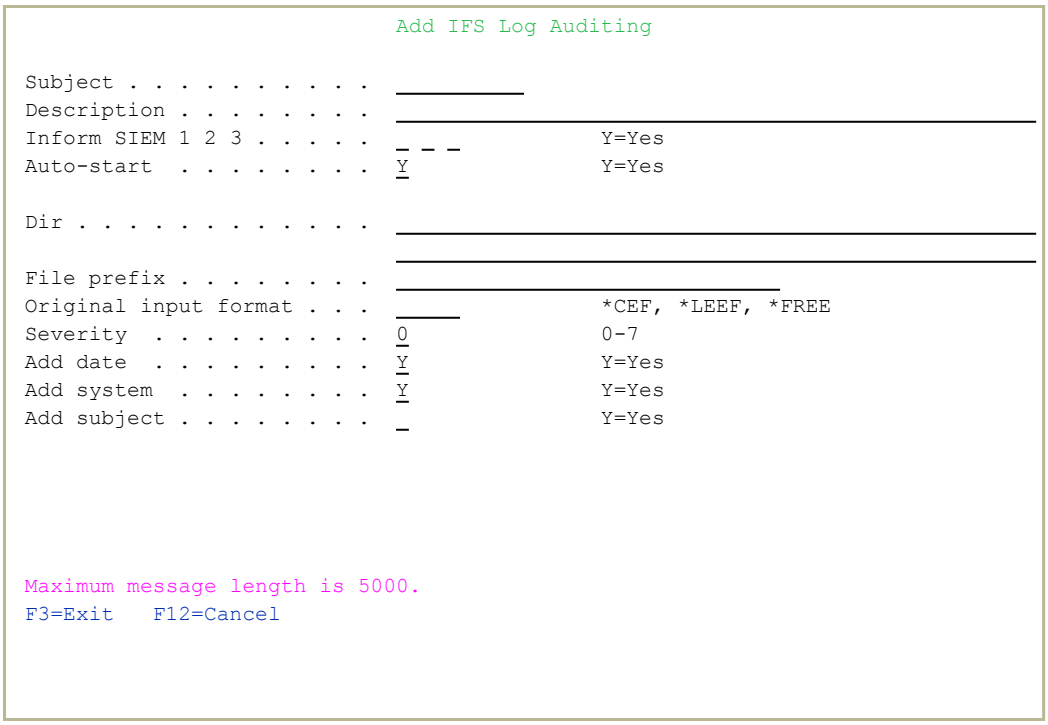


To **change** the logging settings on a file, enter **1** in the **Opt** field for the file.

To **delete** the logging settings for a file, enter **4** in the **Opt** field for the file.

To **display** the logging settings for a file, enter **5** in the **Opt** field for the file.

To **log settings for a new file,** press the **F6** key. The **Add IFS Log Auditing** page is displayed.



The body of the screen includes the following fields:

Subject

Indicates the specific server type.

Keep this part blank, as the software will fill that part automatically.

Description

The name of the server.

Inform SIEM 1 2 3

Set which SIEM servers to inform. More information about the different three types can be found under **STRAUD > 81 > 30**.

Auto-Start

Choose **Y** next to the **Auto-Start** section in order for the server to send messages automatically to the desired SIEM system, and to automatically start the IFS Log transmission when Audit is activated.

Dir

Enter the specific path where the server message log is located, such as **/tmp/**

File Prefix

The name of the file within the desired directory containing the messages to be sent to the SIEM system. Normally, the SIEM messaging system works with a specific file. When the file fills up, the system renames the file and continues to write the new logs and messages under the same file. Indicating the correct file name will ensure that the messaging activity and sending works flawlessly.

Original Input Format

The format of log that Raz-Lee IFS gets from the Apache webserver or the IBM websphere. Possible values include **CEF**, **LEEF** or **FREE**.

Severity

Use the severity mechanism to determine the importance level of a message. The possible values are:

- Blank = Do not send
- **0** = Emergency (Default)
- **1** = Alert
- **2** = Critical
- **3** = Error
- **4** = Warning
- **5** = Notice
- **6** = Info
- **7** = Debug

You can change the severity level or an SIEM by going to **STRAUD > 81. System Configuration, 31/32/33 (SIEM 1,2,3)**.

Facility

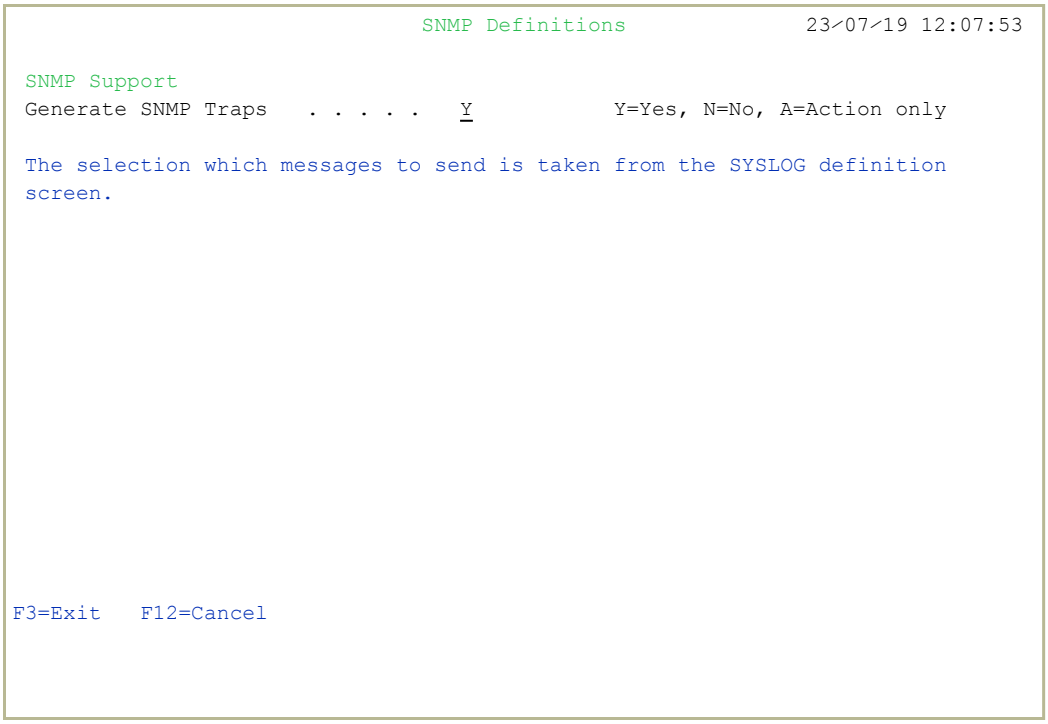
There are 24 levels of facilities to be chosen from (levels 0-23). The FREE facility component indicates the type of program or process that is logging the message. It is recommended to keep this section 0 to keep SIEM default

Audit's default Facility number is marked as 22 (Local use 6 or Local 6).

SNMP Definitions

You can use SNMP traps to supplement your SIEM data and increase security on your system.

1. Select **35. SNMP Definitions** in the **iSecurity/Base System Configuration** menu (*STRAUD* **> 81 > 35**). The **SNMP Definitions** screen appears.



2. Type **Y** to generate SNMP traps to monitor network attached devices for conditions that warrant administrative attention.

   NOTE: The selection of which messages to send is taken from the SYSLOG definition screen (seen in Triple Syslog Definitions.htm

3. To prompt and receive alerts, define an Alert Message in Action (Use **31.Work with Actions** in the Action main menu (*STRAUD***> 61 > 31**)).