Security and Compliance Tools for IBM i

Syslog Reporting Manager V2.3

User’s Guide

Thomas Barlen
Terry Ford

Version 2024.02.08

Syslog Reporting Manager

Table of Contents

1 Introduction

IBM i provides extensive logging and auditing capabilities. System events or file events are typically captured in journals, such as the QAUDJRN system journal. Native IBM i commands exist to analyze collected events.

In recent years more and more companies implement central logging services to collect mostly security related events on a central server. These central servers typically host Security Information and Event Management (SIEM) systems, such as QRADAR, to store events from many systems in an enterprise, analyze the data, and react on monitored events.

A DB2 table function has been introduced in 2017 to query the system audit journal and format entries according to RFC3164 or RFC5424 compliant syslog messages with a payload formatted in the Common Event Format (CEF) as supported by commonly used SIEM solutions. However, audit journal entries are just returned as part of a SQL select statement but not forwarded or logged to a syslog server. The IBM i history log can also be queried via a special table function, but just like the audit journal table function, does not forward returned entries to a syslog server.

Some IBM i customers also expressed interest in monitoring Integrated File System (IFS) stream file changes, message queue events, other system journal events, and database journal changes and report those changes to a central syslog-based logging service.

The Security and Compliance Tools for IBM i - Syslog Reporting Manager (SRM) tool has been created to simplify the monitoring of system audit journal events, history log events, and stream file change events. An administrator can select the events that should be monitored and specify the remote syslog server / SIEM server that should receive the monitored events. All events are sent in either the Common Event Format (CEF) or Log Event Extended Format (LEEF).

Details

The SRM tool is a native IBM i application with the following key characteristics:

- Provides separate monitoring programs for system audit journal events, user audit journal events, QHST history log events, IFS stream file changes, message queue events, generic journal events, and database journal changes (requires additional tool).
- Highly configurable through many custom settings
- Supports RFC3164 and RFC5424 syslog protocol formats
- Entries that are sent to a syslog server can be formatted in either Common Event Format (CEF) or Log Event Extended Format (LEEF).
- Automatic restart capabilities of monitor jobs in case of failures or malicious ending of monitor jobs
- All tool-related programs run as batch programs in a separate subsystem
    - Subsystem name is SLSBS
    - Monitor control job name is SLMONSTR. It is responsible for:
        - for starting event monitor jobs
        - monitoring event monitor job status
        - restarting event monitor jobs
        - reporting statistical data
    - Audit journal monitor job name is SLAUDMON. It is responsible for:
        - retrieving custom set of system audit journal entries. Filters can be applied to limit the number of reported events. The supported filters are user profile names and

    system-type entry specific data (event type field of entry-specific data). For command level auditing, the monitor can also filter on the source of CD entries.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Audit journal monitor job name is SLAUDMONU. It is responsible for:
    - retrieving user-type audit journal entries. Filters can be applied to limit the number of reported events. The supported filters are user profile names.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - QHST history log event monitor job name is SLHSTMON. It is responsible for:
    - retrieving history log events based on a customizable set of filter rules. If no filter rules are defined, all history events are reported.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - IFS stream file monitor job name is SLIFSMONnn. It is responsible for:
    - retrieving IFS stream file changes for monitored stream files. Files to be monitored are added to a journal. There is a SRM-provided journal named IFSJRN. The user can also monitor files in custom-defined journals.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Message queue monitor job names are SLMSGQMON and SLMSQMONS. They are responsible for:
    - retrieving messages from monitored message queues. Filters can be applied to limit the number of reported events. The supported filters are user profile names, message identifier, message types, and the message severity.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - >Journal monitor job name is SLJRNMONnn. It is responsible for:
    - retrieving journal entries from configured journals. If the journal code / journal entry for a retrieved journal entry is enabled, the journal entry specific data is formatted according to defined journal entry formats. The QACGJRN and QIPFILTER journal formats are pre-defined in SRM. Other journals and journal entry formats can be freely configured by the administrator.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server<
  - Database journal monitor job name is SLDB2MON and is started at a configured interval by the SLMONSTR job. Note that this function requires another IBM Technology Expert Labsasset named Journal Extract Tool. It is responsible for:
    - processing all configured database journals in the Journal Extract Tool and convert the retrieved events into the proper SIEM message format.
    - providing retrieved entries to the communication jobs that send the events to a network accessible syslog / SIEM server
  - Communication job name(s) are SLSNDEVTxx. They are responsible for:
    - retrieving events from monitor jobs.
    - send retrieved entries to a network accessible syslog / SIEM server
    - the event data is converted from the IBM i job CCSID to the international standard code page ISO 8859-15 by default. The target code page can also be customized.
  - All programs run under the owner profile QZRDSRMOWN
  - Access to configuration commands is granted via group membership to IBM i group profile QZRDSRMGRP.

The monitor programs receive events from the audit journal, the QHST history log, message queues, other system journals, or database journals (in combination with JET) or a dedicated journal for monitoring stream file changes. Events are sent to a syslog server via the syslog protocol over IP protocol UDP or TCP or TLS-encrypted. The syslog message payload contains the events in CEF format. Following are a few event examples:

Audit journal event of an authority failure (AF) in RFC3164 format:

```
<36>Aug 25 14:52:08 i5osp4 102F5F: CEF:0|IBM|IBM i|7.4|QSYS-
QAUDJRN|T-AF|Medium|reason=Authority failure msg=Not authorized to
object fileType=*PGM cs1Label=objName cs1=QZRDSECSRM/CFGJSCR
suser=THOMAS sproc=722470/THOMAS/QPADEV000P shost=I5OSP4
src=192.168.126.71 spt=36868 evtAggregation=*NO entryTypeField=A
```

Stream file change event in RFC5424 format:

```
<134>1 2023-08-25T21:55:41.520032+02:00 ctcsect5.rchland.ibm.com
IBMiPSCSRM IFSMON 10338AF - CEF:0|IBM|IBM i|7.4|IFSMON|IFS File
Monitor Journal Entry Type  B-WA|3|act=B-WA Write, after-image
event sproc=722496/BARLEN/QZSHSH suser=BARLEN shost=CTCSECT5
filePath=/home/barlen/ifsmon/weblog2.log fileType=*STMF
cs2Label=changedDataLength cs2=0000000064 cs3Label=changedDataPart
cs3=*ONLY cs4Label=changedDataFileOffset cs4=0000000000000788915
cs1Label=changedData cs1=Unauthorized access to Web resource
accountInfo by user TBARLEN<LF>
```

Audit journal event of a command (CD) entry type in RFC5424 format:

```
<38>1 2022-02-25T19:48:12.136816+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM AUDMON 102F5F - CEF:0|IBM|
IBM i|7.4|QSYS-QAUDJRN|T-CD|Low|reason=Command string audit
msg=Command run interactively from a command line or by choosing a
menu option that runs a CL command - CHGENVVAR ENVVAR(test4)
VALUE(77777) LEVEL(*SYS) fileType=*CMD cs1Label=objName
cs1=QSYS/CHGENVVAR suser=BARLEN sproc=721738/BARLEN/QPADEV000Q
shost=I5OSP4 src=192.168.126.71 spt=36888 evtAggregation=*NO
entryTypeField=C
```

QHST history log event of a job start in RFC5424 format (CEF) with second header:

```
<14>1 2020-08-25T18:59:04.791738+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM HSTMON 102F5F - CEF:0|IBM|
IBM i|7.4|QSYS-QHST|CPF1124|Low|reason=CPF1124 msg=Job
722506/QZRDSRMOWN/SLMSQMONS started on 25.08.20 at 18:59:04 in
subsystem SLSBS in QZRDSECSRM. Job entered system on 25.08.20 at
18:59:04. suser=QZRDSRMOWN sproc=722506/QZRDSRMOWN/SLMSQMONS
```

IFS stream file change log event in RFC5424 format where a custom tag of THOMAS5 was specified in LEEF format:

```
<134>1 2020-08-25T15:02:04.006928+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM IFSMON THOMAS5 - LEEF:2.0|
IBM|IBM i|7.4|IFSMON|x09|act=B-WA Write, after-image event
sproc=722519/BARLEN/QZSHSH usrName=BARLEN resource=I5OSP4
filePath=/home/barlen/ifsmon/weblog2.log  fileType=*STMF
changedDataLength=0000000055 changedDataPart=*ONLY
changedDataFileOffset=0000000000000788979 changedData=User BARLEN
removed access permission from user THOMAS<LF>
```

Custom generated event in RFC5424 format where a custom tag of P4MON was specified in LEEF format:

```
<14>1 2020-08-25T15:05:12.856000+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM CUSEVT P4MON - LEEF:2.0|
IBM|IBM i|7.4|CUSEVT-IBMi|x09|
resource=i5osp4.ai.stgt.spc.ihost.com usrName=MARION
sproc=721736/BARLEN/QPADEV000M cat=Loan application msg=User gave
0% interest rate for account 1294192
```

Message queue monitor event in RFC5424 format in CEF format:

```
<11>1 2020-04-30T11:35:29.886549+02:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM MSGMON 102F5F - CEF:0|IBM|
IBM i|7.4|MSGMON|CPF0907|5|cat=MSG Queue Messages rt=2020-04-30-
11.35.29.886549 reason=CPF0907 cs1Label=msgSev cs1=ERROR
cs2Label=msgQueue cs2=QSYS/QSYSOPR cs3Label=pgmName cs3=QWCATARE
msg=Serious storage condition may exist. Press HELP. cs4Label=srdb
cs4=I5OSP4 suser=QSYS sproc=541034/QSYS/QSYSARB5 shost=I5OSP4
```

Database journal monitor event via the Journal Extract Tool in RFC3164 syslog format and SIEM CEF message format:

```
<14>Apr 30 12:11:52 i5osp4 102F5F: CEF:0|IBM|IBM i|7.4|DB2MON|DB2
change monitoring (Journal Extract Tool)|3|act=UPDATE rt=2020-04-
30-12.11.52.265056 sproc=551907/BARLEN/QPADEV000D shost=I5OSP4
suser=BARLEN fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName
cs1=CFGSLHSTP cs2Label=updatedColumnNames
cs2=EVTUSER1,EVTMSGID1,EVTMSGID2,EVTMSGID3 cs5Label=rowDataBefore
cs5=QJ_JOURNAL_ENTRY_TYPE\="UB" QJ_RECEIVER_NAME\="DETRCV0010"
QJ_SEQUENCE_NUMBER\="22145" EVTUSER1\="BARLEN" EVTMSGID1\
="CPF1122" EVTMSGID2\="CPF9998" EVTMSGID3\="SLS0040"
cs4Label=rowDataAfter cs4=QJ_JOURNAL_ENTRY_TYPE\="UP"
QJ_RECEIVER_NAME\="DETRCV0010" QJ_SEQUENCE_NUMBER\="22146"
EVTUSER1\="BARLEN3" EVTMSGID1\="CPF1129" EVTMSGID2\="CPF9997"
EVTMSGID3\="SLS0042"
```

<**Account journal (QACGJRN) job data event in RFC5424 syslog format and SIEM CEF message format:**

```
<134>1 2023-11-10T09:03:16.005392-06:00 ctcsect4.rchland.ibm.com
IBMiPSCSRM JRNMON SRM230 - CEF:0|IBM|IBM i|7.4|JRNMON|A-JB|3|
reason=Journal QACGJRN entry A-JB jobName=QRWTSRVR jobUser=QUSER
jobNumber=764417 accountingCode=SECURITY processingTime=18
numRoutingSteps=0 jobEntryDate=111023 jobEntryTime=003738
jobStartDate=111023 jobStartTime=003738 totalTransactionTime=0
numTransactions=0 syncAuxIODbOps=808 jobType=B complCode=99
numPrintLines=0 numPrintPages=0 numPrintFiles=0 numDbWriteOps=0
numDbReadOps=0 numDbUpdDelOps=5 numComWriteOps=0 numComReadOps=0
timeJobActive=0 timeJobSuspended=2293
timestampJobEntry=11102023003738 timestampJobStart=11102023003738
asyncIoDbNonDbOps=32 expCpuTime=18 expSynAuxIoOps=808
expAsynAuxIoOps=32 expNumDbPut=0 expNumDbGet=5 expNumDbUpdDel=0
expNumLinesPrinted=0 expNumPagesPrinted=0 expNumPrintFiles=0
sourceServiceName=QSYS/QACGJRN jrnEntryType=A-JB pgmName=QWTCHGJB
suser=QWKUSER sproc=764417/QUSER/QRWTSRVR shost=CTCSECT4>
```

Information about syslog formats, the Common Event Format, and the Log Event Extended Format can be found at the following Web resources:

- RFC3164 IETF standard

- RFC5424 IETF standard
- Log Event Extended Format

  https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_LEEF_Format_Guide_intro.html

- Common Event Format information

  Using your favorite Internet search engine search for the following string:
  "common event format (cef)"

  There are several PDF documents that point to the same document describing the CEF format and outline.

2 What's new in V2.3 (7th December 2023)

This section describes the enhancements in this version of the tool including the highlights about introduced changes.

To help you see where technical changes have been made, the following markers are used throughout the document.

- The > mark where new or changed information begins.
- The < mark where new or changed information ends.

>The following list summarizes the enhancements and changes in this version:

- SRM has been enhanced to support events to be stored in a database table rather than being sent to a remote syslog / SIEM server. The CFGSLENV command has new parameters that allow you to specify an event output file name. If *OUTFILE is specified on the SERVER parameter, the OUTFILE parameter can be specified with a file name of a table that will receive the monitored events. An external event handler could then read the data from the table and process it as needed. The external event handler is also responsible to clean up (delete) processed events. SRM is only adding events to the file but is not performing any delete or cleanup operations. If SRM cannot insert any additional events to the table anymore, SRM stops working.
- A new parameter EVTCCSID has been added to the CFGSLENV command. This parameter lets you specify the CCSID of the outbound event when sent via the syslog protocol to the remote syslog / SIEM server. In the past this was hardcoded to 923 (ISO/IEC 8859-15). You have now the choice to convert the events to another code page.
- A new journal monitor has been added to SRM. It has predefined system journals (QACGJRN and QIPFILTER) with all their possible journal entries. An administrator can also add their own journal and define custom formats to generate custom SIEM key-value pairs. It is a generic journal monitor that is meant to report security critical events. Other journals and entry types can be added by an administrator and the event format of the entry specific data (ESD) can be customized.
- A new option for handling end-of-line (EOL) characters in an IFS file change has been added. It affects line feed (LF) and carriage return (CR) control characters. The default behavior is that the corresponding hex characters are translated to a text representation of <LF> or <CR>. The new enhancements allows you to select an EOL option to translate LF and CR characters to a blank character. This enhances the readability of the SIEM event.
- The maximum number of send jobs has been increased from 9 to 50. It provides better support for a very high volume of events to be sent. The send job name length is now longer. The job names are SLSNDEVTxx where xx is 01 to 50.
- The audit journal monitor for system-type entries has been enhanced for the CD (Command String) entry type. If command auditing has been turned on for a user profile, a CD entry is written for every CL command that is executed by that user. This includes commands entered interactively as well as commands that are run as part of a program or API call. This can lead to a significant number of events. The new filtering option is only available for CD journal entry types. The option can be used to specify the run environment as defined in the "Where run" column in the CD entry description in the IBM Security Reference, Appendix F. For example, you could report CD entries for interactive calls only.

- **IBM i supported release levels:** As stated in the users guide for SRM 2.2, that release was the last release that supports IBM i V7R2. SRM 2.3 supports IBM i 7.3 and higher.<

3 Important information about the configuration and use of the Syslog Reporting Manager

> Before you install and use the Syslog Reporting Manager, you should understand what the Syslog Reporting Manager's purpose is and what it is not made for.

Use cases of the Syslog Reporting Manager

- Gather security-related events from various log sources on IBM i and report the events in a standardized format (Common Event Format – CEF or Log Event Extended Format – LEEF) via the Syslog protocol to a remote Security Information and Event Management (SIEM) system.

- It is strongly recommended to consult your corporate security policy and determine what the logging requirements are. A good policy should contain an audit and logging section that describes the type of event that needs to be collected and reported.

- The configuration should be done in a manner to only send the required events and not to overwhelm the remote SIEM server with millions of events per day that are not processed and not even relevant.

- Depending on system resources, the Syslog Reporting Manager (SRM) can send easily 40 – 70 thousands events per minute. This might need an increase in the number of send jobs in the configuration. However, the tool is not made for sending any event that the system might be able to generate. For example, if you turn on object auditing on a database table that is accessed by the business application thousands of times per second, SRM should not be used to report audit ZR entries for all table read operations. In fact, nobody will ever analyze those events on the SIEM side.

What the Syslog Reporting Manager is not made for

- SRM is not made for gathering all generated messages and audit events that the IBM i operating environment might be able to generate.

- There are limits in the number of events that can be handled by SRM. For example, the message monitor is made for monitoring security-related messages or critical system messages, but not for processing thousands of messages per minute. SRM has been tested to send about 80000 to 100000 events per minute. That heavily depends on the network and SIEM server performance. If the receiving side is not able to handle this amount of events, the SRM send data queue runs full and SRM will end itself because it cannot process any more events. In this case, you must evaluate and question the audit and log requirements. Typically you will never find a security policy that demands sending of every database read or instruction that has been executed on a system.

4 Implementation and use

The following sections guide you through installation, configuration, and usage of the SRM utility.

4.1 Software and PTFs

The Syslog Reporting Manager, PTFs, and documentation can be found at the following Web page:

https://www.ibm.com/support/pages/ibm-i-security

Navigate to Assets and Tools and click on the Syslog Reporting Manager download link.

Note that you will always find the latest code and information on that Web site.

4.1 Maintenance and support

The Syslog Reporting Manager is (SRM) supported by IBM Technology Expert Labs. It is not an IBM product itself and therefore a ticket cannot be opened with the regular IBM support. Instead you have to contact: systems-expert-labs@ibm.com

You will only get support for the current SRM version and the version prior to the current one. If you experience problems with an older version, you need to upgrade to supported version first.

Support is provided to users with an active maintenance agreement. All other inquiries will be a chargeable service. Users with an active maintenance agreement are also entitled to new releases.

4.2 Prerequisites

The tool is an IBM i native ILE application. The following list shows the prerequisites:

- At least IBM i version 7.3.
- IBM i OS option 39
- The following group PTFs are the minimum levels that are required:
    - IBM i 7.3 - SF99703 Level 22
        - and PTF SI77327 or the PTF(s) that supersedes it
    - IBM i 7.4 - SF99704 Level 10
    - Refer to chapter 11 Audit journal entry type support on page 128 for a list of supported journal entry types and the PTF prerequisites.

- PTF information for IBM i 7.4.
    - There is a problem when retrieving history log entries with the HISTORY_LOG_INFO table function. The configured EOF delay does not properly work. Install the following PTF or the PTF that supersedes it to correct the problem:
        - SI72062
- Database change monitoring also requires the IBM Technology Expert Labs Journal Extract Tool, which must be purchased separately. Refer to the Journal Extract Tool documentation for all details related to the installation and configuration of the tool. The enhanced configuration support of this tool is described in this document.
- SIEM messages contain information about the system that generated and sent the event. The identifier (host name) is derived from the TCP/IP configuration of your IBM i system. This requires that your TCP/IP setup is correct and meets the following specifications:
    - The TCP/IP domain must contain the hostname and the corresponding IP domain. Example:
      ```
      CHGTCPDMN HOSTNAME('i5osp4') DMNNAME('ai.stgt.spc.ihost.com')
      ```
    - The TCP/IP host table must contain an entry that matches the configured fully qualified host name.

Example:

```
ADDTCPHTE INTNETADR('172.17.17.40')
HOSTNAME(('i5osp4.ai.stgt.spc.ihost.com'))
```

4.3 Authorities required to Install the Tool

The user installing the tool must have *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL and *SECADM special authorities or must be QSECOFR or an equivalent profile.

4.3.1 Authorities required to Run the Tool

Users running the tool must be a member of the group QZRDSRMGRP. No special authorities are required for the user profile.

4.4 Installation

The tool consists of one component and optional PTF save files:

1. The IBM Security and Compliance Tools for IBM i Syslog Reporting Manager code
   Save file: `SRMBASE.SAVF`
2. Optionally, there could also be PTFs available. PTFs are shipped in save files too. Their names follow the format `Q5SCnnnn.SAVF`.

Important note when upgrading from a previous version

Versions prior to version 2 of the Syslog Reporting Manager have been shipped in two components (*BASE and option 1 of the license program 5ZRDPSC). In an effort to streamline IBM Technology Expert Labs security asset packaging, the Syslog Reporting Manager needed to undergo several changes as outlined below:

- The product ID has changed from 5ZRDPSC to 5ZRDSRM
- The Syslog Reporting Manager is now packaged in license program option *BASE instead of 1
- The product code library has changed from QZRDSYSLOG to QZRDSECSRM
- The base product library QZRDPSC does not exist anymore
- The product owner profile has changed from QZRDSLOWN to QZRDSRMOWN
- The product administrator group profile has changed from QZRDSLGRP to QZRDSRMGRP.

>Version 1: End all monitor jobs by using the ENDSLMON command prior to installing the new version. After the monitor jobs have ended, end the subsystem SLSBS.

Version 2: End SRM with the ENDSRM command.<

Perform the installation as follows:

Important: Ensure all prerequisite license programs and PTF levels have been installed prior to performing the following steps.

1. FTP the **SRMBASE.SAVF** file and optional PTF save files **Q5SCnnnn.SAVF** to a library of your choice. The example shows the QGPL library.
   ```
   bin
   quote site nam 1
   put SRMBASE.SAVF /QSYS.LIB/QGPL.LIB/SRMBASE.SAVF
   ```
   (optionally, if PTFs exists, upload all PTF save files)
   ```
   put Q5SCnnnn.SAVF /QSYS.LIB/QGPL.LIB/Q5SCnnnn.SAVF
   ```
2. Sign on to your IBM i partition with a user profile that has the authority to restore license programs.

3. >Make sure that the system value QALWOBJRST is set to ALL prior to installing the Syslog Reporting Manager.<
4. Restore the IBM Security and Compliance Tools for IBM i Syslog Reporting Manager:

   ```
   RSTLICPGM LICPGM(5ZRDSRM) DEV(*SAVF) SAVF(QGPL/SRMBASE)
   ```

5. >If you changed the system value QALWOBJRST prior to the install, make sure you change it back to the previous value.<

The installation process performs the following tasks:

- Creates a user profile QZRDSRMOWN. This profile is used as the owner profile for all objects that belong to the tool. In addition, all monitor jobs run as batch jobs under this profile.
- Creates a group profile QZRDSRMGRP. Membership to this profile grants access to the configuration and management commands of the Syslog Reporting Manager.
- Creates a library QZRDSECSRM. This library contains all QSYS.LIB file system objects of the tool including programs, commands, files, etc.
- In case of a version upgrade, all existing configuration settings will be migrated to the new version when running the RSTLICPGM commands.

>If you also downloaded PTFs (Q5SCnnnn.SAVF) from the download page, install the PTFs now. The Q5SCnnnn.MBR files contain the PTF cover letters.

The regular PTF installation process must be followed. A description of the PTFs can be found in the IBM Box document *PTF Information.boxnote*. Following is an example of a PTF installation:

Example:

```
LODPTF LICPGM(5ZRDSRM) DEV(*SAVF) SELECT(5SC1004)
SAVF(QGPL/Q5SC1004)

APYPTF LICPGM(5ZRDSRM) SELECT(5SC1004)<
```

Important: The tool requires a license key. The key must be obtained from your IBM Technology Expert Labs contact. The key will be entered as part of the setup. Note that the tool comes with a 70 day trial license. That lets you run the the tool for 70 days without the need to enter a valid license key.

4.5 Upgrade information related to V2R3M0 from a previous version

>Version 2.3 of the Syslog Reporting Manager (SRM) supports a migration path from previous versions 1.4, 2.1, and 2.2. A migration path from versions prior to version 1.4 is not supported. If you have an older version installed, you need to upgrade first to version 1.4 or 2.1 before performing the migration.

4.5.1 Migration overview from version 1.4

The migration is performed in multiple steps. The following overview summarizes the migration process:

Important: Migration can only be performed when both, the old version and the new version are installed at the same time.

Attention when IFS file monitoring is active: The migration process will also migrate monitored IFS files from journal QZRDSYSLOG/IFSJRN to journal QZRDSECSRM/IFSJRN. This migration task collected first all journalled file names, ends journalling for QZRDSYSLOG/IFSJRN and then starts journalling again for the collected file names for journal QZRDSECSRM/IFSJRN. This step requires that no process is running that has a lock on a journalled file in the QZRDSYSLOG/IFSJRN journal.

1. Version 1.4 is installed on the system.
2. Version 2.3 is installed on the system.
3. Stop the Syslog Reporting Manager.
4. Run the migration program phase 1 to migrate all configuration data from your previous configuration in library QZRDSYSLOG to the new library QZRDSECSRM.
5. Delete the old Syslog Reporting Manager.
6. Run the migration program phase 2 to complete the migration.
7. Start the new Syslog Reporting Manager.

The following configuration data can be migrated:

- Global configuration data
- Audit monitor settings
- History log monitor settings
- IFS file monitor configuration, the configured IFS journals (only for V1.4), and the monitored file in the SRM journal QZRDSYSLOG/IFSJRN. For custom journals that have been added to the configuration in V1.4, only the journal definition itself will be migrated. The monitored files are not touched by the migration process as they are not impacted.
- The message queue monitor global configuration and monitored message queues.
- Custom program options that have been modified.
- The global configuration of the Journal Extract Tool (JET) integration.
- All timestamps of previously processed events of the various monitors. It ensures that the new version will not loose any entries and starts after the events that have been processed by the previous version.

iASP Information for SRM V1.4

If you used the Independant ASP (iASP) support from version 1.4, the following migration considerations must be taken into account:

- IFS journal definitions of custom journals (command CFGSLIFSJ) and monitored message queues that are not found during migration will be added with an ASP name of *GLOBAL if an ASP Name was set in the CFGSLENV command. If no ASP name was defined in V1.4 in the CFGSLENV command, the ASP name of the migrated definitions is set to *SYSTEM (system ASP).

4.5.2 Performing the migration from V1.4

The following steps guide you through the migration process. It is assumed that you had a working Syslog Reporting Manager version 1.4 (library QZRDSYSLOG) installed and that this version is still installed on the system. It is also assumed that you followed the steps to install the new Syslog Reporting Manager (library QZRDSECSRM).

1. Open a 5250 emulation session and sign on with a user profile that has the *ALLOBJ special authority.
2. Enter the following command to display the jobs in subsystem SLSBS.
   WRKACTJOB SBS(SLSBS)
   No jobs should be listed and the subsystem must not be active. If the subsystem is still active, end the Syslog Reporting Manager and its subsystem before continuing with the next step.
3. Enter the following command to start phase 1 of the migration process.
   QZRDSECSRM/MIGFRMV1 PHASE(1)
   The process should complete with message *“All configuration migration tasks completed successfully.”*
   If you get the completion message *“One or more migration tasks failed. See joblog for more information.”* check the joblog for information which migration step did not complete or had a warning.
   IBM i V7.2 Migration Information:
   If migration step 12 (IFS last processed timestamp migration) fails with error SQL0901 and the migration step 12 shows in the second level text SQL return code 58004, the timestamp has not been successfully migrated due to a system problem. In this case, run the following SQL statements from ACS Run SQL Scripts or STRSQL:
   ```
   DELETE FROM qzrdsecsrm.ifslastart WHERE jrnnam = 'IFSJRN' and
   jrnlib = 'QZRDSECSRM';

   merge INTO qzrdsecsrm.ifslastart t USING
   qzrdsyslog.ifslastart s ON s.jrnlib = t.jrnlib AND s.jrnnam =
   t.jrnnam WHEN NOT  matched THEN  INSERT   VALUES (s.jrnlib,
   s.jrnnam, s.resttime, s.seqnbr, s.jrnrcvlib, s.jrnrcvnam, '',
   '*SYSTEM', '*NO', '*NO', '*NONE')  WHEN matched THEN UPDATE
   SET t.resttime = s.resttime, t.seqnbr = s.seqnbr,
   t.jrnrcvlib = s.jrnrcvlib, t.jrnrcvnam = s.jrnrcvnam;

   UPDATE qzrdsecsrm.ifslastart SET jrnlib = 'QZRDSECSRM'
   WHERE jrnlib = 'QZRDSYSLOG' AND jrnnam = 'IFSJRN';
   ```
4. Enter the following command to open the Syslog Reporting Manager main menu.
   CFGSRM
5. Check all monitor and global configurations. They should contain your migrated definitions and settings.

6. Check with the following command if user QZRDSLGRP has any members. If yes, remove the group from the listed member profiles.
   ```
   DSPUSRPRF USRPRF(QZRDSLGRP) TYPE(*GRPMBR)
   ```
7. Delete the previous version of your Syslog Reporting Manager.
   ```
   DLTLICPGM LICPGM(5ZRDPSC) OPTION(*ALL)
   ```
   Note: Ensure that no object lock is on library QZRDSYSLOG before trying to delete the old Syslog Reporting Manager version.
8. Complete the migration by running phase 2 of the migration process. This phase will recreate the proxy commands in library QSYS.
   ```
   QZRDSECSRM/MIGFRMV1 PHASE(2)
   ```
   If you receive a message that phase 2 cannot start because phase 1 issued warnings or errors and you have identified and solved all issues, you can force phase 2 by issueing the command:
   ```
   QZRDSECSRM/MIGFRMV1 PHASE(2) FORCE(*YES)
   ```
9. Delete the owner user profile of the old version `QZRDSLOWN` with the DLTUSRPRF command.
10. If any members were found in step 6 of the migration and have been removed from the QZRDSLGRP group profile, verify the list of removed users if they are still needed and if yes, add them to QZRDSRMGRP group.

This completes the migration.

4.5.3 Performing the migration from V2.1 or V2.2

Before migrating from SRM V2.1 or V2.2, run the command QZRDSECSRM/CFGSLMQM and press F4. Then press F9 and verify that the specified message queue in the MONMSQ parameter exists on the system. If the message queue does not exist, specify QZRDSECSRM/SLMSGQ as the parameter value.

Migration from SRM V2.1 or V2.2 to V2.3 is rather simple. Just perform an installation as documented in section Installation on page 14. The installation will migrate the configuration from V2.1 / V2.2 to V2.3.

4.6 Granting access to the Syslog Reporting Manager

The SRM tool has been designed to be configured and operated by a user profile without any special authorities. The administrator responsible for managing the SRM tool must be a member of the QZRDSRMGRP group. The group can be added as a primary group or supplemental group profile.

Example of assigning the group as primary group:

```
CHGUSRPRF USRPRF(MYADMIN) GRPPRF(QZRDSRMGRP)
```

Example of assigning the group as a supplemental group:

```
CHGUSRPRF USRPRF(MYADMIN) SUPGRPPRF(QZRDSRMGRP)
```

4.6.1 Granting management access to the Journal Extract Tool

If you have the Journal Extract Tool installed and want the Syslog Reporting Manager administrator to also manage the Journal Extract Tool configuration, you can achieve this in two ways:

1. The administrator user must have the *ALLOBJ special authority
2. The administrator user must be member of the QZRDSRMGRP group profile and you must issue the following command as a user with *ALLOBJ special authority:
   ```
   CALL PGM(QZRDSECSRM/GRTJSACC)
   ```

This program will grant the object permissions for group QZRDSRMGRP to objects in the QJSCRAPE library.

In case you want to remove access from the QZRDSRMGRP profile at a later time from objects in library QJSCRAPE, you need to run the following command:

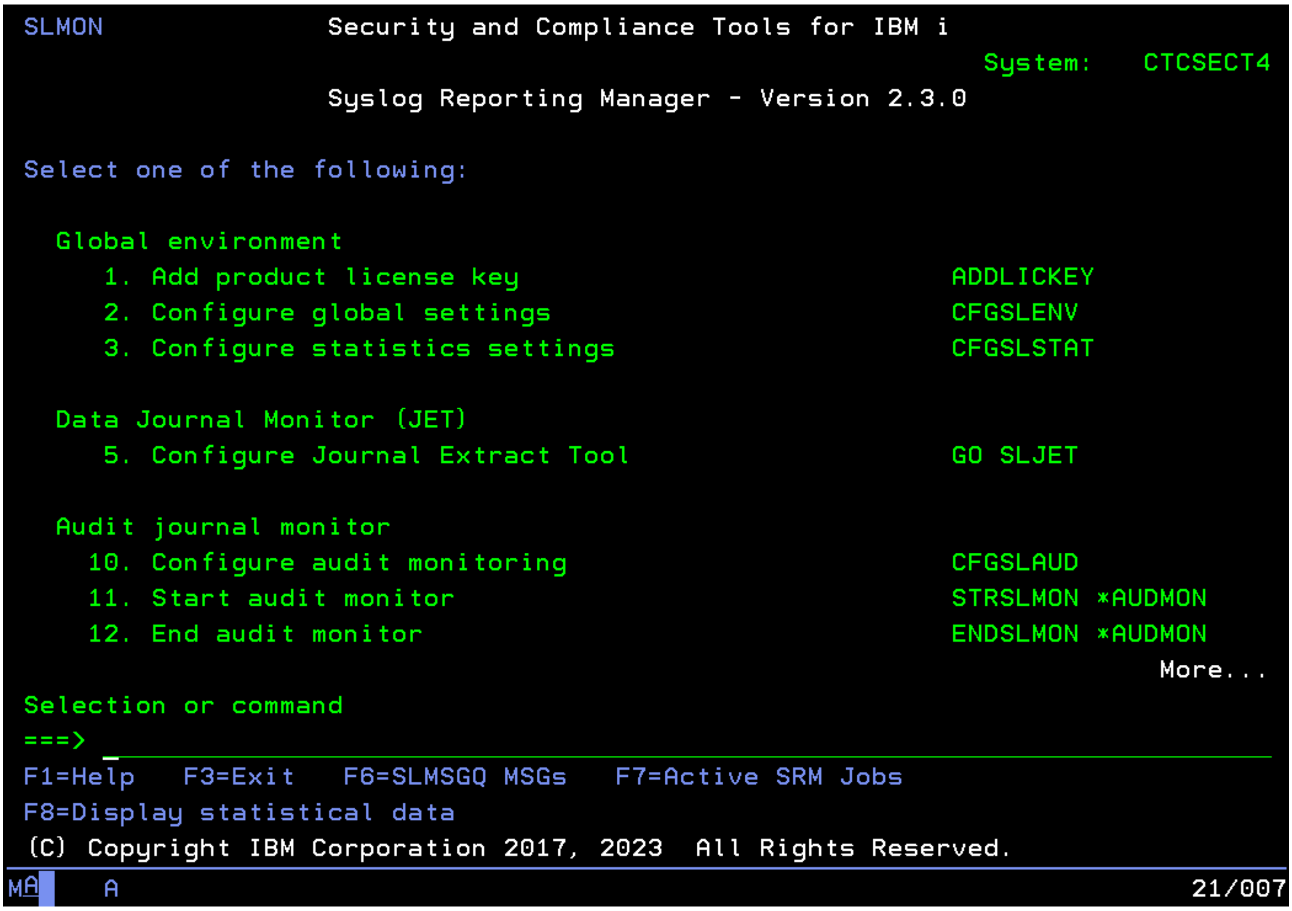
```
CALL PGM(QZRDSECSRM/RVKJSACC)
```

4.7 Registering the license key

After the installation of SRM, you can use the tool for a grace period of 70 days without registering a license key. The grace period starts when SRM is started for the first time. After the grace period has expired, you need to obtain a proper license key for your IBM Power System to continue using the tool.

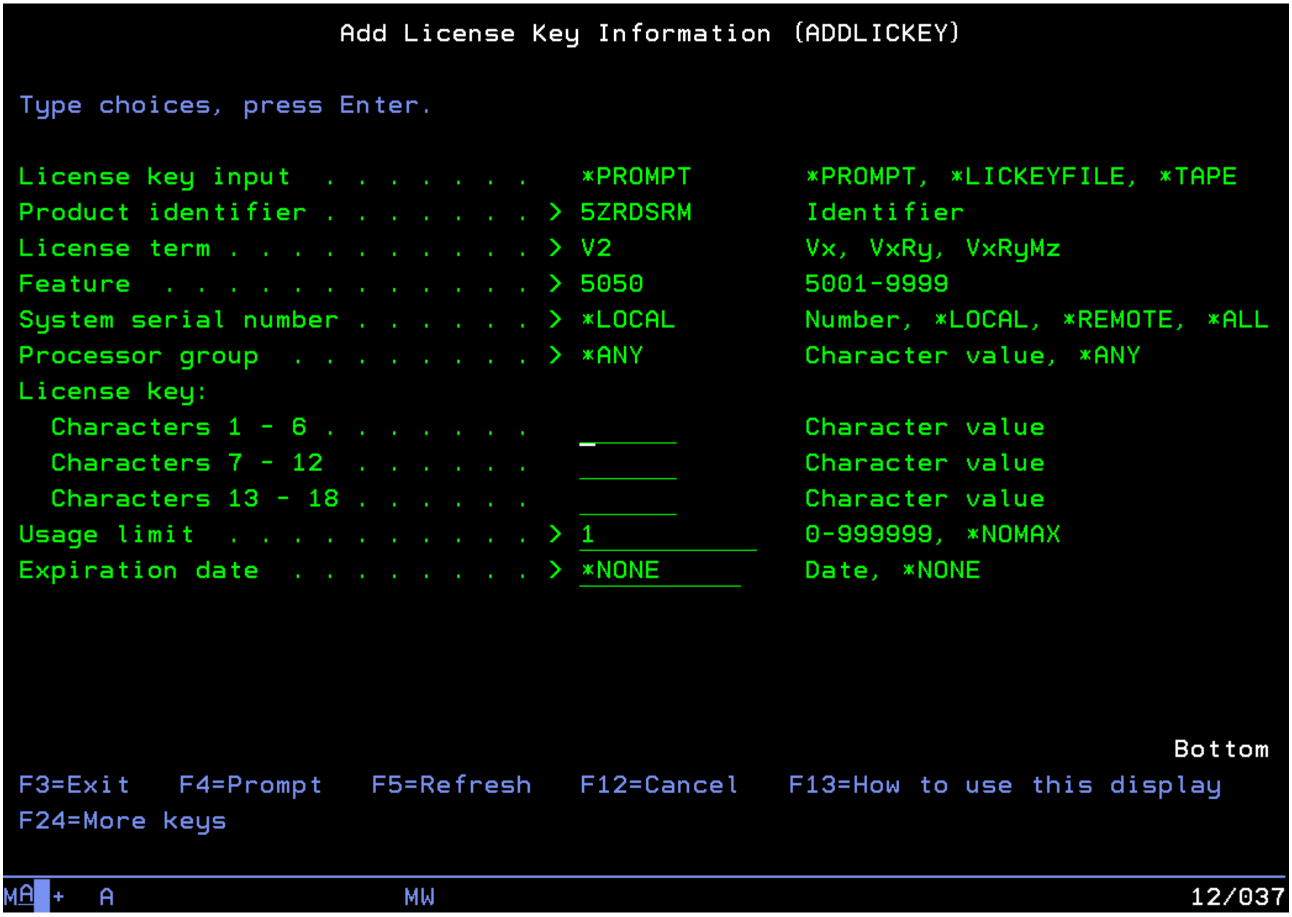
1. Start a 5250 session and sign on with a user that has *ALLOBJ special authority or as a member of the QZRDSRMGRP group.

2. Enter the following command to display the Syslog Reporting Manager menu.
   `CFGSRM`



```
SLMON                  Security and Compliance Tools for IBM i
                                                         System:   CTCSECT4
                       Syslog Reporting Manager - Version 2.3.0

Select one of the following:

  Global environment
     1. Add product license key                            ADDLICKEY
     2. Configure global settings                          CFGSLENV
     3. Configure statistics settings                      CFGSLSTAT

  Data Journal Monitor (JET)
     5. Configure Journal Extract Tool                     GO SLJET

  Audit journal monitor
    10. Configure audit monitoring                         CFGSLAUD
    11. Start audit monitor                                STRSLMON *AUDMON
    12. End audit monitor                                  ENDSLMON *AUDMON
                                                                  More...
Selection or command
===>
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
F8=Display statistical data
(C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                           21/007
```

3. Take option 1 to enter your license key.



```
                        Add License Key Information (ADDLICKEY)

 Type choices, press Enter.

 License key input . . . . . . . .   *PROMPT       *PROMPT, *LICKEYFILE, *TAPE
 Product identifier . . . . . . . > 5ZRDSRM       Identifier
 License term . . . . . . . . . . > V2            Vx, VxRy, VxRyMz
 Feature  . . . . . . . . . . . . > 5050          5001-9999
 System serial number . . . . . . > *LOCAL        Number, *LOCAL, *REMOTE, *ALL
 Processor group  . . . . . . . . > *ANY          Character value, *ANY
 License key:
   Characters 1 - 6 . . . . . . .   ______        Character value
   Characters 7 - 12  . . . . . .   ______        Character value
   Characters 13 - 18 . . . . . .   ______        Character value
 Usage limit  . . . . . . . . . . > 1__________   0-999999, *NOMAX
 Expiration date  . . . . . . . . > *NONE_____    Date, *NONE




                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

MA  +  A                  MW                                            12/037
```

4. Enter the following information:
    - License key
    - Usage limit
    - Expiration date

    Note: The information is provided by IBM Technology Expert Labs. Note that you can also copy and paste the ADDLICKEY command with its parameters that you received from your IBM Technology Expert Labs contact.

5. Press Enter to add your license code.

User configuration recommendation:

It is recommended to create a separate administrator profile and assign the following parameter to the profile:

```
INLMNU(QZRDSECSRM/SLMON)
CURLIB(QZRDSECSRM)
GRPPRF(QZRDSRMGRP)
```

A profile with these user profile settings has full administrative access to the Syslog Reporting Manager.

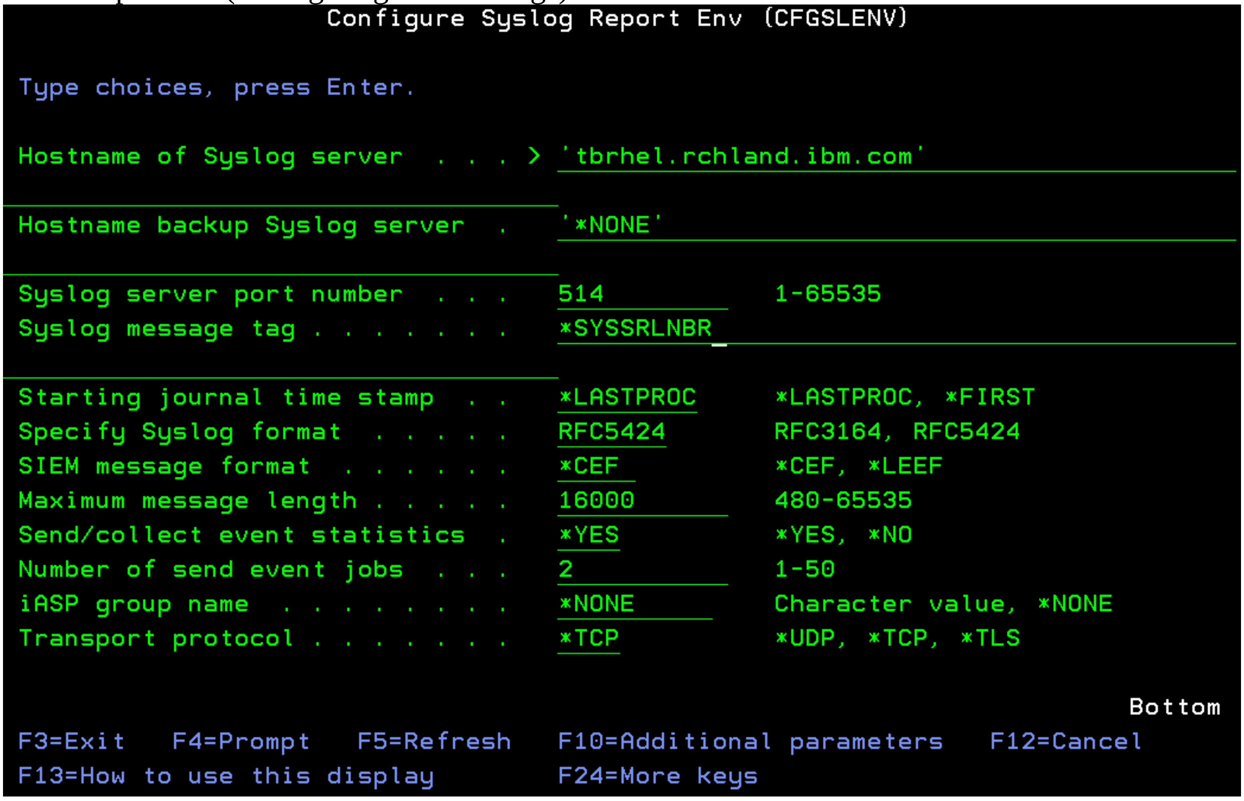
4.8 Basic setup of the Syslog Reporting Manager tool

There are a few global properties that need to be set up first.

1. Display the SLMON menu by entering the command.

   ```
   CFGSRM
   ```

2. Take option 2 (Configure global settings)



```
                     Configure Syslog Report Env (CFGSLENV)

Type choices, press Enter.

Hostname of Syslog server . . . > 'tbrhel.rchland.ibm.com'

Hostname backup Syslog server  .   '*NONE'

Syslog server port number  . . .   514          1-65535
Syslog message tag . . . . . . .   *SYSSRLNBR

Starting journal time stamp  . .   *LASTPROC     *LASTPROC, *FIRST
Specify Syslog format  . . . . .   RFC5424       RFC3164, RFC5424
SIEM message format  . . . . . .   *CEF          *CEF, *LEEF
Maximum message length . . . . .   16000         480-65535
Send/collect event statistics  .   *YES          *YES, *NO
Number of send event jobs  . . .   2             1-50
iASP group name  . . . . . . . .   *NONE         Character value, *NONE
Transport protocol . . . . . . .   *TCP          *UDP, *TCP, *TLS

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Information: Direct access via command: CFGSLENV

3. Provide the global information, such as:
   - Hostname or IP address of primary and backup syslog server that will receive the syslog messages <or the *OUTFILE special value in case you want to store the events in a database table instead of sending them to a remote system.
   - Output file for events when *OUTFILE is specified for the primary hostname parameter.
   - Output control determines if an output file should be recreated when it exists or to not change it if it already exists. Note if the file does not exist, the CFGSLENV command creates it.>
   - The port that the syslog server is listening on.
   - An optional syslog header tag.
   - Starting journal time stamp option
   - Time stamp that is used in the syslog header
   - Syslog standard
   - SIEM message format (LEEF or CEF)
   - Maximum message length
   - Event statistics collection and reporting option
   - Number of send event jobs
   - iASP group name
   - Transport protocol (UDP, TCP, or TLS)

- TCP message transfer method
- Certificate path validation
- Peer certificate check for primary syslog server
- Wildcard certificate check for primary syslog server
- Peer certificate check for backup syslog server
- Wildcard certificate check for backup syslog server
- Filter for SRM audit monitor originated ZC or ZR object auditing events
- Number of rows to fetch for the audit journal monitor for T-journal code events
- Number of rows to fetch for the audit journal monitor for U-journal code events
- Number of rows to fetch for the history log monitor
- <CCSID for event conversion>

Information: Every command and configuration display provides detailed online help for all parameters via the F1 key.

Important: You have to completely end and start the Syslog Reporting Manager if you change the iASP group name.

To be able to use TLS encryption, you need to meet certain prerequisites. See section Transport Layer Security (TLS) implementation information on page 102 for more details.

4. After all global configuration values have been specified, press Enter to save your changes.

4.9 Defining the audit journal monitor environment

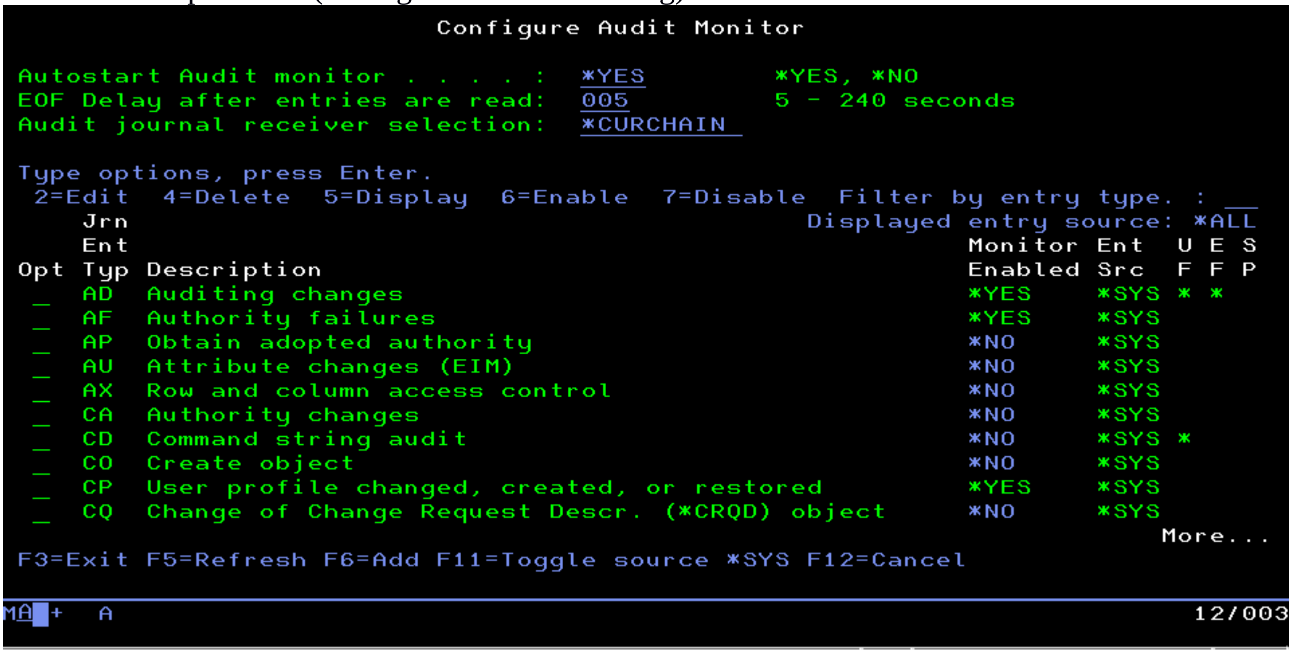
The settings for the audit journal event monitor specify:

- Whether the audit journal event monitor will automatically start when the subsystem SLSBS starts
- The EOF delay specifies the number of seconds to sleep when all events have been read before trying to retrieve new events.
- Whether audit journals should be processed in all attached audit journal receivers (*CURCHAIN) or only in the currently attached receiver (*CURRENT).
- The audit journal event types that the event monitor job should process.

1. Display the SLMON menu by entering the command.

   ```
   CFGSRM
   ```

2. Take option 10 (Configure audit monitoring)



```
                           Configure Audit Monitor

 Autostart Audit monitor . . . . :  *YES        *YES, *NO
 EOF Delay after entries are read:  005         5 - 240 seconds
 Audit journal receiver selection:  *CURCHAIN

 Type options, press Enter.
  2=Edit  4=Delete  5=Display  6=Enable   7=Disable  Filter by entry type. : ___
     Jrn                                          Displayed entry source: *ALL
     Ent                                                    Monitor Ent  U E S
 Opt Typ Description                                        Enabled Src  F F P
  _  AD  Auditing changes                                   *YES    *SYS * *
  _  AF  Authority failures                                 *YES    *SYS
  _  AP  Obtain adopted authority                           *NO     *SYS
  _  AU  Attribute changes (EIM)                            *NO     *SYS
  _  AX  Row and column access control                      *NO     *SYS
  _  CA  Authority changes                                  *NO     *SYS
  _  CD  Command string audit                               *NO     *SYS *
  _  CO  Create object                                      *NO     *SYS
  _  CP  User profile changed, created, or restored         *YES    *SYS
  _  CQ  Change of Change Request Descr. (*CRQD) object     *NO     *SYS
                                                                         More...
 F3=Exit F5=Refresh F6=Add F11=Toggle source *SYS F12=Cancel

MA█+  A                                                                   12/003
```

Information: Direct access via command: CFGSLAUD

3. Enable all events that you want to have the event monitor report as syslog messages to the remote syslog server. See the online help for detailed information about each parameter. With option 2 you can also specify user profile or entry-specific data filters. >For the CD entry type you also specify a filter for run mode (i.e. only for commands run interactively).<

Note: The support for several journal entry types depend on the installed IBM i release and partly also on installed PTFs. See appendix 11   Audit journal entry type support on page 128 for the prerequisites for the various journal entry types of the entry source category *SYS.

4. Optionally you can also add U-journal code event types. They are listed as entry source *USR in the list of events. User type journal event types must be unique. They can be deleted or added as needed. System-type (*SYS) journal event types cannot be deleted.

Audit event processing information

Which events the audit journal monitor processes depends on different criteria. The audit monitor processes all entries that are enabled in the configuration and that match the optional filter criteria (user filter and entry type filter). In addition, the following applies:

- When SRM is installed and starts the first time, it starts with the currently attached audit journal receiver and processes entries from the current time minus 1 hour.
- When SRM runs, the audit monitor keeps track of the last event that has been successfully processed and also the journal receiver in which the event was stored.
- When SRM is stopped and started again, the audit monitor checks whether the previously logged journal receiver still exists, if it does, the event selection is done based on the receiver and timestamp of the last event as the starting point. If the receiver does not exist anymore, the audit monitor starts either from the current chain of receivers (*CURCHAIN) or the currently attached receiver (*CURRENT). This is configurable in audit journal receiver selection parameter in the CFGSLAUD command.

4.10 Defining the IFS stream file change monitor environment

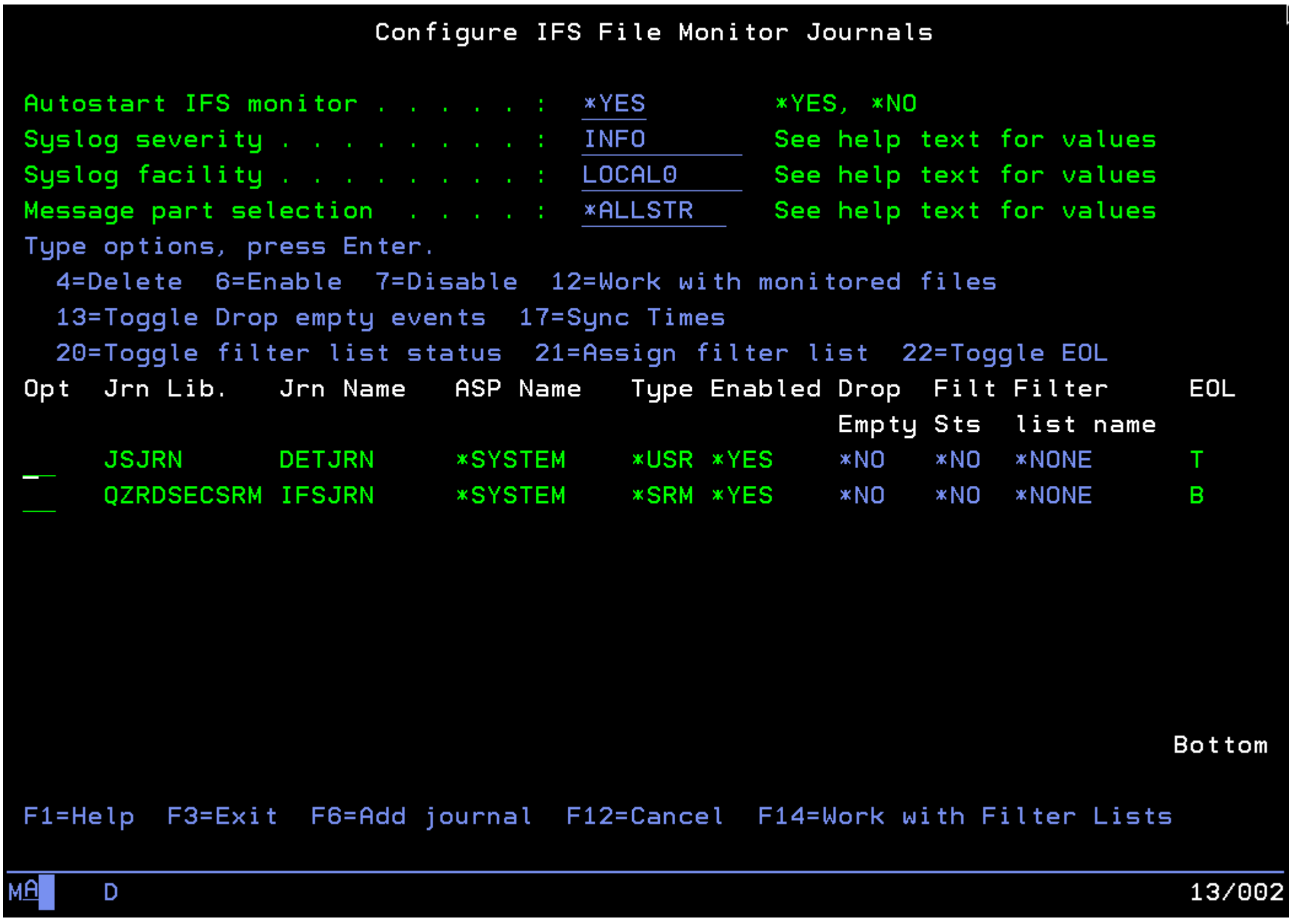
The settings for the IFS file change event monitor specify:

- Select or define journals that monitor for IFS file changes. There is always the default journal QZRDSECSRM/IFSJRN.
- Whether the IFS file change event monitor will automatically start when SRM starts
- If IFS file changes with no changed data are reported (Drop empty events)
- If file list filtering is activated for a specific journal
- The syslog severity that is used for each file change event that is reported via the event monitor. See online help for valid values.
- The syslog facility that is used for each file change event that is reported via the event monitor. See online help for valid values.
- The selection of the data parts of the changed content that will be reported to the remote syslog/SIEM server.
- <Whether Line Feed (LF) or Carriage Return (CR) control characters are represented as text (<LF> or <CR>) in the event of replaced by a blank character.<

1. Display the SLMON menu by entering the command.

```
CFGSRM
```

2. Take option 20 (Configure IFS file monitor)



```
                          Configure IFS File Monitor Journals

 Autostart IFS monitor . . . . . :   *YES         *YES, *NO
 Syslog severity . . . . . . . . :   INFO         See help text for values
 Syslog facility . . . . . . . . :   LOCAL0       See help text for values
 Message part selection  . . . . :   *ALLSTR      See help text for values
 Type options, press Enter.
   4=Delete  6=Enable  7=Disable  12=Work with monitored files
   13=Toggle Drop empty events  17=Sync Times
   20=Toggle filter list status  21=Assign filter list  22=Toggle EOL
 Opt  Jrn Lib.   Jrn Name   ASP Name   Type Enabled Drop  Filt Filter     EOL
                                                    Empty Sts  list name
 __   JSJRN      DETJRN     *SYSTEM    *USR *YES    *NO   *NO  *NONE      T
 __   QZRDSECSRM IFSJRN     *SYSTEM    *SRM *YES    *NO   *NO  *NONE      B

                                                                    Bottom
 F1=Help  F3=Exit  F6=Add journal  F12=Cancel  F14=Work with Filter Lists

MA     D                                                            13/002
```

Information: Direct access via command: CFGSLIFSJ

3. Work with the journals that monitor IFS file changes. You can add or remove journal names, enable or disable processing of events in a defined journal or work with files that are journaled

via a specific journal.

4. Specify the autostart, syslog severity, syslog facility, and message part settings. Note that these parameters are valid for all journals.
   Note that you cannot delete the SRM-provided journal QZRDSECSRM/IFSJRN from the list.

   Option 12 lets you work with files that are journaled via the selected journal.

   Option 13 lets you specify whether file change events with no data are dropped or sent to the configured server. An empty change event is considered as follows:
   - The total length of the change is 0
   - The change contains only a LF, CR, CRLF, or LFCR characters

   If you select *YES for dropping empty events, the selection affects all journaled files for the selected journal.

   Option 17 is only available when the calling user has at least the *AUDIT special authority in its user profile (not inherited from a group membership) and is member of the QZRDSRMGRP group. It is considered an expert mode configuration option and allows you to change synchronization restart properties, such as the timestamp of the last processed event entry. This option should only be used by experts who know what impact the change can have.

   Option 20 activates IFS file filtering for monitored files. If you want to use file filtering, you need to set the filter status to *YES and assign an existing filter list with option 21. If you enable file filtering but have no filter list assigned, the column of the entry is shown in red indicating that filtering does not work. In this case, all file changes are reported.

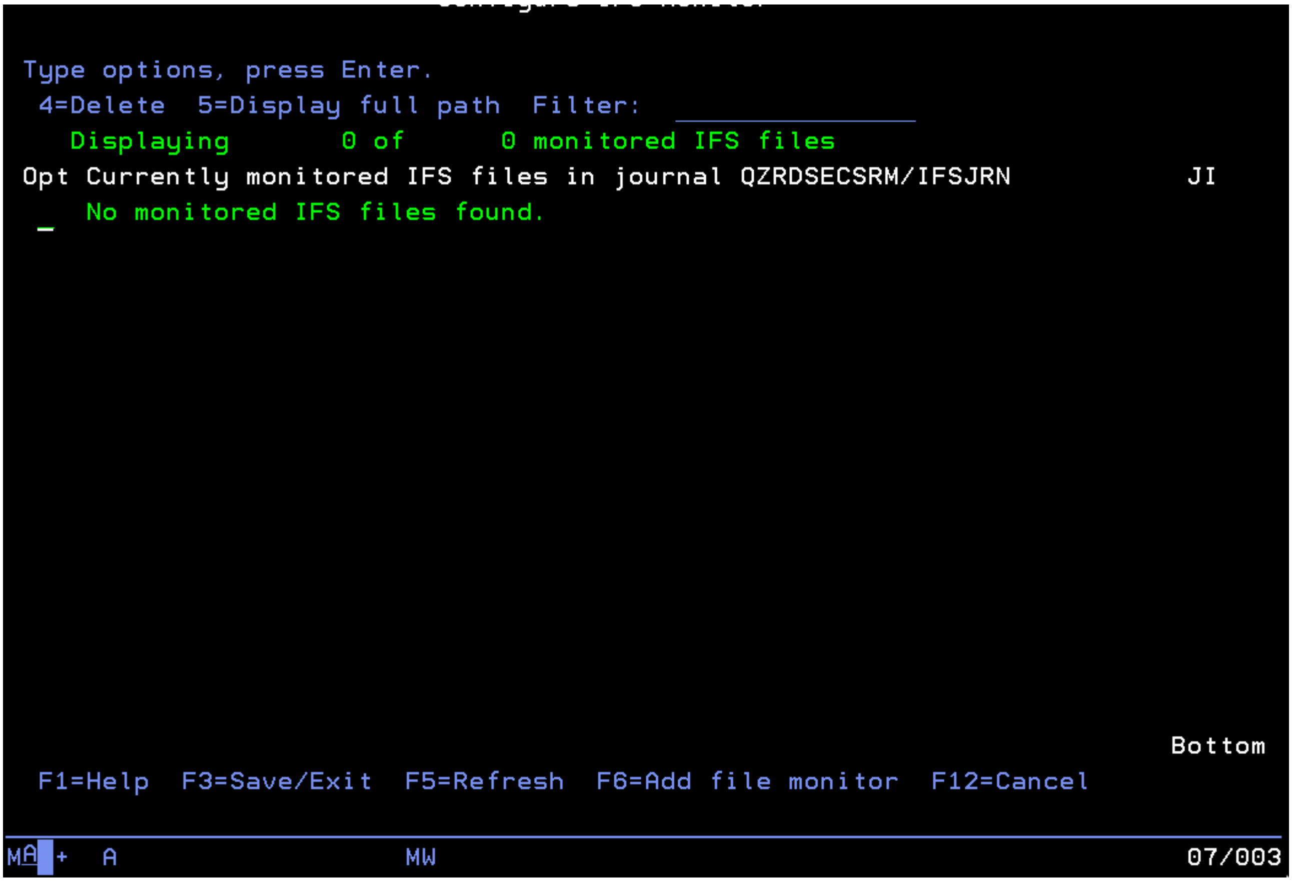
   Option 21 lets you assign an existing filter list to a journal. Filter lists can be managed via the F14 key or by entering the CFGSLIFSFL command.

   >Option 22 lets you define how end-of-line (EOL) characters in an IFS file change are handled. This option provides a toggle between EOL option T or B.

   T = If a hex character is found in the changed IFS data for a line feed (LF) or carriage return (CR) the hex characters are translated to <LF> and <CR> respectively. This is the default.

   B = If a hex character is found in the changed IFS data for a line feed (LF) or carriage return (CR) the hex characters are translated to a blank character. <

Files to be monitored need to be journaled. This can be done with option 12 of the CFGSLIFSJ command on a journal as described above.



```
 Type options, press Enter.
  4=Delete  5=Display full path  Filter: _______________
    Displaying       0 of       0 monitored IFS files
 Opt Currently monitored IFS files in journal QZRDSECSRM/IFSJRN           JI
  _  No monitored IFS files found.

                                                                       Bottom
  F1=Help  F3=Save/Exit  F5=Refresh  F6=Add file monitor  F12=Cancel
MA + A                  MW                                           07/003
```

Information: Direct access via command: CFGSLIFS

To add a new file to be monitored, press F6.
The JI column indicates whether a directory has journal inheritance turned on. The meaning the column values are:

- **-**
  The listed item is a stream file and directory journal inheritance does not apply.
- **N**
  The listed item is a directory and journal inheritance for new objects is not turned on.
- **Y**
  The listed item is a directory and journal inheritance for new objects is turned on. In this case all new objects that are created in the directory are automatically added to the journal.

5. Add IFS files to the list of monitored files. See the online help text for more information.

Alternative method to add or remove IFS files from the monitor list.

- Adding files using the STRJRN command. Example:
  - `STRJRN OBJ(('/www/prodserver/logs/critlog')) JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')`
  - Note that you can also add files generically by using a path such as `www/prodserver/logs/*`
  - You can also add an entire directory and all future files that will be created in a directory:

```
STRJRN OBJ(('/www/prodserver/logs/'))
JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN') INHERIT(*YES)
```

Important note: The path name length of an IFS file is limited to 350 characters.

- Removing files from the monitor list with the ENDJRN command. Example:
  - Removing a single file

    ```
    ENDJRN OBJ(('/www/prodserver/logs/critlog'))
    JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')
    ```

  - Removing all files

    ```
    ENDJRN OBJ(*ALL) JRN('/QSYS.LIB/QZRDSECSRM.LIB/IFSJRN.JRN')
    ```

4.10.1 IFS filtering support

The IFS filtering support lets you limit the number of journaled files for which you want to report file changes to the configured remote syslog server. For example, if the journal that you registered for SRM IFS file monitoring with the CFGSLIFSJ command journals 4000 files but you want to report only file changes of 100 files, you can use the filter support to specify the names or patterns of the 100 file names that that should be reported.

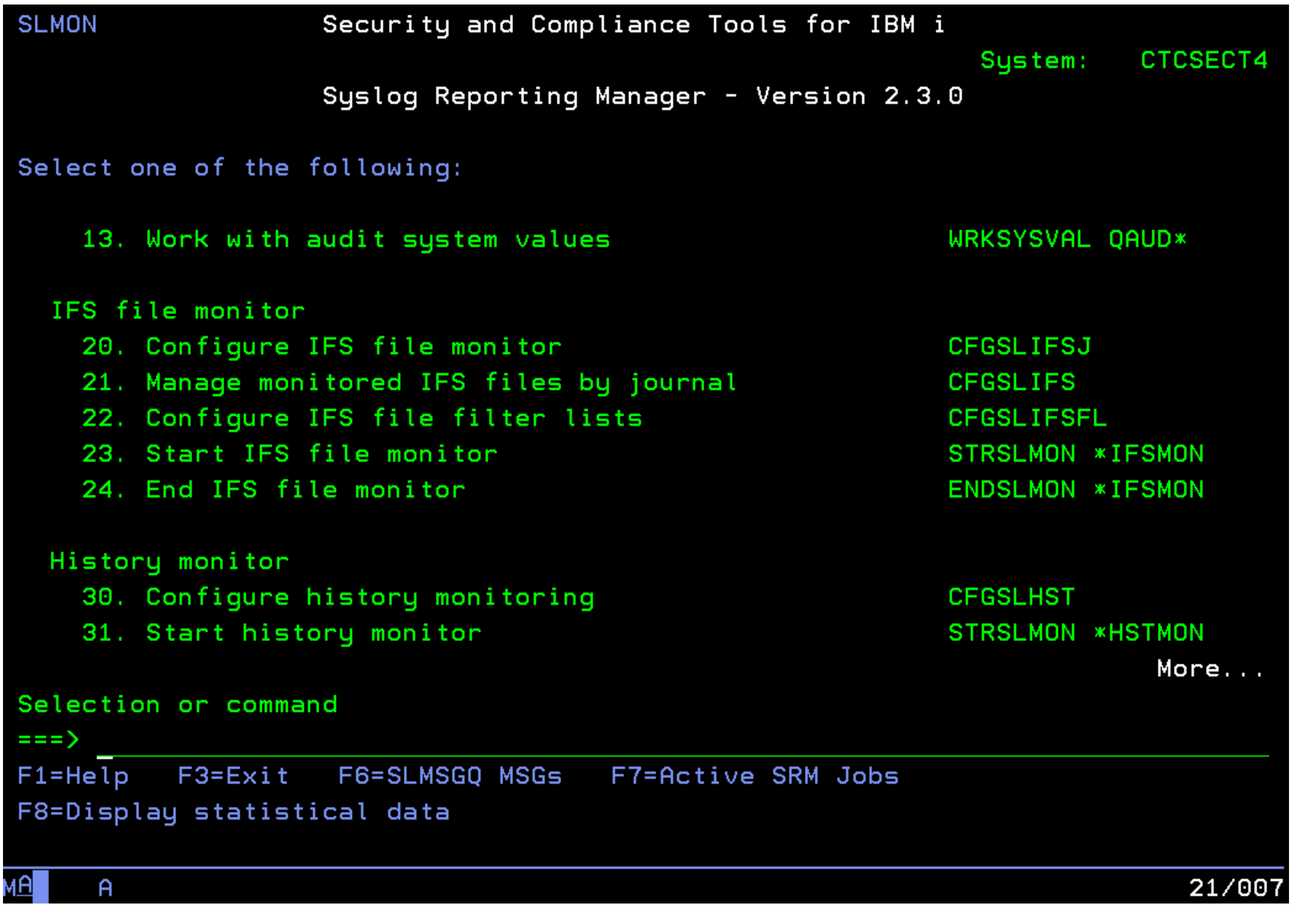
The file names can be defined in a filter list as file definitions. A file definition can be an absolute file name or some generic pattern as described in the following examples:

- Filter for a specific file in a given directory.
  `/appdir/logs/appaccess.log`
- Filter for a specific file name without specifying the directory path. In this case, the file can reside anywhere in the IFS and can even have file name suffixes, such as a date.
  `%error.log%`
- On IBM i, HTTP Web server configurations are normally stored under IFS directory path /www followed by the instance name and specific Web server directories, i.e. /www/tomweb1/logs/access.log
  In this example we want to monitor all access.log files for all existing Web server instances.
  `/www/%/logs/access.log`
- The following definition is a filter for all files that start with /invoices/transaction.log but might have extensions, such as transaction.log_072022 and transaction.log_082022.
  `/invoices/transaction.log%`

Note that the % character represents any number and kind of characters in the specified place. For example, if you specify %logs/error.log, any directory path before logs/error.log is considerend, i.e. /myapp/mydir1/mydir2/logs/error.log or /www/websrv1/logs/error.log.

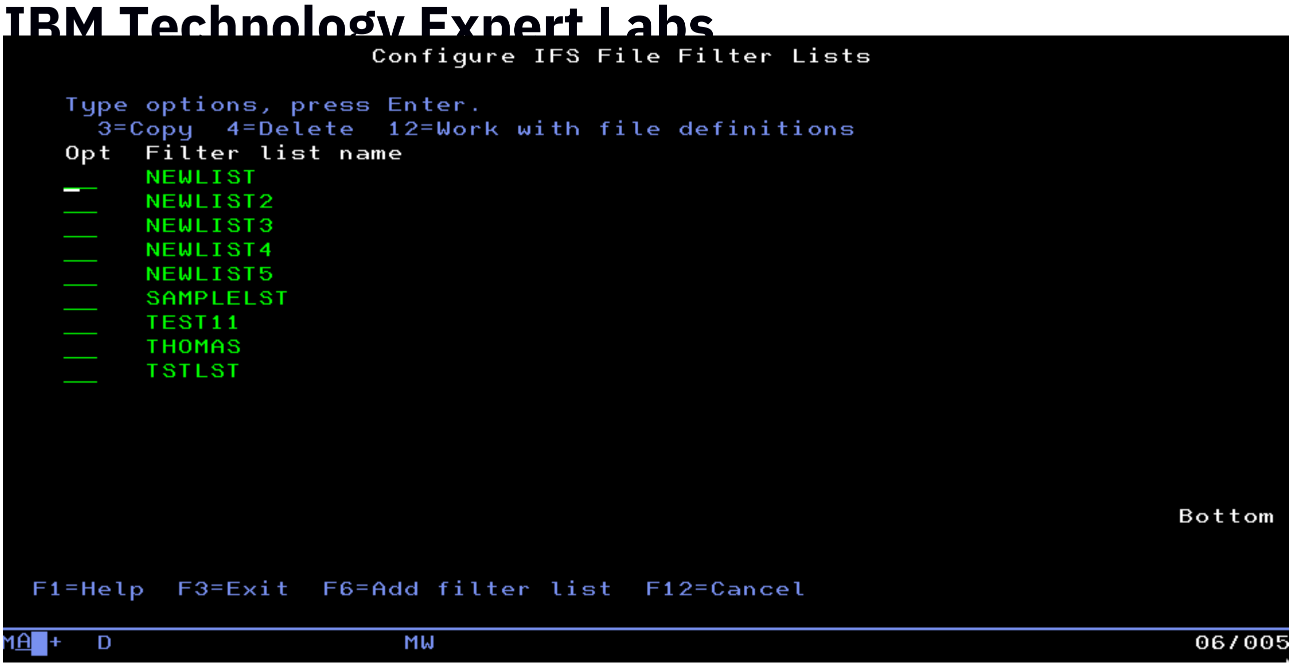
Filter lists are managed and used as follows:

Using the SRM main menu, select option 22 to configure IFS file filter lists.



```
SLMON                 Security and Compliance Tools for IBM i
                                                              System:   CTCSECT4
                      Syslog Reporting Manager - Version 2.3.0

Select one of the following:

    13. Work with audit system values                      WRKSYSVAL QAUD*

  IFS file monitor
    20. Configure IFS file monitor                         CFGSLIFSJ
    21. Manage monitored IFS files by journal              CFGSLIFS
    22. Configure IFS file filter lists                    CFGSLIFSFL
    23. Start IFS file monitor                             STRSLMON *IFSMON
    24. End IFS file monitor                               ENDSLMON *IFSMON

  History monitor
    30. Configure history monitoring                       CFGSLHST
    31. Start history monitor                              STRSLMON *HSTMON
                                                                       More...
Selection or command
===> _
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
F8=Display statistical data

MA     A                                                               21/007
```

Information: Direct access via command: CFGSLIFSFL

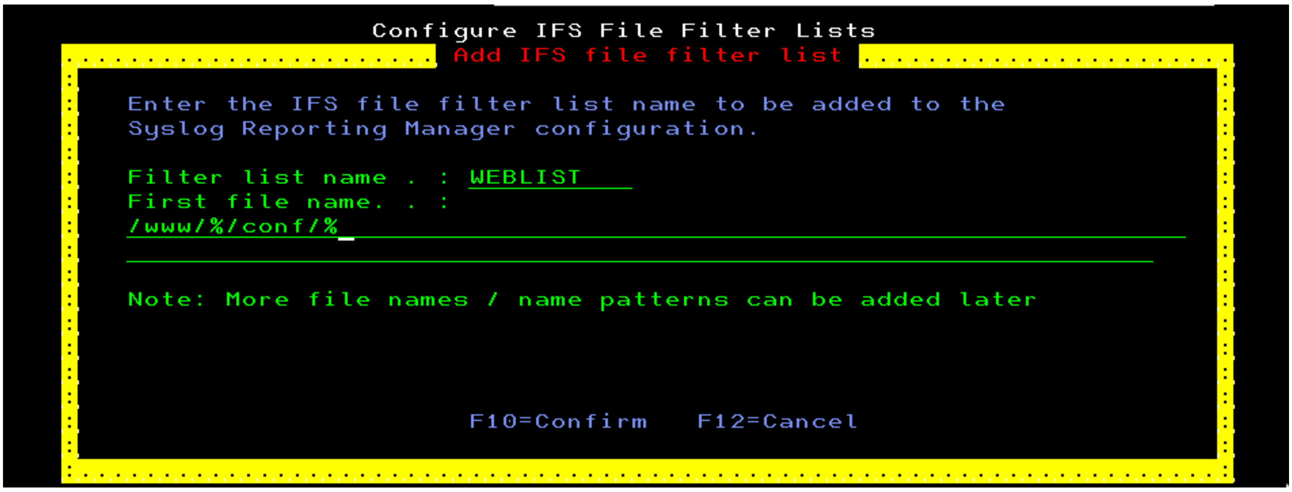


```
                          Configure IFS File Filter Lists

   Type options, press Enter.
     3=Copy   4=Delete   12=Work with file definitions
   Opt    Filter list name
   ___    NEWLIST
   ___    NEWLIST2
   ___    NEWLIST3
   ___    NEWLIST4
   ___    NEWLIST5
   ___    SAMPLELST
   ___    TEST11
   ___    THOMAS
   ___    TSTLST

                                                                          Bottom

 F1=Help   F3=Exit   F6=Add filter list   F12=Cancel
```

With option 3 you can copy an existing filter list into a new list. All file definitions from the original list will be copied too.

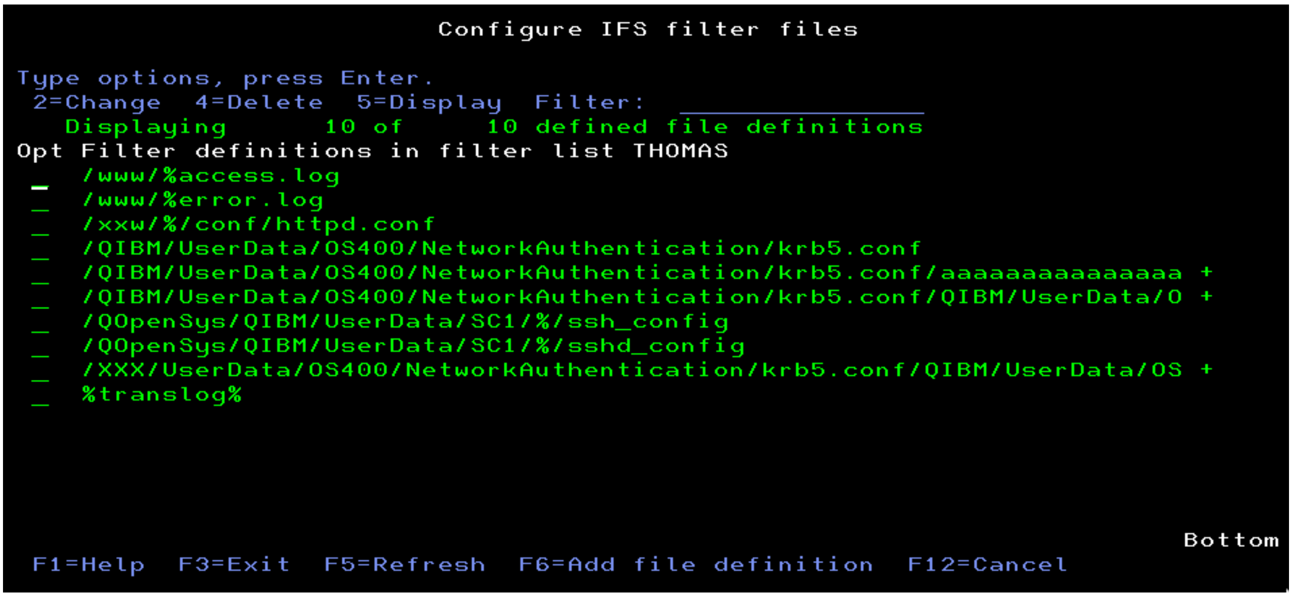
With option 4 you can delete an existing filter list. You can only delete a filter list if it is not assigned to an actively filtered journal. You have to remove the assignment first or deactivate file filtering before you can delete the filter list. The CFGSLIFSJ command lets you manage the filter status and assignment. If a filter list is still assigned to a journal, but the filter is not active, the filter list is deleted and the assigned filter list set to *NONE for the corresponding journal entry in the CFGSLIFSJ command.

Funtion key F6 lets you add a new filter list. When adding a new filter list, you have to specify the name of the new list and one file definition as shown in the following example:



```
                          Configure IFS File Filter Lists
   ........................ Add IFS file filter list ........................
   :                                                                        :
   :    Enter the IFS file filter list name to be added to the              :
   :    Syslog Reporting Manager configuration.                             :
   :                                                                        :
   :    Filter list name . :  WEBLIST                                       :
   :    First file name. . :                                                :
   :    /www/%/conf/%                                                       :
   :                                                                        :
   :                                                                        :
   :    Note: More file names / name patterns can be added later            :
   :                                                                        :
   :                                                                        :
   :                                                                        :
   :                       F10=Confirm    F12=Cancel                        :
   :                                                                        :
   :........................................................................:
```

You can manage existing filter lists by using option 12 to work with the individual file definitions.

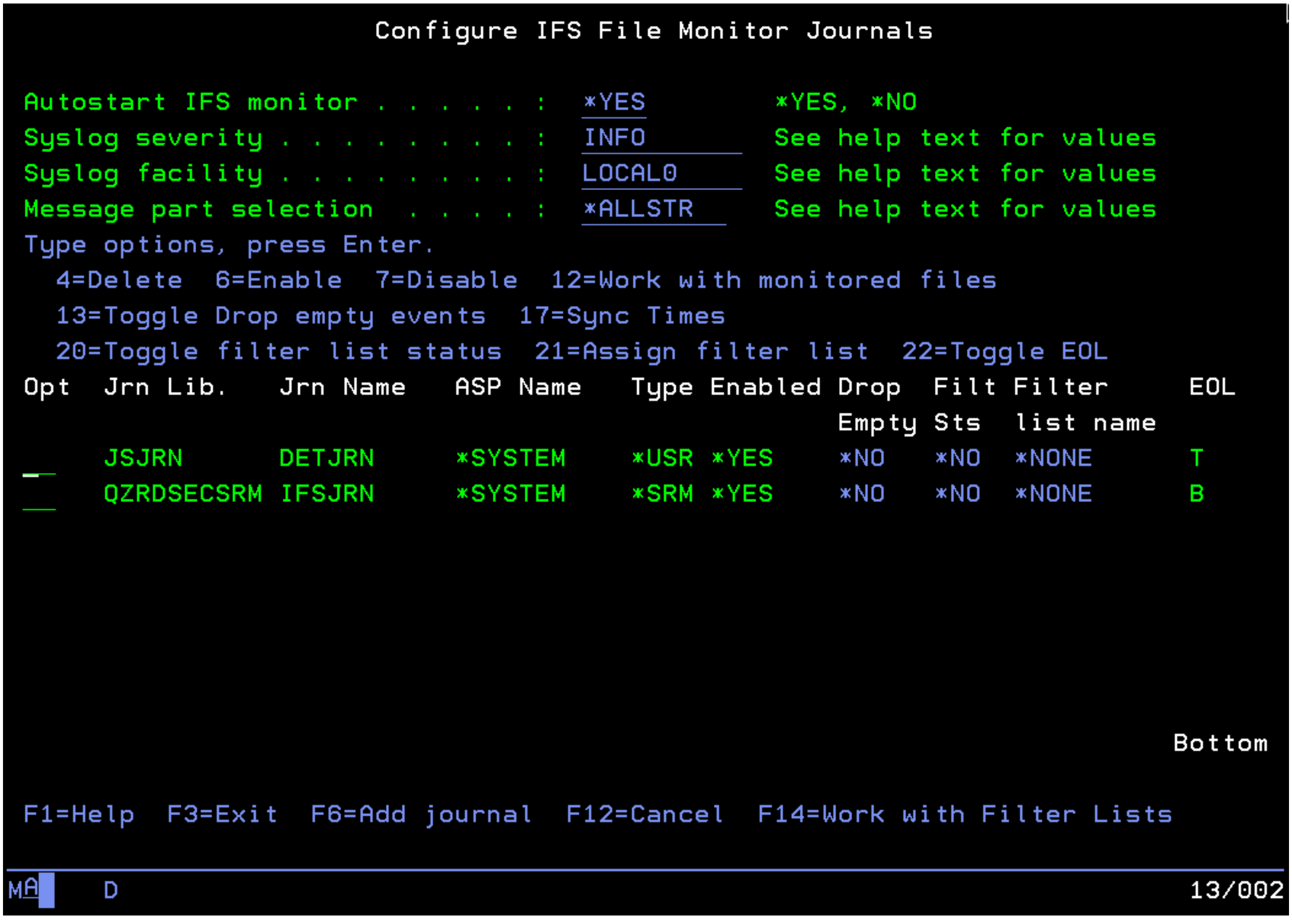


```
                           Configure IFS filter files

Type options, press Enter.
 2=Change   4=Delete   5=Display  Filter: _______________
   Displaying      10 of      10 defined file definitions
Opt Filter definitions in filter list THOMAS
 _   /www/%access.log
 _   /www/%error.log
 _   /xxw/%/conf/httpd.conf
 _   /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf
 _   /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf/aaaaaaaaaaaaaaa +
 _   /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf/QIBM/UserData/O +
 _   /QOpenSys/QIBM/UserData/SC1/%/ssh_config
 _   /QOpenSys/QIBM/UserData/SC1/%/sshd_config
 _   /XXX/UserData/OS400/NetworkAuthentication/krb5.conf/QIBM/UserData/OS +
 _   %translog%





                                                                        Bottom
 F1=Help   F3=Exit   F5=Refresh   F6=Add file definition   F12=Cancel
```

All file definitions for the selected filter list are shown. You can use the options to change, delete, or display an existing definition or function key F6 to add a new definition.

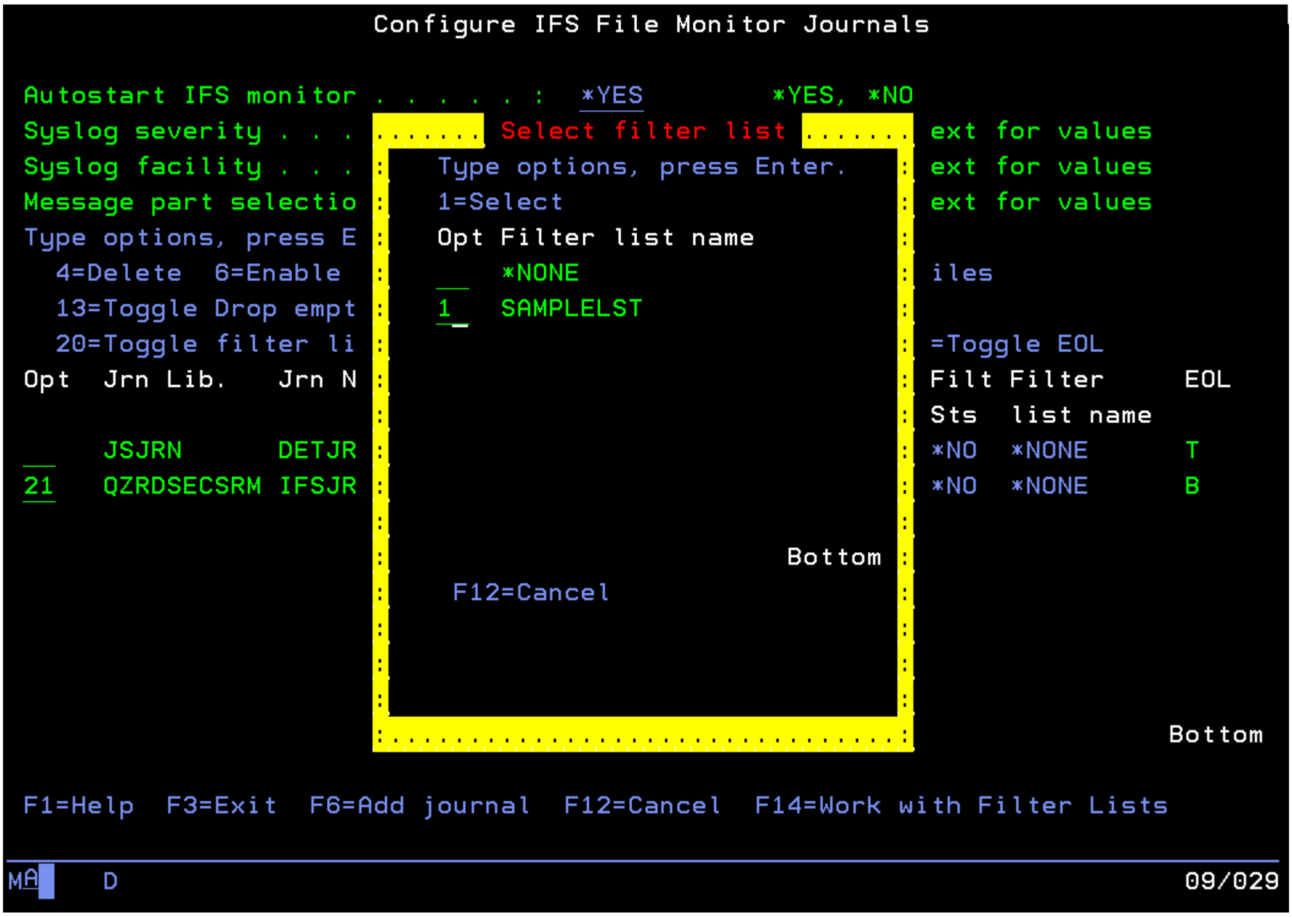
Note: A file definition has a maximum length of 128 characters. If a definition is longer than 70 characters, a + sign is shown on the right side of the display. You can then use option 5 to display the full definition.

Once you have defined your filter definition and filter list, you have to assign it to a journal using the CFGSLIFSJ command.



```
                        Configure IFS File Monitor Journals

Autostart IFS monitor . . . . . . :  *YES          *YES, *NO
Syslog severity . . . . . . . . . :  INFO          See help text for values
Syslog facility . . . . . . . . . :  LOCAL0        See help text for values
Message part selection  . . . . . :  *ALLSTR       See help text for values
Type options, press Enter.
  4=Delete  6=Enable  7=Disable  12=Work with monitored files
  13=Toggle Drop empty events  17=Sync Times
  20=Toggle filter list status  21=Assign filter list  22=Toggle EOL
Opt  Jrn Lib.    Jrn Name    ASP Name    Type Enabled Drop  Filt Filter     EOL
                                                      Empty Sts  list name
___  JSJRN       DETJRN      *SYSTEM     *USR *YES    *NO   *NO  *NONE      T
___  QZRDSECSRM  IFSJRN      *SYSTEM     *SRM *YES    *NO   *NO  *NONE      B








                                                                        Bottom

F1=Help  F3=Exit  F6=Add journal  F12=Cancel  F14=Work with Filter Lists


MA     D                                                               13/002
```

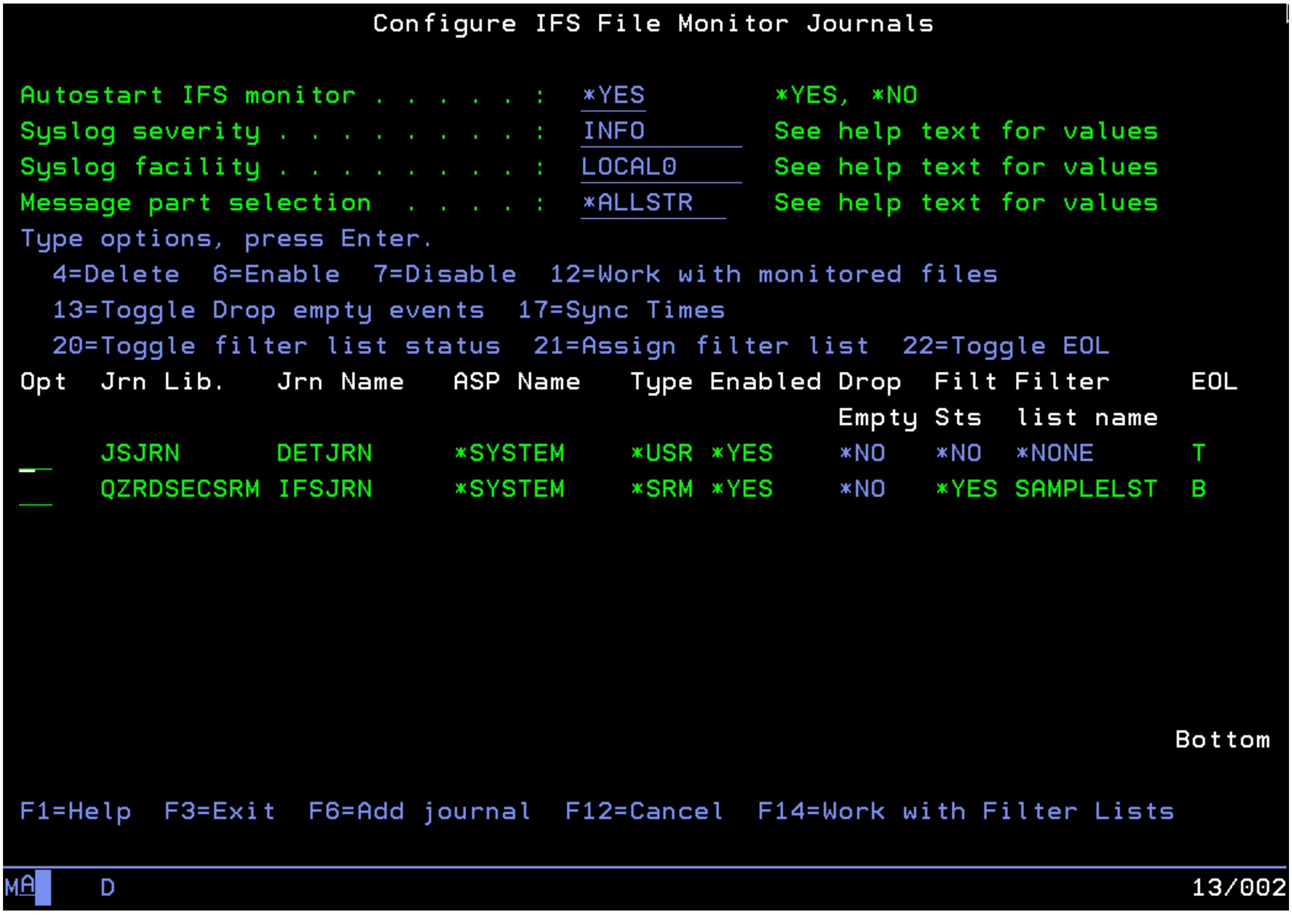
Use option 21 to assign a filter list to a journal. The option shows a list of all existing filter lists.



```
                      Configure IFS File Monitor Journals

Autostart IFS monitor . . . . . :  *YES        *YES, *NO
Syslog severity . . . ....... Select filter list ....... ext for values
Syslog facility . . . :   Type options, press Enter.   : ext for values
Message part selectio :   1=Select                     : ext for values
Type options, press E :   Opt Filter list name         :
  4=Delete  6=Enable  :   ___ *NONE                    : iles
  13=Toggle Drop empt :   1_  SAMPLELST                :
  20=Toggle filter li :                                : =Toggle EOL
Opt  Jrn Lib.   Jrn N :                                : Filt Filter     EOL
                      :                                : Sts  list name
__   JSJRN      DETJR :                                : *NO  *NONE      T
21   QZRDSECSRM IFSJR :                                : *NO  *NONE      B
                      :                                :
                      :                         Bottom :
                      :    F12=Cancel                  :
                      :                                :
                      :                                :
                      :                                :
                      :................................:                Bottom

F1=Help  F3=Exit  F6=Add journal  F12=Cancel  F14=Work with Filter Lists

MA   D                                                                   09/029
```

Select the list that you want to use with option 1 and press Enter.

Then select option 20 to enable the list. The color of an activated filter changes from blue to green.



```
                          Configure IFS File Monitor Journals

 Autostart IFS monitor . . . . . . :   *YES         *YES, *NO
 Syslog severity . . . . . . . . . :   INFO         See help text for values
 Syslog facility . . . . . . . . . :   LOCAL0       See help text for values
 Message part selection  . . . . . :   *ALLSTR      See help text for values
 Type options, press Enter.
   4=Delete  6=Enable  7=Disable  12=Work with monitored files
   13=Toggle Drop empty events  17=Sync Times
   20=Toggle filter list status  21=Assign filter list  22=Toggle EOL
 Opt  Jrn Lib.   Jrn Name   ASP Name   Type Enabled Drop  Filt Filter     EOL
                                                   Empty Sts  list name
 __   JSJRN      DETJRN     *SYSTEM    *USR *YES    *NO   *NO  *NONE       T
 __   QZRDSECSRM IFSJRN     *SYSTEM    *SRM *YES    *NO   *YES SAMPLELST   B









                                                                      Bottom

 F1=Help  F3=Exit  F6=Add journal  F12=Cancel  F14=Work with Filter Lists

MA     D                                                              13/002
```

A filter list has now been activated. Only IFS file changes of monitored files where the file name matches one of the file definitions in the list will be reported to the syslog server. Changes of non-matching files will be skipped.

Important: Please be reminded that a filter does not turn on journaling for a file. You must still enable IFS file journaling for a given file in order for the change to be detected by SRM.

4.11 Defining the QHST history log event monitor environment

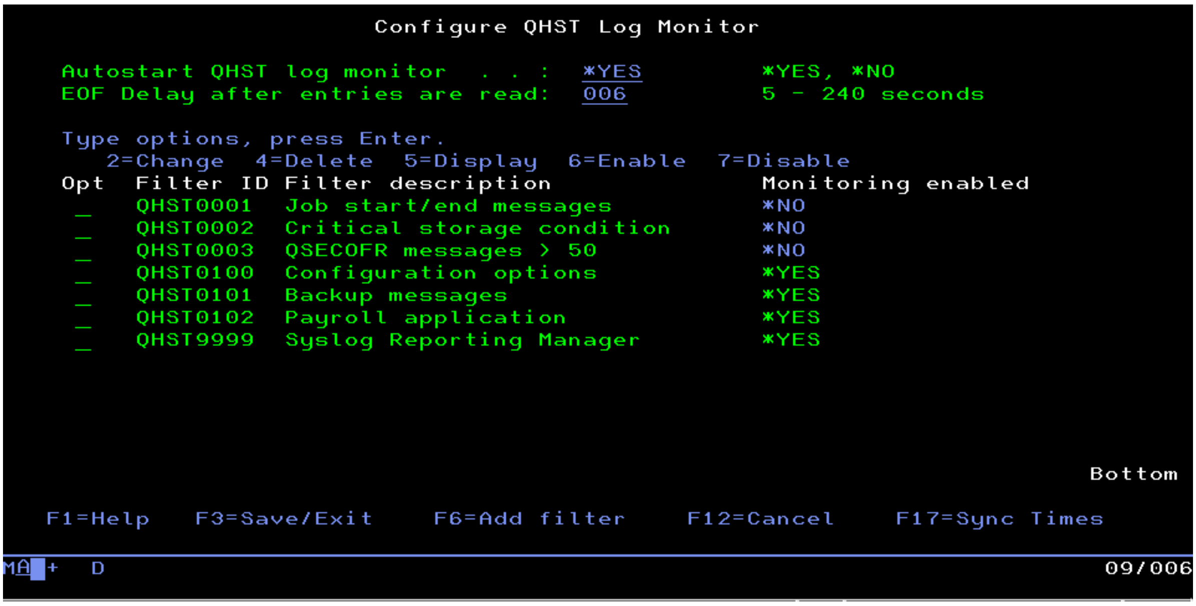
The settings for the QHST history log event monitor specify:

- Whether the history log event monitor will automatically start when the subsystem SLSBS starts
- The EOF delay specifies the number of seconds to sleep when all events have been read before trying to retrieve new events.
- The history selection filter rules that the event monitor job should process.

1. Display the SLMON menu by entering the command.

```
CFGSRM
```

2. Take option 30 (Configure history monitoring)



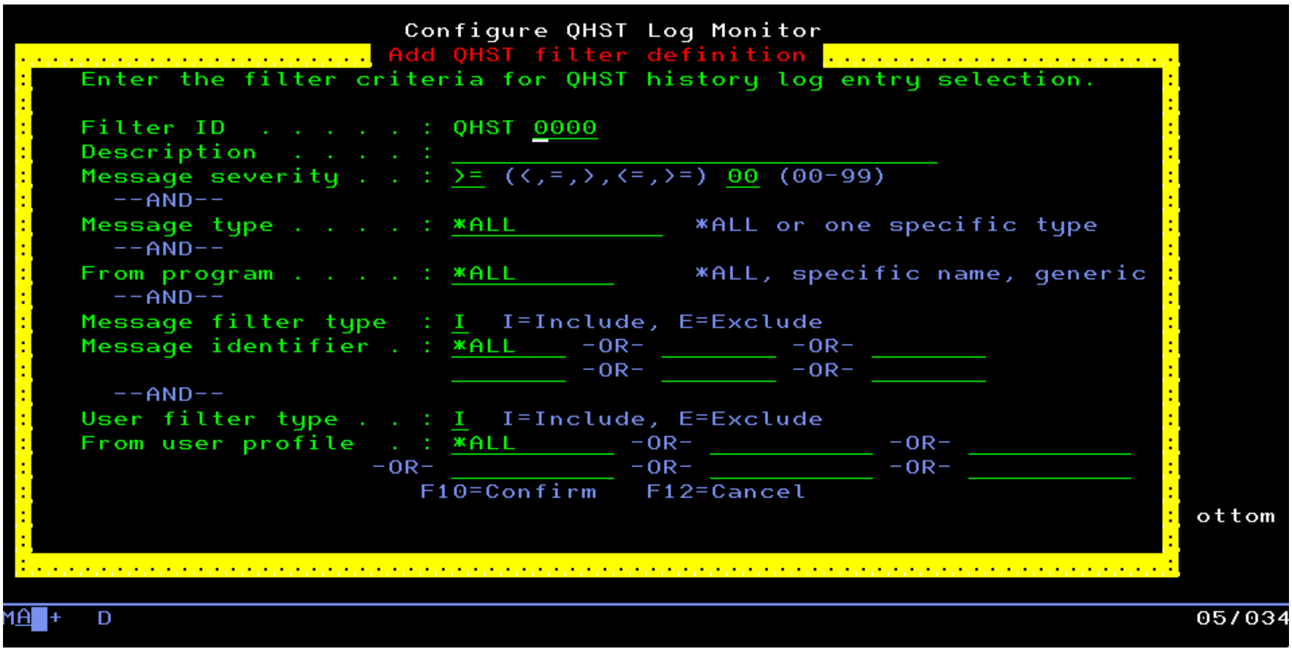
```
                          Configure QHST Log Monitor

   Autostart QHST log monitor  . . :  *YES         *YES, *NO
   EOF Delay after entries are read:  006          5 - 240 seconds

   Type options, press Enter.
      2=Change   4=Delete   5=Display   6=Enable   7=Disable
   Opt  Filter ID Filter description                 Monitoring enabled
    _   QHST0001  Job start/end messages               *NO
    _   QHST0002  Critical storage condition           *NO
    _   QHST0003  QSECOFR messages > 50                *NO
    _   QHST0100  Configuration options                *YES
    _   QHST0101  Backup messages                      *YES
    _   QHST0102  Payroll application                  *YES
    _   QHST9999  Syslog Reporting Manager             *YES




                                                                      Bottom

  F1=Help    F3=Save/Exit    F6=Add filter    F12=Cancel    F17=Sync Times

MA  +   D                                                              09/006
```

Information: Direct access via command: CFGSLHST

3. Specify the autostart and EOF delay parameter. See the online help for detailed information about each parameter.
4. Define one or more history log selection filter rules. A filter rule specifies one or more criteria for selecting history log entries to be reported by the event monitor to the remote syslog server. Only filter rules that are enabled are processed.

   To define a new filter selection rule, press F6.

   IMPORTANT: If you want to report all history log events to a syslog server, do not define or enable any filter selection rule. As soon as at least one filter rule is enabled for monitoring, only events that match the filter criteria will be reported.



```
                     Configure QHST Log Monitor
                     Add QHST filter definition
  Enter the filter criteria for QHST history log entry selection.

  Filter ID . . . . . . : QHST 0000
  Description . . . . . : ______________________________
  Message severity . . : >= (<,=,>,<=,>=) 00 (00-99)
    --AND--
  Message type . . . . : *ALL__________  *ALL or one specific type
    --AND--
  From program . . . . : *ALL______      *ALL, specific name, generic
    --AND--
  Message filter type  : I  I=Include, E=Exclude
  Message identifier . : *ALL____  -OR- _______  -OR- _______
                         _______   -OR- _______  -OR- _______
    --AND--
  User filter type . . : I  I=Include, E=Exclude
  From user profile  . : *ALL______  -OR- __________  -OR- __________
                   -OR- __________  -OR- __________  -OR- __________
                   F10=Confirm   F12=Cancel
                                                                    ottom

MA  +   D                                                          05/034
```

Filter ID: A filter ID is the unique identifier for a history selection filter. You must specify a unique number. Note that the prefix cannot be changed.

Description: Provide a meaningful name for the filter so that you can easily determine its purpose on the overview list.

Message Severity: Use the comparator values and severity numeric values if you want to filter for messages that have a certain severity. If you do not want to limit by severity, leave the default of >= 00.

Message type: You can specify one of message types, such as COMPLETION or DIAGNOSTIC. If you do not want to filter by message type, leave the default of *ALL.

From Program: You can also specify the program from which the history log entry originated from. The name can be *ALL (default for no program filter), a specific program name, or a generic one, such as QCMD*.

>Message filter type: The message filter type determines if history log events for the message identifier listed in the *Message identifier* list will be reported or ignored. It basically specifies whether events for the listed message identifier are included in the reporting or excluded from reporting. <

Message Identifier: You can specify up to 6 message IDs. The filter will meet the selection criteria if one of the messages matches the history log entry. A value of *ALL will not limit the history events by message ID. You can enter complete 7-character message IDs or select message IDs generically, i.e. CPI* for the messages that start with CPI. The wildcard character * can be anywhere in the message ID.

User filter type: The user filter type determines if history log events for the user profiles listed in the *From user profile* list will be reported or ignored. It specifies whether events for the listed user profiles are included in the reporting or excluded from reporting.

From
User Profile: Enter up to 6 user profile names. You can specify an exact name or enter a generic user profile name.

Examples are:

PAYR* = All user profiles that start with PAYR match

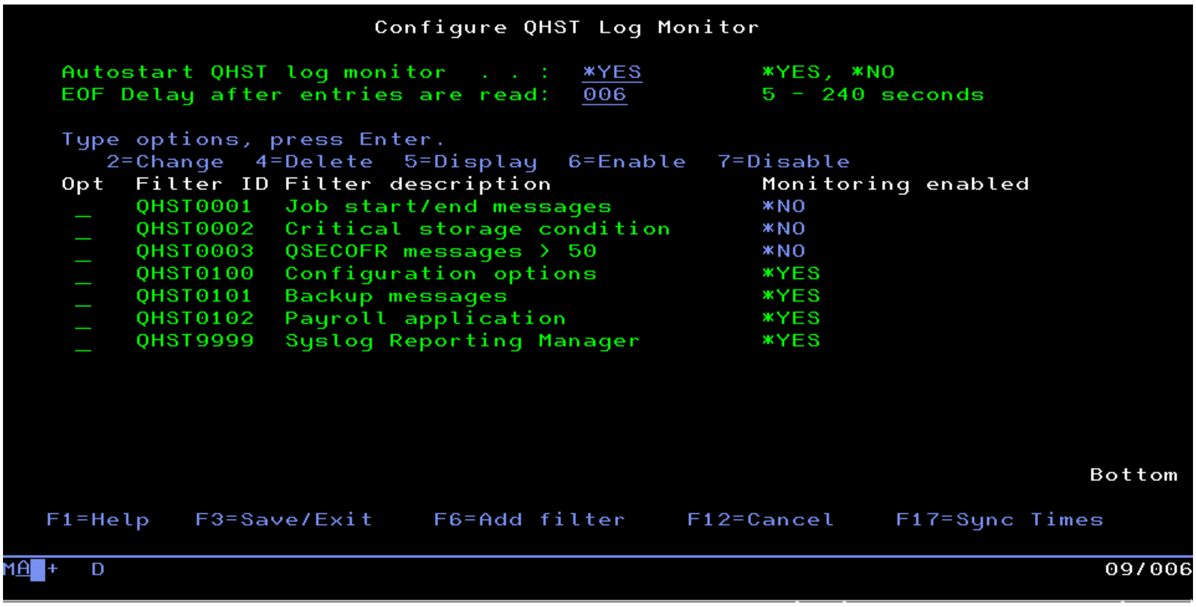
SRV = All user profiles with a name that has somewhere the string SRV match, i.e. ORDSRV1 or SRVBATCH1

*ALL does not limit the events by user profile name.

NOTE: A filter matches a history log event if ALL of the specified criteria for an enabled selection rule matches. Example: Severity > 30 AND User profile = (abc OR def)
It is important to carefully plan the criteria selection to avoid unexpected results. For example, if you exclude message ID CPF9898 in one enabled rule, but include all CPF9* messages in another filter rule, message CPF9898 would still be reported due to the second rule criteria.

5. Press F10 to save your new filter selection rule.
6. Repeat the previous steps to add all your required filter rules.
7. Enable all events that you want to be reported by the history event monitor.

   Option 6 enables a filter and option 7 disables a filter.



```
                         Configure QHST Log Monitor

    Autostart QHST log monitor  . . :  *YES        *YES, *NO
    EOF Delay after entries are read:  006         5 - 240 seconds

    Type options, press Enter.
       2=Change   4=Delete   5=Display   6=Enable   7=Disable
    Opt   Filter ID Filter description             Monitoring enabled
     _    QHST0001  Job start/end messages         *NO
     _    QHST0002  Critical storage condition     *NO
     _    QHST0003  QSECOFR messages > 50          *NO
     _    QHST0100  Configuration options          *YES
     _    QHST0101  Backup messages                *YES
     _    QHST0102  Payroll application            *YES
     _    QHST9999  Syslog Reporting Manager       *YES




                                                                      Bottom

   F1=Help   F3=Save/Exit    F6=Add filter    F12=Cancel    F17=Sync Times

MA +   D                                                                09/006
```

8. You can also use option 2 to change existing filter rules or option 4 to delete a rule entirely.

9. Expert mode option F17 is only available when the calling user has at least the *AUDIT special authority in its user profile (not inherited from a group membership) and is member of the QZRDSRMGRP group. It is considered an expert mode configuration option and allows you to change synchronization restart properties, such as the timestamp of the last processed event entry. This option should only be used by experts who know what impact the change can have.

4.12 Sending database change events via Journal Extract Tool integration

IMPORTANT INFORMATION

The database change event reporting leverages another IBM Technology Expert Labs asset (tool) called Journal Extract Tool (JET). This tool is not part of the Syslog Reporting Manager (SRM) and needs to be purchased separately. Once this tool is installed and operable, it can be integrated into SRM. Without JET installed, SRM cannot generate database change events.

4.12.1 Preparation

- Install the Journal Extract Tool
- Perform any basic configuration that the Journal Extract Tool requires. Refer to the tool's users guide for more information.

4.12.2 Usage information

SRM is only processing information that has been extracted by the JET tool. SRM provides a scheduling function to schedule the PRCJRNENT or PRCFILJRN and GENSUMMARY commands. If JET is not providing data, SRM cannot generate an event. That means, if you are missing database change events, you need to properly set up JET first, test JET and check the JSUMMARY table and individual change data tables for the expected data. If the data that you expect is not in the JET output, SRM cannot process anything. Therefore, your debugging should always start at the JET level. Use the documentation of JET to set up and use JET.

4.12.3 Integration overview

The Journal Extract Tool uses journal objects to extract database table changes from tables that are journaled. Within the tool, you define the following:

- Journal objects that should be processed
- Table names of database tables whose changes should be reported
- User name tables for user profiles whose changes should be reported for the defined tables

The Syslog Reporting Manager provides user interfaces that list all defined journals, tables, and users of the Journal Extract Tool. The user interfaces let you add, remove, and partly change entries of the Journal Extract Tool configuration. A menu provides access to all Journal Extract Tool commands.

As an extension to the standard Journal Extract Tool, the Syslog Reporting Manager provides the following customization options:

- Specify for each table name in the Journal Extract Tool AUDITOBJ table, whether you want to generate syslog events at all, generate only summary events, or generate detailed events that also contain the column data of a changed table row.
- Specify for each journal in the Journal Extract Tool PROCTRACK table, whether you want the Syslog Reporting Manager process the journal for event generation.
- Specify for each journal whether you want to filter database change events by users and table names (this option uses the JET command PRCJRNENT) or by table names only (this option uses the JET command PRCFILJRN). When filtering for table names only, JET is extracting all database changes for tables that are defined in the objects table of JET no matter which user triggered the database change.

In general, with the configuration options of the Syslog Reporting Manager you can further define whether you want to drop/clear the Journal Extract Tool tables at each journal processing job run and the interval in minutes at which the journal processing job runs.

The journal processing job performs the following tasks:

- Executes the PRCJRNENT command (table and user filtering) or PRCFILJRN (table filtering only) for every journal in the PROCTRACK table that is enabled in the Syslog Reporting Manager.
- After all PRCJRNENT / PRCFILJRN commands have been completed, the GENSUMMARY command is executed to generate the change summary table.
- The summary table entries are now processed in the order of table names within the summary collection. Depending on the configured information level, syslog events will be generated:
  - As a summary entry from the data in the summary file
  - As a detailed entry from the data in the summary file and the corresponding data in the individual data tables that were created by the PRCJRNENT / PRCFILJRN command. The content of the event depends on the database action:
    - INSERT or DELETE – All columns of a deleted or inserted row
    - UPDATE – Depending on whether before and after images are captured by the journals, the event might only include the before or after image of a row or both.
- All events are sent in either LEEF or CEF format to the configured remote syslog or SIEM server.
- At the end of the journal processing job a summary event is sent to QSYSOPR, QHST (message SLS0050), and a syslog event with CEF/LEEF header info SRMDB2STAT1 containing statistics about the processed events. An example of such an event is:

  ```
  <14>1 2019-12-04T20:32:43.420000+01:00
  i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM IBMSRM 102F5F -
  CEF:0|IBM|IBM i|7.4|IBMSRM|SRMDB2STAT1|5|
  shost=i5osp4.ai.stgt.spc.ihost.com cat=SRM DB monitoring
  msg=Syslog Reporting Manager DB monitoring journal processing
  finished start=2019-12-04-20.31.58.156000 end=2019-12-04-
  20.32.43.353000 cs1Label=numberSummaryEvents cs1=8
  cs2Label=numberDetailEvents cs2=28
  sproc=384161/QZRDSRMOWN/SLDB2MON
  ```

__**Example of summary events in CEF format using the RFC5424 syslog RFC format:**__

__**Entry 1 (INSERT)**__

```
<181>1 2019-11-29T16:48:33.962144+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=INSERT rt=2019-11-29-16.48.33.962144
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs3Label=memberName cs3=SLTHSTENT
```

__**Entry 2 (DELETE)**__

```
<181>1 2019-11-29T16:48:42.567456+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=DELETE rt=2019-11-29-16.48.42.567456
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs3Label=memberName cs3=SLTHSTENT
```

__**Entry 3 (UPDATE)**__

```
<181>1 2019-11-29T16:51:40.752096+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM DB2MON 102F5F - CEF:0|IBM|
```

```
IBM i|7.4|DB2MON|DB2 change monitoring (Journal Extract Tool)|3|
act=UPDATE rt=2019-11-29-16.51.40.752096
sproc=379504/BARLEN/QPADEV0002 shost=I5OSP4 suser=BARLEN
fname=QZRDSECSRM/SLTHSTENT cs1Label=pgmName cs1=CFGSLHSTP
cs2Label=updatedColumnNames cs2=EVTTEXT,EVTPGM,EVTMSGID1
```

Example of detail events in LEEF format using the RFC3164 syslog RFC format:

Entry 1 (INSERT)

```
<181>Nov 29 16:48:33 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=INSERT devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.48.33.962144 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT memberName=SLTHSTENT rowData=EVTID\
="QHST4440" EVTTEXT\="Test filter Thomas Barlen" SEV\="0"
EVTUSER1\="*ALL" EVTUSER2\="" EVTUSER3\="" EVTUSER4\="" EVTUSER5\
="" EVTUSER6\="" EVTPGM\="*ALL" EVTMSGID1\="*ALL" EVTMSGID2\=""
EVTMSGID3\="" EVTMSGID4\="" EVTMSGID5\="" EVTMSGID6\=""
EVTMSGTYPE\="*ALL" SEVCOMP\=">\=" SEL\="*YES"
QJ_JOURNAL_ENTRY_TYPE\="PX" QJ_COUNT_OR_RRN\="6"
QJ_SEQUENCE_NUMBER\="1050" QJ_RECEIVER_NAME\="DETRCV0001"
```

Entry 2 (DELETE)

```
<181>Nov 29 16:48:42 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=DELETE devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.48.42.567456 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT memberName=SLTHSTENT rowData=EVTID\
="QHST4440" EVTTEXT\="Test filter Thomas Barlen" SEV\="0"
EVTUSER1\="*ALL" EVTUSER2\="" EVTUSER3\="" EVTUSER4\="" EVTUSER5\
="" EVTUSER6\="" EVTPGM\="*ALL" EVTMSGID1\="*ALL" EVTMSGID2\=""
EVTMSGID3\="" EVTMSGID4\="" EVTMSGID5\="" EVTMSGID6\=""
EVTMSGTYPE\="*ALL" SEVCOMP\=">\=" SEL\="*YES"
QJ_JOURNAL_ENTRY_TYPE\="DL" QJ_COUNT_OR_RRN\="6"
QJ_SEQUENCE_NUMBER\="1053" QJ_RECEIVER_NAME\="DETRCV0001"
```

Entry 3 (UPDATE with before and after image)

```
<181>Nov 29 16:51:40 i5osp4 102F5F: LEEF:2.0|IBM|IBM i|7.4|DB2MON|
x09|act=UPDATE devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS
devTime=2019-11-29-16.51.40.752096 sproc=379504/BARLEN/QPADEV0002
resource=I5OSP4 usrName=BARLEN pgmName=CFGSLHSTP
fname=QZRDSECSRM/SLTHSTENT
updatedColumnNames=EVTTEXT,EVTPGM,EVTMSGID1
rowDataBefore=QJ_JOURNAL_ENTRY_TYPE\="UB" QJ_RECEIVER_NAME\
="DETRCV0001" QJ_SEQUENCE_NUMBER\="1059" EVTTEXT\="This is Thomas
Filter" EVTPGM\="*ALL" EVTMSGID1\="CPF4711"
rowDataAfter=QJ_JOURNAL_ENTRY_TYPE\="UP" QJ_RECEIVER_NAME\
="DETRCV0001" QJ_SEQUENCE_NUMBER\="1060" EVTTEXT\="This is Marion
Filter" EVTPGM\="CHKE1" EVTMSGID1\="CPF3333"
```

4.12.4 Configuring the Journal Extract Tool integration

All configuration options are available from the SLMON menu. The configuration of the Journal Extract Tool integration is done via a sub-menu of the SLMON menu.

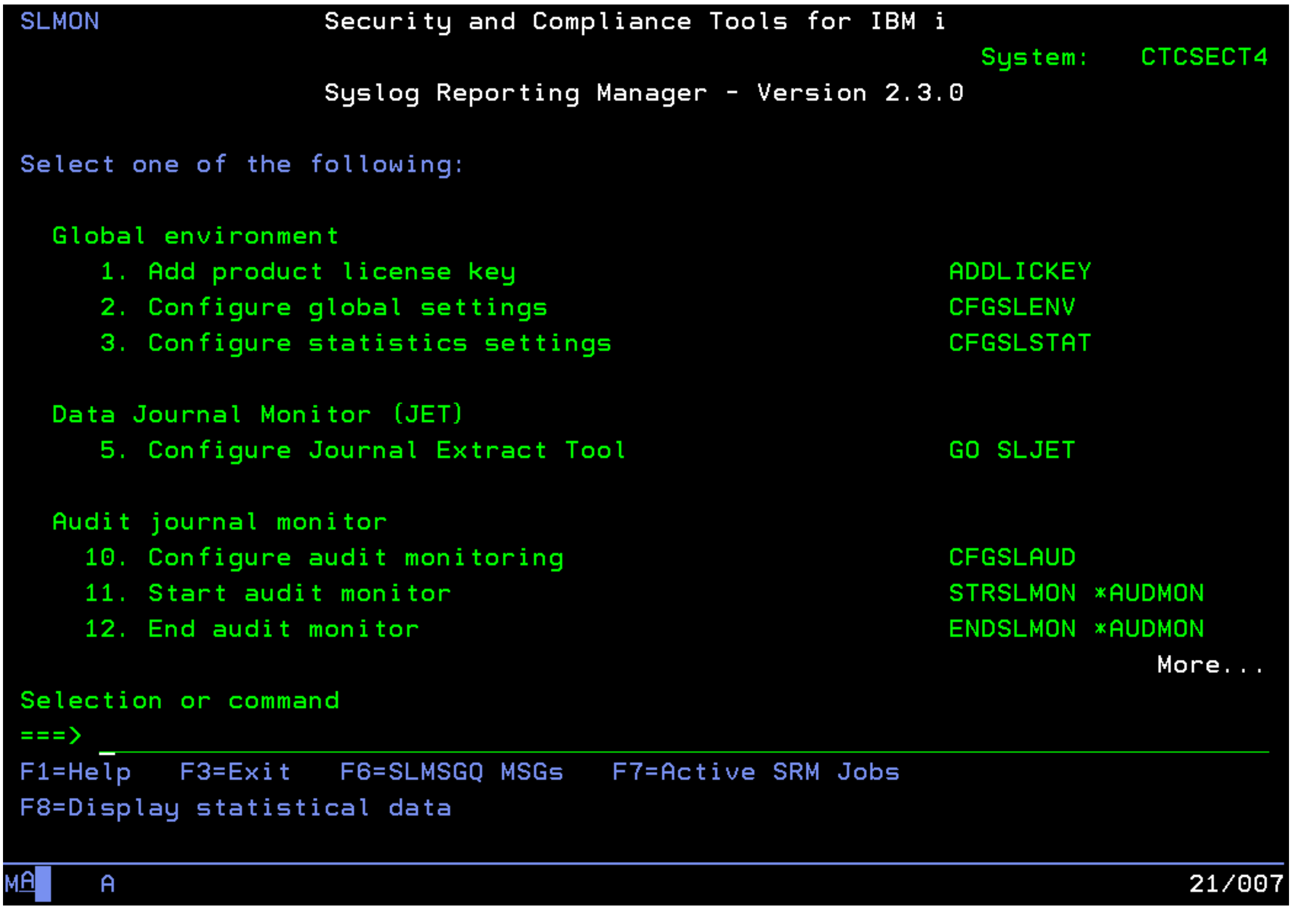
1. Start a 5250 session and sign on with a user that has *ALLOBJ special authority or as a member of the QZRDSRMGRP group.

2. Add the library QZRDSECSRM to the job's library list.

   ```
   ADDLIBLE QZRDSECSRM
   ```

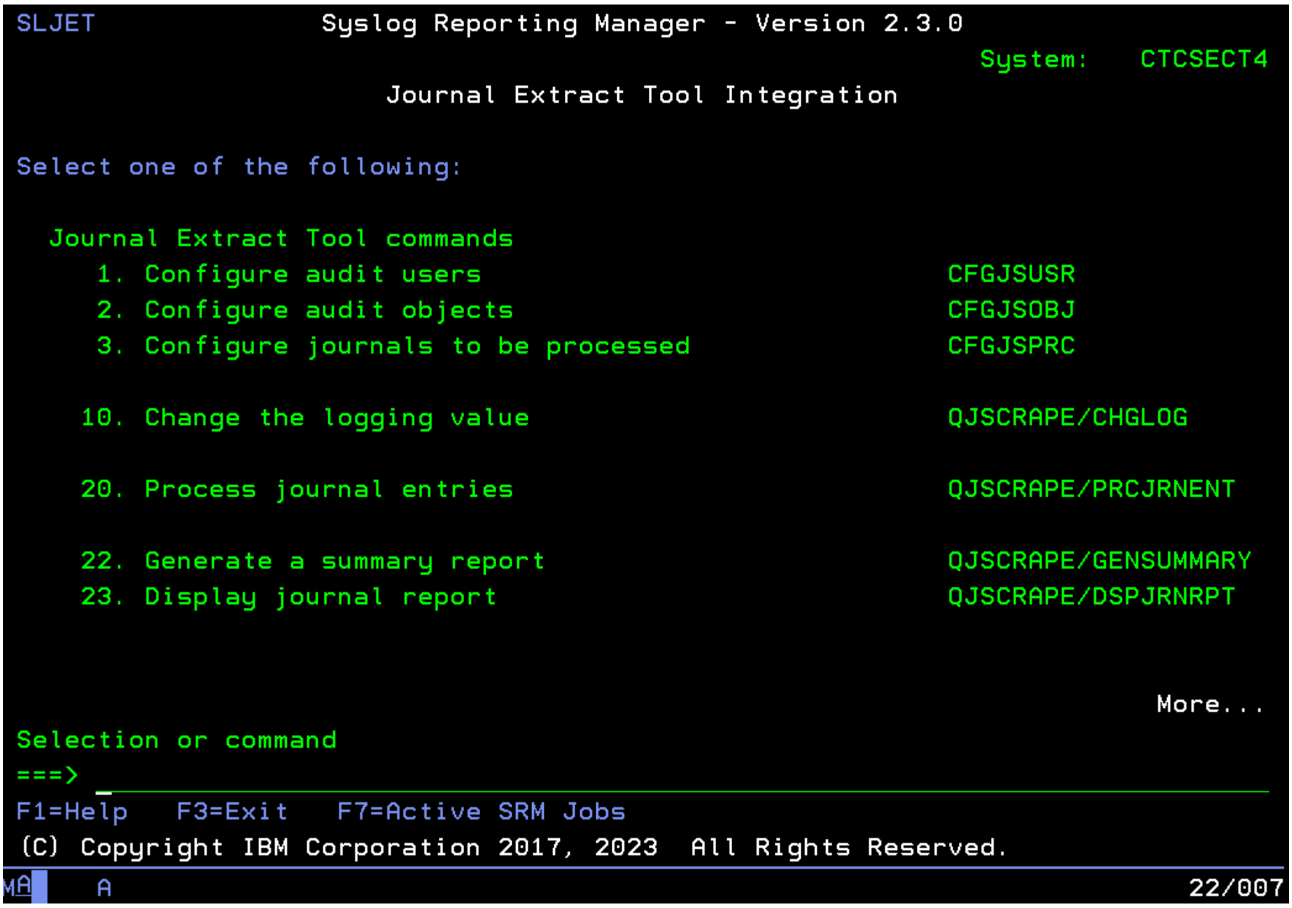
3. It is recommended to permanently assign the library to the administrator's user profile. Enter the following command to display the Syslog Reporting Manager menu.

   ```
   CFGSRM
   ```

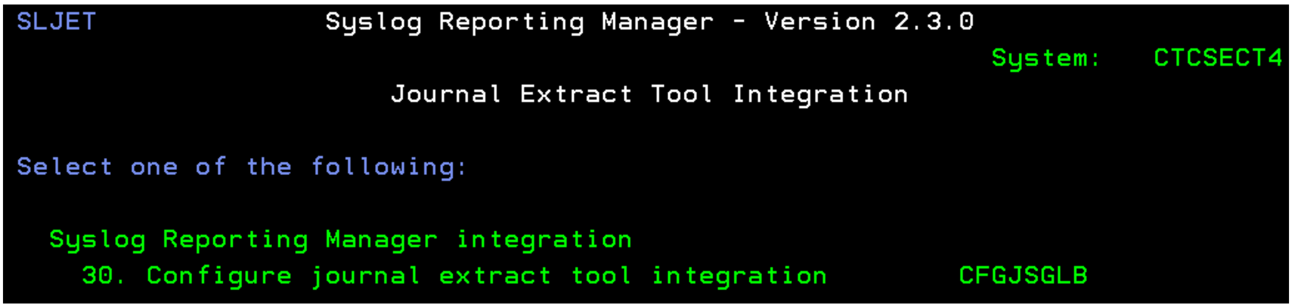


```
SLMON                 Security and Compliance Tools for IBM i
                                                      System:   CTCSECT4
                      Syslog Reporting Manager - Version 2.3.0

Select one of the following:

  Global environment
     1. Add product license key                          ADDLICKEY
     2. Configure global settings                        CFGSLENV
     3. Configure statistics settings                    CFGSLSTAT

  Data Journal Monitor (JET)
     5. Configure Journal Extract Tool                   GO SLJET

  Audit journal monitor
    10. Configure audit monitoring                       CFGSLAUD
    11. Start audit monitor                              STRSLMON *AUDMON
    12. End audit monitor                                ENDSLMON *AUDMON
                                                                  More...
Selection or command
===> _
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
F8=Display statistical data

MA     A                                                            21/007
```

4. Enter option 5 Configure Journal Extract Tool to open the Journal Extract Tool integration menu.
   Note: You need the Journal Extract Tool to be installed on the system to be able to open the menu. Otherwise you will not see the menu option.



```
SLJET                    Syslog Reporting Manager - Version 2.3.0
                                                              System:   CTCSECT4
                              Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                                CFGJSUSR
     2. Configure audit objects                              CFGJSOBJ
     3. Configure journals to be processed                   CFGJSPRC

    10. Change the logging value                             QJSCRAPE/CHGLOG

    20. Process journal entries                              QJSCRAPE/PRCJRNENT

    22. Generate a summary report                            QJSCRAPE/GENSUMMARY
    23. Display journal report                               QJSCRAPE/DSPJRNRPT

                                                                        More...
Selection or command
===> _
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                                 22/007
```



```
SLJET                    Syslog Reporting Manager - Version 2.3.0
                                                              System:   CTCSECT4
                              Journal Extract Tool Integration

Select one of the following:

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration        CFGJSGLB
```

Journal Extract Tool tasks

Before the Syslog Reporting Manager can report database change events, the Journal Extract Tool has to be properly set up. Refer to the documentation of the Journal Extract Tool for detailed information.

The Syslog Reporting Manager integration provides some additional features that are only available via the SLJSCR menu. The features are:

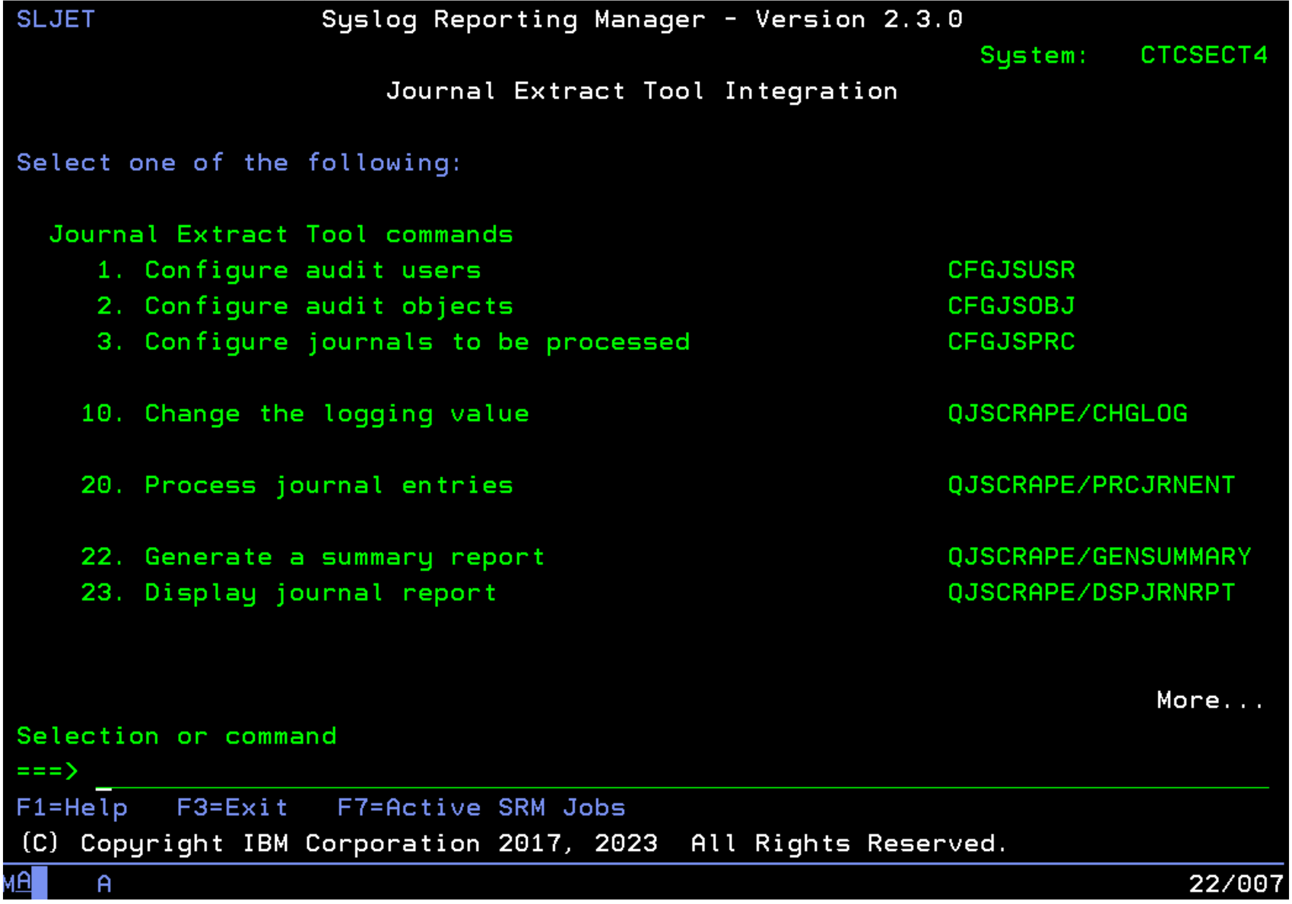
- You can specify the level of detail that should be included
- You can enable individual journals to be processed when the Syslog Reporting Manager reports database change events.

The Journal Extract Tool uses journals to capture database changes. The analysis of the captured data is further filtered by the tables that are registered with the tool and the users who performed the database changes within the registered tables.

Note that the Journal Extract Tool commands are all listed on the Syslog Reporting Manager integration menu, but only the customized configuration is covered in this section of the user's guide. For all details regarding menu options 10, 20, 21, and 22 refer to the documentation of the Journal Extract Tool.

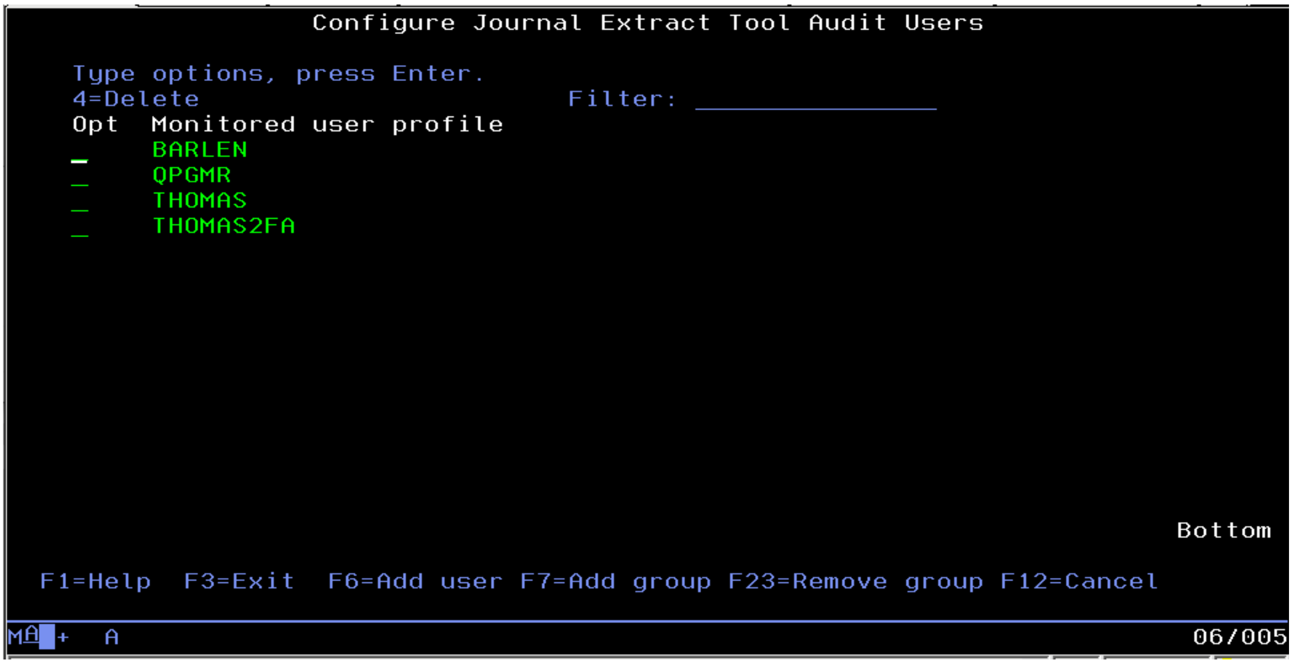
Define users whose database changes are reported

The Journal Extract Tool uses the AUDITUSERS table in the QJSCRAPE library to define all user profile names whose changes are reported for the database tables that are defined in the AUDITOBJ table. The Syslog Reporting Manager lets you view and manage the registered user profiles via the SLJSCR menu. The user profile-based filtering of journal events is only used with the PRCJRNENT command is processed. The filter type in the Syslog Reporting Manager journal definition must be UT (user and table filter).



```
SLJET                Syslog Reporting Manager - Version 2.3.0
                                                          System:   CTCSECT4
                          Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                         CFGJSUSR
     2. Configure audit objects                       CFGJSOBJ
     3. Configure journals to be processed            CFGJSPRC

    10. Change the logging value                      QJSCRAPE/CHGLOG

    20. Process journal entries                       QJSCRAPE/PRCJRNENT

    22. Generate a summary report                     QJSCRAPE/GENSUMMARY
    23. Display journal report                        QJSCRAPE/DSPJRNRPT

                                                                More...
Selection or command
===> _
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                         22/007
```

Take option 1 to view currently registered user profiles and manage them.



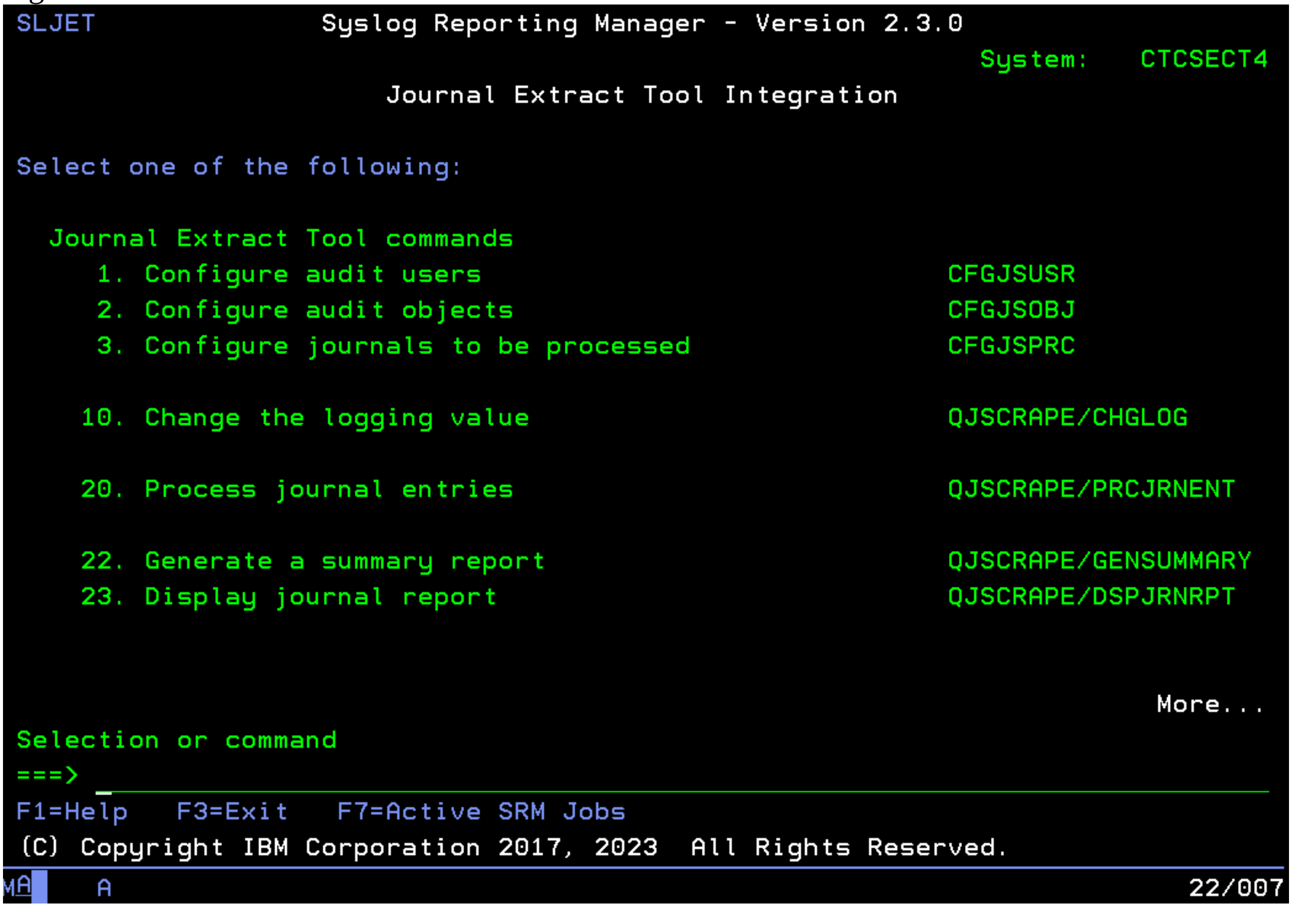
```
                    Configure Journal Extract Tool Audit Users

    Type options, press Enter.
    4=Delete                          Filter: _______________
    Opt  Monitored user profile
    _    BARLEN
    _    QPGMR
    _    THOMAS
    _    THOMAS2FA

                                                                     Bottom
  F1=Help  F3=Exit  F6=Add user F7=Add group F23=Remove group F12=Cancel
MA +   A                                                             06/005
```

You can use the function key F6 to add an individual user profile to the list or use the F7 key to add all users that are member of a specific group to the list. F23 lets you remove all users of a specific group from the list.

Note: If you select F23 to remove users who are member of the specified group, all members are removed even though the user might be a member of another group that you also added with the F7 key.

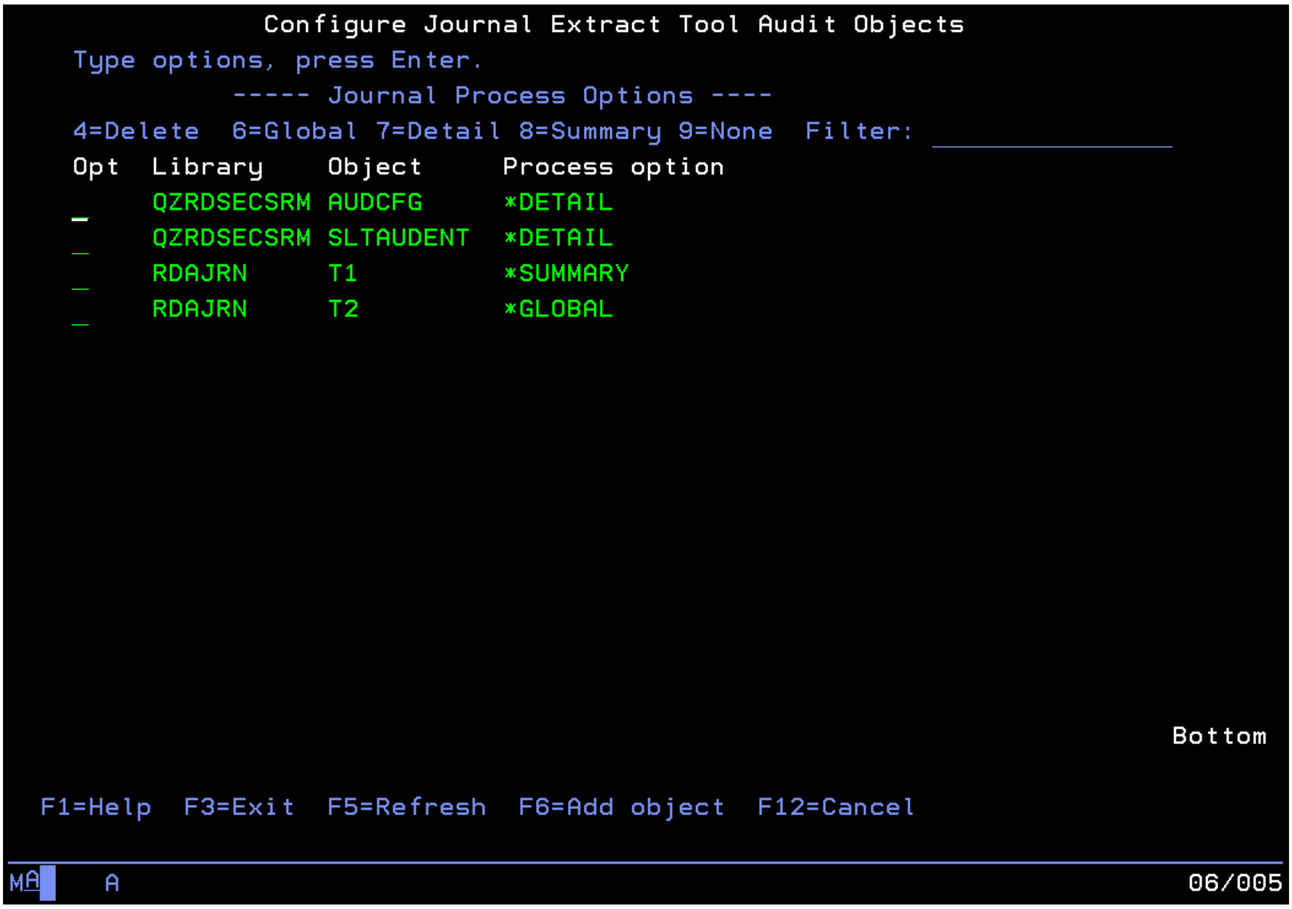
Define database table objects whose changes are reported

The Journal Extract Tool uses the AUDITOBJ table in the QJSCRAPE library to define all database tables whose changes are reported. The Syslog Reporting Manager lets you view and manage the registered tables via the SLJSCR menu.



```
SLJET                  Syslog Reporting Manager - Version 2.3.0
                                                            System:   CTCSECT4
                              Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                                CFGJSUSR
     2. Configure audit objects                              CFGJSOBJ
     3. Configure journals to be processed                   CFGJSPRC

    10. Change the logging value                             QJSCRAPE/CHGLOG

    20. Process journal entries                              QJSCRAPE/PRCJRNENT

    22. Generate a summary report                            QJSCRAPE/GENSUMMARY
    23. Display journal report                               QJSCRAPE/DSPJRNRPT


                                                                        More...
Selection or command
===> _
F1=Help   F3=Exit   F7=Active SRM Jobs
 (C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                                 22/007
```

Take option 2 to view currently registered tables and manage them.



```
                 Configure Journal Extract Tool Audit Objects
    Type options, press Enter.
              ----- Journal Process Options ----
    4=Delete  6=Global 7=Detail 8=Summary 9=None  Filter: _______________
    Opt  Library    Object     Process option
    _    QZRDSECSRM AUDCFG     *DETAIL
    _    QZRDSECSRM SLTAUDENT  *DETAIL
    _    RDAJRN     T1         *SUMMARY
    _    RDAJRN     T2         *GLOBAL

                                                                     Bottom

  F1=Help  F3=Exit  F5=Refresh  F6=Add object  F12=Cancel

MA     A                                                            06/005
```

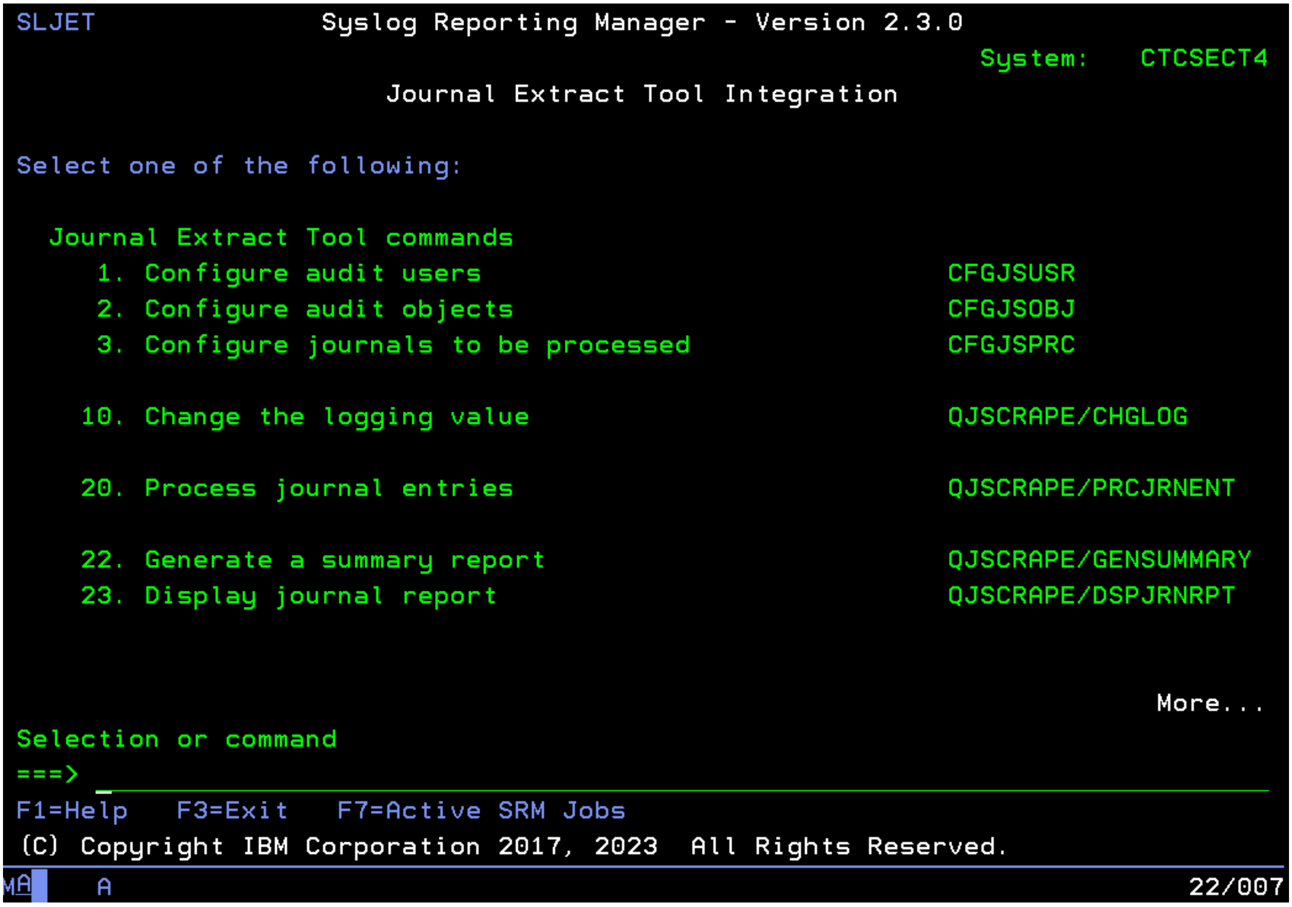
When adding a new table to the AUDITOBJ table, processing option of *GLOBAL is selected. The following process options can be used:

- *GLOBAL
  When this value is set, the syslog information level as defined in the global Syslog Reporting Manager integration configuration is used.
- *SUMMARY
  When this value is set, the event that is generated by the Syslog Reporting Manager consists of data stored in the Journal Extract Tool summary file (QJSCRAPE/JSUMMARY). Details about the actual data values that got changed are not included.
- *DETAIL
  When this value is set, the event that is generated by the Syslog Reporting Manager consists of the data in the summary file and the corresponding data in the individual data tables that were created by the PRCJRNENT command. The content of the event depends on the database action:
  - INSERT or DELETE – All columns of a deleted or inserted row
  - UPDATE – Depending on whether before and after images are captured by the journals, the event might only include the before or after image of a row or both.

Define journals that contains database changes that are reported

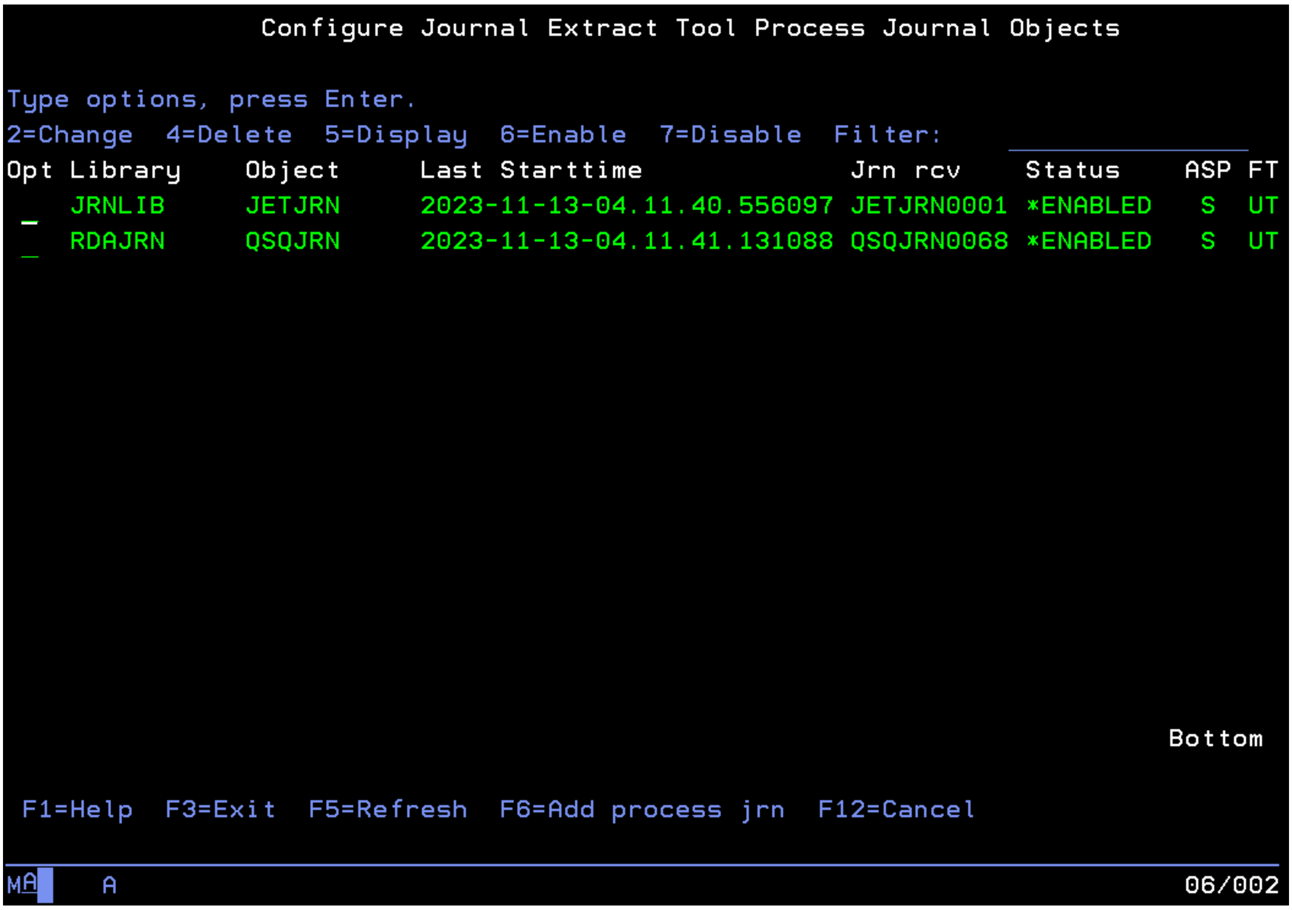
All the analysis and data extraction that is performed by the Journal Extract Tool is based on database changes that are captured in data journals. You have to register existing data journals to the Journal Extract Tool's PROCTRACK table.

The Syslog Reporting Manager lets you view and manage the registered journals via the SLJSCR menu.



```
SLJET                  Syslog Reporting Manager - Version 2.3.0
                                                            System:   CTCSECT4
                            Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                                 CFGJSUSR
     2. Configure audit objects                               CFGJSOBJ
     3. Configure journals to be processed                    CFGJSPRC

    10. Change the logging value                              QJSCRAPE/CHGLOG

    20. Process journal entries                               QJSCRAPE/PRCJRNENT

    22. Generate a summary report                             QJSCRAPE/GENSUMMARY
    23. Display journal report                                QJSCRAPE/DSPJRNRPT


                                                                       More...
Selection or command
===> _________________________________________________________________________
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                               22/007
```

Take option 3 to view currently registered database journals and manage them.



```
                    Configure Journal Extract Tool Process Journal Objects

Type options, press Enter.
2=Change  4=Delete  5=Display  6=Enable  7=Disable  Filter: _______________
Opt Library     Object      Last Starttime             Jrn rcv    Status     ASP FT
 _  JRNLIB      JETJRN      2023-11-13-04.11.40.556097 JETJRN0001 *ENABLED    S  UT
 _  RDAJRN      QSQJRN      2023-11-13-04.11.41.131088 QSQJRN0068 *ENABLED    S  UT









                                                                           Bottom

 F1=Help  F3=Exit  F5=Refresh  F6=Add process jrn  F12=Cancel

MA      A                                                                 06/002
```

The configuration lets you add and remove journals from the PROCTRACK table. In addition, you can select whether the journal extraction analysis will process a journal.

- *ENABLED
  The status *ENABLED indicates that journal processing that is started with the PRCJRNENT command will also process the database changes of the given journal.
- *DISABLED
  When the status of journal is *DISABLED, the journal processing will ignore the journal and database changes in this journal will not be reported.

The ASP column indicates the ASP in which the journal objects resides. The following values can be shown:

- S = *SYSTEM ASP
- G = *GLOBAL is the ASP group name that is specified in the CFGSLENV command.
- O = Other ASP. An ASP name has been specified and you can change the name with option 2 or display its name using option 5.

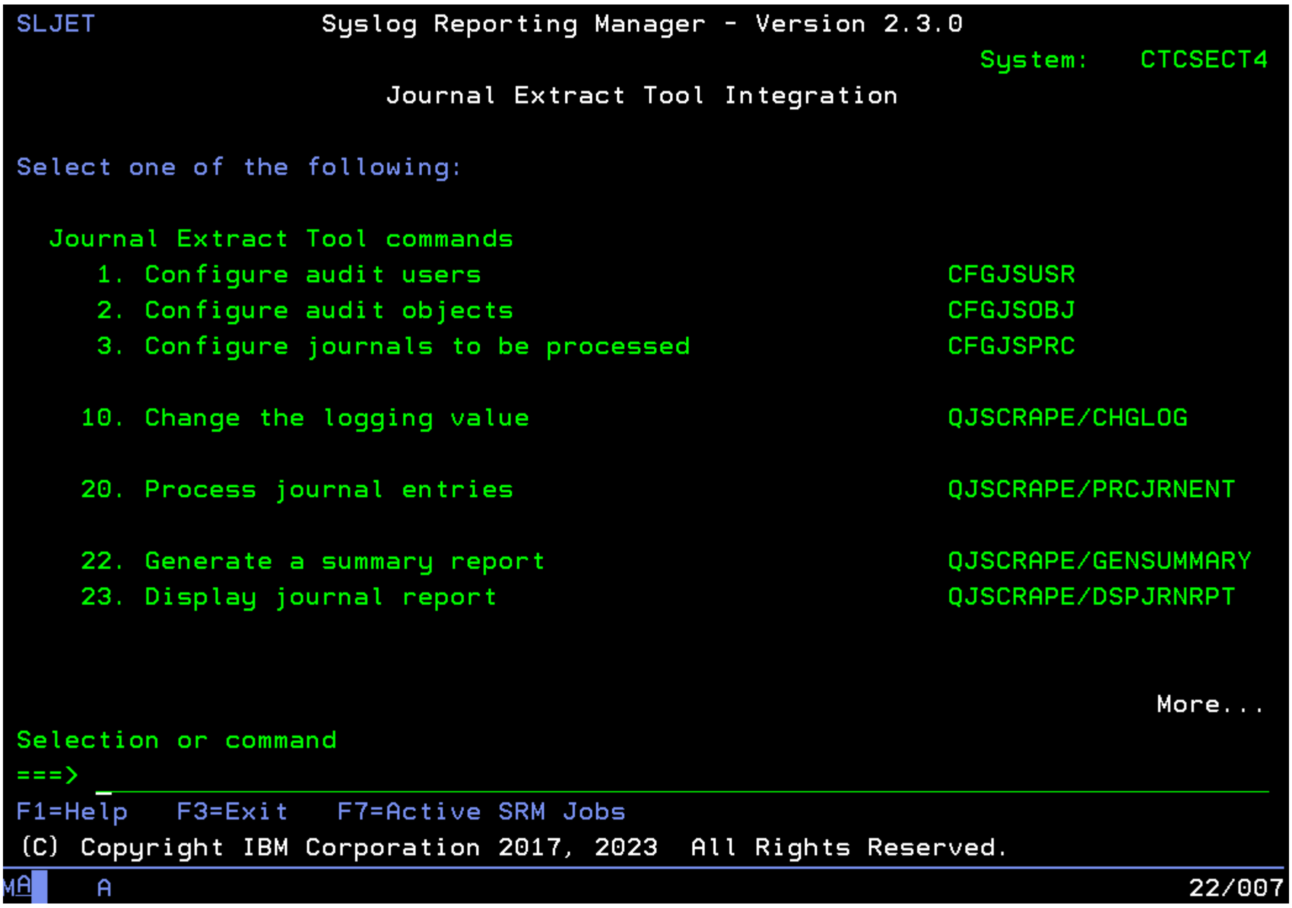
The FT column represents the filter type for processing journals. The following values can be shown:

- UT = Filtering is applied based on user profile entries in the AUDITUSERS table and table names defined in the AUDITOBJ table.
- TO = Filtering is applied based on table names in the AUDITOBJ table only. No user filters are applied.

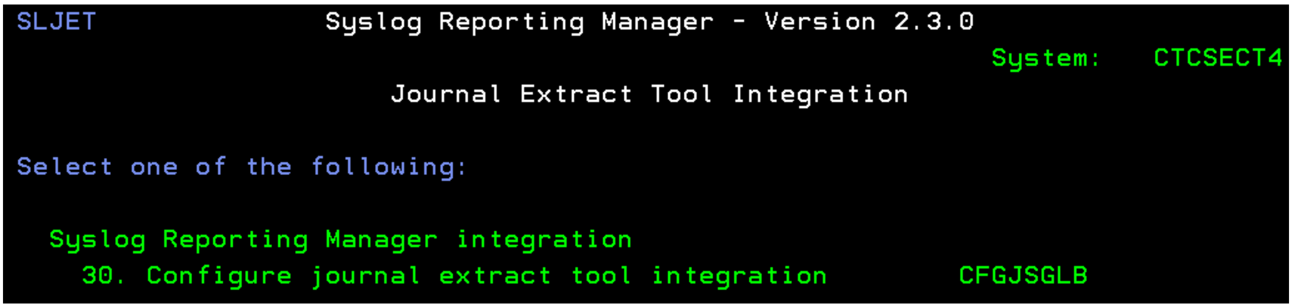
Configure the Syslog Reporting Manager integration

The configuration covered in this section describes the various settings that affect the integration, processing, and reporting of the information provided by the Journal Extract Tool.

The Syslog Reporting Manager lets you view and manage the database change event processing via the SLJSCR menu.

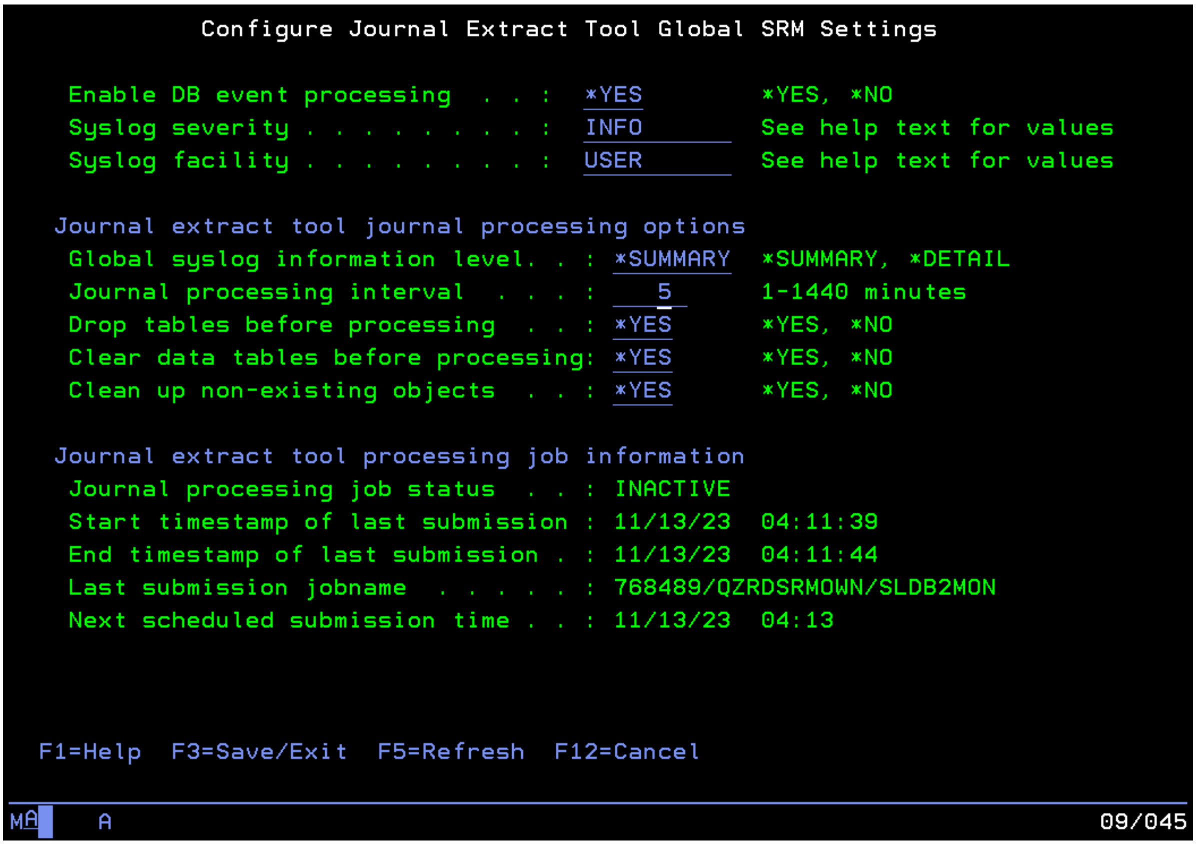


```
SLJET                 Syslog Reporting Manager - Version 2.3.0
                                                            System:   CTCSECT4
                           Journal Extract Tool Integration

Select one of the following:

  Journal Extract Tool commands
     1. Configure audit users                             CFGJSUSR
     2. Configure audit objects                           CFGJSOBJ
     3. Configure journals to be processed                CFGJSPRC

    10. Change the logging value                          QJSCRAPE/CHGLOG

    20. Process journal entries                           QJSCRAPE/PRCJRNENT

    22. Generate a summary report                         QJSCRAPE/GENSUMMARY
    23. Display journal report                            QJSCRAPE/DSPJRNRPT

                                                                     More...
Selection or command
===>
F1=Help   F3=Exit   F7=Active SRM Jobs
(C) Copyright IBM Corporation 2017, 2023  All Rights Reserved.
MA     A                                                              22/007
```



```
SLJET                 Syslog Reporting Manager - Version 2.3.0
                                                            System:   CTCSECT4
                           Journal Extract Tool Integration

Select one of the following:

  Syslog Reporting Manager integration
    30. Configure journal extract tool integration        CFGJSGLB
```

Take option 30 to configure the integration options.



```
             Configure Journal Extract Tool Global SRM Settings

    Enable DB event processing  . . :  *YES         *YES, *NO
    Syslog severity . . . . . . . . :  INFO         See help text for values
    Syslog facility . . . . . . . . :  USER         See help text for values

   Journal extract tool journal processing options
    Global syslog information level. . : *SUMMARY  *SUMMARY, *DETAIL
    Journal processing interval  . . . :     5      1-1440 minutes
    Drop tables before processing  . . : *YES       *YES, *NO
    Clear data tables before processing: *YES       *YES, *NO
    Clean up non-existing objects  . . : *YES       *YES, *NO

   Journal extract tool processing job information
    Journal processing job status  . . : INACTIVE
    Start timestamp of last submission : 11/13/23  04:11:39
    End timestamp of last submission . : 11/13/23  04:11:44
    Last submission jobname  . . . . . : 768489/QZRDSRMOWN/SLDB2MON
    Next scheduled submission time . . : 11/13/23  04:13



  F1=Help  F3=Save/Exit  F5=Refresh  F12=Cancel

MA     A                                                                09/045
```

The configuration options are as follows:

- Enable DB event processing
  The parameter specifies whether the database monitor and reporting job will process events generated by the Journal Extract Tool at the interval specified at the Journal processing interval parameter. The events will be processed and send by the Syslog Reporting Manager.
  - ***YES**
    The database change monitor job will be started when the IBM i Syslog Reporting Manager tool starts and runs at the specified interval as defined in the Journal processing interval parameter.
  - ***NO**
    The database change monitor job will not start when the the IBM i Syslog Reporting Manager tool starts. The job needs to be started manually.
- Syslog severity
  The parameter specifies the Syslog severity that will be used by the monitor job to report events via the syslog protocol to the Syslog server. See the online help for detailed information about each parameter.
- Syslog facility
  The parameter specifies the Syslog facility name that will be used by the monitor job to report events via the syslog protocol to the Syslog server. See the online help for detailed information about each parameter.
- Global syslog information level
  You can also select a processing option for journal processing and the level of details that you want to send to the Security Information and Event Management (SIEM) system or remote syslog server. This is the global settings for the level of detail. If a file that is defined in the AUDITOBJ table via the Syslog Reporting Manager interface, you can override the detail level on a per file basis. Only files that are defined with a information level of *GLOBAL will use the settings in this parameter. The following options can be selected:

  - ***DETAIL**
    When this option is selected, the information from the Journal Extract Tool summary report and the detailed information for the specified file is sent to the SIEM server. This includes the before and after information of the changed data, assuming that both images are captured in the journal.
  - ***SUMMARY**
    With this option selected, only the information in the Journal Extract Tool summary report are processed for the selected file.
- Journal processing interval
  The Syslog Reporting Manager (SRM) runs a journal processing job that analyzes each enabled journal of the Journal Extract Tool. The interval determines how often this job runs. Depending on the number of journals to be processed and the files that are journaled, the processing time of the job varies. SRM runs only one instance of the journal processing job at a time. If you monitor a large number of files and the journal processing takes longer than the interval specified, you may not get the job processed as often as you want. Therefore, you should start with a higher interval and then take a look at the processing job information section. You will see when the job started and ended. This gives you an indication on how to set the interval. Important to know is that the specified number of minutes are used to calculate the next processing time after the previous processing job ended.
  - number of minutes
    The interval is specified in minutes. The minimum value is 1 minute and the maximum value 1440 minutes (1 day).
- Drop tables before processing
  The Syslog Reporting Mananger uses the Journal Extract Tool command PRCJRNENT command to analyze the data journals and to create the tables with the changes. The DROPTBL parameter of the PRCJRNENT command determines if all data tables that are created by the PRCJRNENT command are removed from the QJSCRAPE library. If *YES is specified, then ALL existing QJSCRxxxxx tables are removed, not just those tables associated with the journal name specified. The following options can be selected:
  - ***NO**
    No QJSCRxxxxx tables in library QJSCRAPE will be removed when running the PRCJRNENT command.
  - ***YES**
    The Journal Extract Tool removes ALL existing QJSCRxxxxx tables, not just those tables associated with the journal name specified. *YES causes all QJSCRxxxxx tables to be deleted for each journal that is enabled for processing.
- Clear data tables before processing
  The Syslog Reporting Mananger uses the Journal Extract Tool command PRCJRNENT command to analyze the data journals and to create the tables with the changes. The CLRDATA parameter of the PRCJRNENT command determines if all data tables that are created by the PRCJRNENT command are cleared in the QJSCRAPE library. If *YES is specified, then ALL existing QJSCRxxxxx tables are cleared, not just those tables associated with the journal name specified. The following options can be selected:
  - ***NO**
    No QJSCRxxxxx tables in library QJSCRAPE will be cleared when running the PRCJRNENT command.
  - ***YES**
    The Journal Extract Tool clears ALL existing QJSCRxxxxx tables, not just those tables associated with the journal name specified.
    IMPORTANT: Set this parameter only to *YES for a single run of the database change

analysis process. *YES causes all QJSCRxxxxx tables to be cleared for each journal that is enabled for processing.

- Clean up non-existing objects
  The default behavior of the Journal Extract Tool is that you can add objects to the AUDITOBJ table that do not have to exist on the system. However, if you run the PRCJRNENT or >PRCFILJRN< command or run the equivalent journal processing job within the Syslog Reporting Manager, objects that are defined in the AUDITOBJ file but do not exist on the system, can cause problems. Therefore, the Syslog Reporting Manager contains a function that can be enabled via this parameter to check that every object in the AUDITOBJ and PROCTRACK tables actually exist on the system. If automatic cleanup is enabled, entries in those two tables will be removed if the specified object does not exist on the IBM i partition.
  This includes objects that reside in ASP that is not varied on or otherwise not available on the system. Note that the automatic cleanup process could have an impact on the performance of the journal processing job. This heavily depends on the number of rows in the AUDITOBJ and PROCTRACK tables. The following options can be selected:
  - ***YES**
    When this option is selected, the journal processing job will check that all objects within the AUDITOBJ and PROCTRACK files exist on the system. If not, the corresponding entries are removed from the AUDITOBJ and PROCTRACK files. The check also verifies the existence on configured ASPs.
  - ***NO**
    With this option selected, the journal processing job will not check that all objects within the AUDITOBJ and PROCTRACK files exist on the system. Objects that might not exist could cause problems when running the journal processing job.
- Database monitoring event processing job information
  The information section gives you details about the journal processing job.
  - Job status - The status gives you an indication whether the journal processing is active. The status INACTIVE indicates that the job is neither running nor currently in a job queue. The status SUBMITTED indicates that the SRM control job has submitted the journal processing job, but it has not started yet. ACTIVE indicates that the job is currently running in the SLSBS subsystem.
  - Start timestamp - Is the date and time when the journal processing job started the last time.
  - End timestamp - Is the date and time when the journal processing job finished the last time.
  - Jobname - This is the fully qualied jobname of the most recent journal processing job.
  - Next scheduled submission time - Is calculated by adding the processing interval to the last end timestamp.

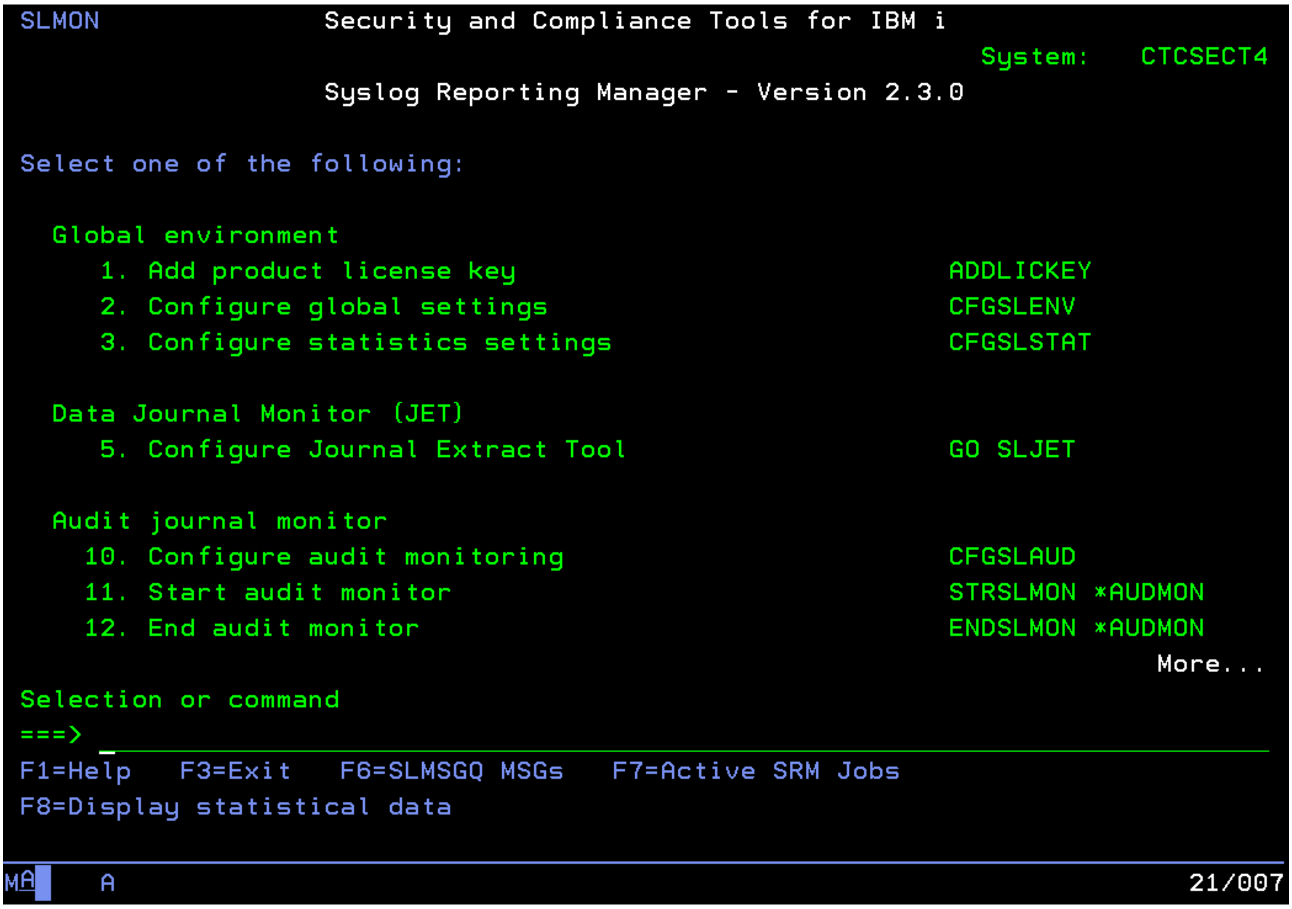
4.13 Sending message queue events

The Syslog Reporting Manager can also monitor message queues within IBM i. Messages that appear in a monitored message queue are reported at a predefined interval.

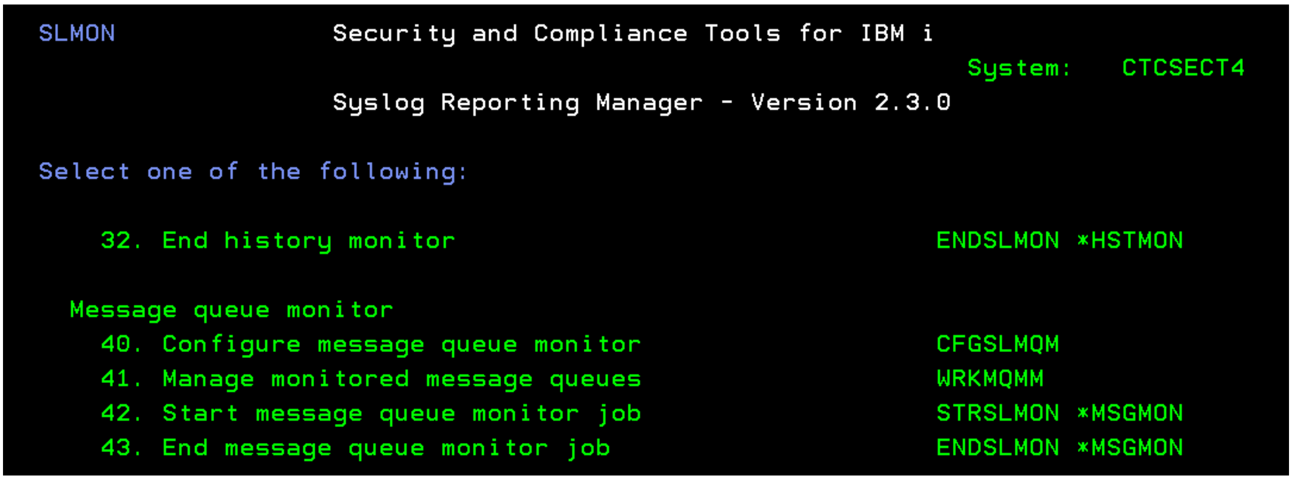
Following is an example of a raw syslog message in syslog RFC5424 format and SIEM format *LEEF:

```
<11>1 2020-01-13T12:58:01.422426+01:00
i5osp4.ai.stgt.spc.ihost.com IBMiPSCSRM MSGMON 102F5F - LEEF:2.0|
IBM|IBM i|7.4|MSGMON-CPF9898|x09|cat=MSG Queue Messages
devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS devTime=2020-01-13-
12.58.01.422426 reason=CPF9898 msgSev=ERROR
msgQueue=QUSRSYS/BARLEN pgmName=CVTDBTOM msg=Database conversion
job ended in an error.
```

The Syslog Reporting Manager configuration menu provides options 40 – 43 that let you define and control the message queue monitoring and reporting.



```
SLMON                   Security and Compliance Tools for IBM i
                                                          System:   CTCSECT4
                        Syslog Reporting Manager - Version 2.3.0

Select one of the following:

  Global environment
     1. Add product license key                         ADDLICKEY
     2. Configure global settings                       CFGSLENV
     3. Configure statistics settings                   CFGSLSTAT

  Data Journal Monitor (JET)
     5. Configure Journal Extract Tool                  GO SLJET

  Audit journal monitor
    10. Configure audit monitoring                      CFGSLAUD
    11. Start audit monitor                             STRSLMON *AUDMON
    12. End audit monitor                               ENDSLMON *AUDMON
                                                                  More...
Selection or command
===>
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
F8=Display statistical data

MA     A                                                           21/007
```



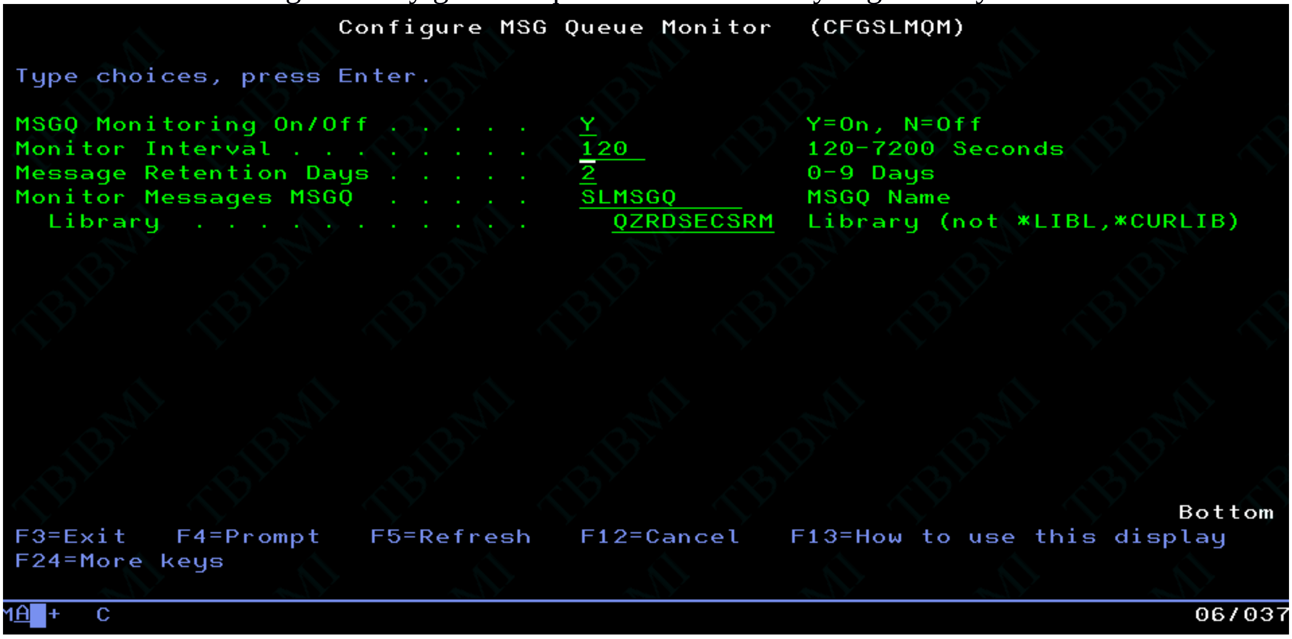
```
 SLMON                Security and Compliance Tools for IBM i
                                                            System:    CTCSECT4
                      Syslog Reporting Manager - Version 2.3.0

 Select one of the following:

     32. End history monitor                               ENDSLMON *HSTMON

   Message queue monitor
     40. Configure message queue monitor                   CFGSLMQM
     41. Manage monitored message queues                   WRKMQMM
     42. Start message queue monitor job                   STRSLMON *MSGMON
     43. End message queue monitor job                     ENDSLMON *MSGMON
```

4.13.1 Configure the global message queue monitoring settings

The Configure MSG Queue Monitor command sets the global parameter for the message queue monitor. You can monitor different message queues and if a message meets the monitoring criteria (severity, message queue name, enabled status), an event is generated and send to the configured syslog server.

The syslog facility and severity of message events are as follows:

- Facility is always USER
- Severity depends on the IBM i message severity itself.
  - Message severity 00 is sent with syslog severity INFO
  - Message severity 10 is sent with syslog severity NOTICE
  - Message severity 20 is sent with syslog severity WARNING
  - Message severity greater equal 30 is sent with syslog severity ERROR



```
                     Configure MSG Queue Monitor  (CFGSLMQM)

 Type choices, press Enter.

 MSGQ Monitoring On/Off . . . . . .   Y            Y=On, N=Off
 Monitor Interval . . . . . . . . .   120          120-7200 Seconds
 Message Retention Days . . . . . .   2            0-9 Days
 Monitor Messages MSGQ  . . . . . .   SLMSGQ       MSGQ Name
   Library  . . . . . . . . . . . .     QZRDSECSRM Library (not *LIBL,*CURLIB)










                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA█+  C                                                                 06/037
```

The configuration parameter for the global settings are as follows:

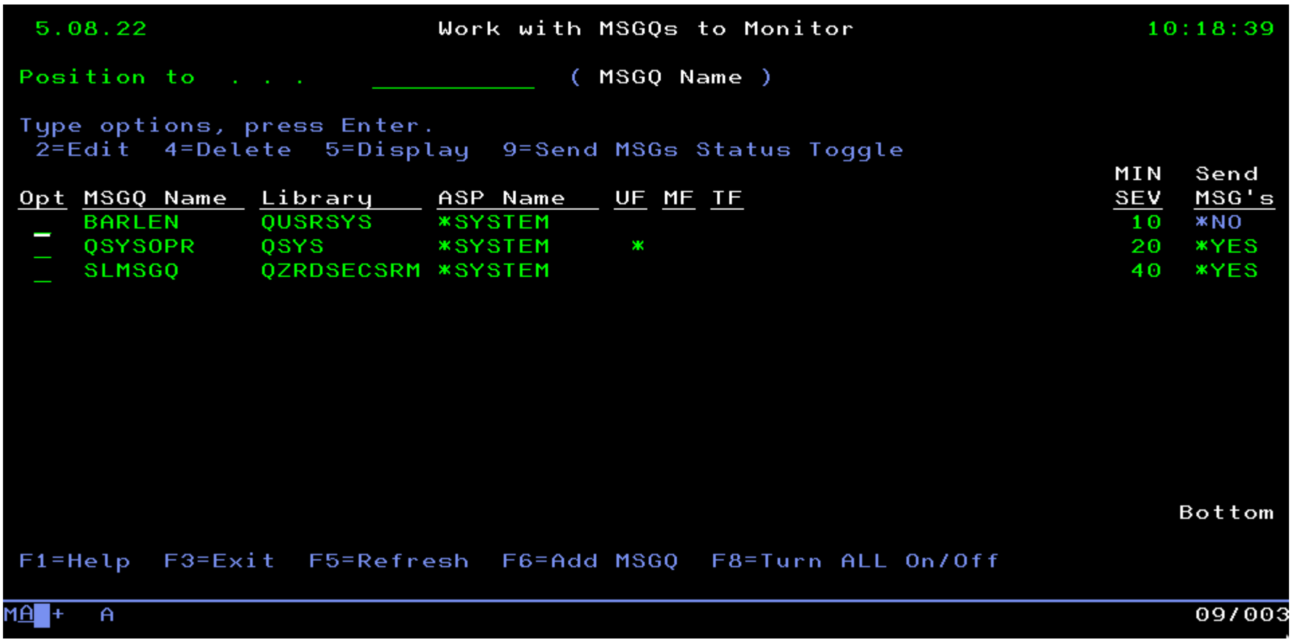
- MSGQ Monitoring On/Off
  This parameter specifies whether the message queue monitor starts when the subsystem SLSBS starts. If the parameter is set to *YES and the job has not been started yet, the SLMSGQMON job is started in the SLSBS subsystem.

  - **Y**
    The Y specifies that the message message queue monitor is started if it is not already running and will be started again when the subsystem starts the next time.
  - **N**
    The value N specifies that the message queue monitor ends after the next processing interval and will not be restarted when the subsystem SLSBS will be started again.
- Monitor Interval
  This parameter specifies the interval in number of seconds how often the monitored message queues are analyzed for new messages.
  - number
    Specify the number of seconds for the monitor interval. The range of valid values are between 120 and 7200 seconds.
- Message Retention Days
  This parameter specifies the number of days that messages that are retrieved from monitored message queues are kept in a database table.
  - number
    Number of days how long processed messages are kept in the Syslog Reporting Manager tool. The range of valid values are 0 to 9 days. 0 indicates that messages that are retrieved from monitored messages queues are removed after they have been processed and sent to the configured syslog server.
- Monitor Messages MSGQ
  This parameter specifies the message queue library and name of a message queue that receives messages related to jobs and messages that are processed by the message queue monitoring function.
  - QZRDSECSRM/SLMSGQ
    The default is the SLMSGQ message queue.
  - name
    You can also specify a different message queue that will receive message related to the message queue monitoring process.

  Information: Direct access via command: CFGSLMQM

4.13.2 Defining message queues to be monitored

Option 41 lets you manage the message queues that you want the Syslog Reporting Manager to monitor.



```
 5.08.22                  Work with MSGQs to Monitor                  10:18:39

Position to  . . .    __________  ( MSGQ Name )

Type options, press Enter.
 2=Edit  4=Delete  5=Display  9=Send MSGs Status Toggle
                                                                    MIN  Send
Opt MSGQ Name  Library    ASP Name   UF MF TF                       SEV  MSG's
 _  BARLEN     QUSRSYS    *SYSTEM                                    10  *NO
 _  QSYSOPR    QSYS       *SYSTEM     *                              20  *YES
 _  SLMSGQ     QZRDSECSRM *SYSTEM                                    40  *YES








                                                                        Bottom

F1=Help  F3=Exit  F5=Refresh  F6=Add MSGQ  F8=Turn ALL On/Off

MA + A                                                                09/003
```

The Work with MSGQs to monitor command lets you define all message queues that you want to monitor. All enabled message queues that meet the minimum severity level, the user filter type, the configured user profile filter, message identifier filter, and message type filter are monitored and an event is generated.

The list contains all message queues that you want to monitor. If a message is received on a monitored message queue that meets the configured filter criteria and is set as *YES for the Send MSGQ option, a syslog event is generated and sent to the configured syslog server. Note that the F8 function key will toggle between *YES and *NO for the Send MSGQs option for all listed message queues.

The filter type columns indicate whether certain filters have been defined for the listed message queue:

- UF – A user profile filter has been defined when a * is displayed
- MF – A message identifer filter has been defined when a * is displayed
- TF – A message type filter has been defined when a * is displayed

Information: Direct access via command: WRKMQMM

4.13.3 Starting the message queue monitor

You can start the message queue monitor with option 42 of the SLMON menu.

Information: Direct access via command: STRSLMON MONJOB(*MSGMON)

4.13.4 Ending the message queue monitor

You can end the message queue monitor with option 43 of the SLMON menu.

Information: Direct access via command: ENDSLMON MONJOB(*MSGMON)

4.14 Sending journal events

>The Syslog Reporting Manager (SRM) can also monitor other journals besides the QAUDJRN system journal. Journals that should be monitored must exist and are not created as part of the SRM configuration. Journals that are enabled in the SRM monitoring will retrieve entries from the journal and extract data from the common journal headers as well as the entry-specific data for each journal entry type.

NOTE: This function is not intended to monitor database journals that handle huge amounts of transactions. If you need to report DB table changes, you should use the Journal Extract Tool (JET) integration as described in 4.12 Sending database change events via Journal Extract Tool integration on page 39.

SRM comes with the following systems journals predefined. This does not mean that these journals actually exist on the system, but SRM has all the necessary journal definitions, entry types, and formatting information.

- QACGJRN - The system accounting journal, if created and accounting is enabled on the system level, can report the following journal entry types:
  - A-JB Job accounting information
  - A-SP Print output via spool function information
  - A-DP Print output for direct printing information
- QIPFILTER This journal is automatically created when IP Packet Rules (filtering) is configured on the system and the journal option is selected for at least one packet rule. Once activated, SRM can report the following journal-specific entry types:
  - M-TF IP filter rules actions, such as as DENY or PERMIT actions for inbound or outbound IP packets along with source and destination IP addresses and ports.

In addition to the predefined journals, an administrator can also add their own journals, i.e. data area journals, to report on data changes including the before and after images.

Examples:

A-JB Accounting Journal entry

```
<134>1 2023-10-12T09:23:30.491776-05:00 CTCSECT5.RCHLAND.IBM.COM
IBMiPSCSRM JRNMON IBMiEvent - CEF:0|IBM|IBM i|7.5|JRNMON|A-JB|3|
reason=Journal QACGJRN entry A-JB jobName=QDFTJOBD jobUser=BARLEN
jobNumber=194369 accountingCode=BARLENAC processingTime=8
numRoutingSteps=1 jobEntryDate=071223 jobEntryTime=092330
jobStartDate=071223 jobStartTime=092330 totalTransactionTime=0
numTransactions=0 syncAuxIODbOps=46 jobType=B complCode=0
numPrintLines=46 numPrintPages=1 numPrintFiles=1 numDbWriteOps=1
numDbReadOps=0 numDbUpdDelOps=0 numComWriteOps=0 numComReadOps=0
timeJobActive=0 timeJobSuspended=31
timestampJobEntry=07122023092330 timestampJobStart=07122023092330
asyncIoDbNonDbOps=17 expCpuTime=8 expSynAuxIoOps=46
expAsynAuxIoOps=17 expNumDbPut=0 expNumDbGet=0 expNumDbUpdDel=0
expNumLinesPrinted=46 expNumPagesPrinted=1 expNumPrintFiles=1
sourceServiceName=QSYS/QACGJRN jrnEntryType=A-JB pgmName=QWTMCEOJ
suser=BARLEN sproc=194369/BARLEN/QDFTJOBD shost=CTCSECT5
```

M-TF IP Filter entry

```
<134>1 2023-10-17T03:48:39.432096-05:00 CTCSECT5.RCHLAND.IBM.COM
IBMiPSCSRM JRNMON IBMiEvent - CEF:0|IBM|IBM i|7.5|JRNMON|M-TF|3|
reason=Journal QIPFILTER entry M-TF deviceInterface=CLOUDINIT0
deviceDirection=I act=PERMIT proto=6 src=10.15.167.141 spt=32134
dst=10.15.167.122 dpt=389 sourceServiceName=QUSRSYS/QIPFILTER
jrnEntryType=M-TF pgmName=QCMD suser=QTCP
sproc=143960/QTCP/QTOFJRN shost=CTCSECT5
```

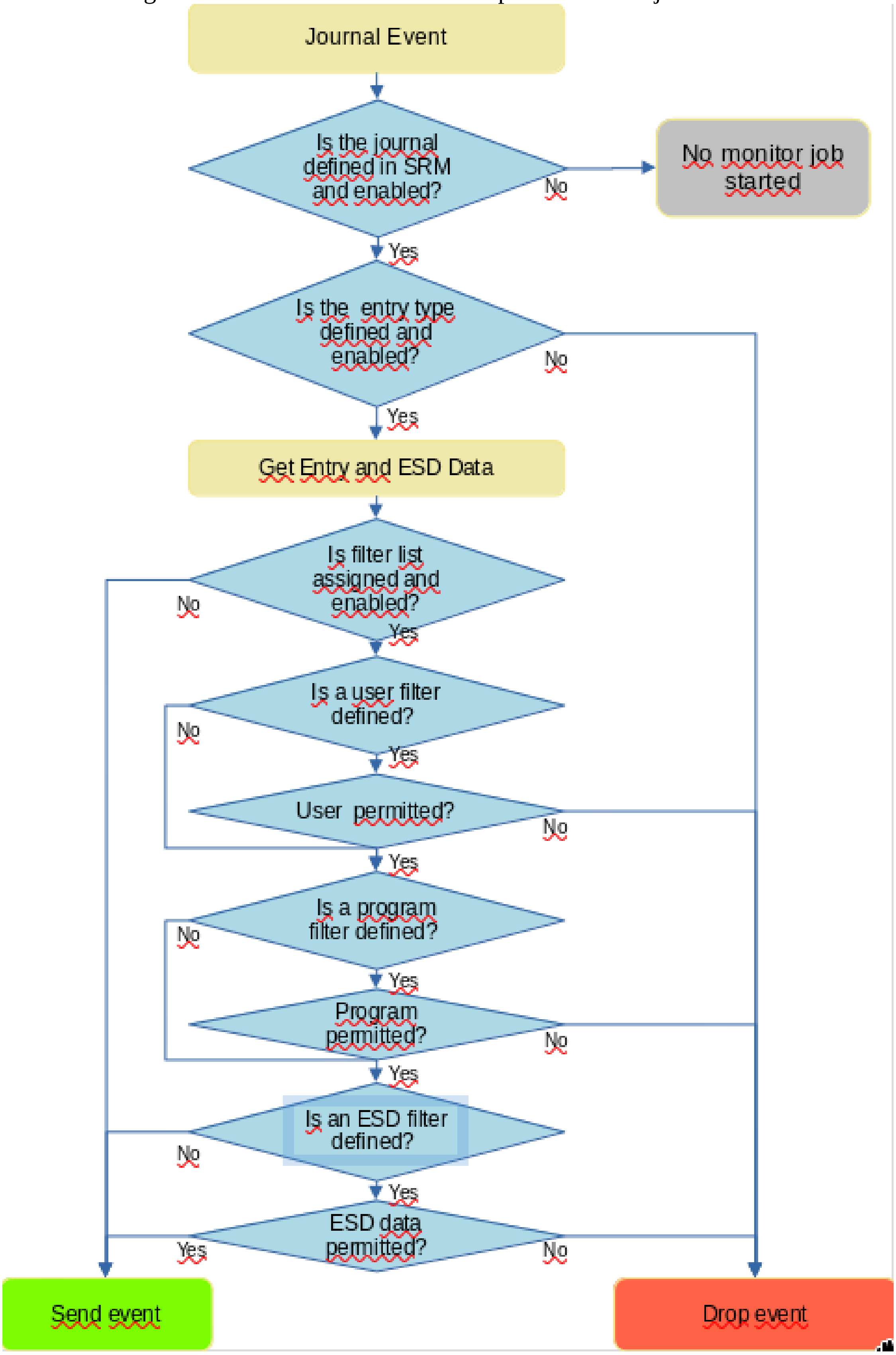
4.14.1 Journal monitor definitions and objects

The journal monitor processing is influenced by various factors. Depending on the configuration settings and definitions, an event could be reported in different ways or even omitted. The following table lists the various components and describes their purpose.

Configuration Settings	Command	Description
Journal configuration	CFGSLJRNJ	Every journal that you want to monitor needs to be added to the journal configuration.
Journal entry type configuration	CFGSLJRNE	For each configured journal, you need to define the journal entry types you want the monitor to report. SRM-provided journal definitions are already pre-defined.
Journal entry format	CFGSLJRNEF	For each defined journal entry type, you need to define the SIEM key-value pair names for the CEF and LEEF format along with the data type and offset. These definitions format the Entry Specific Data of a journal entry only. SRM-provided journal entry type formats are already pre-defined.
Journal filter lists	CFGSLJRNFL	A filter list can be activated for each configured journal. The list can be assigned to the journal. Each list can have one or more user, program, or Entry Specific Data (ESD) filter definitions.
Journal filter list entries	CFGSLJRNFN	The filter list entry represents an individual filter rule for a journal entry. There are three different rule types: • User filter (the user profile name in the journal entry) • Program filter (the program that triggered the journal entry to be generated) • ESD filter (can be a key-value pair in the ESD part of a journal entry)

4.14.2 Journal monitor workflow

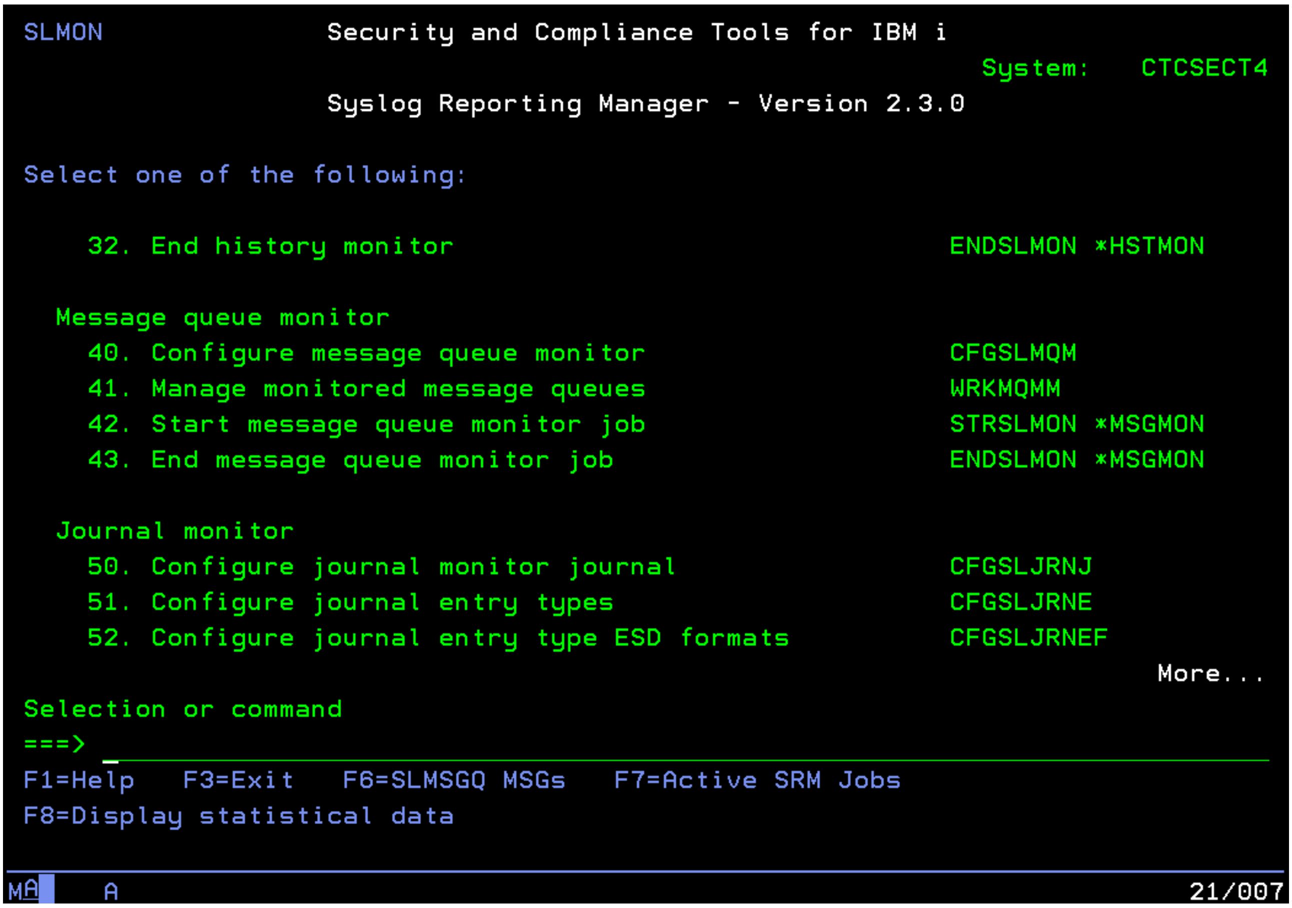
Multiple factors can have an impact on whether a journal event is sent to the configured SIEM server. The following workflow describes the decision process for the journal monitor:


Journal Event
Is the journal defined in SRM and enabled?
No
No monitor job started
Yes
Is the entry type defined and enabled?
No
Yes
Get Entry and ESD Data
Is filter list assigned and enabled?
No
Yes
Is a user filter defined?
No
Yes
User permitted?
No
Yes
Is a program filter defined?
No
Yes
Program permitted?
No
Yes
Is an ESD filter defined?
No
Yes
ESD data permitted?
Yes
No
Send event
Drop event

4.14.3 Journal definition

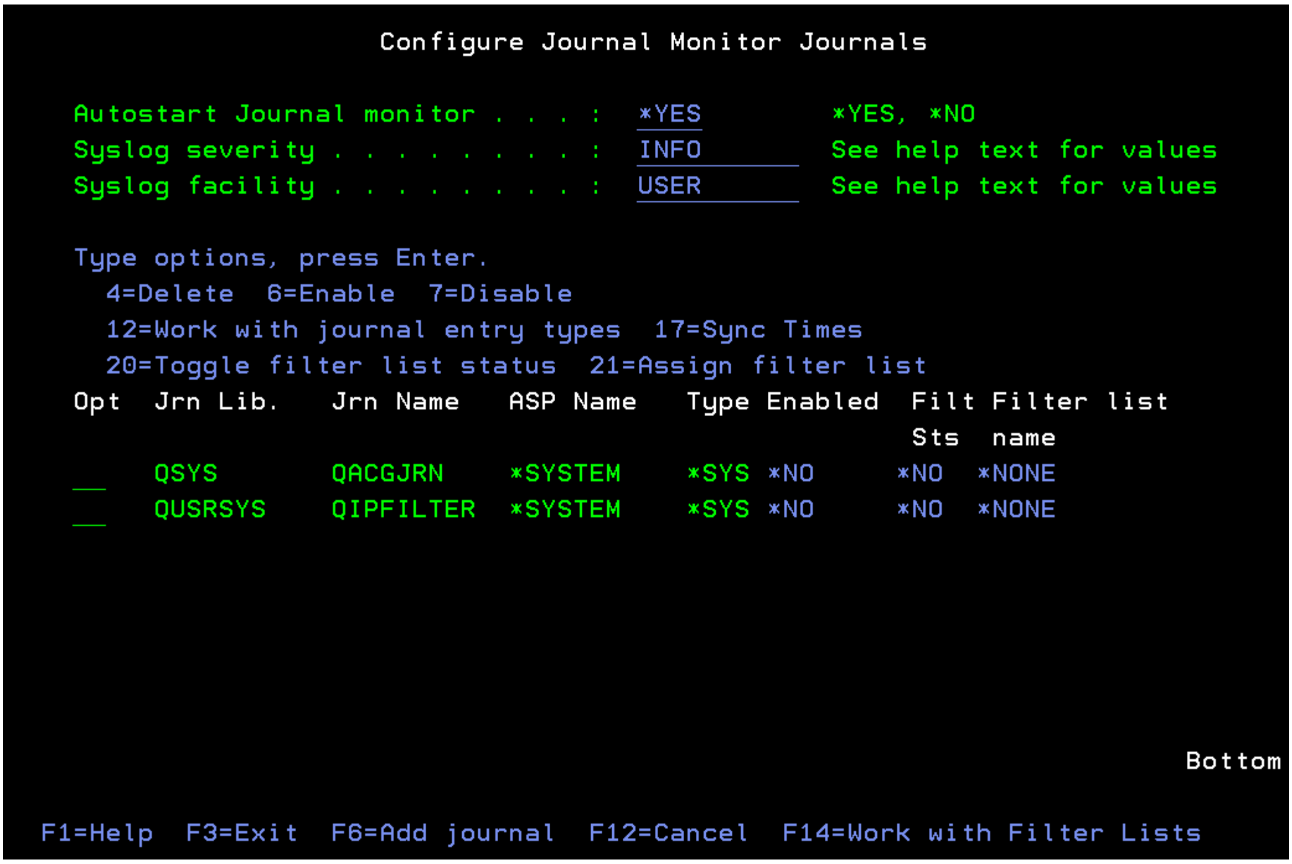
A journal can only be monitored when it exists on the system. The existing journal can then be defined in SRM via the following steps:

1. Enter the following command to display the Syslog Reporting Manager menu.
   `CFGSRM`



```
SLMON                Security and Compliance Tools for IBM i
                                                         System:   CTCSECT4
                     Syslog Reporting Manager - Version 2.3.0

Select one of the following:

    32. End history monitor                                ENDSLMON *HSTMON

  Message queue monitor
    40. Configure message queue monitor                    CFGSLMQM
    41. Manage monitored message queues                    WRKMQMM
    42. Start message queue monitor job                    STRSLMON *MSGMON
    43. End message queue monitor job                      ENDSLMON *MSGMON

  Journal monitor
    50. Configure journal monitor journal                  CFGSLJRNJ
    51. Configure journal entry types                      CFGSLJRNE
    52. Configure journal entry type ESD formats           CFGSLJRNEF
                                                                   More...
Selection or command
===> _
F1=Help   F3=Exit   F6=SLMSGQ MSGs   F7=Active SRM Jobs
F8=Display statistical data

MA     A                                                             21/007
```

2. Take option 50 (Configure journal monitor journal)



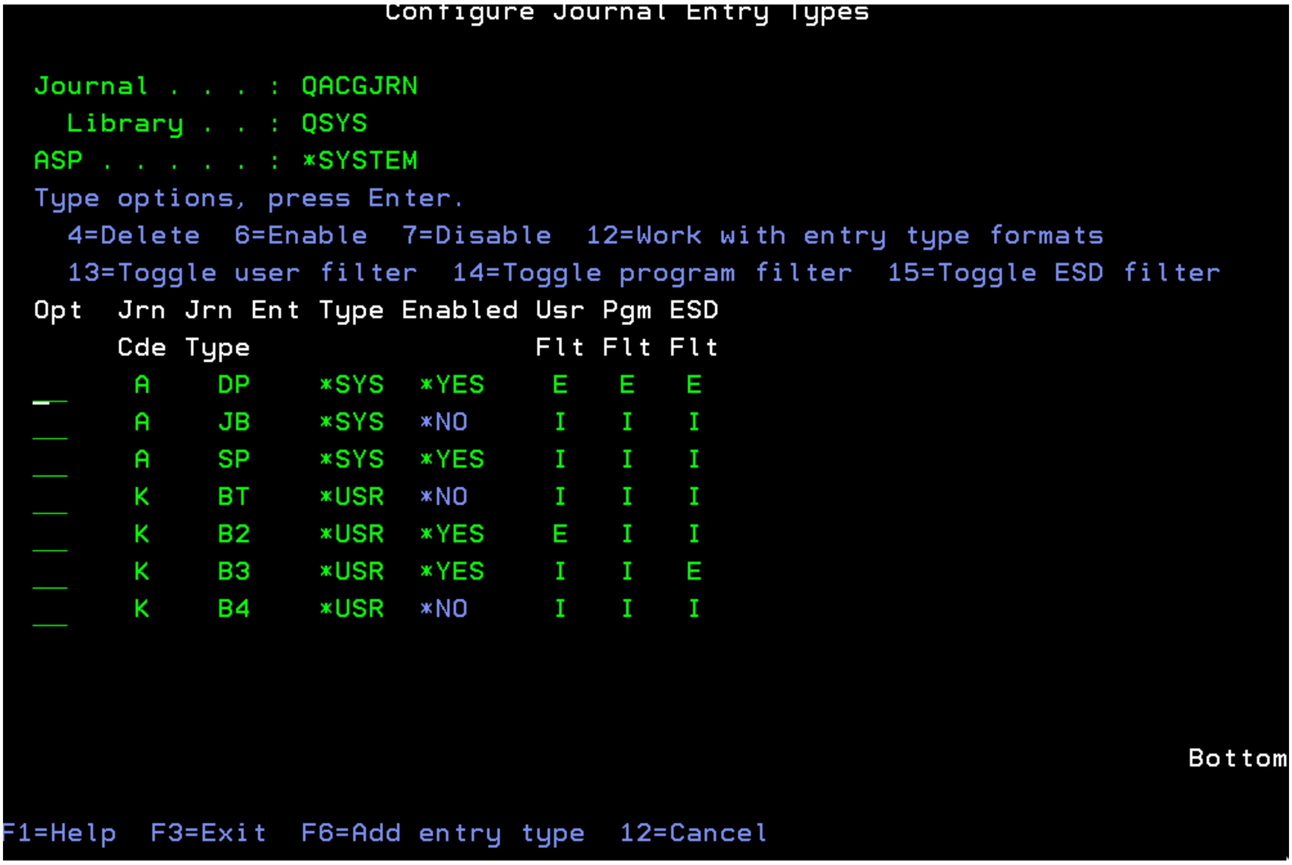
```
                    Configure Journal Monitor Journals

    Autostart Journal monitor . . . :  *YES        *YES, *NO
    Syslog severity . . . . . . . . :  INFO        See help text for values
    Syslog facility . . . . . . . . :  USER        See help text for values

    Type options, press Enter.
      4=Delete  6=Enable  7=Disable
      12=Work with journal entry types  17=Sync Times
      20=Toggle filter list status  21=Assign filter list
    Opt  Jrn Lib.    Jrn Name    ASP Name    Type Enabled  Filt Filter list
                                                           Sts  name
    __   QSYS        QACGJRN     *SYSTEM     *SYS *NO      *NO  *NONE
    __   QUSRSYS     QIPFILTER   *SYSTEM     *SYS *NO      *NO  *NONE




                                                                      Bottom

  F1=Help  F3=Exit  F6=Add journal  F12=Cancel  F14=Work with Filter Lists
```

Information: Direct access via command: CFGSLJRNJ

3. Work with the journals that that you want to monitor. You can add or remove journal names, enable or disable processing of events in a defined journal, work with journal entry types for a specific journal, or assign and enable journal filter lists.
   You can also specify the autostart, syslog severity, and syslog facility settings. Note that these parameters are valid for all journals.
   Note that you cannot delete the SRM-provided journals QSYS/QACGJRN and QUSRSYS/QIPFILTER from the list. These journals do not exists by default on the system, but the formats and entries have already been defined in SRM.
   - Option 4 lets you delete a defined journal (only *USR types can be deleted).
   - Option 6 lets you enable processing for the selected journal.
   - Option 7 lets you disable processing for the selected journal.
   - Option 12 lets you work with journal entry types for the selected journal.
   - Option 17 is only available when the calling user has at least the *AUDIT special authority in its user profile (not inherited from a group membership) and is member of the QZRDSRMGRP group. It is considered an expert mode configuration option and allows you to change synchronization restart properties, such as the timestamp of the last processed event entry. This option should only be used by experts who know what impact the change can have.
   - Option 20 activates journal entry filtering for journals. If you want to use filtering, you need to set the filter status to *YES and assign an existing filter list with option 21. If you enable file filtering but have no filter list assigned, the column of the entry is shown in red indicating that filtering does not work. In this case, all entries are reported.
   - Option 21 lets you assign an existing filter list to a journal. Filter lists can be managed via the F14 key or by entering the CFGSLJRNFL command.

Once you have a journal defined, you need to configure the journal entry types that you want to be processed by the journal monitor. Depending on the journal, there might be one or more journal entry types that are written to the journal.

4. Take option 51 (Configure journal entry types) or use option 12 for a selected journal in the CFGSLJRNJ command.



```
                       Configure Journal Entry Types

 Journal . . . : QACGJRN
   Library . . : QSYS
 ASP . . . . . : *SYSTEM
 Type options, press Enter.
   4=Delete  6=Enable  7=Disable  12=Work with entry type formats
   13=Toggle user filter  14=Toggle program filter  15=Toggle ESD filter
 Opt  Jrn Jrn Ent Type Enabled Usr Pgm ESD
      Cde Type                 Flt Flt Flt
 __    A    DP    *SYS  *YES    E   E   E
 __    A    JB    *SYS  *NO     I   I   I
 __    A    SP    *SYS  *YES    I   I   I
 __    K    BT    *USR  *NO     I   I   I
 __    K    B2    *USR  *YES    E   I   I
 __    K    B3    *USR  *YES    I   I   E
 __    K    B4    *USR  *NO     I   I   I




                                                                        Bottom

F1=Help  F3=Exit  F6=Add entry type  12=Cancel
```

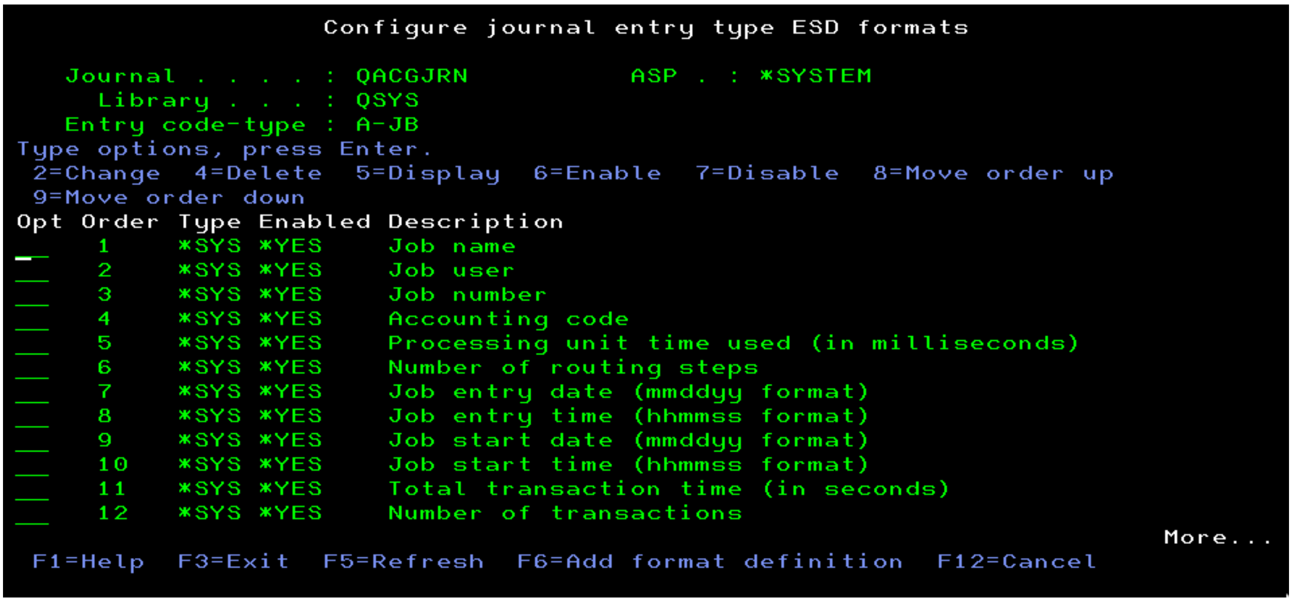
Information: Direct access via command: CFGSLJRNE

5. Only journal entries for enabled entry types are processed by the journal monitor. This command allows you disable or enabled listed entry types and to define new entry types for the displayed journal using the F6 function key.
   Note that you can only delete entry types for *USR definition types.
   Options 13 to 15 let you define whether a filter rule in a filter list should be processed as an Include or Exclude filter for the entry type. There are filter rules for:
   - User filter
     You could add one or more user profile names as a user type filter to a filter list.
   - Program filter
     You could add one or more program names as a program type filter to a filter list.
   - ESD filter
     You could add one or more entry specific data filters to a filter list.
   - The Include or Exclude option specifies if journal entries that match filter rules of a certain type should be included into the event reporting or excluded from being reported.

   Option 12 lets you work with formatting definitions of the ESD for a specific journal entry type.

For every journal entry type that you added for the selected journal, you need to define the format of the ESD information. The Entry Specific Data (ESD) are unique for every journal code / journal entry type combination. You need to review the journal format layout description to find the correct format definition.

6. Take option 52 (Configure journal entry type ESD formats) or use option 12 for a selected journal entry type in the CFGSLJRNE command.



```
                    Configure journal entry type ESD formats

   Journal . . . . . : QACGJRN           ASP . : *SYSTEM
     Library . . . . : QSYS
   Entry code-type : A-JB
Type options, press Enter.
 2=Change  4=Delete  5=Display  6=Enable  7=Disable  8=Move order up
 9=Move order down
Opt Order Type Enabled Description
___  1    *SYS *YES    Job name
___  2    *SYS *YES    Job user
___  3    *SYS *YES    Job number
___  4    *SYS *YES    Accounting code
___  5    *SYS *YES    Processing unit time used (in milliseconds)
___  6    *SYS *YES    Number of routing steps
___  7    *SYS *YES    Job entry date (mmddyy format)
___  8    *SYS *YES    Job entry time (hhmmss format)
___  9    *SYS *YES    Job start date (mmddyy format)
___  10   *SYS *YES    Job start time (hhmmss format)
___  11   *SYS *YES    Total transaction time (in seconds)
___  12   *SYS *YES    Number of transactions
                                                                 More...
 F1=Help  F3=Exit  F5=Refresh  F6=Add format definition  F12=Cancel
```

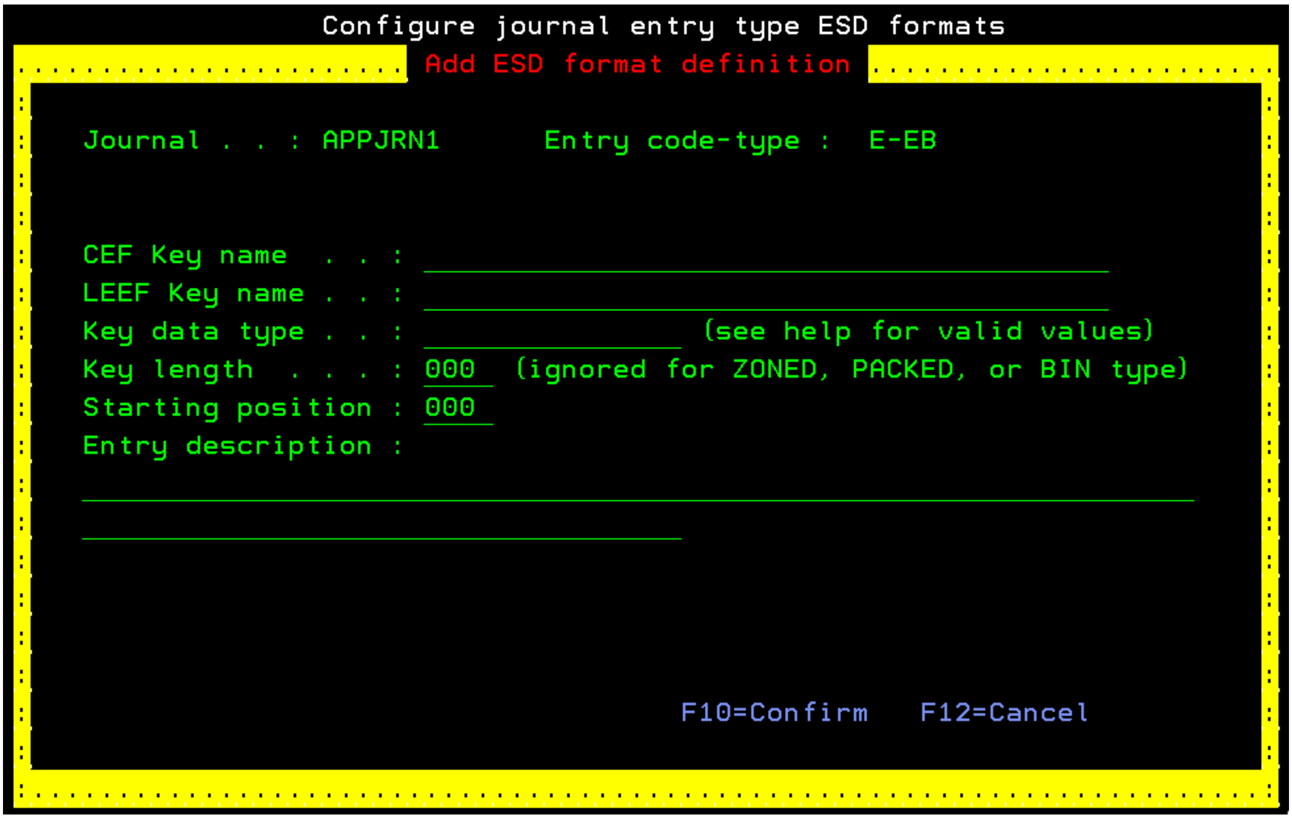
Information: Direct access via command: CFGSLJRNEF

The ESD format definitions describe the offset (starting position) of the information, the length, and the data type as stored in a particular journal entry. They also describe the key names for the SIEM events for the Common Event Format (CEF) and Log Event Extended Format (LEEF). The journal monitor processes a journal entry’s entry specific data and extracts the data from the journal entry according to the defined format definition.

Format definition entries can be enabled or disabled. Only enabled entries are processed by the journal monitor and included in the SIEM event.

The journal format definitions that are shipped with the Syslog Reporting Manager are listed as type *SYS. These entries cannot be deleted. When changing *SYS-type entries, only the CEF and LEEF key names can be customized. For manually added entries, which are listed as *USR-type entries, you can modify all parameters and can also delete the entries.

7. Use function key F6 to add a new format definition for entry specific data:



```
                    Configure journal entry type ESD formats
 ......................... Add ESD format definition ..........................
 :                                                                             :
 :   Journal . . : APPJRN1      Entry code-type :  E-EB                        :
 :                                                                             :
 :                                                                             :
 :   CEF Key name  . . : ________________________________________              :
 :   LEEF Key name . . : ________________________________________              :
 :   Key data type . . : _______________ (see help for valid values)           :
 :   Key length  . . . : 000  (ignored for ZONED, PACKED, or BIN type)         :
 :   Starting position : 000                                                   :
 :   Entry description :                                                       :
 :   _________________________________________________________________         :
 :   ___________________________________                                       :
 :                                                                             :
 :                                                                             :
 :                                                                             :
 :                                     F10=Confirm   F12=Cancel                :
 :                                                                             :
 :.............................................................................:
```

Note: Information about IBM i journal entry codes and types can be found in the IBM i Documentation page:
https://www.ibm.com/docs/en/i/7.4?topic=information-all-journal-entries-by-code-type

You need to provide information for the following parameter:

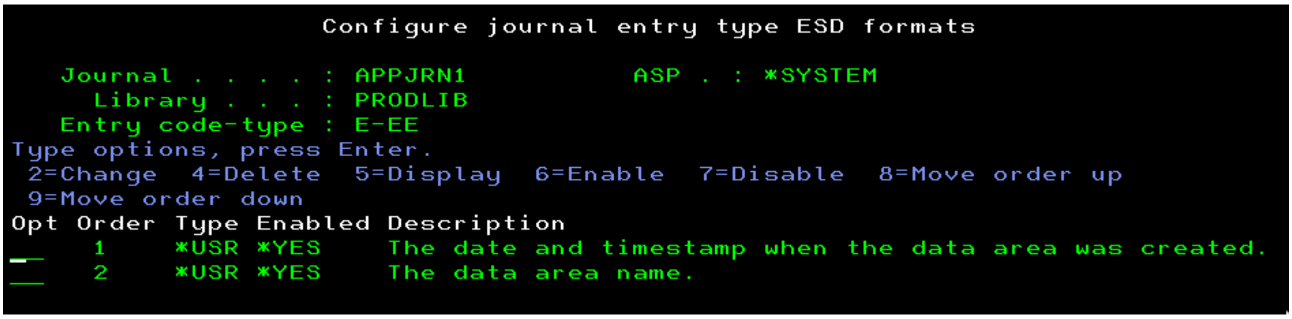
- **CEF Key name**
  - Enter a Common Event Format (CEF) key name for the new definition. SIEM events contain key-value pairs. The key is the identifier of the payload and the value contains the information related to the key. The value data is retrieved from the journal entry's specific data and assigned to the key. The format in the SIEM event is: key=value.
- **LEEF Key name**
  - Enter a Log Event Extended Format (LEEF) key name for the new definition. SIEM events contain key-value pairs. The key is the identifier of the payload and the value contains the information related to the key. The value data is retrieved from the journal entry's specific data and assigned to the key. The format in the SIEM event is: key=value.
- **Key data type**
  - Specify the data type of the key value that is retrieved from the entry specific data. The journal layout definition provides the details about the format and length information. Three data types are supported:
    - **CHAR** - character data type. This data type also requires the key length to be specified.
    - **ZONED_n_d** - This is a ZONED numeric data type. **n** stands for the whole number of positions and **d** for the decimals. 1-32 are the supported values for the number part and 0-2 are the supported values for the decimal part (right of the decimal point). For example, if your ESD contains a ZONED numeric value of length 4 with 0 decimal points, you would enter ZONED_4_0.
      Supported values:

    - ZONED_1_0 to ZONED_32_0
      ZONED_1_1 to ZONED_32_1
      ZONED_1_2 to ZONED_32_2
    - **PACKED_n_d** - This is a PACKED numeric data type. **n** stands for the whole number of positions and **d** for the decimals. 1-32 are the supported values for the number part and 0-2 are the supported values for the decimal part (right of the decimal point). For example, if your ESD contains a PACKED numeric value of length 5 with 1 decimal points, you would enter PACKED_5_1.
      PACKED_1_0 to PACKED_32_0
      PACKED_1_1 to PACKED_32_1
      PACKED_1_2 to PACKED_32_2
    - **BIN_n** - binary data type. **n** stands for the whole number of positions as described in the journal format layout sections in the IBM i documentation center. For this data type, only the following values are valid: BIN_4, BIN_8, BIN_16, BIN_31, BIN_32, and BIN_64.
    - Note that the key length is automatically calculated for ZONED, PACKED, and BIN data types.
- **Key length**
  - For character (CHAR) data type keys, enter the length of the data in the ESD that contains information that should be assigned to the key. You do not need to enter a value for ZONED, PACKED, or BIN data types. The length for numeric data of these types are automatically calculated. If you enter a value for a ZONED, PACKED, or BIN data types, the configuration command performs its own calculation and overrides the manually entered value.
- **Starting position**
  - The starting position is the offset within the entry specific data where the information element starts.
- **Entry description**
  - Enter a descriptive text that describes the content and purpose of the definition.

Note: You have to provide a CEF and LEEF key even though you might use only once format when sending events to the configured SIEM server. CEF and LEEF formats contains standardized key names and also provide options for custom keys. Consult the documentation for the two SIEM formats for more information about the log format.

Example of a data area journal with entry code E and entry type EE for the first 2 fields in the entry.

Relative offset	Field	Format	Description
1 (**Starting position=1**)	Create time of day and date	Char (8) **Key data type=CHAR** **Key length=8**	The date and timestamp when the data area was created.
9 (**Starting position=9**)	Data area name	Char(10) **Key data type=CHAR** **Key length=10**	The data area name.



```
                   Configure journal entry type ESD formats

   Journal . . . . : APPJRN1           ASP . : *SYSTEM
     Library . . . : PRODLIB
   Entry code-type : E-EE
Type options, press Enter.
 2=Change   4=Delete  5=Display  6=Enable   7=Disable   8=Move order up
 9=Move order down
Opt Order Type Enabled Description
__    1    *USR *YES    The date and timestamp when the data area was created.
__    2    *USR *YES    The data area name.
```

8. Repeat the add operation for each field in the journal entry ESD that you want to report in a SIEM event.
9. You can also use the following list item options:
   - Option 2=Change
     - Select this option to change an existing format definition. Note that not all parameters can be changed for *SYS type entries.
   - Option 4=Delete
     - Select this option to delete a format definition from the displayed definition list. *SYS type entries cannot be deleted.
   - Option 5=Display
     - Select this option to display all attributes of the selected format definition.
   - Option 6=Enable
     - Select this option to enable the definition for processing by the journal monitor.
   - Option 7=Disable
     - Select this option to disable the definition for processing by the journal monitor. The journal monitor is not reporting the definition element in the SIEM event.
   - Option 8=Move order up
     - Select this option to move the selected definition up in the displayed list. The order number is changed to the next higher order number. The definition elements are listed in the SIEM event in the displayed order.
   - Option 9=Move order down
     - Select this option to move the selected definition down in the displayed list. The order number is changed to the next lower order number. The definition elements are listed in the SIEM event in the displayed order.

From that point on the Syslog Reporting Manager is monitoring your configured journals with their enabled journal entry types and reports the entries according to configured ESD formatting to the configured syslog server.

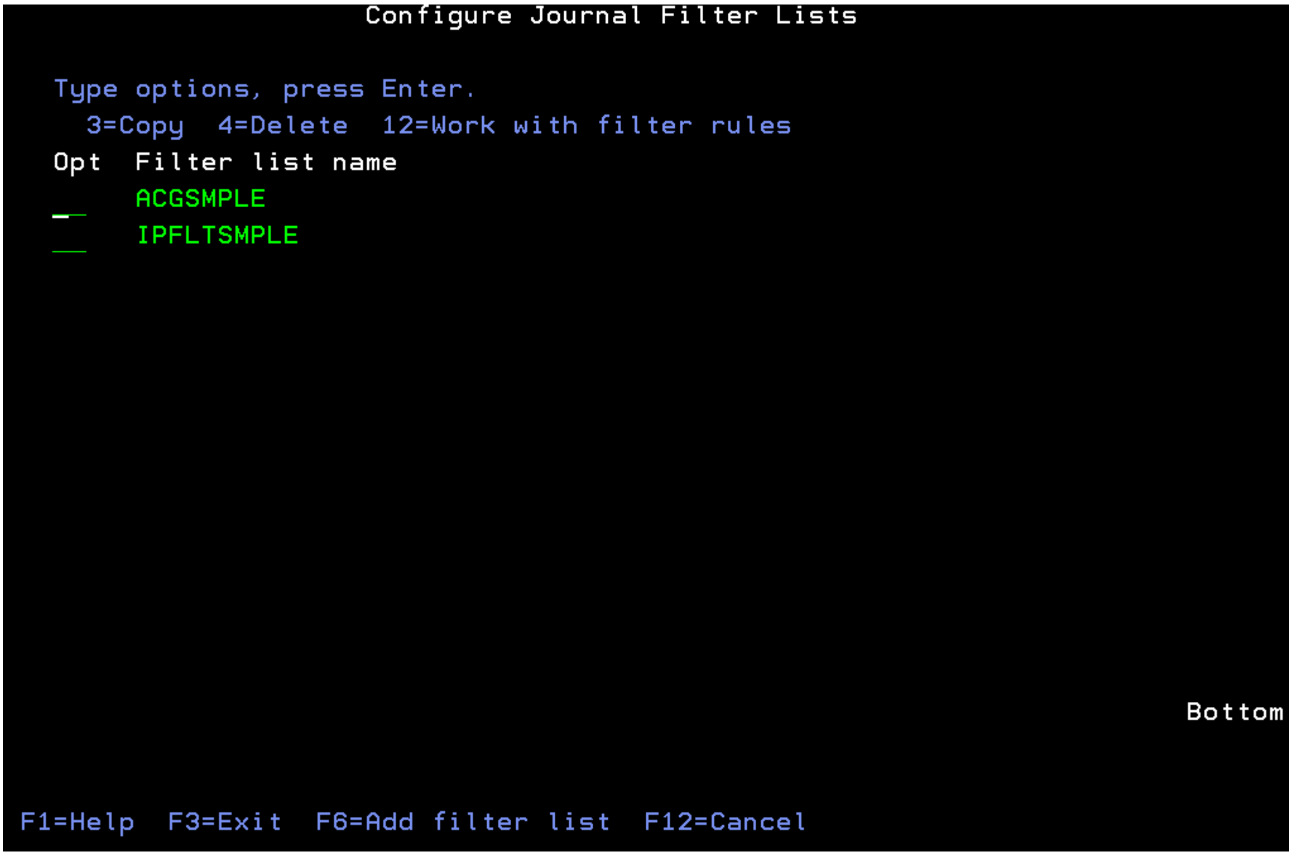
4.14.4 Journal filter

Journal filters let you filter on certain attributes of a journal entry and determine whether a processed journal entry is sent as a SIEM event to the configured syslog server. The attributes that you can filter on are:

- User profile names (qualified names only)
  These are the source user profiles of a journal entry.
- Program names (no libraries)
- Entry Specific Data (ESD) information
  ESD information is the unique piece of information that differs for every journal entry type. SRM first formats the ESD according to your entry type format into key-value pairs, i.e. jobtype=I, and then applies the ESD filter rules.

The individual filter rules of the different types are assigned to filter lists. A filter list can then be applied to a filter journal. The following steps guide you through the process of defining filter lists with their rules.

1. From the CFGSRM menu take option 53 (Configure journal filter lists)

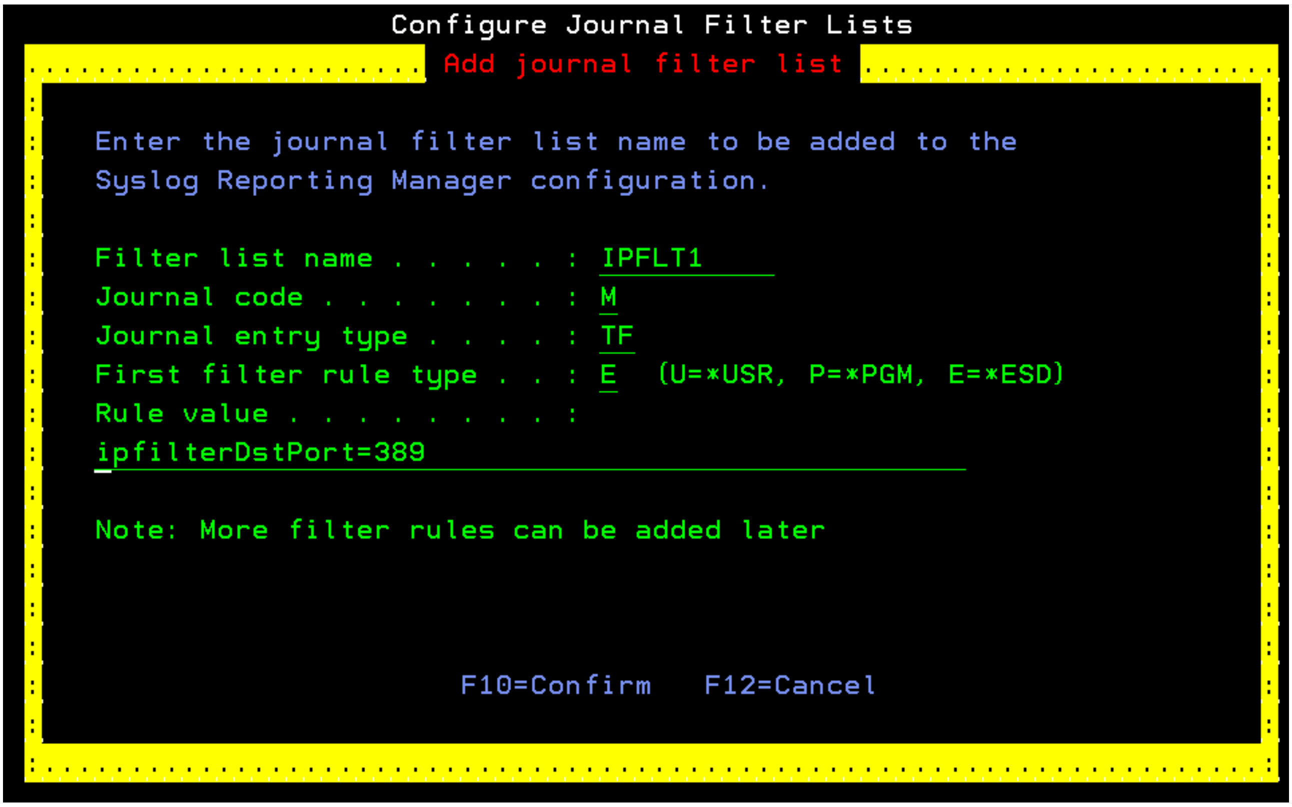


```
                      Configure Journal Filter Lists

  Type options, press Enter.
    3=Copy   4=Delete   12=Work with filter rules
  Opt   Filter list name
  __      ACGSMPLE
  __      IPFLTSMPLE

                                                                  Bottom

 F1=Help   F3=Exit   F6=Add filter list   F12=Cancel
```

Information: Direct access via command: CFGSLJRNFL

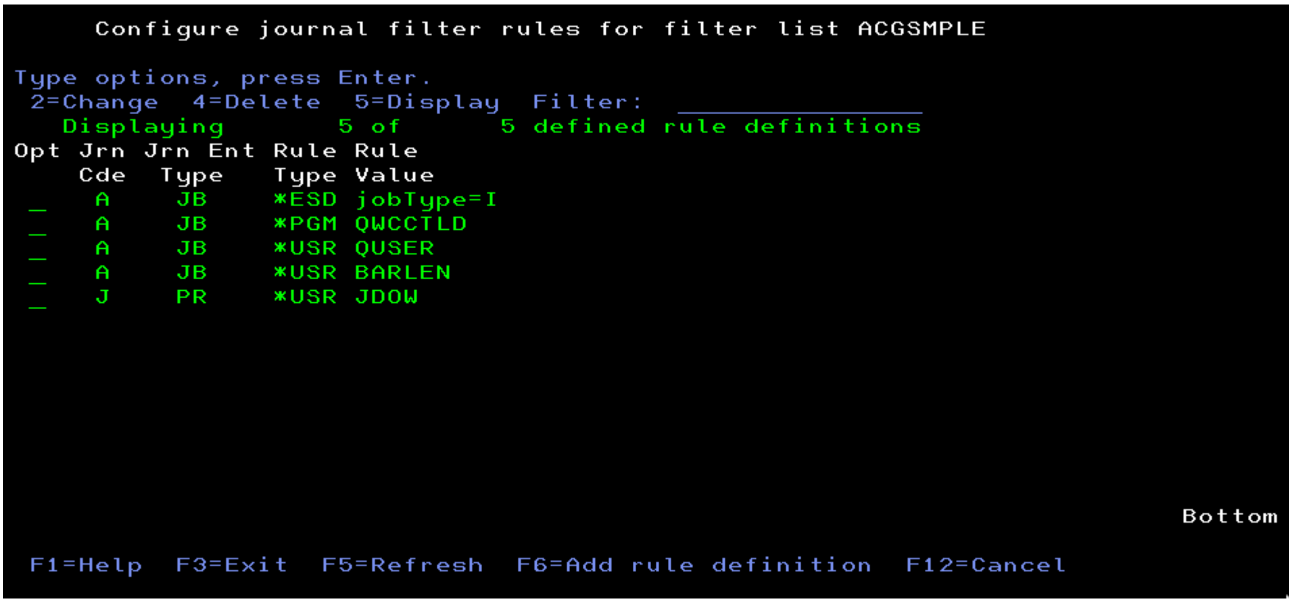
- With option 3 you can copy an existing filter list into a new list. All rule definitions from the original list will be copied too.
- With option 4 you can delete an existing filter list. You can only delete a filter list if it is not assigned to an actively filtered journal. You have to remove the assignment first or deactivate journal filtering before you can delete the filter list. The CFGSLJRNJ command lets you manage the filter status and assignment. If a filter list is still assigned to a journal, but the filter is not active, the filter list is deleted and the assigned filter list set to *NONE for the corresponding journal entry in the CFGSLJRNJ command.

2. Function key F6 lets you add a new filter list. When adding a new filter list, you have to specify the name of the new list and at least the information for the first filter rule as shown in the following example:



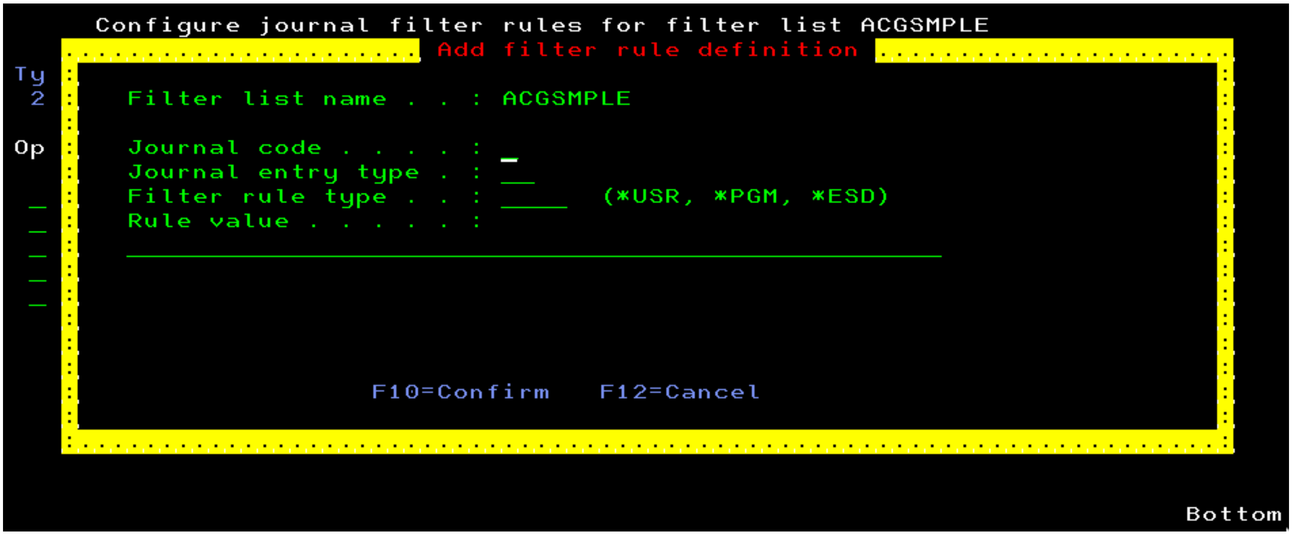
```
                    Configure Journal Filter Lists
 ....................... Add journal filter list .........................
 :                                                                        :
 :   Enter the journal filter list name to be added to the                :
 :   Syslog Reporting Manager configuration.                              :
 :                                                                        :
 :   Filter list name . . . . . : IPFLT1____                              :
 :   Journal code . . . . . . . : M                                       :
 :   Journal entry type . . . . : TF                                      :
 :   First filter rule type . . : E  (U=*USR, P=*PGM, E=*ESD)             :
 :   Rule value . . . . . . . . :                                         :
 :   ipfilterDstPort=389__________________________________                :
 :                                                                        :
 :   Note: More filter rules can be added later                           :
 :                                                                        :
 :                                                                        :
 :                                                                        :
 :                     F10=Confirm   F12=Cancel                           :
 :                                                                        :
 :........................................................................:
```

3. You can manage existing filter lists by using option 12 to work with the individual filter rule definitions for the selected filter list.



```
     Configure journal filter rules for filter list ACGSMPLE

Type options, press Enter.
 2=Change   4=Delete   5=Display   Filter: _______________
   Displaying        5 of       5 defined rule definitions
Opt Jrn Jrn Ent Rule Rule
    Cde  Type   Type Value
 _   A    JB    *ESD jobType=I
 _   A    JB    *PGM QWCCTLD
 _   A    JB    *USR QUSER
 _   A    JB    *USR BARLEN
 _   J    PR    *USR JDOW










                                                                    Bottom

 F1=Help  F3=Exit  F5=Refresh  F6=Add rule definition  F12=Cancel
```

4. All rule definitions for the selected filter list are shown. You can use the options to change, delete, or display an existing definition or function key F6 to add a new definition as shown in the next screen



```
     Configure journal filter rules for filter list ACGSMPLE
   ......................  Add filter rule definition  ......................
Ty :                                                                        :
 2 :   Filter list name . . :  ACGSMPLE                                     :
   :                                                                        :
Op :   Journal code . . . . :  _                                            :
   :   Journal entry type . :  __                                           :
 _ :   Filter rule type . . :  ____    (*USR, *PGM, *ESD)                   :
 _ :   Rule value . . . . . :                                               :
 _ :   __________________________________________________                   :
 _ :                                                                        :
 _ :                                                                        :
   :                                                                        :
   :                                                                        :
   :                  F10=Confirm   F12=Cancel                              :
   :                                                                        :
   :........................................................................:

                                                                     Bottom
```

A filter rule identifies which journal events should be included into the event reporting to the configured SIEM / syslog server. The filter is applied to the entire journal that has the filter list assigned and enabled. All filter rules that match the processed journal code and journal entry type are evaluated for user, program, and ESD filter rules. Only events that match all the configured rules for the processed entry type are sent. The rules are processed with a logical OR operation for the same filter type and a logical AND between different filter types. Each filter type processing option can be defined in the journal entry configuration as an Include or Exclude filter.

Journal entry types for a journal are configured with the CFGSLJRNE command.

Example:

For journal code/entry type A-JB is a *USR filter for users BARLEN, SMITH, and BAKER as an Exclude filter as well as an Include program filter for USREXT with an ESD Include filter of jobtype=I, only entries that do not match any of the listed users and match the program USREXT and where the program was run interactively are reported.

The following attributes need to be specified when a new rule definition is added:

Journal entry type

Enter a journal entry type of a journal entry for which the filter rule should apply.

Filter rule type

Specify the filter rule type. This can be either *USR for user type filter, *PGM for program type filter, or *ESD for Entry Specific Data information.

Filter rule value

Enter the filter rule value for the specified rule type. For the *USR type the value must be a valid user profile name, for *PGM it must be a valid program name, and for *ESD the value must be a SIEM format key/value pair in the format of "key=value". Note that the ESD keys

must be configured in the journal entry format file via the CFGSLJRNEF command.
Example:

deviceInterface=ETHLINE2

5. Once you have defined your filter definition and filter list, you have to assign it to a journal using the CFGSLJRNJ command. <

4.15 Sending custom events

Custom events are events that are generated by user applications and not the operating system or the Syslog Reporting Manager itself. Examples could be:

- You have created your own monitor tool for a message queue and want to forward specific messages as a SIEM event to the remote SIEM server.
- You want to send specific events that occurred in your business application to the SIEM server.

Permissions required:

To be able to use the SNDEVT command, the user should be granted *USE access to the following two objects:

QZRDSECSRM/SNDEVT	*CMD
QZRDSECSRM/SNDEVTP	*PGM

Two different methods can be used to send custom events:

1. There is a `SNDEVT` CL command to send a custom event.
2. You can use the `sendCustomEvent`, `sendCustomFmtEvent`, or `sendCustomFmtEventP` procedures in your ILE program to send custom events.

The following two sections describe more details about each method.

The CL command as well as the procedures can also be used in different ways. The major difference is that one method requires you to specify more information about the source (sending) job and user and the command/procedure will format the SIEM message completely for you or the second method, which gives you the freedom to create your own key-value pairs as expected by the SIEM server. In the latter case you are fully responsible to use the correct key names and also format the values according to the CEF or LEEF specifications.

Custom messages are sent as follows:

<u>Method 1: Proving source user and qualified job name</u>

The following information must be provided in the CL command or procedure sendCustomEvent:

- Syslog facility (used in the syslog header)
  Valid values are: `KERNEL, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CLOCK, AUTHPRIV, LOGAUDIT, LOGALERT, CRON, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7`
  For more information regarding syslog facilities, refer to the specifications of RFC3164 or RFC5424.
- Syslog severity (used in the syslog header)
  Valid values are: `EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO, DEBUG`
  For more information regarding syslog severities, refer to the specifications of RFC3164 or RFC5424.
- Timestamp information for the event (can be either the value *CURTIME in which case the syslog header timestamp is the date/time of when the command/procedure was run or it can be a custom provided timestamp in ISO format YYYY-MM-DD-HH.MM.SS.mmmmmm.

- A SIEM header value that will be added to the SIEM header. Depending on the chosen SIEM format, the value is placed as follows:
  - CEF – value added in the NAME field of CEF header
  - LEEF – value added in the EventID field of the LEEF header after the value CUSEVT-
- Source user profile name
  This is the IBM i user profile name of the user that will be sent as the origin of the event. The user profile name can also be *CURUSER in which case the source user is the user who performs the SNDEVT command or calls the corresponding procedure.
  SIEM payload key:
  CEF: suser
  LEEF: usrName
- Qualified source job name
  A custom provided job name in the format JOBNUMBER/JOBUSER/JOBNAME (i.e. 329701/BARLEN/QPADEV0002) that identifies the job that triggered the event or the special value *CURJOB which uses the job name of the job that performs the SNDEVT command or calls the corresponding procedure.
  SIEM payload key:
  CEF: sproc
  LEEF: sproc
- Event category
  Sources of SIEM evens are often grouped in categories. This parameter lets you specify a category value for your custom event.
  SIEM payload key:
  CEF: cat
  LEEF: cat
- Event text
  This is the actual event message text you want to send.
  SIEM payload key:
  CEF: msg
  LEEF: msg
- Note: your source host will automatically be added by the custom send function. This is not a parameter you can specify:
  SIEM payload key:
  CEF: shost
  LEEF: resource

<u>Method 2: Format the custom event payload yourself</u>

The following information must be provided in the CL command or procedure sendCustomEvent:

- Syslog facility (used in the syslog header)
  Valid values are: `KERNEL, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CLOCK, AUTHPRIV, LOGAUDIT, LOGALERT, CRON, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7`

  For more information regarding syslog facilities, refer to the specifications of RFC3164 or RFC5424.
- Syslog severity (used in the syslog header)
  Valid values are: `EMERG, ALERT, CRIT, ERROR, WARNING, NOTICE, INFO,`

`DEBUG`

For more information regarding syslog severities, refer to the specifications of RFC3164 or RFC5424.

- Timestamp information for the event (can be either the value *CURTIME in which case the syslog header timestamp is the date/time of when the command/procedure was run or it can be a custom provided timestamp in ISO format YYYY-MM-DD-HH.MM.SS.mmmmmm.
- A SIEM header value that will be added to the SIEM header. Depending on the chosen SIEM format, the value is placed as follows:
  - CEF – value added in the NAME field of CEF header
  - LEEF – value added in the EventID field of the LEEF header after the valued CUSEVT-
- Note: if your source your source host has not been added by yourself, it will automatically be added by the custom send function :
  SIEM payload key:

CEF:	shost
LEEF:	resource

- Event text
  This parameter contains all the key-value pairs that you provide. It is the responsibility of the user to specify all required keys and their values as expected by the SIEM server. The custom send event function does not perform any syntax checking or escaping of reserved characters.
  SIEM payload key:

CEF:	does not apply, provided by user
LEEF:	does not apply, provided by user

4.15.1 Sending custom events with the SNDEVT commands

If you need to send custom events occasionally, the Send Event (SNDEVT) command has been created for that.

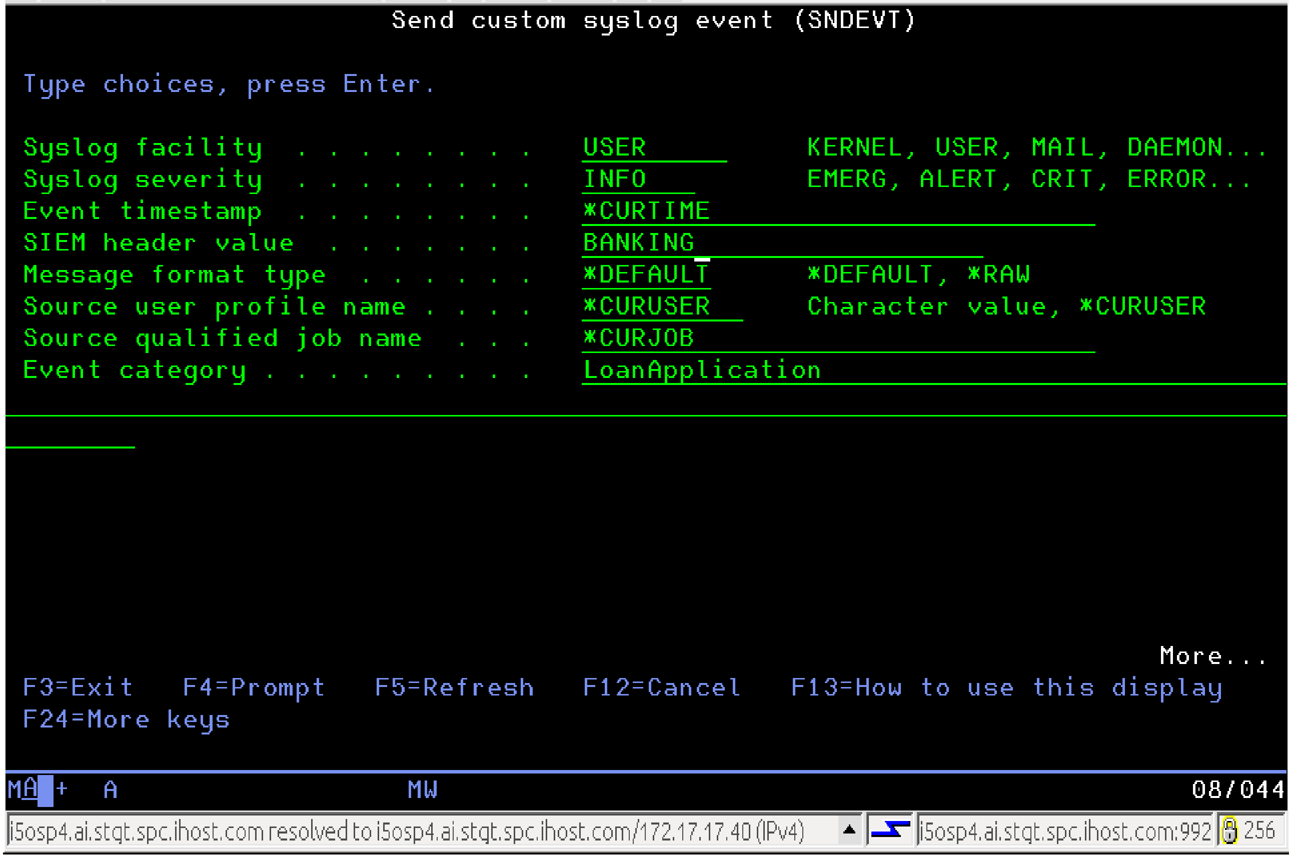
IMPORTANT: There are some restrictions with custom events:

- Only a limited number of special characters are supported. It varies based on used code pages.
- It is strongly recommended to run the job that sends custom events with CCSID 37.

You can use the command in the two ways described in the previous section. Which way you use is selected in the Message format type (MSGTYPE) parameter:

- *DEFAULT – automatic formatting is done and the event text is sent with the msg key-value
- *RAW – own formatting. All key-value pairs for the SIEM payload need to be provided by the user.

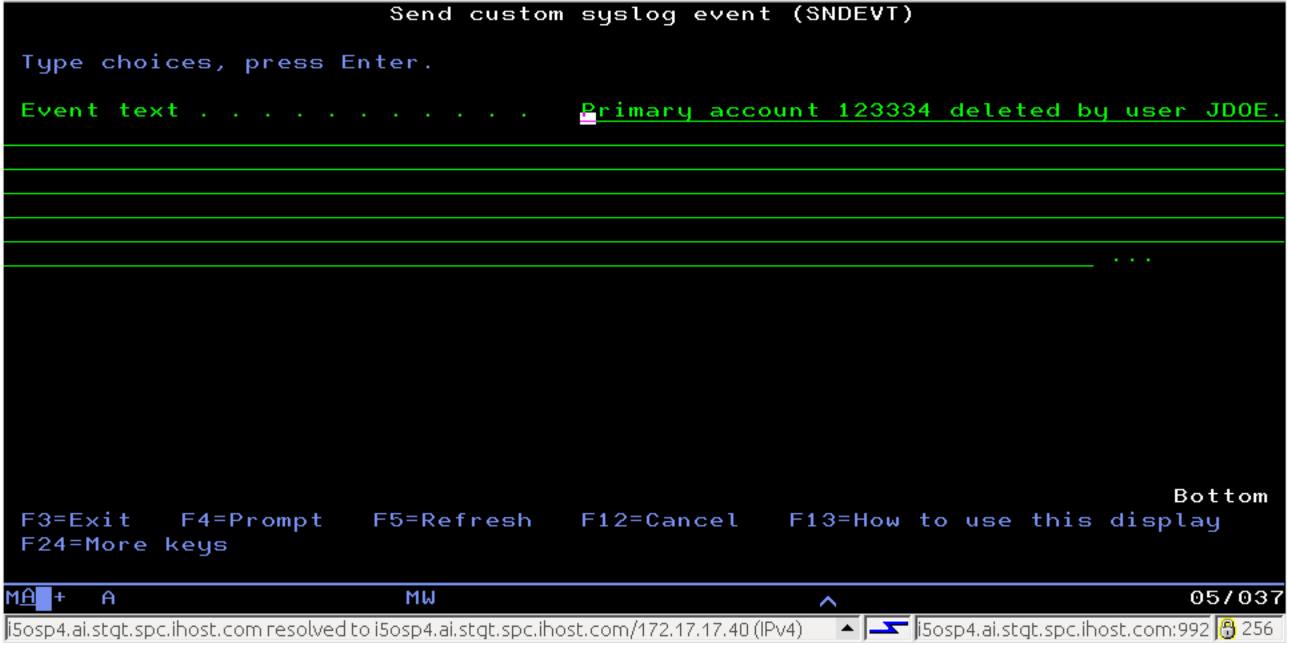
Example of the SNDEVT command with automatic formatting:



```
                        Send custom syslog event (SNDEVT)

 Type choices, press Enter.

 Syslog facility  . . . . . . . .   USER          KERNEL, USER, MAIL, DAEMON...
 Syslog severity  . . . . . . . .   INFO          EMERG, ALERT, CRIT, ERROR...
 Event timestamp  . . . . . . . .   *CURTIME
 SIEM header value  . . . . . . .   BANKING
 Message format type  . . . . . .   *DEFAULT      *DEFAULT, *RAW
 Source user profile name . . . .   *CURUSER      Character value, *CURUSER
 Source qualified job name  . . .   *CURJOB
 Event category . . . . . . . . .   LoanApplication




                                                                        More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA  +  A                        MW                                       08/044
```

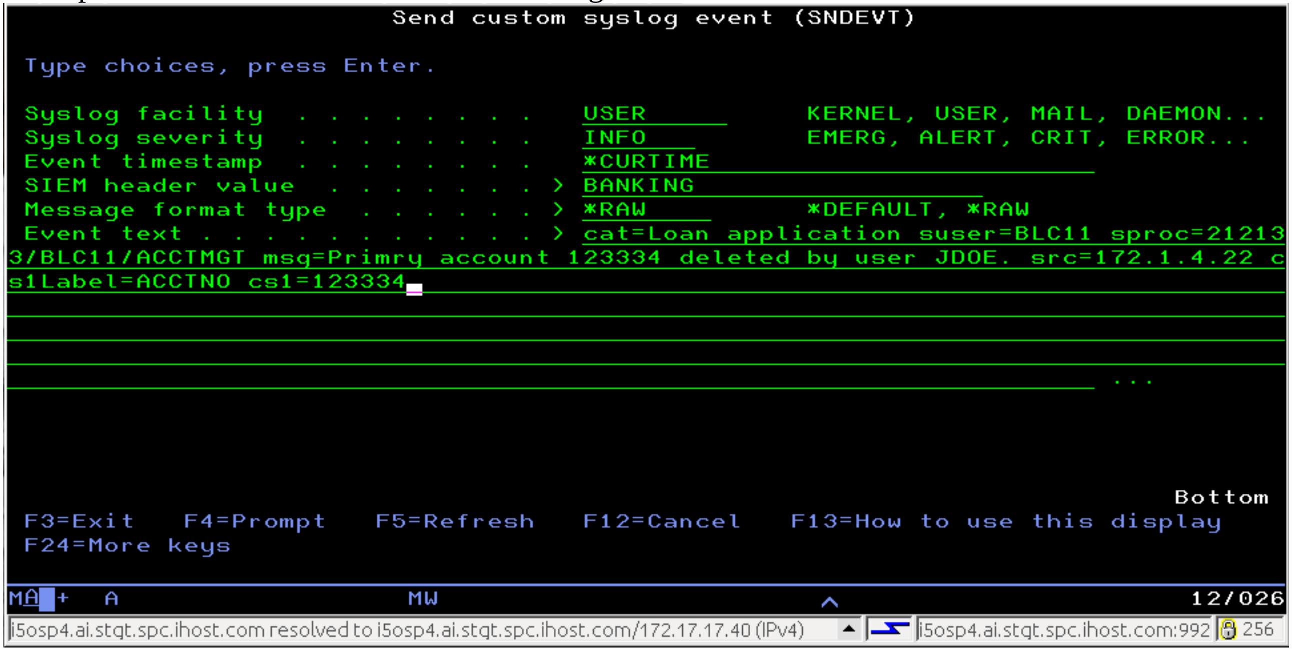
i5osp4.ai.stqt.spc.ihost.com resolved to i5osp4.ai.stqt.spc.ihost.com/172.17.17.40 (IPv4)
i5osp4.ai.stqt.spc.ihost.com:992
256

Second page of command:



```
                       Send custom syslog event (SNDEVT)

 Type choices, press Enter.

 Event text . . . . . . . . . . .   Primary account 123334 deleted by user JDOE.




                                                                      . . .









                                                                          Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA + A                MW                         ^                        05/037
i5osp4.ai.stqt.spc.ihost.com resolved to i5osp4.ai.stqt.spc.ihost.com/172.17.17.40 (IPv4)   i5osp4.ai.stqt.spc.ihost.com:992  256
```

Example of the command with own formatting:



```
                       Send custom syslog event (SNDEVT)

 Type choices, press Enter.

 Syslog facility . . . . . . . .   USER         KERNEL, USER, MAIL, DAEMON...
 Syslog severity . . . . . . . .   INFO         EMERG, ALERT, CRIT, ERROR...
 Event timestamp . . . . . . . .   *CURTIME
 SIEM header value . . . . . . . > BANKING
 Message format type . . . . . . > *RAW         *DEFAULT, *RAW
 Event text . . . . . . . . . . . > cat=Loan application suser=BLC11 sproc=21213
3/BLC11/ACCTMGT msg=Primry account 123334 deleted by user JDOE. src=172.1.4.22 c
s1Label=ACCTNO cs1=123334



                                                                      . . .




                                                                          Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA + A                MW                         ^                        12/026
i5osp4.ai.stqt.spc.ihost.com resolved to i5osp4.ai.stqt.spc.ihost.com/172.17.17.40 (IPv4)   i5osp4.ai.stqt.spc.ihost.com:992  256
```

4.15.2 Sending custom events with ILE procedures

The send custom event ILE procedures that are provided with the Syslog Reporting Manager have the following parameter structures:

Parameter	Type	Used in sendCustomEvent procedure	Used in sendCustomFmtEvent procedure
Syslog Facility	CHAR(9) IN	YES	YES
Syslog Severity	CHAR(7) IN	YES	YES
Timestamp value	CHAR(26) IN	YES	YES
SIEM header	CHAR(20) IN	YES	YES
Source user	CHAR(10) IN	YES	NO
Source job	CHAR(28) IN	YES	NO
Event category	CHAR(100) IN	YES	NO
Event text *1	CHAR(2048) IN	YES	YES
Reserved (*2)	CHAR(33) IN	NO	NO
Return code from proc	INT(5)	YES	YES

*1 = See the description of the parameter in the introduction of this chapter. For the sendCustomFmtEvent procedure, the parameter contains all key-value pairs that are provided by the programmer.
*2 = Parameter can be omitted

>Prototypes and example program information

There is a source physical file shipped with SRM called SOURCES. It contains the prototype definitions for send custom event procedures and an example program on how to use the procedures.

IMPORTANT: If you want to use these sources, copy them to your own source file. The SOURCES file with all its content is overridden during installation or upgrade of the Syslog Reporting Manager.<

Procedure prototypes:

NOTE: An include file with the prototype definitions is in the following file:
QZRDSECSRM/SOURCES Member: SNDEVTINC

```
//-----------------------------------------------------------------------
//Declarations and prototypes for sending a custom event where the

//provided parameter are sent as follows:
//evtHdrSuffix - in the LEEF or CEF header (see intro)
//evtSrcUser - send as suser (CEF) or usrName (LEEF) attribute in the
//             payload
//evtSrcJob  - send as the sproc key in the payload
//evtCategory - send as the cat key in the payload
//evtText    - send as the msg key in the payload
//Formatted means that all key value pairs in the payload of a CEF or
//LEEF message must be set by the caller of the procedure.
//------------------------------------------------------------------------
 dcl-pr   sendCustomEvent  int(5);
    syslogFacility     char(9) value; //Facility (see intro section)
    syslogSeverity     char(7) value; //Severity (see intro section)
```

```
          evtTimestamp        char(26) value;//Event timestamp(see intro section
          evtHdrSuffix        char(20) value;//SIEM header suffix (see intro)
          evtSrcUser          char(10) value;//Source user profile of event
          evtSrcJob           char(28) value;//Qualified job name of sending job
          evtCategory         char(100) value;//event category (see intro)
          evtText             char(2048) value;//Event data (see intro)
          evtSpc              char(33) options(*nopass); //Reserved

       end-pr;



      //-----------------------------------------------------------------------
      //Declarations and prototypes for sending a formatted event text
      //Formatted means that all key value pairs in the payload of a CEF or
      //LEEF message must be set by the caller of the procedure.
      //------------------------------------------------------------------------
       dcl-pr   sendCustomFmtEvent  int(5);
          syslogFacility      char(9) value; //Facility (see intro section)
          syslogSeverity      char(7) value; //Severity (see intro section)
          evtTimestamp        char(26) value;//Event timestamp(see intro section
          evtHdrSuffix        char(20) value;//SIEM header suffix (see intro)
          evtText             char(2048) value;//Event data (see intro)
          evtSpc              char(33) options(*nopass); //Reserved

       end-pr;
```

Coding and compilation information

The library QZRDSECSRM contains the following objects that you need when using the custom procedures.

QZRDSECSRM/SRMBND   *BNDDIR

The following source file contains a program with an example on how to call the send custom event procedures.

QZRDSECSRM/SOURCES   *FILE
        Member: SNDEVT   *RPGLE

After you created the module for your program, use the following command to create the program itself:

```
CRTPGM PGM(MYLIB/SNDMYEVT) BNDDIR(QZRDSECSRM/SRMBND)
```

Performance-optimized custom event procedure

>Some of the Syslog Reporting Manager clients use the send function for custom events to process a higher volume of custom events (i.e. 30000-40000 / minute). The regular sendCustomEvent and sendCustomFmtEvent ILE procedures perform several checks to ensure proper event formatting, debugging options, etc. Of course, these additional checks are costly in terms of CPU cycles. To facilitate the need to send higher volumes of custom events, the sendCustomFmtEvent procedure has been duplicated and optimized for performance. For example, on a Power System model S824 and one processor, the regular sendCustomFmtEvent procedure sent 10000 events in 46 seconds while the performance-optimized procedure sendCustomFmtEventP sent 10000 events in 17 seconds. While this sounds great, the performance optimization comes with a price. All syntax or content checking, payload sanitation, debug logging, etc. has been removed. It is now up to the

implementer to perform thorough checking before calling the sendCustomFmtEventP procedure. It follows the principle “Garbage in – garbage out”.

Note that the performance-optimized custom event procedure is only provided for the sendCustomFmtEvent procedure and not the sendCustomEvent procedure.

DISCLAIMER:

If you select the performance-optimized version of the sendCustomFmtEvent procedure called sendCustomFmtEventP, you are fully responsible for providing a proper payload in the evtText parameter that complies with the selected CEF or LEEF formats. IBM does not provide any support if you experience problems using this version of the procedure. You only get support, assuming you have a valid maintenance agreement, if you experience problems when using the regular sendCustomFmtEvent procedure and this one also causes problems.

```
//-----------------------------------------------------------------------
//Declarations and prototypes for sending a formatted event text
//with the performance-optimized procedure.
//Formatted means that all key value pairs in the payload of a CEF or
//LEEF message must be set by the caller of the procedure.
//------------------------------------------------------------------------
 dcl-pr   sendCustomFmtEventP  int(5);
    syslogFacility     char(9) value; //Facility (see intro section)
    syslogSeverity     char(7) value; //Severity (see intro section)
    evtTimestamp       char(26) value;//Event timestamp(see intro section
    evtHdrSuffix       char(20) value;//SIEM header suffix (see intro)
    evtText            char(2048) value;//Event data (see intro)
    evtSpc             char(33) options(*nopass); //Reserved

 end-pr;
```

If you already use the sendCustomFmtEvent procedure and want to use the performance-optimized version, you just need to replace **sendCustomFmtEvent** with **sendCustomFmtEventP** procedure name and recreate your program.<

4.16 Starting and ending the Syslog Reporting Manager

The tool can be started with the Start Syslog Reporting Manager (STRSRM) command. The command performs the following tasks:

- Check if the Syslog Reporting Manager is already active, if it is check also that the control job is running. If the subsystem is running, but the control job is missing, the start process will restart the subsystem.
- Start the subsystem SLSBS.

The tool can be ended with the End Syslog Reporting Manager (ENDSRM) command. The command performs the following tasks:

- Ends the automatic restart process of the control job.
- Ends all monitor jobs
- Ends all send event jobs
- Ends the SLSBS subsystem

4.17 Autostarting the Syslog Reporting Manager at IPL

All jobs related to the Syslog Reporting Manager run in the SLSBS subsystem. This subsystem has an autostart job which will automatically start all event monitor jobs that have been set to autostart *YES.

To start the Syslog Reporting Manager job environment at IPL, add the following command to your IBM i startup program that is defined in system value QSTRUPPGM.

```
QZRDSECSRM/STRSRM
```

Also grant the user who runs the startup program, usually QPGMR, *USE access to the command and command program. Example:

```
GRTOBJAUT OBJ(QZRDSECSRM/STRSRMP) OBJTYPE(*PGM) USER(QPGMR) AUT(*USE)
GRTOBJAUT OBJ(QZRDSECSRM/STRSRM) OBJTYPE(*CMD) USER(QPGMR) AUT(*USE)
```

4.18 Exporting and importing configuration settings

The Syslog Reporting Manager provides export and import functions to save your configuration settings and restore them when needed. The export function can be used to create a backup of your SRM configuration. The saved configuration can also be used to import the configuration on a different system. That way, you only need to create the configuration once and can then distribute it to other systems you want to monitor.

IMPORTANT: You can only import a configuration on a system that runs the same Syslog Reporting Manager version as on the system where the export operation has been performed.

4.18.1 Exporting the configuration

The export operation saves the following configuration:

- The global configuration:
  - Hostname or IP address of the primary and backup syslog server
  - >Output file for storing events and output file action<
  - Port number of remote syslog server
  - Syslog message tag
  - Starting journal time stamp
  - Syslog format (RFC3164 or RFC5424)
  - Transport protocol (TCP or UDP)
  - Maximum message length
  - SIEM message format (CEF or LEEF)
  - Autostart options for event monitor jobs
  - EOF delays for history and audit monitoring
  - Syslog severity used for all IFS file change events
  - Syslog facility used for all IFS file change event messages
  - Event statistics and reporting option
  - TCP message transfer method
  - Number of send event job
  - Filter for SRM audit monitor originated ZC or ZR object auditing events
  - Certificate path validation
  - Peer certificate check for primary syslog server
  - Wildcard certificate check for primary syslog server
  - Peer certificate check for backup syslog server
  - Wildcard certificate check for backup syslog server
  - >Event code page<
- Audit journal monitor specific configuration
  - Audit journal entry type monitoring status
- History log monitor specific configuration
  - History filter selection definitions
- IFS file monitor specific configuration
  - A list of all IFS files that are currently monitored
  - IFS file filter lists
- >Journal entry monitor specific configuration
  - A list of configured journals that are currently monitored
  - A list of all defined journal entry types for a given journal
  - All ESD formatting defintions
  - Journal entry filter lists<
- Message queue monitor configuration
  - List of message queues to be monitored

- Database change monitor configuration for the Journal Extract Tool integration
  - Global settings related to the interval and processing options for processing Journal Extract Tool tasks
  - Reporting levels related to tables registered in the Journal Extract Tool
  - Processing status of the journals that are registered in the Journal Extract Tool
- Special configuration settings

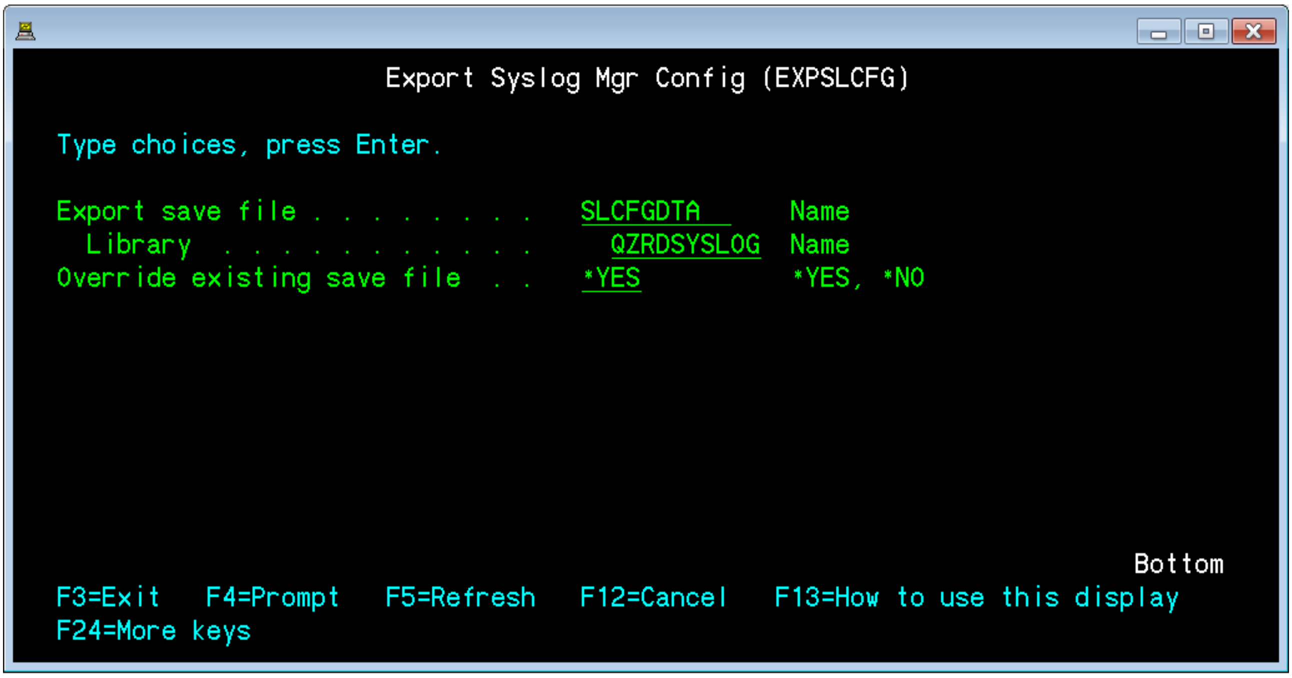
Perform the following steps to export the configuration:

1. Sign on with the SRM administrator and make sure library QZRDSECSRM has been added to the library list.

2. Open the SLMON menu (CFGSRM) and use option 70 (Export configuration) to start the export process.

   Information: Direct access via command: EXPSLCFG

   The exported configuration is saved into a save file. By default, the save file is QZRDSECSRM/SLCFGDTA.



```
                      Export Syslog Mgr Config (EXPSLCFG)

 Type choices, press Enter.

 Export save file . . . . . . . .   SLCFGDTA      Name
   Library  . . . . . . . . . . .     QZRDSYSLOG  Name
 Override existing save file  . .   *YES          *YES, *NO




                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

   If you previously exported the configuration and the save file already contains data, you can leave the override parameter at *YES. This will clear the save file before saving the configuration data.

3. Press **Enter** to export the configuration.

You can now keep the save file as a backup of your configuration or transfer the save file to another system to be used for an import operation.

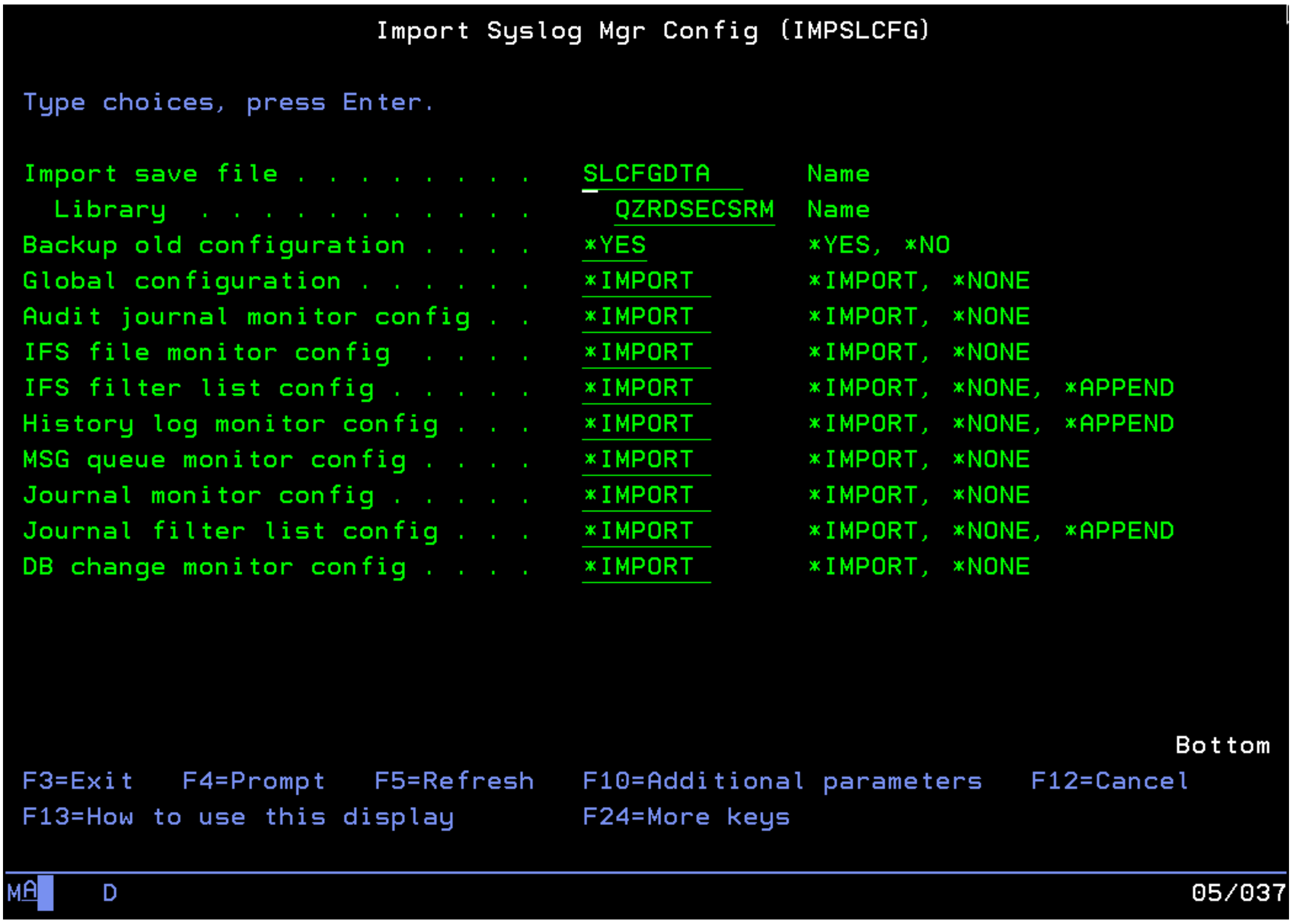
4.18.2 Importing the configuration

IMPORTANT: Importing a configuration is only supported from the same SRM version where the export was performed.

The import configuration process requires that you have the save file that was created by the export configuration process. Perform the following to import the SRM configuration:

1. Sign on with the SRM administrator and make sure library QZRDSECSRM has been added to the library list.
2. Open the SLMON menu (CFGSRM) and use option 71 (Import configuration) to start the import process.

   Information: Direct access via command: IMPSLCFG



```
                     Import Syslog Mgr Config (IMPSLCFG)

 Type choices, press Enter.

 Import save file . . . . . . . .   SLCFGDTA      Name
   Library  . . . . . . . . . . .     QZRDSECSRM  Name
 Backup old configuration . . . .   *YES          *YES, *NO
 Global configuration . . . . . .   *IMPORT       *IMPORT, *NONE
 Audit journal monitor config . .   *IMPORT       *IMPORT, *NONE
 IFS file monitor config  . . . .   *IMPORT       *IMPORT, *NONE
 IFS filter list config . . . . .   *IMPORT       *IMPORT, *NONE, *APPEND
 History log monitor config . . .   *IMPORT       *IMPORT, *NONE, *APPEND
 MSG queue monitor config . . . .   *IMPORT       *IMPORT, *NONE
 Journal monitor config . . . . .   *IMPORT       *IMPORT, *NONE
 Journal filter list config . . .   *IMPORT       *IMPORT, *NONE, *APPEND
 DB change monitor config . . . .   *IMPORT       *IMPORT, *NONE




                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys

MA    D                                                                  05/037
```

Important information for Journal Extract Tool configuration data:

The import process adds all exported table and process journal entries to the corresponding Syslog Reporting Manager tables. However, if the actual tables or journals are not defined in the AUDITOBJ or PROCTRACK tables of the Journal Extract Tool, the entries get deleted from the Syslog Reporting Manager integration tables.

- Specify the library and name of the save file that has been created by the export configuration process.
- By default, the import process will save the current configuration prior to importing the new configuration. The configuration is saved into save file QZRDSECSRM/IMPBACKUP.
- Specify whether you want to import (*IMPORT) the following configuration values:

  - Hostname or IP address of the primary and backup syslog server
  - >Output file for storing events and output file action<
  - Port number of remote syslog server
  - Syslog message tag
  - Starting journal time stamp
  - Syslog format (RFC3164 or RFC5424)
  - Transport protocol (TCP, UDP, or TLS)
  - Maximum message length
  - SIEM message format (CEF or LEEF)
  - Autostart options for event monitor jobs
  - EOF delays for history and audit monitoring
  - Syslog severity used for all IFS file change events
  - Syslog facility used for all IFS file change event messages
  - Status whether you want statistical events to be collected and sent
  - TCP message transfer method
  - Number of send event jobs
  - Filter for SRM audit monitor originated ZC or ZR object auditing events
  - Certificate path validation
  - Peer certificate check for primary syslog server
  - Wildcard certificate check for primary syslog server
  - Peer certificate check for backup syslog server
  - Wildcard certificate check for backup syslog server
  - >Event code page (CCSID)<

  NOTE: The `*IMPORT` option will override all existing values.

- Specify whether you want to import (`*IMPORT`) the following audit journal event configuration values:

  - Audit journal entry type monitoring status. The monitoring status determines what journal entry types will be monitored.

  NOTE: The `*IMPORT` option will override all existing values.

- Specify whether you want to import (`*IMPORT`) the IFS file names that have been actively monitored on the system where the export operation was performed:

  - For IFS files that have been monitored on the system where the export was performed, the import process will try to add all IFS file names to the monitor list. In fact, the files will be added to be journaled by the IFSJRN journal. If a file is already monitored or the file does not exist, the IFS file is skipped.

- Specify whether you want to import (`*IMPORT`) or append non-existing IFS file filter lists that have been defined on the system where the export operation was performed:
  - *IMPORT – All exported IFS file filter lists are imported. Existing ones are overridden.
  - *APPEND - Only IFS file filter lists that do not exists on the system where you run the import command are added. Existing filter lists are not overridden.

  NOTE: The `*IMPORT` option will override all existing values.

- >Specify whether you want to import (*IMPORT) the journal monitor definitions that have been actively monitored on the system where the export operation was performed:
  - The import option restores the:
    - configured journal objects including all journal specific settings
    - defined journal entry types including their specific settings
    - journal entry specific data (ESD) formatting information

- Specify whether you want to import (*IMPORT) or append non-existing journal entry filter lists that have been defined on the system where the export operation was performed:
  - *IMPORT – All exported journal file filter lists are imported.
  - *APPEND - Only journal entry filter lists that do not exists on the system where you run the import command are added. Existing filter lists are not overridden.

  NOTE: The *IMPORT option will override all existing values.<

- Specify whether you want to import (*IMPORT) the following message queue monitoring configuration values:

  - Global configuration values about the collection and reporting interval, the number of days that messages are kept on the system, and the message queue that the message queue monitor process used.
  - The list of message queues that are monitored by the message queue monitoring process.

  NOTE: The *IMPORT option will override all existing values.

- Specify whether you want to import (*IMPORT) the following database change monitoring configuration values:

  - Global configuration values:
    - Enable DB event processing
    - Global syslog information level
    - Journal processing interval
    - Drop tables before processing
    - Clear data tables before processing
    - Clean up non-existing objects
  - The list of tables that have been defined for database journal processing
    Note: If a journal has not been added to the AUDITOBJ Journal Extract Tool table prior to running the import, the entries are not imported.
  - The list of journals that will be processed
    Note: If a journal has not been added to the PROCTRACK Journal Extract Tool table prior to running the import, the entries are not imported.

  NOTE: The *IMPORT option will override all existing values.

- Specify the import operation for special function settings. Besides not importing values (option *NONE) you can specify the following additional option:

  - ***IMPORT**

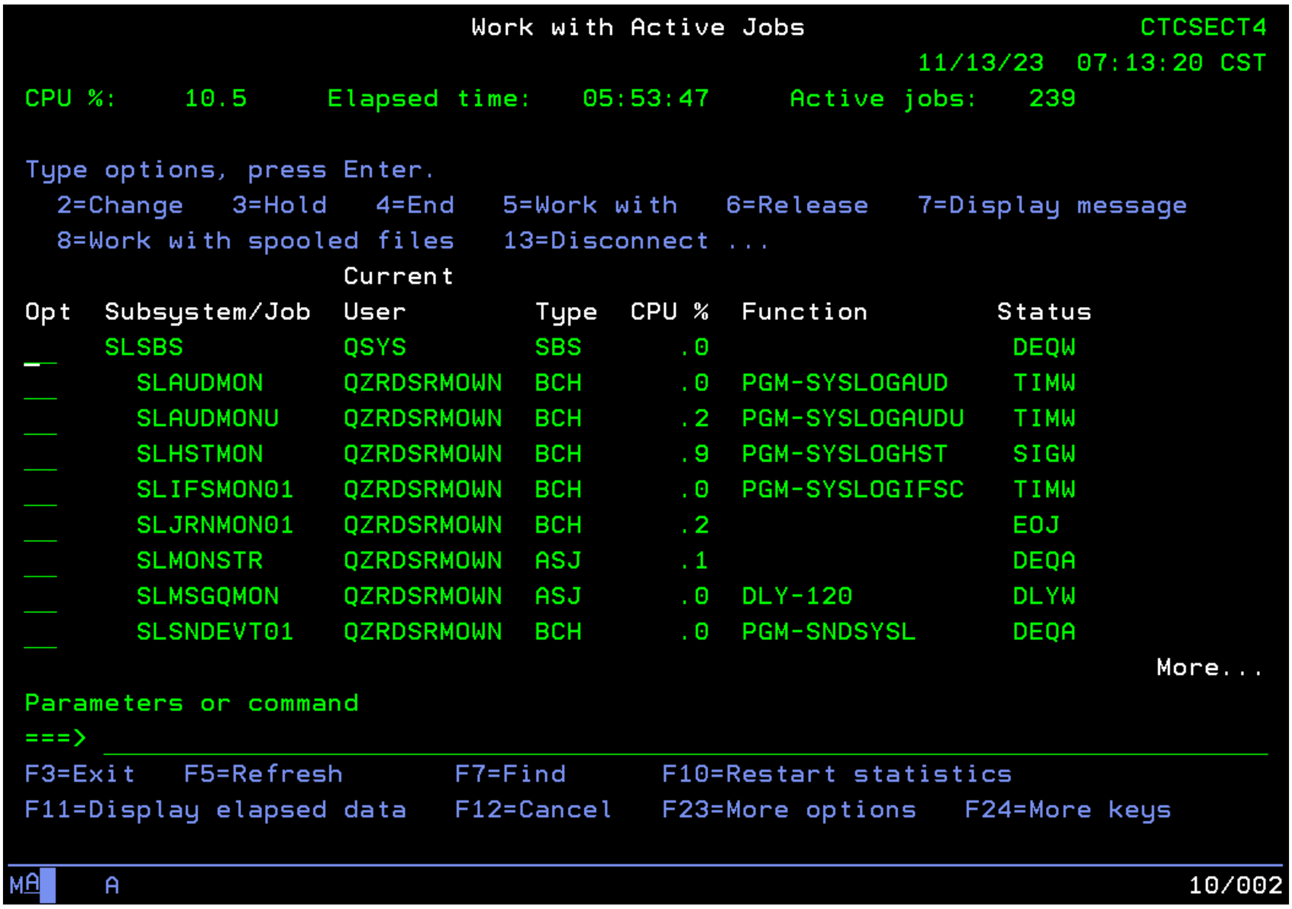
    The value specifies that the special function configuration will be imported. All existing function settings will be overridden.

3. Press **Enter** to start the import process.

5 Managing the job environment

As previously stated, it is recommended to automatically start the subsystem QZRDSECSRM/SLSBS at IPL time via the system startup program. During the subsystem start, the control monitor job will start all event monitor jobs that have specified *YES for the autostart parameter.

If all jobs are running, the WRKACTJOB SBS(SLSBS) command output looks like the following:



```
                           Work with Active Jobs                    CTCSECT4
                                                         11/13/23  07:13:20 CST
CPU %:     10.5     Elapsed time:   05:53:47     Active jobs:   239

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect ...
                             Current
Opt  Subsystem/Job  User         Type  CPU %  Function        Status
__   SLSBS          QSYS         SBS      .0                   DEQW
__     SLAUDMON     QZRDSRMOWN   BCH      .0  PGM-SYSLOGAUD    TIMW
__     SLAUDMONU    QZRDSRMOWN   BCH      .2  PGM-SYSLOGAUDU   TIMW
__     SLHSTMON     QZRDSRMOWN   BCH      .9  PGM-SYSLOGHST    SIGW
__     SLIFSMON01   QZRDSRMOWN   BCH      .0  PGM-SYSLOGIFSC   TIMW
__     SLJRNMON01   QZRDSRMOWN   BCH      .2                   EOJ
__     SLMONSTR     QZRDSRMOWN   ASJ      .1                   DEQA
__     SLMSGQMON    QZRDSRMOWN   ASJ      .0  DLY-120          DLYW
__     SLSNDEVT01   QZRDSRMOWN   BCH      .0  PGM-SNDSYSL      DEQA
                                                                    More...
Parameters or command
===> ________________________________________________________________________
F3=Exit   F5=Refresh        F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys

MA     A                                                                10/002
```

The purpose of each job is:

Job name	Description
SLAUDMON	Audit journal event monitor job. It retrieves all operating system provided audit journal entry types (journal code T) that have been enabled with the CFGSLAUD command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server.
SLAUDMONU	Audit journal event monitor job. It retrieves all user generated audit journal entry types (journal code U) that have been enabled with the CFGSLAUD command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server. If no event types of source event category *USR have been enabled, the monitor job automatically ends and needs to be manually restarted when user type entries are added and enabled for processing.
SLHSTMON	QHST history log event monitor job. It retrieves all history log entries that have been enabled with the CFGSLHST command and sends the CEF- or LEEF-formatted syslog messages to the specified syslog server. If no history log selection rule is enabled, all received history log events are processed.
SLIFSMONnn	IFS file change monitor job. The IFS file change monitoring is using the configured and enabled journals to feed the monitor job. Every IFS file that needs to be monitored for changes, are added to

	be journaled via one of the configured journals. The command to configure the IFS file monitoring is CFGSLIFSJ (managing journals) and CFGSLIFS (managing monitored files for a selected journal). A separate job is started for each configured and enabled journal.
>SLJRNMONnn	Journal entry monitor job. The journal monitoring is using the configured and enabled journals to feed the monitor job. Every journal that needs to be monitored for new entries, are added to be journaled via one of the configured journals. The command to configure the journal entry monitoring is CFGSLJRNJ (managing journals) and CFGSLJRN (managing monitored entry types for a selected journal), and CFGSLJRNEF to define the formatting of the journal entry specific data (ESD). A separate job is started for each configured and enabled journal.<
SLMONSTR	This is the control monitor job that is auto-started when the subsystem SLSBS starts or by using the STRSRM command. It submits the event monitor jobs at startup for event monitor jobs that have specified autostart *YES. It also monitors all started jobs and if one event monitor job fails, it will restart the event monitor job. If an event monitor job is ended with the ENDSLMON command, job monitoring ends and no new event monitor job is submitted. The control monitor job also contains detailed messages about all event monitor job activities, such as restarting an event monitor job.
SLSNDEVT01-50	This job is the communication job that processes events that were reported by the various monitor jobs. It establishes a communication via UDP/IP or TCP/IP or TLS (over TCP) to a configured syslog or SIEM server and sends the events to the remote host. There can be 1 to 50 of these send event jobs in subsystem SLSBS. The number of started send event jobs can be configured with the CFGSLENV command. The SLSNDEVTx jobs restart every 12 hours to perform some housekeeping tasks.
SLMSGQMON	The SLMSGQMON job is the scheduling job of the message queue monitor part of the tool. It runs the analysis of the monitored message queues at the interval that is configured with the CFGSLMQM command. The analysis job name is SLMSQMONS and is also active in the SLSBS subsystem as long as the analysis lasts.
SLDB2MON	This job is started by the control monitor job at the interval defined in the CFGJSGLB command. It processes the database journal change events that have been collected by the Journal Extract Tool. This job is only active as long as the analysis lasts.

If a configuration command, such as CFGSLAUD command is used to change a configuration, the event monitor job is restarted to pick up the changed configuration.

5.1 Send job recovery and restart information

>The SLSNDEVTnn jobs are responsible for sending the captured events to the configured remote syslog server. The jobs take the events from the SNDSYSLQ data queue and establish the connection to the remote syslog server. The send jobs are staying active for 12 hours and then get restarted for housekeeping purposes (temporary storage, etc.). This is a normal behavior.

In case of communication problems, i.e. the remote syslog server is down or a communication link failure, the send jobs tries 5 times to reestablish the connection and send an event. If the job is not able to send the events, the job ends and a recovery process is initiated by the SLMONSTR job (see next section).<

5.2 SRM job recovery information

>The Syslog Reporting Manager (SRM) control job SLMONSTR is responsible for starting, ending, and recovering all SRM monitor and send jobs. For example, when the STRSLMON command is run to start a monitor, the SLMONSTR will submit the job and monitors the job that it stays up and running until ended by the corresponding ENDSLMON or ENDSRM command.

Monitor and send jobs normally run and perform their jobs. However, in some situations, i.e. the communication link is down and the send jobs cannot send any more events or someone deleted the IFS journal for IFS file monitoring, a monitor or send job could fail. If this happens, the control job tries to restart the failing jobs after approx. 5 seconds. If the job fails again, the control job tries to restart the failing job up to 10 times. If the restart fails 10 times, the control jobs pauses 10 minutes for the failing job and then starts the recovery process (trying to restart 10 times) again. This process has been implemented to ensure SRM continuous operations.

The maximum number of restart attempts and the pause between the recovery phases cannot be changed via regular configuration commands. If jobs keep failing there is a reason for this and this reason must be debugged and solved. In case the number of restart attempts and pause interval need to be changed, contact IBM Technology Expert Labs. There is a custom configuration option to change these timers.<

5.3 Send event process information

>This section provides some background information about the process of extracting and sending monitored events. The Syslog Reporting Manager (SRM) uses internally data queues to communicate between the different jobs. A critical role has the SNDSYSLQ data queue. It is defined to grow to the maximum of 2GB. Considering a maximum event size of roughly 64000 bytes, the queue can hold up to 33100 event entries. Each monitor job, i.e. audit journal monitor or history log monitor, extracts the events from its log source, formats the events according to the setup, and sends the event to the SNDSYSLQ data queue. The SLSNDEVT01-50 jobs are the communication jobs that take the events from the SNDSYSLQ data queue, establish a connection to the configured syslog server, and send the events to the syslog server. In a normal environment the events are taken from the data queue in a very short amount of time and the data queue size is relatively small. In case of network or communication problems to the configured syslog server or problems at the syslog server, the SLSNDEVT1-50 jobs cannot send any event anymore. In this case the monitor jobs keep filling up the SNDSYSLQ data queue but the send jobs cannot take any events from the queue. Eventually the queue will be full and the monitor jobs cannot put additional events on the queue. The monitor jobs will then retry to send the events and eventually give up after 10 retries and end. The SLMONSTR job monitors the SNDSYSLQ data queue size. If the size grows up to 75% of its maximum, it starts sending message SLE0326 to the QSYSOPR message queue and the history log every 10 minutes. If the size reaches 85% the job sends this message every 2 minutes. It is now up to the system administrator or responsible person to start debugging the situation. The configured syslog server must be reachable and responsive. If this is not the case, the problem should be solved soon. If the data queue size reaches 97%, the SLE0326 message is not only sent to QSYSOPR and the history log but also generates an audit journal entry and then ends SRM. At this point the issues communicating to the syslog server must be analyzed and solved. You can then restart SRM. After SRM starts, it tries to send the events from the SNDSYSLQ data queue to the remote syslog server for 2 minutes. If the size decreases below 97% SRM stays active and keeps processing events. If the size does not decrease, there is still a problem and SRM ends again.

Note: If the size of the data queue increases you should also check the SLSNDEVTnn jobs in subsystem SLSBS. For example, if you have two send jobs active and the status is constantly RUN, it means that more events are put onto the queue than the two send jobs can send. In this case you might want to consider increasing the number of send jobs with the CFGSLENV command. This increases parallel processing of sending events.<

5.4 Manually starting and stopping event monitor jobs

There are two commands that are used to manually start and stop event monitor jobs. Each command has three valid parameter values:

- ***AUDMON** Monitor job for audit journal event processing
- ***HSTMON** Monitor job for history log event processing
- ***IFSMON** Monitor job for IFS file change event processing
- >***JRNMON** Monitor job for journal entry event processing<
- ***MSGMON** Monitor job for message queue event processing
- ***SNDEVT** Restarts any missing send event jobs. The number of missing send event jobs is determined by actual number or active SLSNDEVTn jobs and the number of configured send event jobs.

Starting

```
STRSLMON    MONJOB(*AUDMON)
```

Stopping

```
ENDSLMON    MONJOB(*AUDMON)
```

Note that the start and end process can take a while due to current processing activities or delays. All start and end requests are passed to the control monitor job and handled by this job.

6 Special function settings

Starting with SRM V1R1M2, special function settings are supported. These settings are not configurable via regular configuration commands as they can have a significant impact on base functions of the tool. Wrong usage of such functions might cause the tool to not function properly. Currently, the following special functions are implemented:

- Disable ICMP connectivity check to the configured remote syslog/SIEM server.
- Adjust the maximum number of automatic job restart attempts for monitor jobs that fail.
- Sending the event timestamp in the syslog header and as part of the message payload opposed to the default behavior from SRM 1.2.0 that only sends the event timestamp as part of the syslog header and not the payload.
- Adjust the idle timeout value for TCP connections.
- Change the default delimiter character of key-value pairs in a LEEF message. The default is ASCII HEX 09 (TAB character) as defined in the LEEF specifications.
- Enabling debugging.
- Changing the timestamp of the last processed event for the various monitor jobs.
- Changing the time between job recovery attempts.
- Changing the Digital Certificate Manager default client application name

Contact your IBM Technology Expert Labs contact to get instructions on how to change the listed properties.

7 CEF and LEEF key mapping information

The following table shows the key names that are used for the various information units in a SIEM message in the Common Event Format (CEF) and Log Event Extended Format (LEEF). It also provides a short description of each element.

The information in the table lists the standard elements that are used by SRM audit, history, and IFS monitoring. The custom event message as used by the SNDEVT CL command or the sndevent* procedures might also use the keys but their use is up to the programmer who uses the command or procedures.

CEF key	LEEF key	Usage in Monitor	Description
act	act	IFS DB2	IFS: Device action that was carried out. This is a B_WA Write action. DB2: Contains the action that was performed on a database table (INSERT, DELETE, UPDATE)
cat	cat	CUS / MSG	CUS: Event category as provided in the raw message format of the custom event or the CAT parameter of the SNDEVT command. MSG: The message queue monitoring category "MSG Queue Messages".

cs1Label= changedData
cs1=value
	changedData	IFS	IFS: The actual data that has been changed in the monitored IFS file. Depending on the maximum message size that is allowed to be sent, the data in this value can be truncated. If truncation occurs, a corresponding text is added at the end of the value.

cs2Label= changedDataLength
cs2=value
	changedDataLength	IFS	IFS: Length in bytes of the data that was changed

cs3Label= changedDataPart
cs3=value
	changedDataPart	IFS	IFS: Depending on the size of the changed data in the monitored IFS file, the change can span one or more IFS journal entries. If it spans across multiple entries, the changedDataPart indicates if it is the first (*FIRST) packet of a change that spans multiple entries, if is is a part in the middle (*MIDDLE) of a change that spans multiple entries, if it is the last (*LAST) part of a change that spans multiple entries, or if is the only (*ONLY) part indicating that the entire change is provided in a single journal entry.

cs4Label= changedDataFileOffset
cs4=value
	changedDataFileOffset	IFS	IFS: Offset within the changed IFS file where the changed data start in the length as identified in changedDataLength.

deviceExternalId	deviceExternalId	AUD	AUD: Device name (extracted from ENTRY_DATA column)
dloName	dloName	AUD	AUD: Document Library Object name (DLO_NAME column)
dloPath	dloPath	AUD	AUD: Document Library Object folder path (FOLDER_PATH column)
dproc	dproc	AUD	AUD: Destination job (process) name (extracted from ENTRY_DATA column)
duser	duser	AUD	AUD: Destination user name (extracted from ENTRY_DATA column)

>entryTypeField	entryTypeField	AUD	AUD: For system audit journal types (journal code T), this value contains the Entry Type 1 character value for a specific audit journal entry type. This 1 character field follows a journal entry header and has a different meaning for each entry type. The CFGSLAUD command let’s you define filters for the entry type field.<
filePath	filePath	AUD / IFS	AUD: IFS stream file path (PATH_NAME column) IFS: IFS stream file path of the file that has been changed (directory path including file name).
fileType	fileType	AUD / IFS	AUD: Object type (OBJECT_TYPE column) IFS: Object type of IFS file path.
fname	fname	AUD/ IFS DB2	AUD: IFS stream file name (OBJECT_FILE_NAME column) >IFS: IFS stream file name of the file that has been changed (file name only).< DB2: DB2 table name as monitored by the Journal Extract Tool.
msg	msg	HST / AUD / MSG	AUD: Additional information from the audit record not included in other keys (extracted from ENTRY_DATA column) HST: The message text (MESSAGE_TEXT column) from the history log message MSG: The message as received from the monitored message queue
cs1Label= objName & cs1=values	objName	AUD	AUD: Object name (OBJECT column)
oldDloName	oldDloName	AUD	AUD: Document Library Object name (before rename) (extracted from ENTRY_DATA column)
oldDloPath	oldDloPath	AUD	AUD: Document Library Object folder path (before rename) (extracted from ENTRY_DATA column)
oldFileName	oldFileName	AUD	AUD: FS stream file name (before rename) (extracted from ENTRY_DATA column)
oldFilePath	oldFilePath	AUD	AUD: IFS stream file path (before rename) (extracted from ENTRY_DATA column)
cs2Label= oldObjName & cs2=values	oldObjName	AUD	AUD: Object name (before rename) (extracted from ENTRY_DATA column)
cs7Label= attrName	attrName	AUD	AUD: Attribute name of the value that is changed. Used in the system audit entry types

& cs7=value			AU, EV, and IP.
cs8Label= attrValue & cs8=value	attrValue	AUD	AUD: Value of the attribute that is listed in the cs7Label=attrName/attrName keys. This key is used with system audit entry types AU and EV.
cs9Label= oldAttrValue & cs9=value	oldAttrValue	AUD	AUD: Contains the old value before the change of the attribute that is listed in the cs7Label=attrName/attrName keys. This key is used with system audit entry type AU.
reason	reason	AUD / HST / CUS / MSG	AUD: Text description of the audit journal entry HST: Text description of the history log message CUS: In a custom event, reason contains the entire event text to be sent. MSG: The message ID of the monitored message.
rt (receiptTime)	devTimeFormat=YYYY-MM-dd-HH.mm.ss.SSSSSS devTime=	DB2 MSG	DB2: The timestamp of the time when the database change has occurred. The timestamp of the message in the monitored message queue.
shost	resource	AUD / IFS / DB2 / MSG	AUD: Source system (host) name (SYSTEM_NAME column) IFS: Source system (host) name DB2: Source system (host) name MSG: The hostname of the system where the monitored message was created. Note: The reported host name is the one as define with CHGNETA parameter SYSNAME.
sproc	sproc	AUD / HST / IFS / DB2 / MSG / CUS	AUD: Source job (process) name (JOB_NAME, JOB_USER, JOB_NUMBER columns) HST: The qualified job name (FROM_JOB column) from the history log message IFS: The qualified job name of the job that performed the IFS file change. DB2: The qualified job name of the job that performed the database table change. MSG: The qualified job name of the job that sent the message to the monitored message queue. CUS: If source job *CURJOB, the value contains the qualified job name of the job sending the event.

spt	srcPort	AUD	AUD: Source port number (REMOTE_PORT column)
src	src	AUD	AUD: Source IP address (REMOTE_ADDRESS column)
suser	usrName	AUD / HST / IFS / DB2 / MSG / CUS	AUD: Source user name (CURRENT_USER column) HST: Current user name (FROM_USER column) from the history log message IFS: Current user name from the user that performed the IFS file change. DB2: Current user name from the user that performed the database table change. MSG: The user profile name of the user who sent the message to the monitored message queue. CUS: If source user *CURUSER, the value contains the user profile name of the current user sending the event.
>userProfile	userProfile	AUD	AUD: This key is reported for system audit journal events (T-journal code) for journal entry types PW and SO and specifies the user profile or SST user that caused the authentication error (PW entry) or server authentication entry that was managed (SO entry). <
cs1Label= pgmName & cs1=value	pgmName	DB2	DB2: The name of the program that was used to perform the change in the monitored database table.

cs2Label=updatedColumnNames
&
cs2=values
	updatedColumnNames	DB2	When an UPDATE action was performed on a monitored database table, the key value contains the names of the columns that have been updated.

cs3Label=memberName
&
cs3=values
	memberName	DB2	When an INSERT or DELETE action was performed on a monitored database table, the key value contains the name of the database table member name that has been changed.

cs4Label=rowData
&
cs4=values
	rowData	DB2	The key value contains all columns and their values including the Journal Extract Tool columns that identify the used journal receiver, sequence number, etc. of the rows that are added (INSERT), deleted (DELETE), or for updates (UPDATE) where only the before or after image is captured.

cs4Label=rowData	rowDataAfter	DB2	The key value contains only the columns and

After & cs4=values			their values of the data after the data has been changed for updates (UPDATE) where both the before and after image is captured.

cs5Label=rowDataBefore
&
cs5=values
	rowDataBefore	DB2	The key value contains only the columns and their values of the data before the data has been changed for updates (UPDATE) where both the before and after image is captured.

cs1Label= msgSev & cs1=value	msgSev	MSG	The message severity text representation of the severity. The IBM i message severity is reported as follows: - Severity 0 as INFO - Severity 10 as NOTICE - Severity 20 as WARNING - Severity 30 and higher as ERROR
cs2Label= msgQueue & cs2=value	msgQueue	MSG	Library and name of the monitored message queue that contains the reported event.
cs3Label= pgmName & cs3=value	pgmName	MSG	The program that sent the message to the monitored message queue.
cs4Label= srdb & cs4=value	srdb	MSG	The relational database name of the system where the monitored message queue exists.
>deviceInterface	deviceInterface	JRN	QIPFILTER journal M-TF entry line description name
deviceDirection	ipfilterDirection	JRN	QIPFILTER journal M-TF entry IP Filter Direction (I=Inbound / O=Outbound)
act	ipfilterAction	JRN	QIPFILTER journal M-TF entry IP Filter Action
proto	proto	JRN	QIPFILTER journal M-TF entry IP Transport Protocol Number
src	ipfilterSrcAddr	JRN	QIPFILTER journal M-TF entry Source IP Address
spt	ipfilterSrcPort	JRN	QIPFILTER journal M-TF entry Source IP Port
dst	ipfilterDstAddr	JRN	QIPFILTER journal M-TF entry Destination IP Address
dpt	ipfilterDstPort	JRN	QIPFILTER journal M-TF entry Destination IP Port
sourceServiceName	sourceServiceName	JRN	Journal monitor source of event, i.e. QUSRSYS/QIPFILTER journal or QSYS/QACGJRN journal
pgmName	pgmName	JRN	All journal events. Describes the program name that generated the event.
fileLib	fileLib	JRN	If the processed monitored journal entry is for a

			physical file / table, the key value identifies the library where the file is stored.
fileName	fileName	JRN	If the processed monitored journal entry is for a physical file / table, the key value identifies the name of the file / table that relates to the journal entry.
fileMember	fileMember	JRN	If the processed monitored journal entry is for a physical file / table, the key value identifies the member name of the file that relates to the journal entry.
jobName	jobName	JRN	QACGJRN journal A-JB, A-SP, A-DP entry job name
jobUser	jobUser	JRN	QACGJRN journal A-JB, A-SP, A-DP entry job user
jobNumber	jobNumber	JRN	QACGJRN journal A-JB, A-SP, A-DP entry job number
accountingCode	accountingCode	JRN	QACGJRN journal A-JB, A-SP, A-DP entry job accounting code
processingTime	processingTime	JRN	QACGJRN journal A-JB entry Processing unit time used (in milliseconds)
numRoutingSteps	numRoutingSteps	JRN	QACGJRN journal A-JB entry Number of routing steps
jobEntryDate	jobEntryDate	JRN	QACGJRN journal A-JB entry Job entry date (mmddyy format)
jobEntryTime	jobEntryTime	JRN	QACGJRN journal A-JB entry Job entry time (hhmmss format)
jobStartDate	jobStartDate	JRN	QACGJRN journal A-JB entry Job start date (mmddyy format)
jobStartTime	jobStartTime	JRN	QACGJRN journal A-JB entry Job start time (hhmmss format)
totalTransactionTime	TotalTransaction Time	JRN	QACGJRN journal A-JB entry Total transaction time (in seconds)
numTransactions	numTransactions	JRN	QACGJRN journal A-JB entry Number of transactions
SyncAuxIODb Ops	syncAuxIODbOps	JRN	QACGJRN journal A-JB entry Synchronous auxiliary I/O operations and DB operations (including page faults for any reason)
jobType	jobType	JRN	QACGJRN journal A-JB entry job type
complCode	complCode	JRN	QACGJRN journal A-JB entry Completion code
numPrintLines	numPrintLines	JRN	QACGJRN journal A-JB entry Number of print lines

numPrintPages	numPrintPages	JRN	QACGJRN journal A-JB entry Number of printed pages
numPrintFiles	numPrintFiles	JRN	QACGJRN journal A-JB entry Number of print files
numDbWriteOps	numDbWriteOps	JRN	QACGJRN journal A-JB entry Number of database write operations
numDbReadOps	numDbReadOps	JRN	QACGJRN journal A-JB entry Number of database read operations
numDbUpdDelOps	numDbUpdDelOps	JRN	QACGJRN journal A-JB entry Number of database update, delete FEOD, release, commit, and rollback operations
numComWriteOps	numComWriteOps	JRN	QACGJRN journal A-JB entry Number of communications write operations
numComReadOps	numComReadOps	JRN	QACGJRN journal A-JB entry Number of communications read operations
timeJobActive	timeJobActive	JRN	QACGJRN journal A-JB entry Time job was active (in milliseconds)
timeJobSuspended	timeJobSuspended	JRN	QACGJRN journal A-JB entry Time job was suspended (in milliseconds)
timestampJobEntry	timestampJobEntry	JRN	QACGJRN journal A-JB entry Timestamp job entered system (mmddyyyyhhmmss)
timestampJobStart	timestampJobStart	JRN	QACGJRN journal A-JB entry Timestamp job started (mmddyyyyhhmmss)
AsyncIoDbNonDbOps	AsyncIoDbNonDbOps	JRN	QACGJRN journal A-JB entry Asynchronous I/O for database and non-database operations
expCpuTime	expCpuTime	JRN	QACGJRN journal A-JB entry Expanded CPU time used
expSynAuxIoOps	expSynAuxIoOps	JRN	QACGJRN journal A-JB entry Expanded synchronous auxiliary I/O operations
expAsynAuxIoOps	expAsynAuxIoOps	JRN	QACGJRN journal A-JB entry Expanded asynchronous auxiliary I/O operations
expNumDbPut	expNumDbPut	JRN	QACGJRN journal A-JB entry Expanded number of database puts
expNumDbGet	expNumDbGet	JRN	QACGJRN journal A-JB entry Expanded number of database gets
expNumDbUpdDel	expNumDbUpdDel	JRN	QACGJRN journal A-JB entry Expanded number of database updates and deletes
expNumLinesPrinted	expNumLinesPrinted	JRN	QACGJRN journal A-JB entry Expanded number of lines printed
ExpNumPages	ExpNumPages	JRN	QACGJRN journal A-JB entry

Printed	Printed		Expanded number of pages printed
expNumPrintFiles	expNumPrintFiles	JRN	QACGJRN journal A-JB entry Expanded number of print files
devFileName	devFileName	JRN	QACGJRN journal A-SP, A-DP entry Device file name
devFileLib	devFileLib	JRN	QACGJRN journal A-SP, A-DP entry Library in which device file is stored
devName	devName	JRN	QACGJRN journal A-SP, A-DP entry Device name
devType	devType	JRN	QACGJRN journal A-SP, A-DP entry Device type
devModel	devModel	JRN	QACGJRN journal A-SP, A-DP entry Device model
totalNumPrint Pages	totalNumPrintPages	JRN	QACGJRN journal A-SP, A-DP entry Total number of print pages produced
totalNumPrintLines	totalNumPrintLines	JRN	QACGJRN journal A-SP, A-DP entry Total number of print lines produced
splFileName	splFileName	JRN	QACGJRN journal A-SP entry Spooled file name
splFileNum4	splFileNum4	JRN	QACGJRN journal A-SP entry Spooled file number (JASPNB)
outputPrio	outputPrio	JRN	QACGJRN journal A-SP entry Output Priority
formType	formType	JRN	QACGJRN journal A-SP entry Form type
totalBytesSentPrt	totalBytesSentPrt	JRN	QACGJRN journal A-SP entry Total number of bytes sent to the printer
userData	userData	JRN	QACGJRN journal A-SP, A-DP entry Print user data
splFileNum6	splFileNum6	JRN	QACGJRN journal A-SP entry Spooled file number (JALSPN)
splFileSysnam	splFileSysnam	JRN	QACGJRN journal A-SP entry Spooled file job system name
splFileCrtDate	splFileCrtDate	JRN	QACGJRN journal A-SP entry Spooled file create date (cyymmdd format)
splFileCrtTime	splFileCrtTime	JRN	QACGJRN journal A-SP entry Spooled file create time (hhmmss format)
devFileAsp	devFileAsp	JRN	QACGJRN journal A-SP entry ASP name for device file library
Custom keys	*Custom keys*	*JRN*	*For journals that an administrator adds, the administrator defines its own key names in the Entry Specific Data formats.* <

The “Usage in Monitor” column values specify:
AUD = Events that are monitored by the QAUDJRN audit journal
HST = Events that are monitored by the history log monitor
IFS = Events that are monitored by the IFS file change monitor
DB2 = Events that are generated by the DB2 Journal Extract Tool integration
MSG = Message queue monitoring events
>JRN = Events that are monitored by the general journal monitor<

8 Transport Layer Security (TLS) implementation information

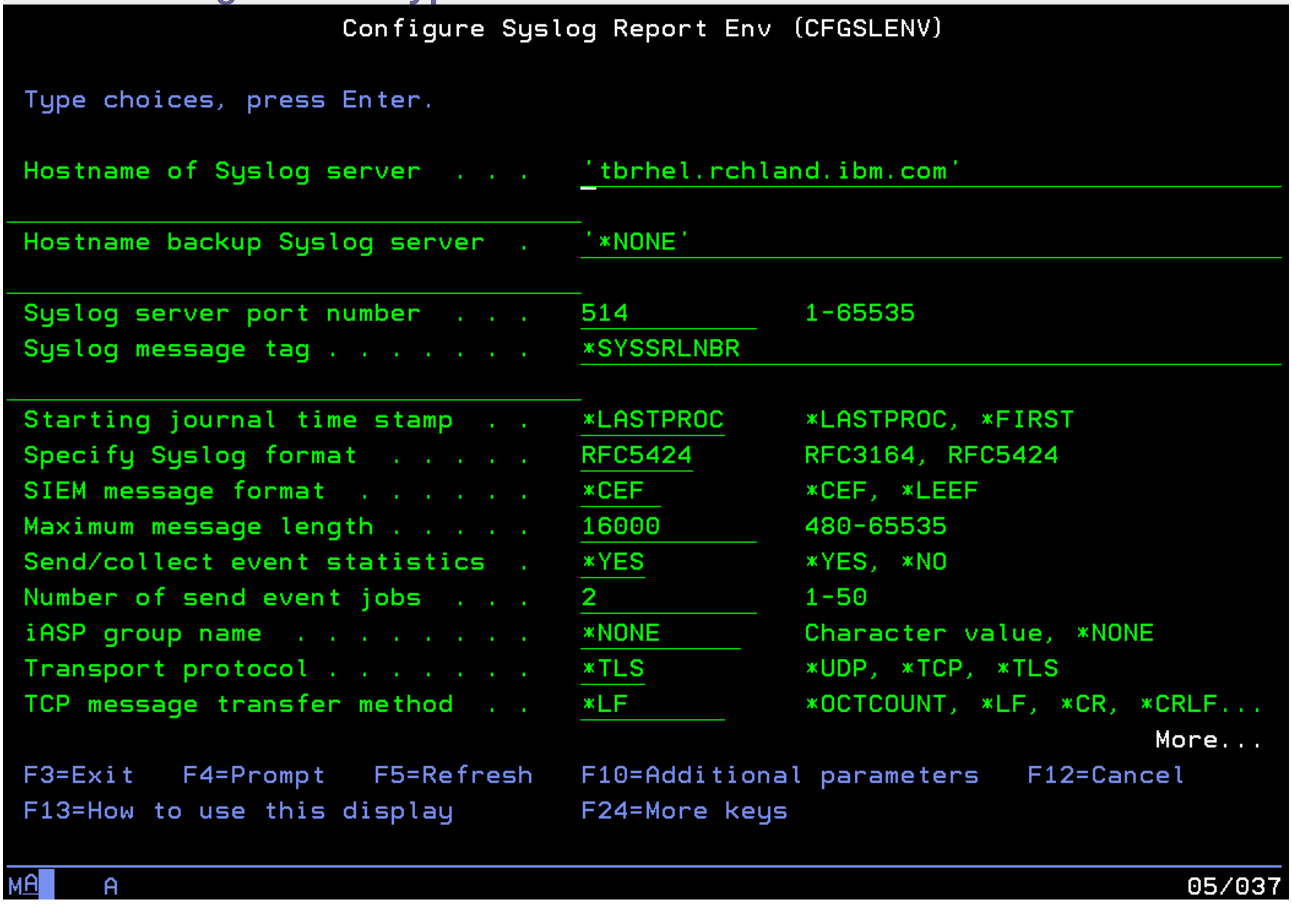
Since the reporting of syslog/SIEM events can also contain confidential and senstive information, the communication from the IBM i partition to the configured syslog server can be encrypted. If enabled, the communication is encrypted via the Transport Layer Security (TLS) protocol (see RFC5425).

8.1 Prerequisites

TLS encrypted communication is only working when the following prerequisites are met:

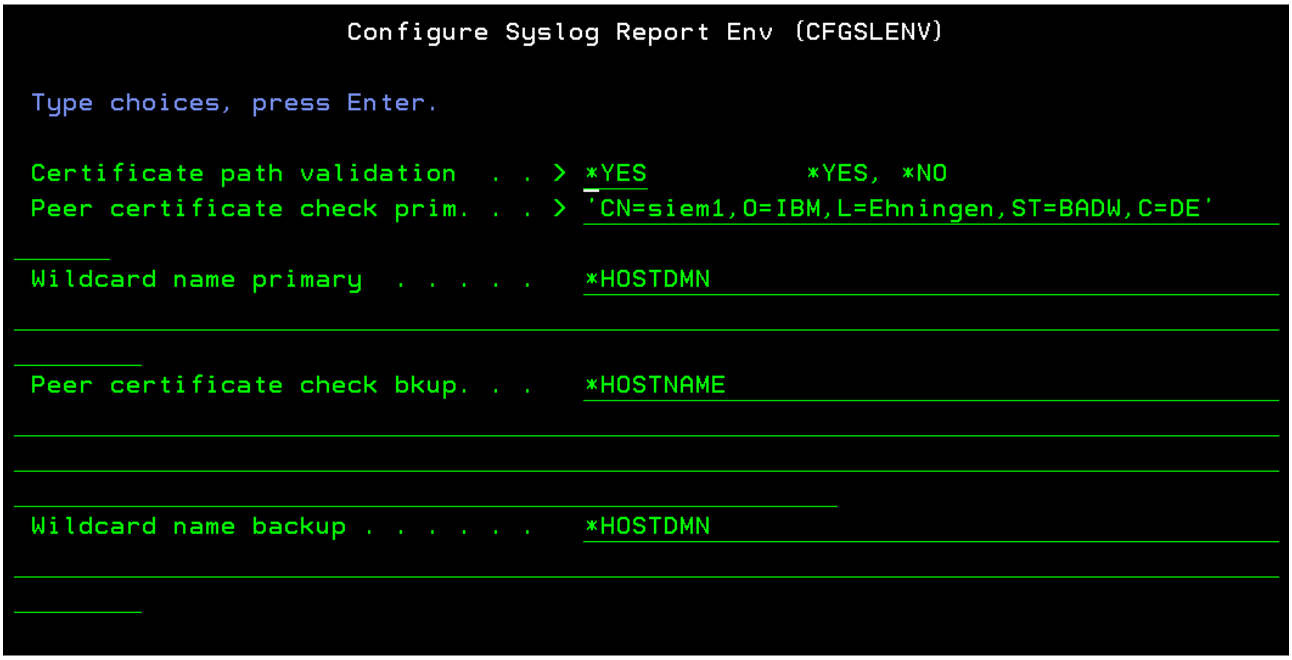
- The remote syslog server is configured to accept TLS-encrypted communication. The default port for TLS-encrypted traffic is 6514.
- The *SYSTEM certificate store must be created on the IBM i partition. See the IBM Docs (Knowledge Base) under Security → Digital Certificate Manager for information on how to set up and work with DCM.
- The Certificate Authority (CA) certificate(s) of the CA that issued the server certificate of the syslog/SIEM server must be imported into the *SYSTEM certificate store. The administrator of the syslog/SIEM server should be able to provide the CA certificates.
- The supported TLS protocols and cipher suites should be reviewed in the QSSLPCL and QSSLCSL system values. If necessary adjust the values. Note that the system values must contain a protocol, i.e. TLSV1.2 and a cipher suite, i.e. *RSA_AES_256_GCM_SHA384, that the remote syslog/SIEM server also supports. A TLS session can only be established when both sides support at least one common protocol and cipher suite.

8.2 Enabling TLS encrypted communication



```
                    Configure Syslog Report Env (CFGSLENV)

 Type choices, press Enter.

 Hostname of Syslog server  . . .   'tbrhel.rchland.ibm.com'

 Hostname backup Syslog server  .   '*NONE'

 Syslog server port number  . . .   514           1-65535
 Syslog message tag . . . . . . .   *SYSSRLNBR

 Starting journal time stamp  . .   *LASTPROC     *LASTPROC, *FIRST
 Specify Syslog format  . . . . .   RFC5424       RFC3164, RFC5424
 SIEM message format  . . . . . .   *CEF          *CEF, *LEEF
 Maximum message length . . . . .   16000         480-65535
 Send/collect event statistics  .   *YES          *YES, *NO
 Number of send event jobs  . . .   2             1-50
 iASP group name  . . . . . . . .   *NONE         Character value, *NONE
 Transport protocol . . . . . . .   *TLS          *UDP, *TCP, *TLS
 TCP message transfer method  . .   *LF           *OCTCOUNT, *LF, *CR, *CRLF...
                                                                       More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys

MA     A                                                              05/037
```

Encrypted communication is defined via the CFGSLENV command.



```
                    Configure Syslog Report Env (CFGSLENV)

 Type choices, press Enter.

 Certificate path validation  . . > *YES          *YES, *NO
 Peer certificate check prim. . . > 'CN=siem1,O=IBM,L=Ehningen,ST=BADW,C=DE'

 Wildcard name primary  . . . . .   *HOSTDMN


 Peer certificate check bkup. . .   *HOSTNAME



 Wildcard name backup . . . . . .   *HOSTDMN

```

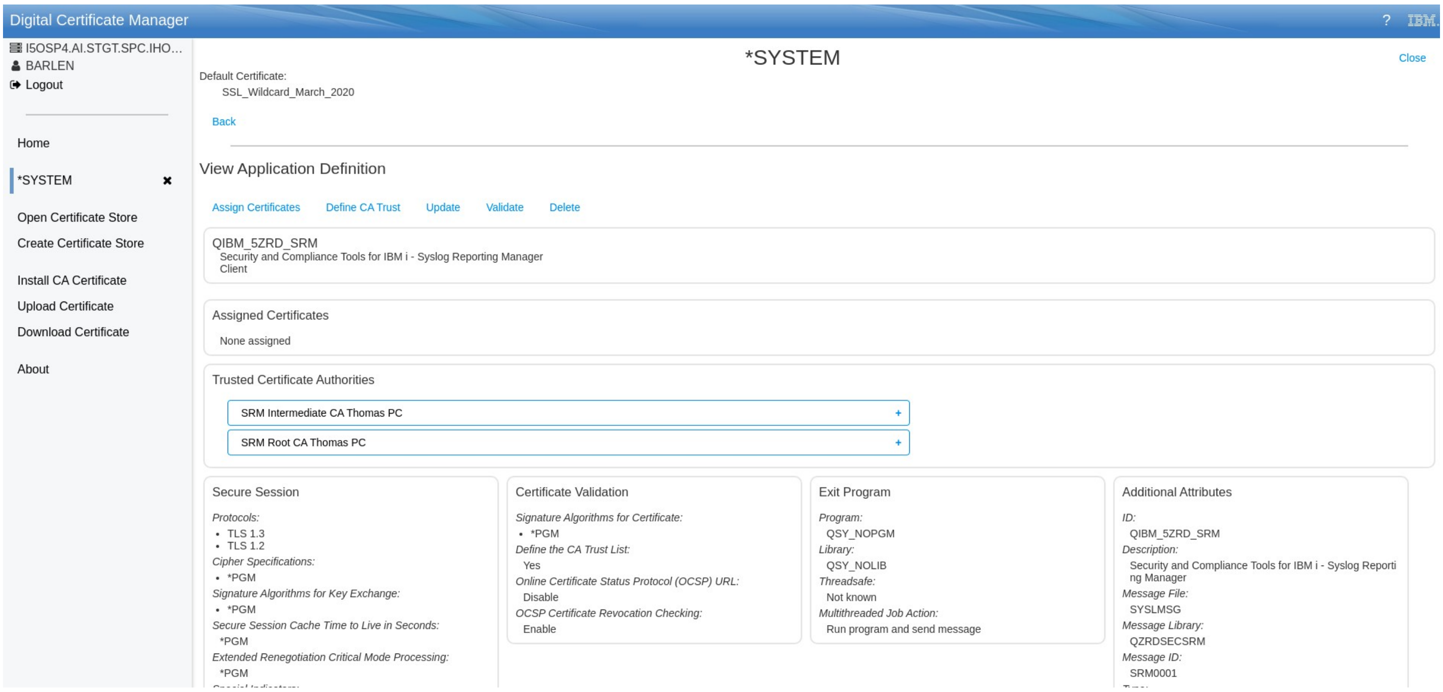
First you need to specify *TLS in the Transport protocol (COMMTYPE) parameter. This triggers the SRM application QIBM_5ZRD_SRM application to be registered in the Digital Certificate Manager (DCM). It also switches to a secure encrypted channel. In addition, you can define the following TLS encryption related configuration parameter:

- Certificate path validation (CERTVLD)
  - This parameter specifies whether the certificate that is presented by the peer syslog server during a TLS handshake must succeed the following checks for a successful session initiation.
    - The peer certificate must be issued by a Certificate Authority (CA) that is trusted by the Syslog Reporting Manager (SRM) DCM application. If no application CA Trust List is configured, the issuer CA certificates must be in the DCM *SYSTEM store and must be enabled. If a CA Trust List is enabled in the SRM DCM application QIBM_5ZRD_SRM, the issuer CA certificate or certificate chain must be in the DCM application CA Trust List.
    - The certificate must not be expired.
  - For debugging purposes you can disable the previously listed checks. For added security, it is strongly recommended to enable this check.
- Peer certificate check for the primary and backup syslog server
  - This parameter specifies criteria to be used when checking the subject distinguished name (DN) of the peer X509 certificate that is presented by the syslog server when establishing a TLS-encrypted session. The check is optional. If value *ANY is used, no check is performed. If another value is used and the certificate's subject DN content does not match the configured criteria, the connection request is rejected and no connection is established.
- Wildcard name check for the primary and backup syslog server
  - This parameter specifies criteria to be used when checking the subject distinguished name (DN) of the peer X509 certificate when the certificate uses a wildcard common name (CN). A wildcard name example is *.mydomain.local. Such a certificate could be used by several servers that belong to the same TCP/IP domain.

Note that the online help of the CFGSLENV command provides detailed information about each configuration option.

8.3 Digital Certificate Manager integration

The Syslog Reporting Manager (SRM) tightly integrates with the Digital Certificate Manager (DCM). SRM is registered as a client application QIBM_5ZRD_SRM in DCM.
Note that DCM administration is outside the scope of this document. Consult the official IBM Knowledge Base / IBM Docs for your release to get more information about using DCM.
Note that the following screen capture shows the new DCM interface that was introduced in 2020.



*SYSTEM

Default Certificate:
SSL_Wildcard_March_2020

View Application Definition

QIBM_5ZRD_SRM
Security and Compliance Tools for IBM i - Syslog Reporting Manager
Client

Assigned Certificates
None assigned

Trusted Certificate Authorities
SRM Intermediate CA Thomas PC +
SRM Root CA Thomas PC +

Secure Session
Protocols:
- TLS 1.3
- TLS 1.2

Cipher Specifications:
- *PGM

Signature Algorithms for Key Exchange:
- *PGM

Secure Session Cache Time to Live in Seconds:
*PGM
Extended Renegotiation Critical Mode Processing:
*PGM

Certificate Validation
Signature Algorithms for Certificate:
- *PGM

Define the CA Trust List:
Yes
Online Certificate Status Protocol (OCSP) URL:
Disable
OCSP Certificate Revocation Checking:
Enable

Exit Program
Program:
QSY_NOPGM
Library:
QSY_NOLIB
Threadsafe:
Not known
Multithreaded Job Action:
Run program and send message

Additional Attributes
ID:
QIBM_5ZRD_SRM
Description:
Security and Compliance Tools for IBM i - Syslog Reporti ng Manager
Message File:
SYSLMSG
Message Library:
QZRDSECSRM
Message ID:
SRM0001

When opening the *SYSTEM certificate store and selecting the option Manage Application Defintions, you find the application QIBM_5ZRD_SRM. You can then use DCM to configure the following options:

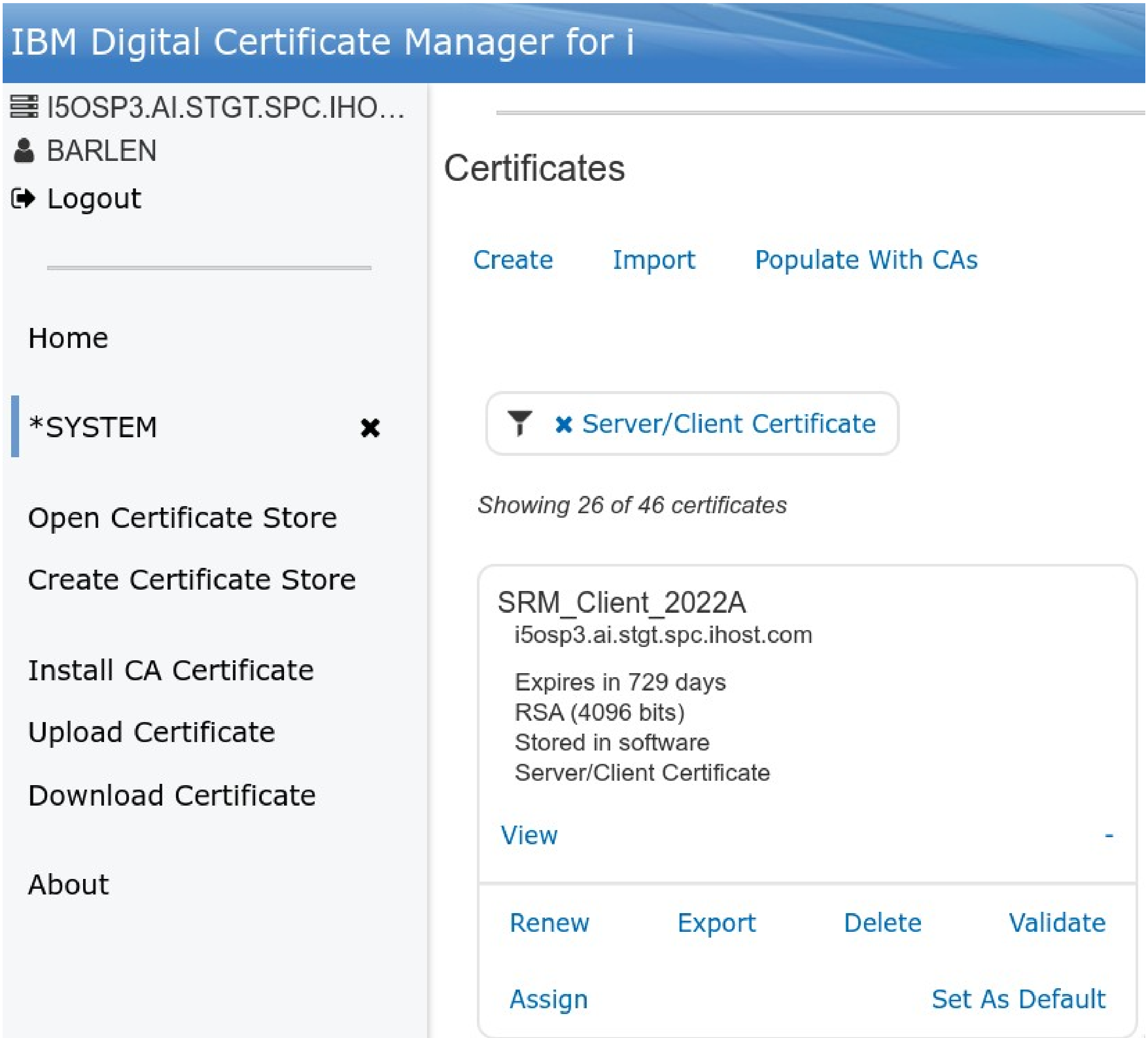
- CA Trust List
- Supported protocols
- Supported cipher specifications
- OCSP checking properties
- Timeout values
- Certificate assignment

8.4 Client authentication

The Syslog Reporting Manager (SRM) TLS encryption support also supports certificate-based client authentication. Without client authentication, SRM verifies the Syslog/SIEM server certificate, but the Syslog/SIEM server performs no authentication.

The following steps outline the setup for client authentication:

1. Configure the Syslog/SIEM server and SRM as described in the previous sections for TLS encryption.
2. Obtain a certificate that will be used by SRM to authenticate to the Syslog/SIEM server. Usually you will get this certificate from the Syslog/SIEM administrators.
3. Import the provided certificate via DCM to the *SYSTEM store. In this example, it was imported with the certificate label SRM_Client_2022A.

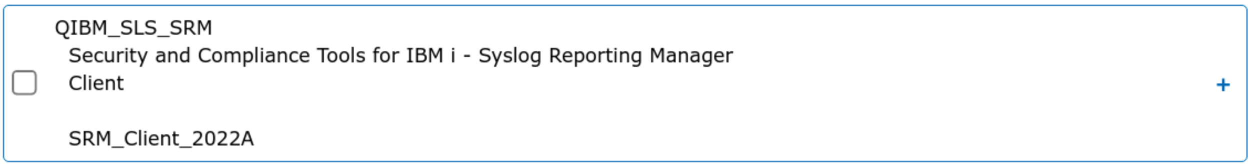


Showing 26 of 46 certificates

SRM_Client_2022A
i5osp3.ai.stgt.spc.ihost.com

Expires in 729 days
RSA (4096 bits)
Stored in software
Server/Client Certificate

4. Assign the certificate to the QIBM_SLS_SRM client application.



QIBM_SLS_SRM
Security and Compliance Tools for IBM i - Syslog Reporting Manager
Client

SRM_Client_2022A

5. Restart SRM (ENDSRM and then STRSRM).
6. The Syslog/SIEM administrator has to ensure in the configuration of the server that the client certificate is permitted access.

8.5 Example: rsyslog with client authentication

The rsyslog daemon is a syslog daemon that is commonly used on Linux as well as AIX platforms. This section describes the important configuration parameter in the rsyslog.conf file to enable client authentication as well as the common configuration directives to enable TLS encryption. This might be useful when trying to test SRM with your own Syslog server.

It is assumed that you installed rsyslog on your system. In this example, it was installed on a Centos Linux partition on an IBM Power System. The installation and basic configuration is out of the scope of this document. Refer to the publicly available documentation on the Internet, i.e. https://www.linuxtechi.com/configure-rsyslog-server-centos-8-rhel-8/

You also need a certificate authority to issue the certificate for the rsyslog server and your IBM i partition. Following is a page with an example of how to use the certtool utility to generate the certificates:
https://rsyslog.readthedocs.io/en/latest/tutorials/tls.html

Once you have your certificates ready, you can customize your rsyslog.conf file. This file is typically found under /etc/rsyslog.conf.
The following directives are the key directives for TLS encryption with client authentication where only a client with a certificate that is trusted and has a Common Name attribute set to i5osp3.ai.stgt.spc.ihost.com.

```
$ModLoad imuxsock # local messages
$ModLoad imtcp # TCP listener
$DefaultNetstreamDriver gtls
####Certificate files
# File that contains the CA certificate(s) that issued the server
# and client certificates
$DefaultNetstreamDriverCAFile /etc/pki/rsyslog/cacerts.pem
# rsyslog daemon server certificate file
$DefaultNetstreamDriverCertFile /etc/pki/rsyslog/centoshost-cert.pem
# rsyslog daemon server private key of the certificate
$DefaultNetstreamDriverKeyFile /etc/pki/rsyslog/centoshost-key.pem

# Clients that need to communicate via TLS must authenticate with a certificate
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
# Only the client with the Common Name in the certificate of
# i5osp3.ai.stgt.spc.ihost.com is permitted to send events via
# TLS-encrypted session
$InputTCPServerStreamDriverPermittedPeer i5osp3.ai.stgt.spc.ihost.com
```

You can repeat the InputTCPServerStreamDriverPermittedPeer for more clients.

The rsyslog daemon logs errors in case of a client authentication error as shown in the following examples:

- Client/peer certificate has been issued by a certificate authority that is not stored in the CA file (DefaultNetstreamDriverCAFile):

```
Feb 15 13:50:53 centos1 rsyslogd: not permitted to talk to peer, certificate
invalid: signer not found [v8.24.0-57.el7_9.1]
Feb 15 13:50:53 centos1 rsyslogd: invalid cert info: peer provided 3
certificate(s). Certificate 1 info: certificate valid from Tue Feb 15 13:18:19
2022 to Thu Feb 15 13:18:19 2024; Certificate public key: RSA; DN:
C=DE,ST=Rheinland-Pfalz,L=Wolfsheim,O=IBM,OU=Technology
Services,CN=i5osp3.ai.stgt.spc.ihost.com; Issuer DN: C=DE,ST=Baden-
Wuerttemberg,L=Ehningen,O=IBM,OU=Technology Services,CN=IBM i Technology Expert
LabsIIC Intermediate CA Thomas; SAN:DNSname: i5osp3;  [v8.24.0-57.el7_9.1]
```

- Client/peer certificate name is not listed in the permitted peer directive:

```
Feb 15 13:53:37 centos1 rsyslogd: error: peer name not authorized -  not
permitted to talk to it. Names: DNSname: i5osp3; CN:
i5osp3.ai.stgt.spc.ihost.com;  [v8.24.0-57.el7_9.1 try
http://www.rsyslog.com/e/2088 ]
```

```
Feb 15 13:53:37 centos1 rsyslogd: netstream session 0x3fff58014b00 from
172.17.17.31 will be closed due to error  [v8.24.0-57.el7_9.1 try
http://www.rsyslog.com/e/2089 ]
Feb 15 13:53:50 centos1 rsyslogd: error: peer name not authorized -  not
permitted to talk to it. Names: DNSname: i5osp3; CN:
i5osp3.ai.stgt.spc.ihost.com;  [v8.24.0-57.el7_9.1 try
http://www.rsyslog.com/e/2088 ]
```

- The client/peer did not provide a certificate during the TLS handshake (no certificate has been assigned the SRM client application in DCM):

```
Feb 15 14:23:38 centos1 rsyslogd: peer did not provide a certificate, not
permitted to talk to it [v8.24.0-57.el7_9.1 try http://www.rsyslog.com/e/2085 ]
Feb 15 14:23:38 centos1 rsyslogd: netstream session 0x3fff680132d0 from
172.17.18.6 will be closed due to error  [v8.24.0-57.el7_9.1 try
http://www.rsyslog.com/e/2089 ]
```

9 Additional information

9.1 Working with event statistics

The Syslog Reporting Manager has an option to collect information about the number of events that have been sent for the different monitor categories. You turn this option on by specifying *YES in the statistics configuration CFGSLSTAT EVTSTAT(*YES). Note that event statistics are only collected when this option is set to *YES.

When statistics are turned on, you will get the following information:

- Every 24 hours you get a message in the QSYSOPR message queue, the history log, and an event sent to the configured remote syslog server about the number of events that have been sent for categories:
  - Audit journal entries (AUD)
  - History log events (HST)
  - IFS file changes (IFS)
  - >Journal monitor events (JRN)<
  - Message queue monitor events (MSG)
  - Database journal events using the Journal Extract Tool (DB2)
  - Custom events (CUS)
  - Special events (SPC)
  - Syslog Reporting Manager tool events (SRM)
  - Number of total events sent (TotalCount)

  Example:

  ```
  <14>1 2023-11-10T00:00:07.962177-06:00 ctcsect4.rchland.ibm.com IBMiPSCSRM
  IBMSRM IBMiEvent - CEF:0|IBM|IBM i|7.4|IBMSRM|SRMEVENTSTAT|5|
  shost=CTCSECT4 cat=SRM statistics msg=Syslog Reporting Manager processing
  statistics for sent events eventStatisticsDate=2023-11-09 AUD=683 HST=0
  IFS=7 JRN=105 MSG=0 DB2=0 CUS=0 SPC=0 SRM=0 TotalCount=795
  ```

  The statistics are kept in the tool by default for 7 days. You can change the number of days that SRM keeps the statistical data by using the CFGSLSTAT command.

  The following example shows how to change the number of days to 14 days:

  ```
  CFGSLSTAT RETDAYS(14)
  ```

  You can use SQL query the statistics. The following example is a SELECT statement that displays the sum for each event monitor category grouped by the send event job name:

  ```
  SELECT
  SOURCEJOB,SUM(STATAUD),SUM(STATHST),SUM(STATIFS),SUM(STATMSG)
  ,SUM(STATDB2),SUM(STATCUS),SUM(STATSPC),SUM(STATSRM),
  SUM(STATTOTAL)FROM slstat GROUP BY sourcejob ORDER BY
  sourcejob
  ```

  ```
  Source job name  SUM ( STATAUD ) SUM ( STATHST ) SUM ( STATIFS ) SUM ( STATMSG )
    SLSNDEVT1                  289           1,209              27              32
    SLSNDEVT2                  251           1,223              31              25
    SLSNDEVT3                  223           1,230              33              31
    SLSNDEVT4                  219           1,290              55              25
    SLSNDEVT5                  237           1,237              43              21
    SLSNDEVT6                  218           1,292              22              17
  ```

  Note: The previous output shows only a part of the output for readability.

- A statistics event for database journal events using the Journal Extract Tool every time monitored journals have been processed. The event contains the number of summary and detailed events that have been processed and sent.

  Example:

  ```
  <14>1 2020-02-07T08:50:39.233000+01:00
  i5osp5.ai.stgt.spc.ihost.com IBMiPSCSRM IBMSRM 102F5F -
  CEF:0|IBM|IBM i|7.4|IBMSRM|SRMDB2STAT1|5|
  ```

```
shost=i5osp5.ai.stgt.spc.ihost.com cat=SRM DB monitoring
msg=Syslog Reporting Manager DB monitoring journal processing
finished start=2020-05-01-08.50.35.670000 end=2020-05-01-
08.50.39.199000 cs1Label=numberSummaryEvents cs1=192772
cs2Label=numberDetailEvents cs2=82314
sproc=237125/QZRDSRMOWN/SLDB2MON
```

9.2 User-type audit journal entries

IBM i sends events as entry code T entries to the system audit journal (QAUDJRN). User applications can also send their own events to the audit journal using the SNDJRNE command or equivalent Send Journal Entry (QJOSJRNE) API. These entries are marked with journal code U in the audit journal. Also IBM Technology Expert Labs assets (tools) send audit events to the audit journal. The following tables list the events that Technology Expert Labs tools generate along with their layout.

Syslog Reporting Manager

Entry type: SL

Model output file: QZRDSECSRM/SRMAUDFMT

Offset Type 5	Field	Format	Description
1			Heading fields common to all entry types. See “Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” in the IBM i Security Reference for the format details.
608	SLSOURCE	CHAR(10)	User event source ID. For the Syslog Reporting Manager the value is always IBMLSSRM
618	SLRESULT Result	CHAR(10)	Result code from the operation reported by the Syslog Reporting Manager facility. The valid result codes are SUCCESS, ERROR, or INFO.
628	SLPROC Command	CHAR(10)	The command or facility name that generated the journal entry.
638	SLUSER User	CHAR(10)	The user profile name of the user who ran the command or facility reported in the Command column.
648	Reserved	CHAR(10)	Reserved area
658	Entry data	CHAR(2800)	Entry specific data. This is a free format text describing the event.

Network Firewall (Exit Point Security)

The Network Firewall is also a tool from IBM Technology Expert Labsthat can control access from remote clients via exit point programs. The tool also generated a series of user type audit journal events. The event types are pre-populated into the Syslog Reporting Manager and the description of the entries start with *IBM LS XPT*. If you use the tool, you can use the CFGSLAUD command to enable the reporting of the individual event types. For a complete description of the event types, refer to the documentation of the Network Firewall tool.

9.3 Deleting the Syslog Reporting Manager

The Syslog Reporting Manager has been installed with the Restore License Program (RSTLICPGM) command. Likewise, when you want to delete the license program, you need to use the DLTLICPGM command. The following steps describe the tasks that need to be performed to completely remove SRM from the system.

1. End SRM with the **`ENDSRM`** command.
2. Verify that the subsystem SLSBS has ended with the **`WRKACTJOB SBS(SLSBS)`** command. The subsystem must be ended before proceeding with the next steps.
3. Check if group profile QZRDSRMGRP has any members.
   ```
   DSPUSRPRF USRPRF(QZRDSRMGRP) TYPE(*GRPMBR)
   ```
   If it does, remove all members.
4. Delete the license program.
   ```
   DLTLICPGM LICPGM(5ZRDSRM)
   ```
5. Delete the owner user profile **`QZRDSRMOWN`** with the DLTUSRPRF command.

9.4 Expert mode configuration

There are several configuration options available for administrators to change properties and settings of the Syslog Reporting Manager (SRM) that can have a significant impact on the functionality of SRM. These options are called expert configuration options and should only be used by a person who knows what impact the change has on SRM. An administrator who is not absolutely sure what the outcome of the change is should not use these options.

To limit the use of expert mode configuration options, the user who wants to use these options must meet the following criteria:

- The user profile must have the *AUDIT special authority. It is not enough to get the special authority via a group membership. The authority must be assigned to the user profile itself.
- The user must also be a member of the QZRDSRMGRP group.

If one of the permission prerequisites are not met, the configuration options are either not shown on the configuration screens or end with a corresponding error message.

Disclaimer: Expert mode configuration must be used carefully and at the discretion of the user. IBM cannot be held responsible for configuration changes that are done in expert mode.

8.4.1 Monitor restart timestamps

Each monitor, i.e. the audit journal monitor or history log monitor keeps track of the last processed event. Depending on the monitor job, the associated timestamps are stored in different objects. Normally there is absolutely no reason to adjust the timestamps as the monitors do a great job in maintaining them. However, there might be situations when you consider adjusting the timestamps. For example, assume you stopped SRM for a few days and a lot of entries have not been processed. You security department and auditors agree that only entries from the time SRM is restarted should be processed and older entries, even though they have not been processed yet, should be ignored. In this case, you could adjust the restart timestamps.

Important: You have to know what the impact of such a change is. If you adjust a timestamp to a time before the currently stored timestamp, you might end up sending duplicate events. Adjusting the timestamp to a later time than the currently stored timestamp you might end up skipping events. Therefore you should only adjust a timestamp if you have checked that the change would not cause any compliance violation in your organization.

Depending on the monitor, there are sometimes additional information that is kept for the monitor job to find the right restart synchronization point. The following table lists the different monitors, the type of properties that are kept for each monitor, whether the restart properties apply to the entire monitor or parts of it, and if the expert configuration option is accessed by a function key or option.

Monitor	Applicable to	Type of information	Config method
Audit monitor – system type entries	Monitor job	- Timestamp - Journal receiver	CFGSLAUD command F17 key
Audit monitor – user type entries	Monitor job	- Timestamp - Journal receiver	CFGSLAUD command F17 key
History log entries	Monitor job	- Timestamp	CFGSLHST command F17 key

Monitor	Applicable to	Type of information	Config method
IFS file monitor	IFS journal	- Timestamp - Journal entry sequence number	CFGSLIFSJ command journal option 17
>Journal entry monitor	Journal monitor job	- Timestamp - Journal entry sequence number	CFGSLJRNJ command journal option 17<
Message queue monitor (*1)	Monitor job	- Timestamp	WRKMQMM command F17 key
Database change monitor (*2)	Database journal	-Timestamp	CFGJSPRC command journal option 2
*1 = The message queue monitor keeps track by the timestamp of the last logged message it processed. The timestamp is stored along with the message itself. When you adjust the timestamp to a time in the past, all timestamps of messages that are younger than the new timestamp are adjusted to the customized timestamp minus 1 microsecond. *2 = The database change monitor requires an additional Technology Expert Labs asset called Journal Extract Tool (JET). This is not part of SRM. SRM only provides integration with JET so that it schedules JET processing and generates SRM events. Note that the command CFGJSPRC is part of JET and is not considered an expert mode configuration option. Refer to the JET documentation for more information.			
Note that the F17 function key or option 17 is only shown when you meet the access permission requirements.			

9.5 Daylight Savings Time information

Events that are logged in the various logs on IBM i, such as the audit journal, history log, message queues, etc. are logged with the timestamp of the log entry when it was written to the log. In case of daylight savings time (DST) adjustments in Spring and Fall each year, many applications need to be stopped before the time change and restarted after the time change.

For the Syslog Reporting Manager it is strongly recommended to stop SRM with the ENDSRM command before the time adjustment and start it again with the STRSRM command after the adjustment. This ensures proper processing of all events.

9.6 Deploying SRM on multiple IBM i partitions

If you have purchased the enterprise license of the Syslog Reporting Manager (SRM), you are entitled to install and run SRM on multiple IBM i partitions. This section provides some information about deploying SRM on multiple partitions with the least amount of effort. Ideally the information will help you to automate the roll-out. It is assumed that you want the same SRM configuration on all partitions.
The following list describe the tasks involved:

- Install SRM on your first partition and perform the entire configuration, i.e. setting up the global configuration, audit journal monitoring, history log monitoring, etc.
- Test the configuration on the first system. If all your tests are successful and SRM provides the expected output, continue with the next steps.
- Export the configuration with the EXPSLCFG command, i.e.
  ```
  EXPSLCFG SAVF(SRMROLLOUT/SLCFGDTA)
  ```
- Transfer the exported save file (i.e. SRMROLLOUT/SLCFGDTA) along with the product save file (SRMBASE) and optionally PTF save files to the new IBM i partition.
- <Accept the license agreement prior to installation.
  ```
  CALL PGM( QSYS/QLPACAGR) PARM('5ZRDSRM' 'V2R3M0' '0000' 0)  >
  ```
- Install SRM.
  ```
  RSTLICPGM LICPGM(5ZRDSRM) DEV(*SAVF) SAVF(QGPL/SRMBASE)
  ```
- >Load and apply SRM PTFs when available, i.e.
  ```
  LODPTF LICPGM(5ZRDSRM) DEV(*SAVF) SELECT(5SC1005)
  SAVF(QGPL/Q5SC1005)
  APYPTF LICPGM(5ZRDSRM) SELECT(5SC1005)<
  ```
- Add the license key that you obtained from IBM.
  ```
  ADDLICKEY PRDID(5ZRDSRM) LICTRM(V2) FEATURE(5050)
  SERIAL(7812345) PRCGRP(*ANY) LICKEY(30B64B B8F2E2 276001)
  USGLMT(*NOMAX) EXPDATE(*NONE) VNDDTA(*NONE)
  ```
- Import the configuration.
  ```
  >IMPSLCFG SAVF(SRMROLLOUT/SLCFGDTA) BACKUP(*YES)
  IMPGLB(*IMPORT) IMPAUD(*IMPORT) IMPIFS(*IMPORT)
  IMPIFSFLT(*IMPORT) IMPHST(*IMPORT) IMPMSG(*IMPORT)
  IMPJRN(*IMPORT) IMPJRNFLT(*IMPORT) IMPDB2(*IMPORT)
  IMPSPC(*IMPORT)<
  ```
- In case you want to change some settings, such as the Syslog Tag in the global configuration, you can do that at this point in time. Example:
  ```
  CFGSLENV PORT(514) TAG(PRODSYS) STRTIME(*LASTPROC)
  RFCTYPE(RFC5424) MSGFMT(*CEF) MAXMSGLEN(16000) EVTSTAT(*NO)
  ASPGRP(*NONE) COMMTYPE(*TCP) TCPSEP(*LF) CERTVLD(*NO)
  PEERNAME1(*HOSTNAME) WILDCARD1(*HOSTDMN) PEERNAME2(*HOSTNAME)
  WILDCARD2(*HOSTDMN) CUSTIME(*JRNTIME) FILTZCZR(*YES)
  FETCHROWSH(1) FETCHROWSA(1) FETCHROWSU(1)
  ```
- Start SRM
  ```
  STRSRM
  ```

All the previously listed commands and steps can be packaged, i.e. in an FTP batch program to automate the deployment.

9.7 Using an output file for storing events

<The traditional approach of SRM was to send all captured events via the syslog protocol to the configured remote syslog / SIEM server. An option has been added to store the events in a database table rather than sending the events over the network to a remote server.

To enable the event storage into a table, specify *OUTFILE in the SERVER parameter of the CFGSLENV command (SLMON menu option 2) and then enter the file name and library of the table where the events will be stored.

If *OUTFILE is selected, events are not send via the syslog protocol anymore. They only reside in the specified table.

IMPORTANT:

SRM is only adding events to the file. SRM is not deleting events from the file nor doing any housekeeping activities. It is the responsibility of the event handler program that receives the events from the file to also delete processed entries.

The events table has the following columns:

Column number	Column Name	Type	Length	Description
1	POSITIONID	BIGINT		Row ID. Not added by SRM, but automatically incremented by DB.
2	EVTCAT	CHAR	4	Event source category *AUD – Audit journal *HST – History log *MSG – Message queue *IFS – IFS file monitor *JRN – Journal monitor *SRM – SRM statistics *CUS – Custom events *SPC – Special events
3	EVTTIME	TIMESTAMP	26	Event timestamp in format YYYY-MM-DD-hh.mm.ss.ffffff
4	HOSTNAME	CHAR	128	FQDN of event source host
5	LOGTAG	CHAR	80	Syslog Header Tag
6	EVTDTA	CLOB	65500	Event SIEM header and payload data / event data

>

10 Change History

This section describes the changes and enhancements of previous versions of the Syslog Reporting Manager.

10.1 Version 1.0 dated May 18th, 2018

Initial version of the tool.

10.2 Version 1.1 dated August 8th, 2018

Changes:

- Added option for IFS file changes that are greater than 32 KB. The administrator can now select whether data changes should be reported from the beginning of the changed content or from the end. In addition, if the change spans across multiple captured journal entries, the administrator can select if only the first entry, the last entry, or all entries are sent via syslog messages.
- The control monitor job in subsystem SLSBS has been changed to restrict the number of automatic restart operations for the audit, IFS file, and history log monitor jobs. An automatic restart usually occurs if a monitor job fails. The maximum number of automatic restarts for a failing monitor job is 10.
- The export and import configuration processes have been enhanced to backup and restore special configuration settings.
- The install process has been updated to migrate existing configuration data during an upgrade to a new version of the SRM tool.
- Various bug fixes.
- More extended help text.

10.3 Version 1.2 dated May 24th, 2019

Changes:

- Created a new communication module that acts as a central function to process all events that are generated by all monitoring jobs (i.e. SLAUDMON, SLIFSMON, SLHSTMON). All monitor jobs use now a data queue to store events to be processed. This new functionality increases performance and reliability. The new module has been developed from scratch as a native IBM i module. It eliminates the dependency on Java.
- The Syslog Message Tag (TAG) parameter in the CFGSLENV command has been changed to allow a special value of *DEFAULT. When the new value is used, the syslog header contains the following values according to the used RFC type:
  - RFC3164

    Tag: IBMiPSCSRM
  - RFC5424

APP-NAME:	IBMiPSCSRM
PROCID:	IFSMON or AUDMON or HSTMON or CUSEVT
MSGID:	IBMiEvent
- A new SIEM message format (MSGFMT) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you select the syslog message payload format. It can be either *CEF (Common Event Format) or *LEEF (Log Event Extended Format).
- A new Maximum message length (MAXMSGLEN) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you define the maximum length of a syslog message as sent over the network. Some syslog servers have restrictions on the maximum size of messages that they can process. The new parameter allows you to customize the message size according to the used syslog / SIEM server.
  - Since the maximum message size is now flexible, the Truncate parameter for the RFC5424 RFC has been removed. During upgrade of to the new version, the MAXMSGLEN is set to 1024.

- A new Transport protocol (COMMTYPE) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you select the IP protocol that is used when sending events to the syslog server. Initially, all messages had been sent over the User Datagram Protocol (UDP). You have now the choice to also select the Transmission Control Protocol (TCP).
- A new Hostname for backup syslog server (SERVER2) parameter as been added to the CFGSLMON command (SLMON menu option 2) that lets you specify a hostname or IP address of a backup syslog server if the primary server is not available.
- All events can now be formatted in Log Event Extended Format (LEEF) as supported as the standard format for the IBM QRADAR product.
- The first version of the Syslog Reporting Manager (SRM) appended the event to be sent to a regular syslog header. That means, the syslog server showed the syslog header plus another RFC-type specific header plus the CEF event data. In version 1.2.0 of SRM, the default behavior has been changed to be more in line with other products. The header that is generated, i.e. via the DISPLAY_JOURNAL function is actually used as the syslog header and the syslog server shows as the payload (message) just the CEF / LEEF data. Note if you select *SYSTIME as the Syslog Timestamp type in the CFGSLENV command, the syslog header contains the time when the event was sent and the payload still contains a timestamp of the time the event was originally be generated. If you depend on the old behavior, contact your IBM Technology Expert Labsrepresentative (or via the contact form at) who can help you sending events in the old format.
- A new function has been added to generate custom events. This feature can be used, for example, in an application to use the Syslog Reporting Manager framework to send events to the configured SIEM server. You can either use a CL command SNDEVT or use a provided service program and call procedures in ILE programs to send custom events.

10.4 Version 1.3 dated Jan. 25th, 2020

Changes:

- Added a value *SYSSRLNBR to the Syslog message tag (TAG) parameter of the CFGSLENV command. When specified, the serial number (DSPSYSVAL QSRLNBR) is added as a tag to the syslog header.
- Added a new parameter EVTSTAT to the CFGSLENV command. This parameter specifies whether the event send function will collect statistical counters for each type event that is sent to the remote syslog server. The statistics are also reported via message SLS0040 to the control message queue that is defined in the CFGSLMQM command. If turned on (*YES), the Syslog Reporting Manager sends a summary event after midnight or latest after 24 hours. The event has the following format:

  ```
  cat=SRM statistics msg=Syslog Reporting Manager processing
  statistics for sent events statStartTime=2019-09-25-
  14.05.05.000000 statEndTime=2019-09-25-14.12.18.000000 AUD=10
  HST=0 IFS=0 MSG=0 DB2=0 CUS=0 SRM=1 TotalCount=11
  ```

  The key-value pairs are as follows:

  - AUD – Number of audit journal events
  - HST – Number of history log events
  - IFS – Number of IFS file change events
  - MSG – Number of message queue monitoring events
  - DB2 – Number of database events captured by the IBM Technology Expert Labsasset Journal Extract Tool.
  - SRM – Number of events generated by the Syslog Reporting Manager tool itself.

    - CUS – Number of custom events generated from user applications using the `sendCustomFmtEvent` or `sendCustomEvent` procedures or the `SNDEVT` CL command.
    - Total count of events sent during the reported timeframe.
    - The start timestamp of when the statistic starts.
    - The end timestamp of when the statistic ends.
- Important status messages from the Syslog Reporting Manager are also sent to the IBM i QHST history log. The following messages are sent to QHST:
    - SLS0009 - Monitoring for job &1 started.
    - SLE0019 - Syslog Reporting Manager control job has reached maximum job restart count for monitor job &2.
    - SLS0040 - Syslog Reporting Manager event statistics.
      Daily statistics about number of events sent for each category.
    - SLS0050 - Database change monitoring process completed. Second level text contains job statistics.
    - SLS0051 - Syslog Reporting Manager job &1 will be restarted.
      This message indicates when a monitor job gets restarted for cleanup purposes after 24 hours. The variable contains the job name that was restarted.

  The messages are listed in history filter QHST9999. If enabled, those messages are monitored by the SLHSTMON job and reported to the remote syslog/SIEM server.
  Note: The history filter QHST9999 is only added to new installations. It will not be added when upgrading from a previous version.

- All monitor jobs (SLAUDMON, SLIFSMON, SLHSTMON) and the event send job SLSNDEVT are now restarted every 12 hours to perform some job environment cleanup tasks.

- The default logging level in the SLJOBD job description has been changed to LOG(0 00 *SECLVL) . Therefore no messages are logged in any of the Syslog Reporting Manager jobs anymore.

- IBM Technology Expert Labsalso offers an asset (tool) called Journal Extract Tool. This tool can be used to monitor database table changes. By default, the tool creates tables with the reported changes of the monitored database tables. The Syslog Reporting Manager (SRM) has been enhanced to analyze the data that is generated by the Journal Extract Tool and send the database changes as Syslog messages (in either CEF or LEEF format) to the configured remote Syslog/SIEM server. The enhancements also provide more convenient configuration interfaces to set up and operate the Journal Extract Tool. All configuration options can be accessed from the SLMON menu.
  Note: To be able to use this new enhancement, you need to purchase the Syslog Reporting Manager and the Journal Extract Tool. These are two independent tools. For more information contact IBM Technology Expert Labsat:
  https://www-03.ibm.com/systems/campaignmail/services/labservices/contact.html

- Another enhancement of this Syslog Reporting Manager (SRM) version is the ability to monitor message queues. You can configure the SRM to monitor one more message queues and report the messages to the configured remote Syslog/SIEM server.

10.5 Version 1.4 dated Sep. 30th, 2020

Changes:

- New commands STRSRM and ENDSRM have been added to start and end the Syslog Reporting Manager in a controlled manner.
- A new command CFGSRM has been added to open the main configuration menu.
- The control job SLMONSTR has been enhanced to better handle errors in the send event jobs (SLSNDEVT). Especially in situations where a communication could not be established with a configured syslog / SIEM server, the control job tried 10 times to restart the job. When the connection could still not be established, no events would be sent and the Syslog Reporting Manager would not retry the send process. With this version, the control job will to restart the send event communication jobs after 10 minutes.
  In addition, if the control job SLMONSTR itself fails, it will automatically be restarted along with all monitor jobs to ensure a consistent state of the tool.
- If the audit monitor, history log monitor, or IFS file monitor ended abnormally or a user has ended the job with the ENDJOB command, the SLMONSTR control job tried 10 times (default) to restart the job. If the restart attempts were not successful, the control job stopped restarting the missing monitor jobs. With this version, the control job pauses for 10 minutes and then tries to restart the missing job again for another 10 times. This enhancements ensures that the Syslog Reporting Manager tries to keep all related jobs active unless an administrators ends the tool itself or individual monitor jobs.
- In previous versions of the tool, there has been one communication job SLSNDEVT. This job is in charge of processing all events that the monitor jobs retrieved. The job establishes a communication with the configured syslog / SIEM server and sends the events to the remote host. The Syslog Reporting Manager has been enhanced to support up to 50 send event jobs in this version. In case you observe delays in receiving entries on the remote syslog server, you can start additional send event jobs to increase the throughput of the send process. The started job names are SLSNDEVT01 to SLSNDEVT50. The number of send jobs is configured with the CFGSLENV command.
- The STRSLMON command has been enhanced to provide an additional parameter *SNDEVT. When the command is executed with the *SNDEVT parameter, the control job will check that all configured send event jobs are active. If not, the control job restarts the missing jobs. For example, if you configured to use 4 send event jobs and only job 1,2 and 4 are active, the STRSLMON *SNDEVT would cause number 3 to be started again. Running jobs are not affected.
- Initially introduced in V1.2, events could also be sent via the TCP protocol besides the UDP protocol. The advantage of a TCP session is the reliability and also the option to send multiple events through a single established TCP connection. To differentiate the different events within a single TCP session, V1.2 supported a transfer mode called octect counting as defined in RFC6587. With this method, an event in a TCP session is identified by the message length. The octet count of the length of the entire message is added as a prefix to the syslog message. Based on the length, the receiver knows when an event message ends and the next event starts. This is the newer message transfer mode that is considered more reliable than the second option called non-transparent-framing. Since many SIEM solutions only support the older method, TCP caused a problem when sending events to these SIEM hosts. Version 1.4 has been enhanced to also support the non-transparent-framing transfer mode. It uses a trailer character to indicate the end of a message. The supported trailer characters are LF, CR, CRLF, and NULL. The transfer mode s configured with the CFGSLENV command.
- The startup performance and behavior of the audit monitor job has changed. In previous versions, when the audit monitor job started, the entire chain of journal receivers were examined starting at the last processed timestamp. Since some clients keep a large number of audit journal receivers on the system, the startup of the audit monitor job could have taken hours. The

enhancement in this version does not only keep track of the last processed entry but also of the journal receiver the event was in. When the audit monitor starts, it starts processing entries from the previous timestamp in the journal receiver that the entry was in. If the journal receiver does not exist anymore when the monitor job starts, the currently attached receiver only or the entire current chain of receivers will be examined. This depends on the setting in the CFGSLAUD command's *Audit journal receiver selection* parameter value. If the Syslog Reporting Manager has been installed the first time on a system and the audit monitor job is started only the currently attached journal receiver is examined starting from the time of the installation minus 1 hour.

- On systems that generate a large amount of history log or audit journal entries, the performance of the monitor jobs can be degraded due to the way the monitor jobs process the retrieved entries. Prior to this version, only one entry was read at a time from the log source. In this version, an administrator can decide to increase the number of events that are retrieved in a single SQL FETCH command (read multiple rows). The default is still one row at a time, but you can define between 1 and 200 rows to be fetched at a time for the history monitor and the audit journal monitor. The values are configured with the CFGSLENV command (advanced parameter).
  Important: If the number of entries that your filter selection produce is small and the number of rows to be fetched is large, there will be a delay in sending the events. Read the online help of the CFGSLENV command for further information.
- The audit journal monitor configuration supports now a user profile filter. You can specify up to 9 user profiles per audit journal event type. Wildcards are supported as part of the user profile name. Following are a few examples using the user profile filter:
  - Example 1: QSECOFR filter for entries from QSECOFR only
  - Example 2 : Q* filter for entries from all user profiles that start with Q
  - Example 3: *SRV* filter for entries where the sending user profile name contains somewhere the string SRV like WEBSRV1 or, APPSRVPRF
  - Example 4: *OWN filter for entries where the sending user profile name ends with OWN, such as QZRDSRMOWN, APP1OWN, or APP2OWN
  - The audit journal monitor now supports additional T journal code journal entry types. Following is the list of additional entry types. Note that these entry types are only supported on IBM i releases 7.3 and higher. Certain PTF prerequisites must be met.
    - AP, AU, CQ, CU, CV, CY, DI, EV, IM, IP, IR, IS, JD, JS, KF, ML, M0 (7.4 only), M6 (7.4 only), M7 (7.4 only), M8 (7.4 only), M9 (7.4 only), NA, ND, NE, O1, O2, O3, PF, PO, PS, PU, RQ, SD, SF, SG, SK, SM, VO, VP, XD, X0, X1, X2, YC, and YR.
    - Check section Audit journal entry type support on page 128 for more details about the supported entry types, the minimum release level, and the prerequisite PTF numbers.
  - This version also supports processing of user type audit journal entries that have been produced with the SNDJRNE command or equivalent API. These entries are report under the journal code U in the audit journal. The journal event type depends on the source of the event.
    - The Syslog Reporting Manager generates user type entries of event type SL.
  - Another major enhancements that required changes in many parts of the tool is the support of independent ASPs. You can now specify via the CFGSLENV command the ASP group name of an iASP that contains:
    - Journals that log IFS file changes
    - Journals that log database changes to be processed by the optional Journal Extract Tool (JET) from Technology Services.
  - The IFS file change monitoring supports the monitoring of IFS files that are defined in the Syslog Reporting Manager standard journal IFSJRN. In this version, you can also add custom journals where IFS file changes get logged. This supports journals in an iASP or in the system ASP. The IFS journals are configured via command CFGSLIFSJ.

  - All Syslog Reporting Manager commands are now available as proxy commands in the QSYS library.

10.6 Version 2.1 dated Nov. 6th, 2021

Changes:

- SRM V2.1 is now using license keys to provide access to the tool instead of product access keys. This change has been made to streamline the packaging of IBM Technology Expert Labstools (assets). The advantage is that IBM i administrators can now test-drive the tool within a grace period of 70 days before making a decision to buy the tool. As part of this change, SRM has been changed as follows:
    - The tool library has changed from QZRDSYSLOG to QZRDSECSRM.
    - The owner and group profile has been changed from QZRDSLOWN/QZRDSLGRP to QZRDSRMOWN/QZRDSRMGRP.
    - The license product identifier has changed from 5ZRDPSC (option *BASE and 1) to 5ZRDSRM (option *BASE only).

- The Independent ASP support has been enhanced. V2.1 now supports multiple iASPs for IFS file monitor journals, the Journal Extract Tool integration, and the message queue monitor. Each definition for a message queue, an IFS monitor journal, or a journal that is defined for Journal Extract Tool integration, provides a new parameter to specify an ASP name. The ASP parameter accepts the following values:
    - A name of an ASP
    - The value *SYSTEM which refers to the system ASP (ASP number 1)
    - The value *GLOBAL which refers to the Syslog Reporting Manager global configuration parameter ASPGRP that is defined via the CFGSLENV command.

- The message queue monitoring function has been enhanced to support more selection filter. The new filter criteria, that can be applied on a per message queue level, are:
    - Up to 8 user profile names from which the message was sent. The parameter accepts generic user names.
    - Up to 8 message identifier. The message IDs can also be specified as generic values, i.e. CPI* would only report messages with a message ID that starts with CPI like CPI1E84.
    - Up to 3 message types.

- The audit journal monitor for system-supplied entry types (journal code T) has been enhanced to support additional filter criteria. In particular, the administrator can now select for each journal entry type one or mode entry type codes of the journal entry’s entry-specific data. The IBM i Security Reference describes in Appendix F all IBM i issued journal entry types. The first field of the entry-specific data (the data following the entry headers) is a 1 character field. The meaning of the field varies by journal entry type. The filter does not apply to user type journal entries (journal code U). The filter capability allows you to enter one or more of the entry specific codes. Following are two examples:
    - Example 1: Appendix F lists for the JS (Job Change) journal entry type 18 different entry types, but you are only interested in job hold (H), job release (R), and ENDJOBABN (A) operations. In this case, you would enter `AHR` in the parameter.
    - Example 2: Appendix F lists for the PW (Password) journal entry type 12 different entry types, but you are only interested in password not valid (P), user not valid (U), signon failed due to a disabled user (Q), and when a CHKPWD authentication attempt fails (C) operations. In this case, you would enter `CPUQ` in the parameter.

- The IFS file monitor configuration command has been enhanced to allow you to specify directory journal inheritance for new IFS files that are created in the selected directory. Before this change, you could only enter the corresponding option with the STRJRN command. The configuration list also shows which directory has inheritance turned on.

- The IFS file monitor has been enhanced to autodetect the code page for deleted IFS files. In rare situations, a change of a monitored IFS file could be processed by the monitor after the file has been deleted. In this case the monitor cannot retrieve the code page of the file. This could lead to unreadable data in the reported event. In V2.1, the monitor tries to autodetect whether the changed data was stored in ASCII or EBCDIC format and then formats the output in the syslog event accordingly.

- The global configuration for the IFS file monitor has been moved from the CFGSLIFS command to the CFGSLIFSJ command.

- The Syslog Reporting Manager (SRM) has been enhanced to support Transport Layer Security (TLS) encrypted communication to the configured syslog servers. The encrypted session uses the underlying TCP protocol. SRM registers itself as a client application QIBM_5ZRD_SRM in the Digital Certificate Manager (DCM). DCM can then be used to define properties, such as supported TLS protocols, cipher specs, whether Online Certificate Status Protocol (OCSP) should be used to check for revoked certificates, etc.
  The global configuration command CFGSLENV is used to enable TLS-encrypted communication. It also has some new parameters that determine whether additional checks should be performed on the peer certificate’s subject distinguished name of the syslog server. More information about the TLS implementation can be found in section
  8 Transport Layer Security (TLS) implementation information on page 102.

- SRM also maintains a statistics table SLSTAT in library QZRDSECSRM which keeps the number of events by category that have been processed and sent by SRM. This version has been enhanced with the CFGSLSTAT command to specify the retention period in days for how long SRM will keep the statistics.

- **Statement of direction:** It is planned that V2R1 of the Syslog Reporting Manager will be the last release that supports IBM i V7R2.

10.7 Version 2.2 dated Dec. 5th, 2022

Changes:

- SRM 2.2 has corrected the order of the event keys suser/usrname, sproc, and shost/resource to be reported in the same order for all event types. Before that change, custom events and IFS events did have a different order than other event categories.
- A new configuration option and associated function change has been added to filter audit journal (QAUDJRN) ZC (change) and ZR (read) events that are originated by the SRM audit journal monitor jobs (SYSLOGAUD and SYSLOGAUDU). The background for this change is that if the system is set up for object auditing and the QSYS/QAUDJRN journal object auditing value has been set to *ALL or *CHANGE, ZR or ZC entries are generated in the audit journal whenever a job or user accesses the audit journal for read (*ALL) or change (*CHANGE) access. The Syslog Reporting Manager audit monitor jobs SYSLOGAUD and SYSLOGAUDU also access the audit journal. This would cause ZR entries caused by SRM to be reported to the configured remote server. Using this parameter you can filter out ZR or ZC entries caused by the syslog audit journal monitor jobs of SRM. The new filter can be configured with the CFGSLENV command.
- An audit journal monitor filter for T-journal code (system entries) had been introduced in a previous version to let an administrator filter audit events based on the first field of an event after the journal header. This field is referred to in the IBM i Security Reference as the Entry Type field. While you could filter for the different types, they had not been reported in the event itself. In this version of SRM, the Entry Type field for system audit journal events are reported in the event under event key *entryTypeField*. This enhancements allows the remote syslog/SIEM server to evaluate further details of the reported event. For example, the AF (Authority Failure) journal entry provides in the Entry Type field further information about the reason. ‘A’ indicates that the user was not authorized to access the object while J means a submit profile error.
- A new key-value pair has been added to system audit journal events for the following entry types:
  - PW
  - SO

  The key that has been added is userProfile and specifies the user profile name of the name that was reported in the failed authentication attempt or server authentication entry management operation.
- The audit journal monitor for system and user entries has been enhanced to provide a configuration option to specify whether audit journal events for the configured user profiles should be included in the reporting or excluded from being reported to the configured remote syslog/SIEM server. That way you can easily decide whether all audit journal events for a given entry type should be reported excluding events from specific users or all events should be reported for a select number of user profiles only.
- The history log monitor has also been enhanced to provide a configuration option to specify whether history events for configured user profiles and message identifiers should be included in the reporting or excluded from being reported to the configured remote syslog/SIEM server. That way you can easily decide whether all history events should be reported excluding events from specific users and for specific message identifiers or all events should be reported for a select number of user profiles or message identifiers only.
- The message queue monitor has been enhanced to provide a configuration option to specify whether message queue events for the configured user profiles should be included in the reporting or excluded from being reported to the configured remote syslog/SIEM server.
- The CFGSRM menu has now a new function key F8 to display statistical data. The data contain the number of events for each category that have been sent by the different monitor jobs.

- New configuration options have been added that are considered expert configuration options. They expect the person who performs the configuration changes to know about the impact that the change has to the Syslog Reporting Manager. Administrators who do not know what the change does are strongly advised not to use these options. Additional user permissions are required to use the expert configuration options. The following list highlights the expert options:
  - The restart timestamps of each monitor can be adjusted. This includes additional properties where applicable, i.e. the journal receiver for the audit journal monitor.
  - For more information see Expert mode configuration on page 112.
- This enhancement is related to the integration of the Journal Extract Tool (JET), which can be purchased as a separate tool from IBM Technology Services.
  - The JET tool used to process journal data based on filters for user and table names. Some clients have expressed the need to filter only for table names but report all events no matter which user caused the journal entry. The JET tool has been enhanced to process journal data by table names only. The corresponding JET command is PRCFILJRN. The Syslog Reporting Manager integration has been enhanced to support this JET enhancement. You can now specify a filter type for each monitored journal via the CFGJSPRC command. A filter type of UT indicated the filter for users and tables and the filter type of TO specifies that only table names are used in the JET processing filter.
- The event key *fname* has been added for IFS file change monitor events. It contains the IFS file name only without any path information.
- An additional internal function has been added to check the size of the SNDSYSLQ data queue. This queue holds all events that the various monitor jobs extract. Send jobs are taking these events off the queue and send them to the configured remote syslog server. It has been observed in some cases that due to network issues and remote syslog server issues, that the queue filled completely up and monitor jobs were not able to put new entries on the send queue. This causes monitor jobs to fail. The new check function will check the size of the send queue. If it reaches 75% (approx. 24750 entries) and the size does not decrease, message SLE0326 is sent to the QSYSOPR message queue and the history log every 10 minutes. If the size reaches 85% the monitor job sends this message every 2 minutes. The message should not be ignored. Typically there is an issue with the network or remote syslog server. If the size reaches 97%, the Syslog Reporting Manager ends. After a restart, the Syslog Reporting Manager tries for 2 minutes to send the entries from the send queue. If the size does not decrease within that time, the Syslog Reporting Manager ends again and an administrator must debug the cause of the issue.
  Note also that the data queue object itself can grow over time. In this version, the data queue will be recreated when SRM ends and there were no more entries on the queue. The new object has an initial size of 1 MB.
  -
- A configuration option that can be applied on a per journal basis has been added to the IFS monitor. The option is called *Drop empty events*. If set to *YES, IFS journal entries for monitored file changes that contain no data in the changed data payload are dropped and do not generate a syslog event. A payload is considered empty when:
  - the length is 0
  - the payload contains just a Line Feed (LF), Carriage Return (CR) or a combination of the two.
  - By default, the drop empty event option is disabled so that every change to a monitored file is reported even if it was just an empty line that has been added.
  -
- New IFS monitoring filter capabilities have been added in the release. Prior to this enhancement, all IFS file changes of files that are journaled in a registered and enabled journal with SRM have been sent to the configured remote syslog / SIEM server. This has not been a problem for clients that used the SRM journal IFSJRN. However, some clients have already

used journals to journal IFS file changes. They journaled 10s of thousands of files but were only interested to sent changes of several IFS files to the remote syslog server. So far when a journal was registered with SRM changes of all journaled files have been reported. There was no way to limit the reporting to just a few files unless the files were journaled in a different journal.

- In this release you can create filter lists. A filter list can have one or more file definitions. A file definition can be an absolute path, i.e. /www/prodweb/logs/access.log or a file name pattern with generic componentes, i.e. /www/%/logs/access.log. In the latter case all access.log files for any configured Web server is reported, i.e. /www/prodweb/logs/access.log, /www/testweb/logs/access.log, and /www/stagingweb/logs/access.log. The % character represents any number and kind of characters in the specified place. It can be anywhere within the path, at the beginning, or at the end.
For more information see IFS filtering support on page 28.

- The optional syslog header tag field length that can be configured via the CFGSLENV command has been changed from 15 characters to 80 characters. A tag is optional. If one is specified, the entered text is inserted between the facility/severity and the actual payload of the syslog message for RFC3164 and as a value for the MSGID field for RFC5424. It can be used, i.e. to provide additional information that identifies the source system or for filtering purposes on the syslog server side. Per RFC3164 and RFC5424, the length of this value has a maximum length of 32 characters. Using a longer value is at your own risk. A length up to 80 characters has been enabled in the Syslog Reporting Manager to accommodate requirements of some SIEM solutions that use this field as a Log ID field.

- **Statement of direction:** It is planned that V2R2 of the Syslog Reporting Manager will be the last release that supports IBM i V7R2.

11 Audit journal entry type support

The Syslog Reporting Manager was first supported with IBM i release 7.2 and specific group PTF levels. Initially only 30 audit journal entry types were supported. Throughout the years IBM development has added support for more journal entry types. Therefore, certain prerequisites have to be met to be able to leverage all journal entry types.

The following table contains a list of journal entry types including the minimum release level and possible PTF dependencies.

Entry type	Min. Release	PTF prerequsites
AD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
AF	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
AP	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
AU	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
AX	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CP	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
CQ	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CU	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CV	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
CY	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
DI	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
DO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
DS	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
EV	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
GR	7.2	7.2: SF99702 Level 21 and PTF SI67459

Entry type	Min. Release	PTF prerequsites
		7.3: SF99703 Level 10 and PTF SI67460
GS	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
IM	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
IP	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
IR	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
IS	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
JD	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
JS	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
KF	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
LD	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ML	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
M0	7.4	7.4: SF99704 Level 7
M6	7.4	7.4: SI99704 Level 9
M7	7.4	7.4: SI99704 Level 9
M8	7.4	7.4: SI99704 Level 9
M9	7.4	7.4: SF99704 Level 7
NA	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
ND	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
NE	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
OM	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
OR	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
OW	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
O1	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9

Entry type	Min. Release	PTF prerequsites
O2	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
O3	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
PA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
PF	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PG	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
PO	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
PS	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PU	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
PW	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RA	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RJ	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RP	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RQ	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
RU	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
RZ	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
SD	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
SE	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
SF	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SG	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SK	7.3	7.3: SF99703 Level 18

Entry type	Min. Release	PTF prerequsites
		7.4: SF99704 Level 7 7.3: SI74230 (provides additional cipher and protocol information) 7.4: SI74229 (provides additional cipher and protocol information)
SM	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
SO	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ST	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
SV	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
VO	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
VP	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
XD	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
X0	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
X1	7.3	7.3: SF99703 Level 18 7.4: SF99704 Level 7
X2	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
YC	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
YR	7.3	7.3: SF99703 Level 20 7.4: SI99704 Level 9
ZC	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
ZR	7.2	7.2: SF99702 Level 21 and PTF SI67459 7.3: SF99703 Level 10 and PTF SI67460
Note: The listed PTFs represent the PTF number / level where the support was added. There might be newer PTFs available that supersede the listed numbers.		

12 IBM Technology Expert Labs

Privacy and data protection are the responsibility of all. In a world where data is easily acquired, shared and stored (and potential data misuse is a concern) everyone must do their part to handle information in compliance with their company’s requirements and values. IBM research indicates security expenses are growing three times faster than IT budgets. Mounting regulatory and compliance mandates carry stiff government penalties and fines if ignored; every-growing volumes of data tax infrastructures and control capabilities; customer records disappear with alarming frequency; and security breaches cost an average of $6.6 million per incident.

IBM Technology Expert Labs

With the added pressure of a challenging economy, to compete effectively a business cannot tolerate any security exposures. From a minor breach like exposing one's password to a peer or major failure like the disclosure of client data, neither are unacceptable and can result in new administrative procedures, a failed audit or lost business. Some circumstances could even lead to a lawsuit.

Engage the experts of IBM Technology Expert Labs(formerly known as IBM Systems Lab Services) to help uphold your company's commitment to privacy and data security. Our team has developed a multitude of offerings to address your specific security concerns. From help implementing a security feature to additional resources to supplement your staff, our Consulting and Implementation Services provide general and custom consulting. Services include password elimination and single sign-on, data and tape encryption, system auditing setup and analysis, security assessments, breach analysis and penetration testing and IBM® WebSphere® Application Server health checks.

Security Tools

Complementing our security offerings are tools that we have developed over the years to assist us in the delivery of our services. These tools have been written with customers in mind to aid them in the tasks of administrating security and in response to requirements to fill product gaps. They range from easy–to–install tools and utilities to more complex solutions; the latter often includes a services component intended to provide technical training and implementation services so clients and business partners can acquire and maintain mission critical skills. The tools listed below are our most requested. Others exist as well. Perhaps we can build something for you?

IBM i Security Diagnostics Tool (iSAT)

The IBM i Security Diagnostics Tool (iSAT) is an exhaustive security collection tool that is often used during a security assessment to help discover and document security vulnerabilities. More than statistical information found in the Quick Security Check Tool, the iSAT tool drills deep to analyze object authorities, elevated privileges, etc. to enable a holistic methodical approach towards security hardening. It can also be purchased separately for customers wishing to enhance their security reporting capability.

Compliance Assessment and Reporting Tool (includes Event Monitoring)

The Compliance Monitoring Tool is a centralized security and systems information Data Mart. The tool utilizes DB2 Web Query to provide a web-based interface for easy monitoring of compliance on any or all systems in an enterprise. The GUI includes color coding which highlights deviations from policy, unexpected differences of policy settings between systems, and security attributes that do not adhere to corporate security objectives. Additional capabilities provided by the tool also include:

- An ability to quantify and act upon several aspects of security as statistical measurable components as well as compliance to corporate defined objectives for configuration consistency
- A scoring mechanism (seeded with Best Practices) for prioritization of policy items by High, Medium and Low risk that is customizable by customer objectives
- Built in extensibility to add user-defined items for monitoring inventory, auditing, status, etc. with incorporated scoring mechanisms provided by the tool. These items can be customer defined and written or services obtained for enhancements.
- A federated repository of IBM i user profiles that provide cross system observability of profile administration. This repository could be utilized in the development of administrative tools to reduce helpdesk costs associated with user administration.
- An ability to monitor events as they happen - providing near "real time" monitoring of more than 180 of the most common security events. Additional messages and events can be monitored through a customization utility. These events can be made "actionable" through a provided utility that forwards these events to a customer defined message queue for further action, ie., send to email, cell phone or SMS.

Single Sign On (SSO) / Enterprise Identity Mapping (EIM) Populator Tool

The need for multiple user registries, an issue most enterprises face, creates a large administrative challenge. EIM for the IBM i platform offers administrators and application developers an inexpensive solution for easier management of multiple user registries and user identities. EIM creates a system of identity mappings, called associations, between various user identities in various user registries. It provides a common interface across platforms to look up relationships between user identities.

One of the more time-consuming tasks in implementing a single sign-on solution is registering users to the EIM repository. The EPT is a Java-based desktop GUI application that allows an administrator to easily import information from a comma–separated value text file. With EPT, take a spreadsheet of known user IDs and/or names and create identifiers and mappings for each user. Java 1.4 or higher is required.

Certificate Expiration Manager (CEM)

The Certificate Expiration Manager (CEM) is a Java-based tool for simplifying the management of certificate expiration (cross-platform). CEM maintains a log of all expiration activities and can send notifications vial email. An easy to use configuration GUI is included for managing the XML settings. The tool only runs on platforms that support Java.

Single Sign On (SSO) / Enterprise Identity Mapping (EIM) Management Tool

The EIM Management Tool is a Java-based desktop GUI application that allows an administrator to easily manage the information within an EIM repository, via a more user-friendly layout than what is provided in iSeries Navigator. Identifiers, aliases, descriptions, associations, and user registries can be created, deleted, and renamed, all from the same screen. The tool also includes a tree view of the EIM repository, domain management functions to create/delete EIM domains, save/restore of the data in an EIM domain to/from a local XML file, as well as a password synchronization view to manipulate EIM data that pertains to the network password synchronization tool (NPST). Java 1.4 or higher is required.

MS Windows Active Directory to IBM i User Synchronization Tool

The Microsoft Windows Active Directory to IBM i user synchronization tool is a lightweight Java tool that offers a programmatic way to create and change IBM i user profiles when changes are detected on the MS Active Directory. All changes on the IBM i are triggered from actions on the MS Active Directory.

Note: IBM i user profile changes do not trigger changes on the MS Active Directory - all tool actions should be considered “one way” going from the MS Active Directory to the IBM i.

Security Exit Points

The Security Exit Point Tool simplifies the managing of Exit Point definitions for users on an IBM i. Currently, the tool includes programs for managing the Exit Points for CLI, DRDA/DDM, FTP, IFS, ODBC, JDBC, File Transfer, REXEC, RMTCMD, Host Server Signon, and others. Additional Exit Point Programs will be added in the future. The tool provides the Security Administrator with an interface to define which users are allowed to use the defined Exit Point. An Audit Journal record is created whenever a user accesses the defined Exit Points.

Password Validation

Despite warnings, one-in-five users choose a non-compliant password to protect their identity. We’ve developed a program that validates and ensures passwords meets company and industry recommended rules and guidelines. The tool also allows the security administrator to establish a dictionary of excluded terms, to further tighten password security.

Password Synchronization

Studies show that corporate users tend to repeat passwords on the various systems they use. The Password synchronization tool makes it easier for end users to remember these passwords and simplify their access to multiple partitions. This is accomplished by reducing the number of passwords that an end user needs to remember, making it less likely for them to write them down, resulting in fewer calls to the corporate Help Desk and less opportunity for others to gain improper access. In addition to password synchronization, this tool supplements the IBM i Operating System supplied password rules to strengthen your security posture.

For more information about IBM Technology Expert Labs Security Offerings . . .

Terry Ford, Team Leader
Security Services Delivery
+1-507-253-7241 (Office)
taford@us.ibm.com

Thomas Barlen, Senior Managing Consultant
IBM Power System Security
barlen@de.ibm.com

Robert Andrews, Senior Managing Consultant
+1-507-250-2701 (Mobile)
+1-507-253-4205 (Office)
robert.andrews@us.ibm.com

Ron Bibby, Proposal Specialist
+1-281-455-6573 (Mobile)
+1-281-455-6573 (Office)
ronbibby@us.ibm.com

Beatrice Luquet, Proposal Specialist
+33-6-88062235 (Mobile)
beatrice.luquet@fr.ibm.com

Or visit our website at:
https://www.ibm.com/support/pages/ibm-i-security
https://www.ibm.com/products/expertlabs