iSecurity AP Journal

User Guide
Version 10.03

www.razlee.com

Contents

Software Version: 10.03

About this Manual

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

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

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

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

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

Intended Audience

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

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

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

Native IBM i (OS/400) User Interface

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

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

Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

SRTJR **> 81 > 32**

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

Menus

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

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

Manual Revised: Wednesday, April 16, 2025

Contacts

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

Introducing AP-Journal

Overview

IBM i applications are based upon databases which include multiple tables. Each of these tables includes items of information that are used by one or more sub-applications. Any changes made to tables are logged by a process known as journaling. During a journal operation, changed information from a table is sent to a journal receiver. The journal receiver usually includes journaled information as well as journal meta-data that includes, for example, the name of the user who preformed the change, the name of the changed file, the date and time of change, the data image before and after the change, and so on.

Another way of looking at this is that IBM i user applications are usually based upon sub-applications appropriate for different groups of users. The various sub-applications many times use different data structures and sometimes one item of information can be represented in different ways in different tables. For example, the names of the fields that represent an account number, indeed even the length or data format of these fields and their location can differ from one table to another.

Let's assume that a hospital uses one application to keep track of surgical proceedings executed by its staff, a second application to keep track of the prescriptions written by its staff and a third application to keep track of the patients being examined by its staff. The information relating to each application is stored in a different table, and different journal receivers store journaled information generated by the different applications.

Therefore, if a manager wishes to determine the activities of a certain staff member on a certain day (participated in a surgical procedure, dispensed prescriptions and examined a number of patients), the manager will have to manually combine information from different applications.

The AP-Journal Solution

AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal. This cutting-edge security solution provides expert field-tracking and monitoring. AP-Journal is

a valuable tool for Sarbanes-Oxley compliance and other auditing regulations.

Until now, database management has lacked the proper tools to monitor data modification down to the field level. This product offers a streamlined, easy-to-use solution. With AP-Journal, every field is tracked and monitored so that a trigger may be initiated if, for example, the amount of a bank loan has been modified by more than 20%. AP-Journal also provides tools and analysis capabilities to compare the changed data values and results with the previous data.

How AP-Journal Works

AP-Journal generates a control data structure representing multiple items of information that were journaled, from a group of tables to a group of journal receivers. AP-Journal's journal data structure easily associates between different table representations for any particular item of information. AP-Journal also receives requests to retrieve journaled information items as necessary.

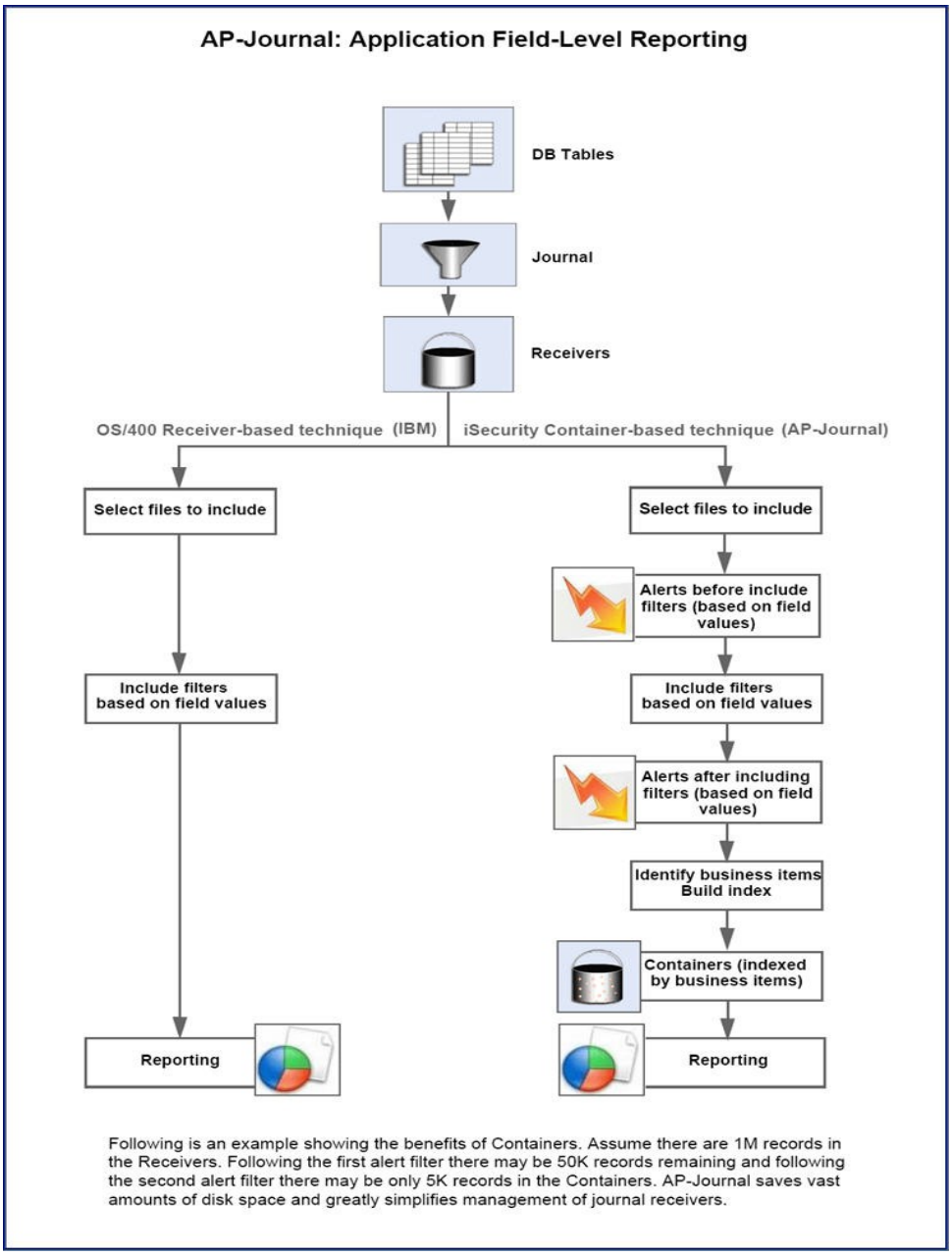
AP-Journal is fed by the IBM receiver, therefore it is enough to install AP-Journal in the machine where the receiver is located.

There is one point that has to be considered, an image of the running application database has to be defined in the remote system, in order to be able to retrieve into the application the file/field names. That image can be of course, empty files. Once this is done, AP-Journal can retrieve the information from the remote journal receiver that is located "locally".

Figure 1 compares the direct, IBM, approach to reporting on data base changes recorded in journal receivers with AP-Journal's container-based approach.

In comparison with using journal receivers, AP-Journal:

- saves disk space
- simplifies management of journal receivers
- reduces I/O and CPU time when retrieving data
- provides real-time e-mail or message alerts based upon changes to field values



Native IBM i (OS/400) Text Based User Interface

AP-Journal's reports specify not only the changes in data but also who made the changes, at what time, from which application, and more. Journaled data from several files can be cross-referenced by referral to joint information in all relevant files; that is, fields from different files can be identified as containing the same logical information (item number, loan ID, patient identifier, and so on). With this feature it is possible to obtain the history of a transaction by referring to the same ID across many files. Information

accumulated over many years can be accessed in near real time mode. Data retrieval is simple and is defined in accordance with user needs. AP-Journal provides users more control than ever before over the flow of information within the organization.

AP-Journal is a valuable addition in industries such as finance, health-care, commerce, insurance, military, and others. As part of Raz-Lee's iSecurity suite, AP-Journal offers you top functionality, ease-of-use, and tomorrow's technology today.

AP-Journal is designed to be a user-friendly product. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

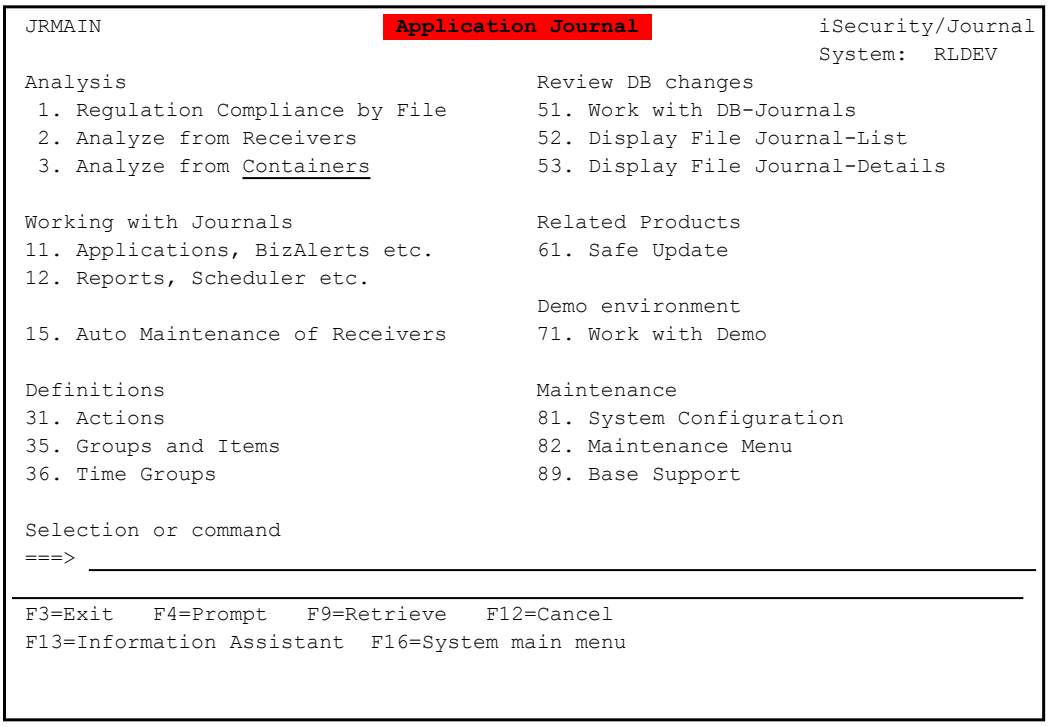
Many features are also accessible via the command line, for the convenience of experienced users.

Regulation Compliance

AP-Journal's reports specify the changes in data but also who made the changes, at what time, from which application, and more. With this feature it is possible to obtain the history of a transaction by referring to the same ID across many files. Information accumulated over the years can be accessed in near real time mode.

Start working with AP-Journal

To **start AP-Journal**, type the *STRJR* command at the command line. The **AP-Journal** main menu appears.



To work with file updates, select **`1. Regulation Compliance by File`**. The **Regulation Compliance** screen appears as shown in "Working with Single Files " on page 16.

To **work with business analysis for journal receivers**, select **`2. Analyze from Receivers`**. The **Business Analysis** screen for journal receivers appears as shown in "Business Analysis Journal Receivers" on page 26.

To **work with business analysis for containers**, select **`3. Analyze from Containers`** from the main menu (*STRJR*). The **Business Analysis** screen for containers appears as shown in "Business Analysis Containers" on page 34.

To **start working with Applications, BizAlerts - Definitions**, select **`11. Applications, BizAlerts etc.`** from the main menu (*STRJR*). The **Applications, BizAlerts - Definitions** screen appears as shown in "Working with Applications and BizAlerts" on page 46.

To define reports, scheduler, etc., select **12.Reports, Scheduler etc.** from the main menu (*STRJR*) as shown in "Reporting and Scheduling " on page 94.

To work with IBM Journal Receivers, select **15. Auto Maintenance of Receivers** from the main menu (*STRJR*) or select **75. Auto Maintenance of Receivers** from the Applications, BizAlerts – Definitions screen (*STRJR > 11*). The Work with Journal Receivers Maintenance screen appears as shown in "Auto Maintenance of Receivers" on page 89.

To work with actions, select **31. Actions** from the main screen (*STRJR*) as shown in "Actions" on page 113

To work with group types, select **35. Groups and Items** from the main menu (*STRJR*) as shown in "Groups and Items" on page 117

To define a time group, select **36. Time Groups** from the main menu (*STRJR*) as shown in "Time Groups" on page 122.

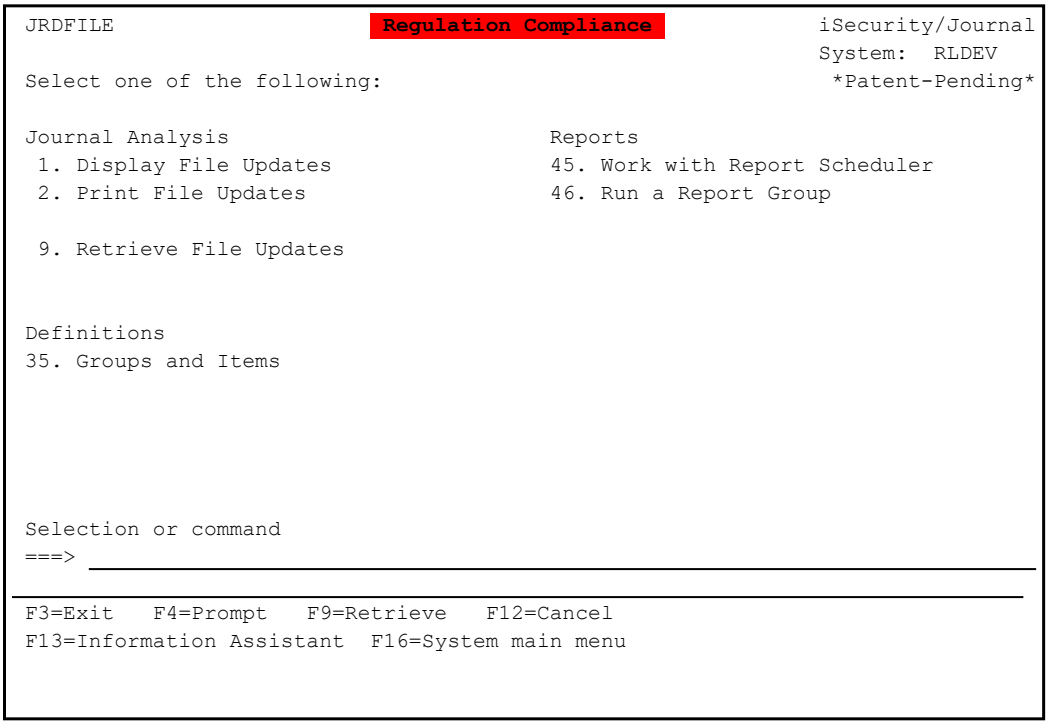
To review database changes, use option **51. Work with DB-Journals**, **52. Display File Journal-List**, **53. Display File Journal-Details** as appropriate, as shown in "Reviewing Database Changes" on page 125

To work with system configuration, select **81. System Configuration** from the main menu (*STRJR*). The iSecurity/AP-Journal System Configuration screen appears as shown in "Configuration and Maintenance" on page 127.

To access the Maintenance Menu, select **82. Maintenance Menu** from the main menu (*STRJR*). The Maintenance Menu screen appears as shown in "Configuration and Maintenance" on page 127.

To access the BASE Support menu, select **89. BASE Support** in the product's main menu (*SRTJR>* **89**). The BASE Support screen appears as shown in "BASE Support" on page 142.

Working with Single Files



To **view changes** that were done to a single file, select **`1. Display File Updates`** from the **Regulation Compliance** menu (*STRJR*> **`1`**) as shown in "Displaying File Updates " on the facing page. The section is also included the Setting Filter Conditions explanation.

To **print the file changes**, select **`2. Print File Updates`** from the **Regulation Compliance menu** (*STRJR*> **`1`**) as shown in "Print File Updates" on page 22.

To **retrieve updates** and put them into a new output file, select **`9. Retrieve File Updates`** from the **Regulation Compliance** menu (*STRJR* > **`1`**) as shown in "Retrieving Data-Base Journals" on page 22

To **work with groups**, select **`35. Groups and Items`** from the **Regulation Compliance** menu (*STRJR > 1*) as shown in "Groups and Items" on page 117.

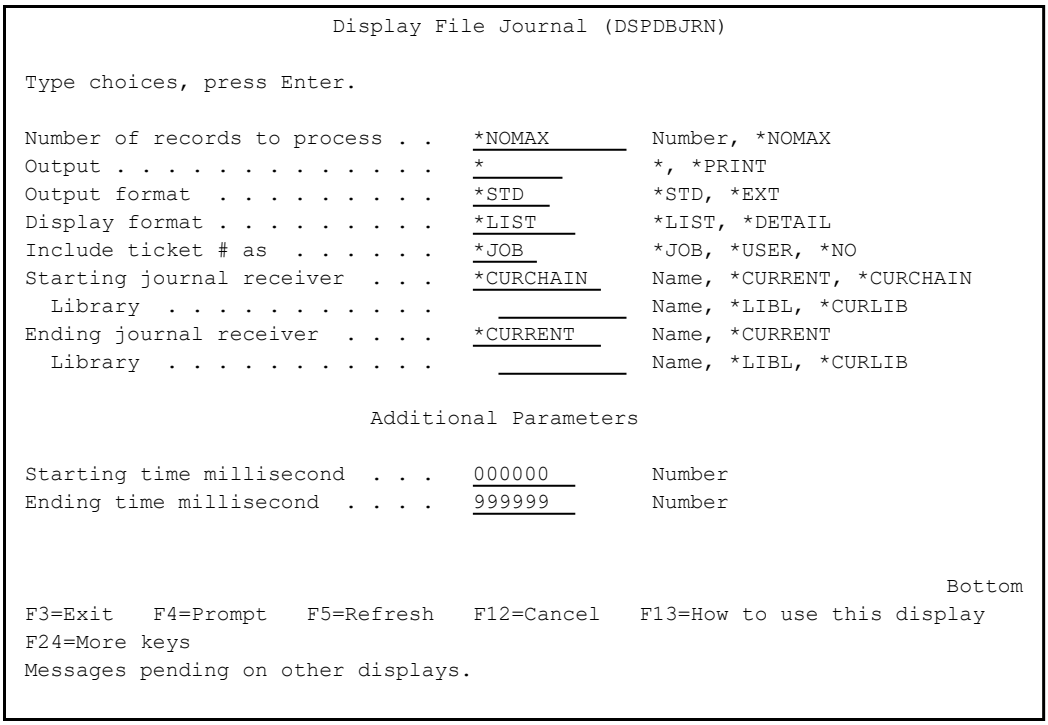
To **work with report scheduler**, select **`45. Work with Report Scheduler`** from the **Regulation Compliance** screen (*STRJR > 1*). The **Work with Report Scheduler** screen appears as shown in "Define Report Schedules " on page 98.

To **run a report group**, select **`46. Run a Report Group`** from the**Regulation Compliance** screen (*STRJR > 1*). The **Run Report Group (RUNRPTGRP)** screen appears as shown in "Define Report Schedules " on page 98.

Displaying File Updates

To **view changes** that were done to a single file, select **`1. Display File Updates`** from the **Regulation Compliance** menu (*STRJR>* **`1`**). The **Display File Journal (DSPDBJRN)** screen appears.

```
                      Display File Journal (DSPDBJRN)

Type choices, press Enter.

File . . . . . .                 _________     Name
  Library  . . . . . .             *LIBL       Name, *LIBL, *CURLIB
                                   _________
                                    *LIBL
Display last minutes . . . . . .  *BYTIME      Number, *BYTIME
Starting date and time:
  Starting date  . . . . . .      *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .      000000       Time
Ending date and time:
  Ending date  . . . . . .        *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . .        235959       Time
User profile . . . . . .          *ALL         Name, *ALL
Program name . . . . . .          *ALL         Name, *ALL
Job name . . . . . .              *ALL         Name, *ALL
  User . . . . . .                 __________  Name
  Number . . . . . .               ______      000000-999999
                                                                    More...
F3=Exit    F4=Prompt    F5=Refresh    F10=Additional parameters    F12=Cancel
F13=How to use this display         F24=More keys
```



NOTE: Ensure that you have defined the outputs for the file as described in "Output Fields per File" on page 78.

File

The file to be displayed.

Library

The library containing the file.

NOTE: You can specify two different files, using the fields under this one for the second **File** and **Library**.

Display last minutes

To view activity in the immediate past, enter a number corresponding to the number of minutes that you would like to check. For example, to check activity in the past 120 minutes, enter 120 in this field. This value would override starting and ending date and time fields.

Starting date and time

Starting date

The day or date on which the included data begins.

Allowed values include:

- ***CURRENT**: The current date
- ***YESTERDAY**: Yesterday's date
- ***WEEKSTR**: The first day of the current week. By default, this is Sunday.
- ***PRVWEEKS**: The first day of the previous week
- ***MONTHSTR**: The first day of the current month
- ***PRVMONTHS**: The first day of the previous month
- ***YEARSTR**: The first day of the current year
- ***PRVYEARS**: The first day of the previous year
- ***MON**: Monday
- ***TUE**: Tuesday
- ***WED**: Wednesday
- ***THU**: Thursday
- ***FRI**: Friday
- ***SAT**: Saturday
- ***SUN**: Sunday

Starting time

The time on the Starting date at which the included data begins, in **HHMMSS** format.

Ending date and time

Ending date

The day or date on which the included data ends.

Allowed values are the same as for **Starting date**.

Ending time

The time on the **Ending date** at which the included data ends, in **HHMMSS** format.

User profile

The user who updated the file.

Program name

The name of the program that changed the file's information

Job name

The name of the job that changed the file's information

Number of records to process

The maximum number of records to process. For an unlimited number, enter ***NOMAX**.

Output

Where to send the output. Possible values include:

- ***PRINT** to send output to the print queue
- ***** to send output to the display

Output format

NOTE: This field only appears if you set the **Output** field to ***PRINT**.

The format of the output. Possible values include:

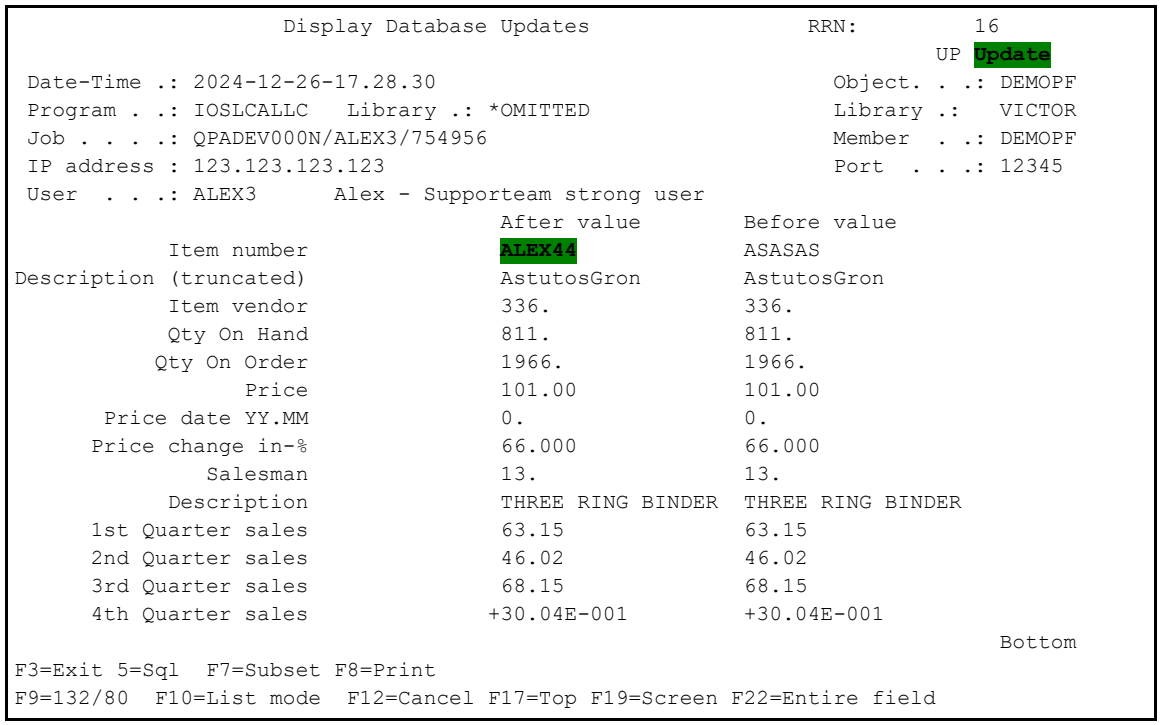
- ***STD** for standard format
- ***EXT** for extended information, such as the name of the program that made the changes.

Include ticket # as

NOTE: This field only appears if you set the **Output** field to ***PRINT**.

- ***JOB**
- ***USER**
- ***NO**

Type the file and library name, set the criteria and press Enter. The Display Database Updates screen appears, showing the information of the requested file before and after the changes. The fields that were changed will appear in inverse.



The screen contains these fields:

Date-Time

The date and time of the update.

Program

The name of the program that changed the file's information

Job

The name of the job that changed the file's information

IP Address

The IP address from which the change was made (in VSR3 and upward).

User

The user who updated the file.

Object

The file that was updated.

Library

The library containing the file.

Member

The member that was updated.

Port

The network port used for the connection when the change was made.

The body of the screen lists the files included in the search.

To filter the results, press the F7=Subset key, the Define Include Filters screen appears as shown in Setting Filter Conditions.

Print File Updates

To print the file changes, select **2. Print File Updates** from the Regulation Compliance menu (*STRJR*> **1**). The Display File Journal (DSPDBJRN) screen appears with the **Output** field set to ***PRINT**.

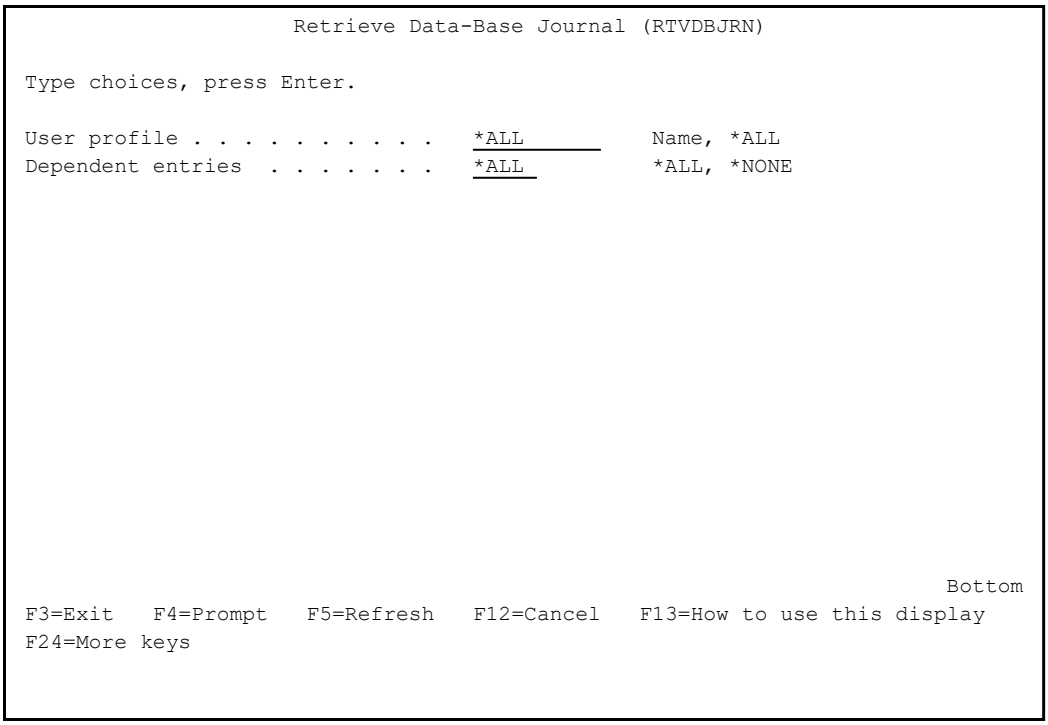
NOTE: In the output, a special character appears next to fields that were changed. By default, it is the right-arrow character ("**>**"). You can change this from the System Configuration screen (*STRJR* **> 81**).

Retrieving Data-Base Journals

To retrieve updates and put them into a new output file, select **9. Retrieve File Updates** from the Regulation Compliance menu (*STRJR* **> 1**). The Retrieve Data-Base Journal (RTVDBJRN) screen appears.

```
                    Retrieve Data-Base Journal (RTVDBJRN)

 Type choices, press Enter.

 File . . . . . .              _________    Name
   Library  . . . . . .          *LIBL      Name, *LIBL
 File to receive output . . . . .  _________  Name, *TEMP, *FILE
   Library  . . . . . .          QTEMP      Name, *LIBL
 Output member options:
   Member to receive output . . .  *FIRST     Name, *FIRST
   Replace or add records . . . .  *REPLACE   *REPLACE, *ADD
 Output (on interactive job)  . .  *          *, *PRINT, *NO
 Journal  . . . . . .          *CURRENT   Name, generic*, *CURRENT, *ALL
   Library  . . . . . .          _________  Name, *LIBL, *CURLIB
 Range of journal receivers:
   Starting journal receiver  . .  *CURRENT   Name, *CURRENT, *CURCHAIN
     Library  . . . . . .          _________  Name, *LIBL, *CURLIB
   Ending journal receiver  . . .  _________  Name, *CURRENT
     Library  . . . . . .          _________  Name, *LIBL, *CURLIB

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

```
                    Retrieve Data-Base Journal (RTVDBJRN)

Type choices, press Enter.

Starting date and time:
  Starting date  . . . . . .    _________    Date
  Starting time  . . . . . .    ________     Time
Ending date and time:
  Ending date  . . . . . .      _________    Date
  Ending time  . . . . . .      ________     Time
Number of journal entries  . . .  *ALL        Number, *ALL
Member of retrieved file . . . .  *ALL        Name, *FIRST, *ALL
Journal codes:                  _
  Journal code value . . . . . .  *ALL        *ALL, A, C, F, J, L, M, O...
  Journal code selection . . . .  _______     *ALLSLT
             + for more values  _
Job name . . . . . .          *ALL        Name, *ALL
  User . . . . . .              _________  Name
  Number . . . . . .            ______     000000-999999
Program  . . . . . .          *ALL        Name, *ALL
                                                                   More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```



The screen contains these fields:

File

The file that was updated.

Library

The library containing the file.

File to receive output

The file that should receive the data.

Library

The library containing the file.

Output member options

Member to receive output

The member that should receive the output.

Replace or add records

Specify if you want to replace or add the records.

Output (on interactive job)

Specify if you want to have an output on screen, printed or no output needed.

Journal

The database journal that contains the updates.

Library

The library containing the journal.

Range of journal receivers

Specify from start and end of journal receivers that you want to retrieve data from

Starting date and time

Specify the start date/time that you want to retrieve data from

Ending date and time

Specify from start and end of journal receivers that you want to retrieve data to

Number of journal entries

Specify how many journal receiver entries you want to proceed.

Member of retrieved file

Specify the members of the source file that you want to retrieve.

Journal codes

Specify what journal codes you want to use for retrieval.

Job name

Specify from what job data should be retrieved.

Program

Here you can specify from what program the data were changed that you want to retrieve.

User profile

Here you can specify from what user the data were changed that you want to retrieve.

Dependent entries

Here you can specify if you want to retrieve also dependent entries to the output file.

Business Analysis

Overview

Business Analysis allows users to find database changes based on the pure data within the database journal receivers or from so-called containers.

Database journal receivers are usually used for applications that need commitment control to write database changes in the files once a complete chain of transactions is completed or for HA purposes where changes in files are written in database journals, transferred to the HA system, and restored there.

AP-Journal uses technology to retrieve database changes from the database journal receivers, filter them, and put needed information to analyze for a longer period into log files – Containers. The solution allows users to decide how long to store data online.

Business Analysis Journal Receivers

To work with business analysis for journal receivers, select **`2. Analyze from Receivers`** from the main menu (*STRJR*). The Business Analysis screen for journal receivers appears.

```
JRDSET                          Business Analysis              iSecurity/Journal
                                                               System:  RLDEV
Select one of the following:                                    *Patent-Pending*

Business Analysis Journal Receivers      Reports
 1. Display list of updates              41. Reports
 2. Display updates                      45. Work with Report Scheduler
 3. Display Journal (by journal name)    46. Run a Report Group
 5. Print updates
 6. Print updates (extended info)        Use options 1-7 to run Reports
 7. Print Journal (by journal name)      over Journal Receivers.

Definitions
35. Groups and Items

The above options are based upon Journal Receivers.
Business Analysis requires a report definition (option 41).

Selection or command
===> ____________________________________________________________________________

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

To **display the list of changes** that were done on a set of files, select **1. Display list of updates**. The **Display APP Current Journal (DSPAPCRJ)** screen appears.

```
                    Display APP Current Journal (DSPAPCRJ)

 Type choices, press Enter.

 Report or Application F4=Names     *SELECT       Name, *SELECT, *JRN, AUXXJ...
 Display last minutes . . . . . .   *BYTIME       Number, *BYTIME
 Starting date and time:
   Starting date  . . . . . .       *CURRENT      Date, *CURRENT, *YESTERDAY...
   Starting time  . . . . . .       000000        Time
 Ending date and time:
   Ending date  . . . . . .         *CURRENT      Date, *CURRENT, *YESTERDAY...
   Ending time  . . . . . .         235959        Time
 User profile . . . . . .           *ALL          Name, *ALL
 Program name . . . . . .           *ALL          Name, *ALL
 Job name . . . . . .               *ALL          Name, *ALL
   User . . . . . .                                Name
   Number . . . . . .                              000000-999999
 Number of records to process . .   *NOMAX        Number, *NOMAX
 Output . . . . . .                 *            *, *PRINT, *PDF, *HTML..
 Add column headings  . . . . . .   *YES          *NO, *YES
                                                                      More...
 F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

Report or Application

Set of files to display

*JRN = Press F9 and Page Down twice, then enter a name in the "For APP(*JRN) - Journal" field as well as a library name of the file that was updated.

Display last minutes

Last N minutes to display.

Starting date and time

Specify the start date/time that you want to retrieve data from

Select only those records occurring within the range specified by the starting and ending time specified below

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

Ending date and time

Specify from start and end of journal receivers that you want to retrieve data to

Select only those records occurring within the range specified by the starting and ending time specified below

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

User profile

User profile who conducts the file's update

Program

Name of the program used to change the file's information.

Job name

Name of the job that changed the file's information.

Number of records to process

Specify how many journal receiver entries you want to proceed.

Output

* = to display only

*PRINT = to print

*PDF = PDF file

*HTML = HTML file

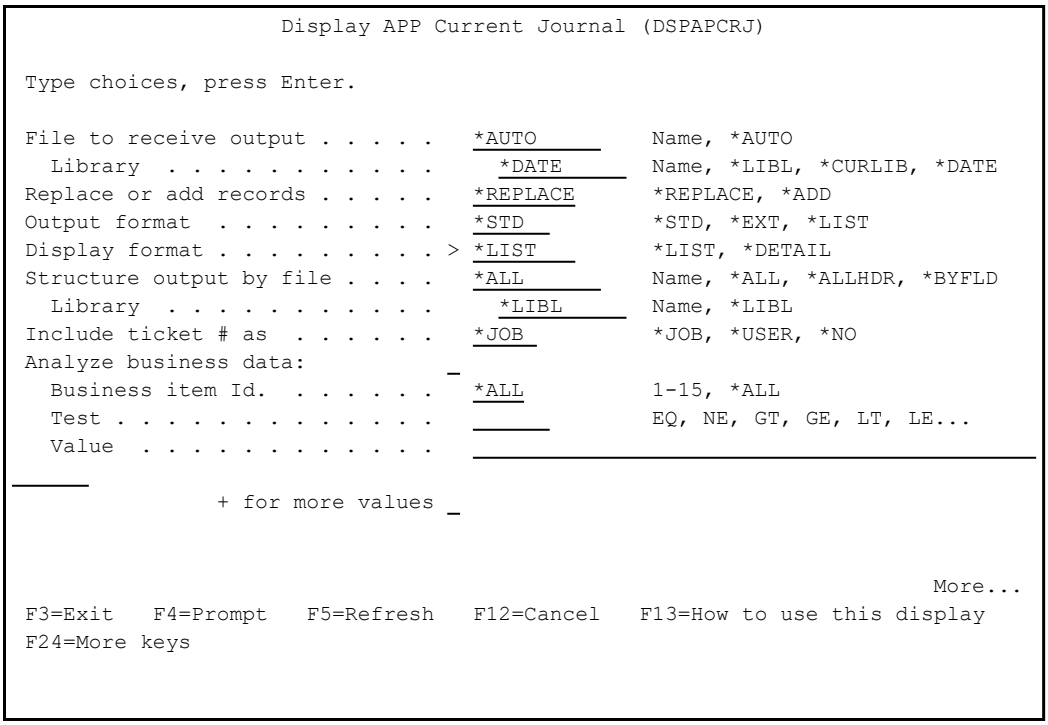
*OUTFILE

*PRINT1-*PRINT9 = Select correct print option.

Press F9/F10 for more parameters.

Add column headings

In case of output options in pc format, you can add column headings to make it easier to handle the document.



File to receive output

Specify the name of the file that should receive the output in case of Output *OUTFILE. Special value *AUTO creates a file starting with RPTxxx that contains the output.

Library

The library containing the file. Special value *DATE creates a library SMZRyymmdd and puts the outfile here.

Replace or add records

Specify if you want to replace or add the records.

Output format

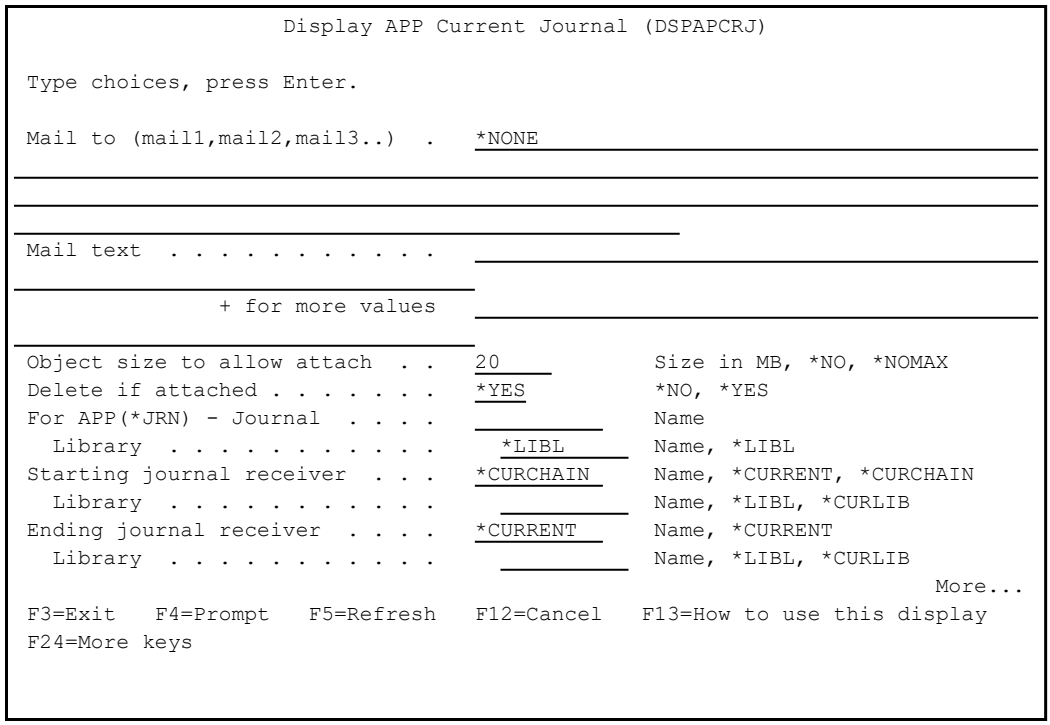
*STD = Standard output shows all journal entries, data only

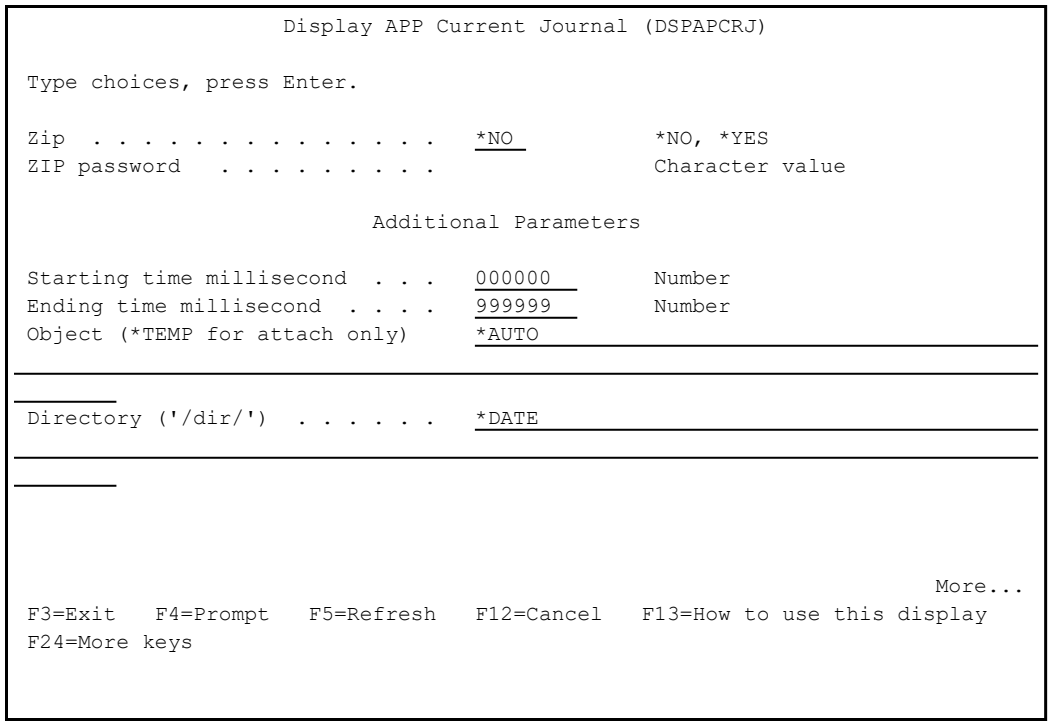
*EXT = Extended output shows all journal entries including header information

*LIST = List output, shows one line header information per journal entry

Display format

*LIST = Shows one line per journal entry. Header information





Type choices and press **Enter**. The **Display Journal Entries** screen appears.

```
                          Display Journal Entries
 Name  . . . .:  DEMO1   Demo Victor
 Type options, press Enter.
  5=Display entire entry  6=SQL  9=Screen  U=Undo

 Opt     Object     Job         Program    User       Date-time                RRN
  _ UP   JRTEST     QPADEV000M IOSLCALLC  VICTOR     2025-01-12-12.51.29        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-12.56.40        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT VICTOR     2025-01-12-12.58.59        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.02.25        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.05.01        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.10.07        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT VICTOR     2025-01-12-13.16.05        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.05.55        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.15.58        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.20.14        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.28.11        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.48.01        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.54.48        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT HAIM       2025-01-13-11.21.56        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT HAIM       2025-01-13-12.24.36        1
  _                                                                       More...
  F3=Exit  F7=Subset  F10=Detail mode  F12=Cancel  F17=Top   F22=Display entire
```

To **display entire entry**, type **5** in the **Opt** field next to the entry. The **Display Database Updates** screen appears as shown below, displaying the changed fields.

```
                    Display Database Updates                RRN:         16
                                                                      UP Update
 Date-Time .: 2024-12-26-17.28.30                          Object. . .: DEMOPF
 Program . .: IOSLCALLC   Library .: *OMITTED              Library .:   VICTOR
 Job . . . .: QPADEV000N/ALEX3/754956                      Member  . .: DEMOPF
 IP address : 123.123.123.123                              Port  . . .: 12345
 User  . . .: ALEX3      Alex - Supporteam strong user
                                    After value        Before value
           Item number              ALEX44             ASASAS
Description (truncated)             AstutosGron        AstutosGron
           Item vendor              336.               336.
           Qty On Hand              811.               811.
          Qty On Order              1966.              1966.
                 Price              101.00             101.00
      Price date YY.MM              0.                 0.
     Price change in-%              66.000             66.000
              Salesman              13.                13.
           Description              THREE RING BINDER  THREE RING BINDER
     1st Quarter sales              63.15              63.15
     2nd Quarter sales              46.02              46.02
     3rd Quarter sales              68.15              68.15
     4th Quarter sales             +30.04E-001        +30.04E-001
                                                                      Bottom
F3=Exit 5=Sql  F7=Subset F8=Print
F9=132/80  F10=List mode  F12=Cancel F17=Top F19=Screen F22=Entire field
```

To **show the SQL statement**, type **6** in the **Opt** field next to the entry. The **SQL Statement** screen appears (if available).

NOTE: The displayed SQL is the most relevant SQL operation for the selected DB Journal operation, assuming that SQL was used. DB Journal does not provide exact information as per the method (*) or SQL statement that caused the transaction. The displayed SQL statement is relevant only if SQL was used. Other SQL statements that were prepared earlier should also be considered. The SQL statements are presented from the iSecurity/Firewall log. (*) On the IBM i, I/O operations are performed by either traditional read/write/update/delete operations or by SQL.

To **show the screen** (if available), type **9** in the **Opt** field next to the entry. Select the screen in the **Select Frame to Start with (then use Page Up/Down)** pop-up window.

To **undo the record change**, type U in the **Opt** field next to the entry. The **Confirm Undo of a Record Change** screen appears. Type choices and press **Enter**.

To **filter the results**, press the **F7=Subset** key, the **Define Include Filters** screen appears. Setting the Filter Conditions and the Order of Rules is described in "Displaying File Updates " on page 17(Setting Filter Conditions).

To **display updates** that were done on a set of files, select **2. Display updates** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Display APP Current Journal (DSPAPCRJ)** screen appears with the predefined Display format parameter to *DETAIL. Type choices and press Enter. The **Display Database Updates** screen appears.

To **display journal**, select **3. Display Journal (by journal name)** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Display APP Current Journal (DSPAPCRJ)** screen appears with the predefined Report or Application parameter to *JRN. Type choices and press **Enter**.

To **print updates**, select **`5. Print updates`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Display APP Current Journal (DSPAPCRJ)** screen appears with the predefined Output parameter to *PRINT. Type choices and press **Enter**.

To **print updates** (extended info), select **`6. Print updates (extended info)`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Display APP Current Journal (DSPAPCRJ)** screen appears with the predefined Output parameter to *PRINT and the Output format parameter to *EXT. Type choices and press **Enter**.

To **print journal** (by journal name), select **`7. Print Journal (by journal name)`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Display APP Current Journal (DSPAPCRJ)** screen appears with the predefined Report or Application parameter to *JRN and the Output parameter to *PRINT. Type choices and press **Enter**.

To **work with groups types**, select **`35. Groups and Items`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Work with Group Types** screen appears as shown in "Groups and Items" on page 117.

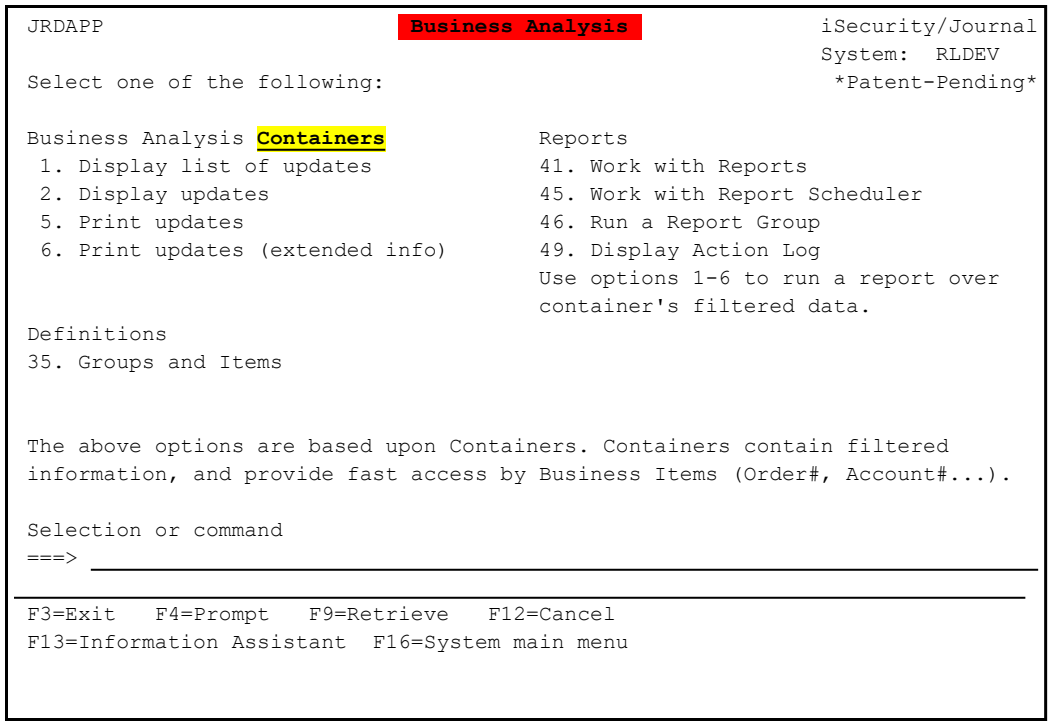
To **work with reports**, select **`41. Reports`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Work with Reports** screen appears as shown in "Working with Reports " on page 95.

To **work with report scheduler**, select **`45. Work with Report Scheduler`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Work with Report Scheduler** screen appears as shown in "Define Report Schedules " on page 98

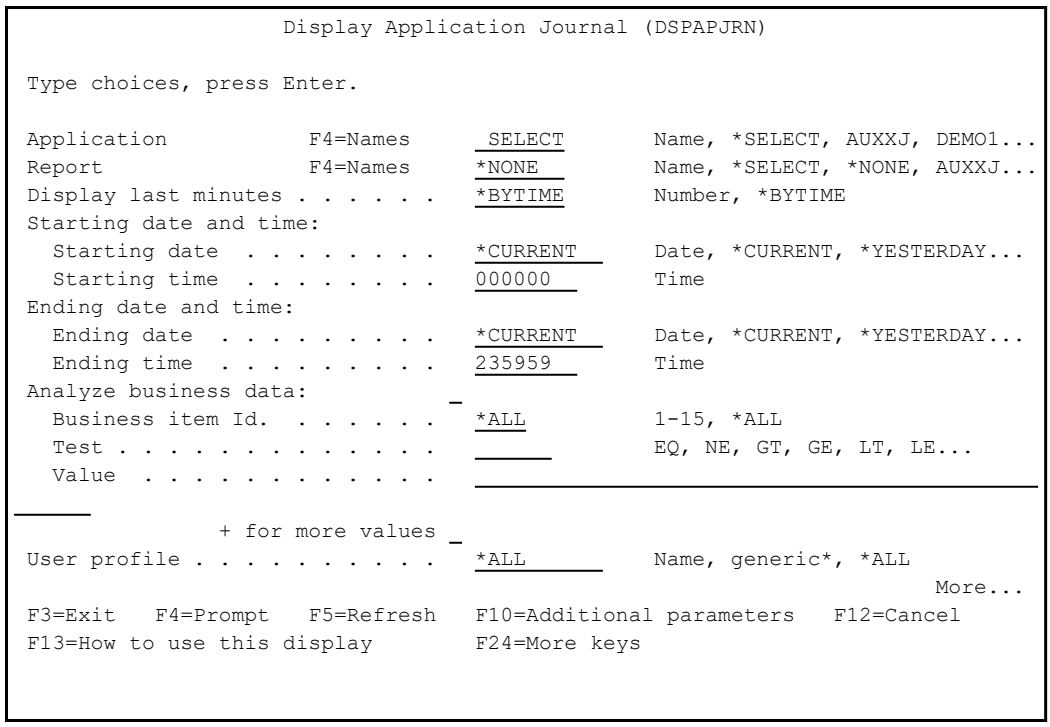
To **run a report group**, select **`46. Run a Report Group`** from the **Business Analysis** screen for journal receivers (*STRJR > 2*). The **Run Report Group (RUNRPTGRP)** screen appears as shown in "Define Report Schedules " on page 98 (Run Report Groups).

Business Analysis Containers

To **work with business analysis for containers**, select **`3. Analyze from Containers`** from the main menu (*STRJR*). The **Business Analysis** screen for containers appears.



To **display the list of changes** that were done on a set of files, select **1. Display list of updates**. The **Display Application Journal (DSPAPJRN)** screen appears.



Application

*SELECT/F4 shows a screen where you can specify the application.

NOTE: To define the application from which you want to see database changes, select **1. Work with Journal Applications** from the Applications, BizAlerts – Definitions screen (*STRJR > 11)*.

Report

*SELECT/F4 shows a screen where you can specify the report.

NOTE: Reports are saved subsets of applications where you can apply predefined filters to work with limited changes in databases. Reports can be used in addition to the Application.

*NONE - No report should be used.

Display last minutes

Last N minutes to display.

Starting date and time

Specify the start date/time that you want to retrieve data from

Select only those records occurring within the range specified by the starting and ending time specified below

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

Ending date and time

Specify from start and end of journal receivers that you want to retrieve data to

Select only those records occurring within the range specified by the starting and ending time specified below

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

Analyze business data

AP-Journal allows users to define Business Items within an Application. These Business Items are specific field names that can be used to filter database changes based on their values.

For example, if users define a Business Item such as CustomerNumber, which appears in multiple files, they can trace all changes related to a specific customer (e.g., customer 4711) across all files associated with the Application.

Business Item ID

Select a specific Business Item (1–15) or use *ALL to apply the filter to all defined Business Items.

Test

Use the **Test** field to define the type of comparison for the Business Item value:

EQ – Equal to

NE – Not equal to

GT – Greater than

GE – Greater than or equal

LT – Less than

LE – Less than or equal

LIKE – Text contains pattern (use % for wildcard)

NLIKE – Text does not contain pattern (use % for wildcard)

LIST – Value is in a list

NLIST – Value is not in a list

Value

Specify the comparison value to be used in conjunction with the selected **Test** operator.

User profile

User profile who conducts the file's update.

Press F9/F10 for more parameters.

```
                    Display Application Journal (DSPAPJRN)

Type choices, press Enter.

Program name . . . . . .   *ALL          Name, generic*, *ALL
  Library  . . . . . .       *ALL        Name, generic*, *ALL
Journal entry types  . . . . . .   *ALL   Character value, *ALL
              + for more values    ____
IPv4 (generic*) or IPv6  . . . .   *ALL
_____
Prefix length for IPv6 . . . . .  *ALL          1-128, *ALL
Job name . . . . . .       *ALL          Name, generic*, *ALL
  User . . . . . .           *ALL        Name, generic*, *ALL
  Number . . . . . .         *ALL        000000-999999, *ALL
Number of records to process . .  *NOMAX        Number, *NOMAX
Output . . . . . .         *            *, *PRINT, *PDF, *HTML..
Add column headings  . . . . . .  *YES         *NO, *YES
Output format  . . . . . .        *STD         *STD, *EXT, *LIST
Display format . . . . . .        *LIST        *LIST, *DETAIL

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

Program name

Name of the program used to change the file's information.

Library

Name of the library that contains the program used to change the file's information.

Journal entry types

Specify either a Journal entry type or *ALL.

IPv4 (generic*) or IPv6

Specify the IP address that was used for doing the database updates.

Prefix length for IPv6

Specify either the prefix length or *ALL.

Job name

Name of the job that changed the file's information.

Number of records to process

Specify how many journal receiver entries you want to proceed.

Output

* = to display only

*PRINT = to print

*PDF = PDF file

*HTML = HTML file

*OUTFILE

*PRINT1-*PRINT9 = Select correct print option.

Add column headings

In case of output options in pc format, you can add column headings to make it easier to handle the document.

Output format

*STD = Standard output shows all journal entries, data only.

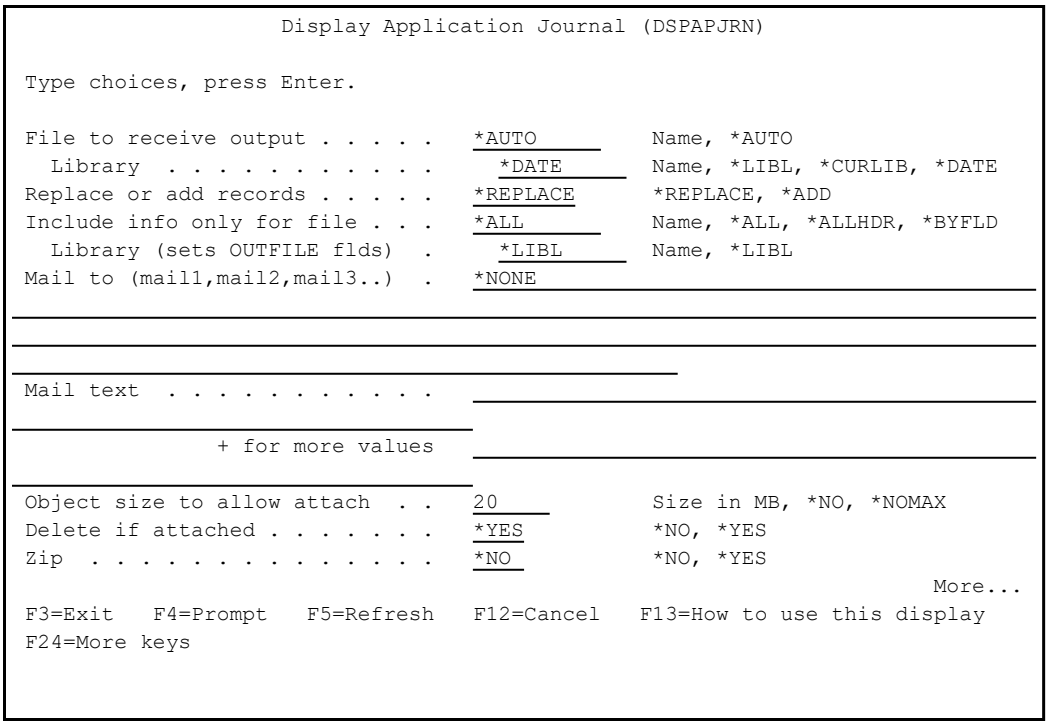
*EXT = Extended output shows all journal entries including header information.

*LIST = List output, shows one line header information per journal entry.

Display format

*LIST = Shows one line per journal entry. Header information.

*DETAIL = displays database updates.



File to receive output

Specify the name of the file that should receive the output in case of Output *OUTFILE. Special value *AUTO creates a file starting with RPTxxx that contains the output.

Library

The library containing the file. Special value *DATE creates a library SMZRyymmdd and puts the outfile here.

Replace or add records

Specify if you want to replace or add the records.

Include info only for file

Specify either *ALLHDR, *BYFLD, or *ALL.

Library (sets OUTFILE flds)

The library containing the file.

Mail to (mail1,mail2,mail3..)

Specify mail addresses, separated by comma, or address book names where you specified multiple mail addresses.

Mail text

Specify your desired email text.

Object size to allow attach

Specify the size in MB up to them. The attachment should be sent by mail or *NOMAX for unlimited.

NOTE: Mail servers may have limits for sending/receiving.

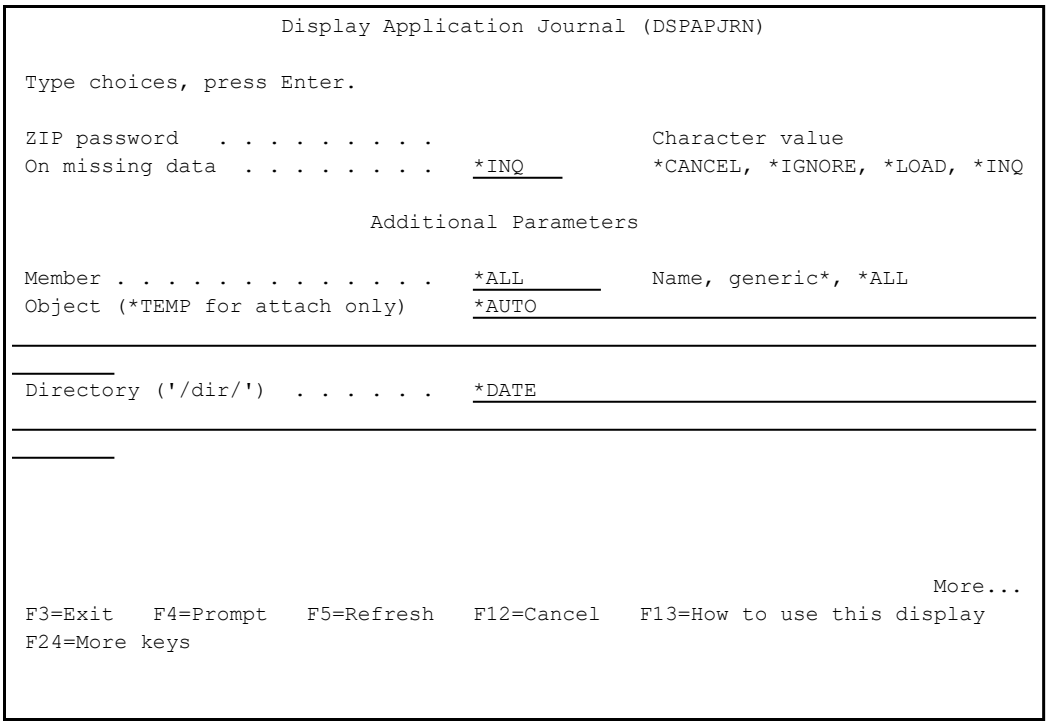
*NO=Do not attach, save it in IFS under /iSecurity/ready reports/date

Delete if attached

Specify if you want to delete the attachment when sent or keep it in IFS under iSecurity/ready reports/date.

Zip

Specify if you want to zip the attachment or not.



ZIP password

Specify an optional password that should be used to protect the ZIP file.

On missing data

Specify what should happen if the report returns no values.

*CANCEL = Stop the report

*IGNORE = Proceed

*LOAD = Start from beginning

*INQ = Send an inquiry message

Member

Specify the member or *ALL.

Object (*TEMP for attach only)

Specify the name of the result object in IFS.

*TEMP = Only temporary, will be deleted at the end

*AUTO = The object name is generated automatically

Name = Your choice of name.

Directory ('/dir/')

The name of the directory containing the object

*DATE = In /iSecurity/report output creates a directory with yymmdd that contains the object.

Type choices and press Enter. The Display Journal Entries screen appears.

```
                          Display Journal Entries
 Name  . . . .:  DEMO1   Demo Victor
 Type options, press Enter.
  5=Display entire entry  6=SQL  9=Screen  U=Undo

 Opt     Object     Job         Program    User       Date-time                RRN
  _ UP   JRTEST     QPADEV000M IOSLCALLC  VICTOR     2025-01-12-12.51.29        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-12.56.40        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT VICTOR     2025-01-12-12.58.59        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.02.25        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.05.01        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-13.10.07        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT VICTOR     2025-01-12-13.16.05        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.05.55        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.15.58        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT AU         2025-01-12-17.20.14        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.28.11        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.48.01        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT GS         2025-01-12-17.54.48        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT HAIM       2025-01-13-11.21.56        1
  _ UP   JRTEST     QZDASOINIT QZDASOINIT HAIM       2025-01-13-12.24.36        1
  _                                                                          More...
  F3=Exit  F7=Subset  F10=Detail mode  F12=Cancel  F17=Top   F22=Display entire
```

To **display entire entry**, type **5** in the **Opt** field next to the entry. The **Display Database Updates** screen appears as shown below, displaying the changed fields.

```
                    Display Database Updates                RRN:         16
                                                                      UP Update
 Date-Time .: 2024-12-26-17.28.30                          Object. . .: DEMOPF
 Program . .: IOSLCALLC   Library .: *OMITTED              Library .:   VICTOR
 Job . . . .: QPADEV000N/ALEX3/754956                      Member  . .: DEMOPF
 IP address : 123.123.123.123                              Port  . . .: 12345
 User  . . .: ALEX3      Alex - Supporteam strong user
                                    After value        Before value
            Item number             ALEX44             ASASAS
Description (truncated)             AstutosGron        AstutosGron
            Item vendor             336.               336.
            Qty On Hand             811.               811.
           Qty On Order             1966.              1966.
                  Price             101.00             101.00
       Price date YY.MM             0.                 0.
      Price change in-%             66.000             66.000
               Salesman             13.                13.
            Description             THREE RING BINDER  THREE RING BINDER
      1st Quarter sales             63.15              63.15
      2nd Quarter sales             46.02              46.02
      3rd Quarter sales             68.15              68.15
      4th Quarter sales            +30.04E-001        +30.04E-001
                                                                       Bottom
F3=Exit 5=Sql  F7=Subset F8=Print
F9=132/80  F10=List mode  F12=Cancel F17=Top F19=Screen F22=Entire field
```

To **show the SQL statement**, type **6** in the **Opt** field next to the entry. The **SQL Statement** screen appears (if available).

NOTE: The displayed SQL is the most relevant SQL operation for the selected DB Journal operation, assuming that SQL was used. DB Journal does not provide exact information as per the method (*) or SQL statement that caused the transaction. The displayed SQL statement is relevant only if SQL was used. Other SQL statements that were prepared earlier should also be considered. The SQL statements are presented from the iSecurity/Firewall log. (*) On the IBM i, I/O operations are performed by either traditional read/write/update/delete operations or by SQL.

To **show the screen** (if available), type **9** in the **Opt** field next to the entry. Select the screen in the **Select Frame to Start with (then use Page Up/Down)** pop-up window.

To **undo the record change**, type U in the **Opt** field next to the entry. The **Confirm Undo of a Record Change** screen appears. Type choices and press **Enter**.

To **filter the results**, press the **F7=Subset** key, the **Define Include Filters** screen appears. Setting the Filter Conditions and the Order of Rules is described in "Displaying File Updates " on page 17(Setting Filter Conditions).

To **display updates** that were done on a set of files, select **2. Display updates** from the **Business Analysis** screen for containers (***STRJR > 3***). The **Display Application Journal (DSPAPJRN)** screen appears with the predefined Display format parameter to *DETAIL. Type choices and press Enter. The **Display Database Updates** screen appears.

To **print updates**, select **5. Print updates** from the **Business Analysis** screen for containers (***STRJR > 3***). The **Display Application Journal (DSPAPJRN)** screen appears with the predefined Output parameter to *PRINT. Type choices and press **Enter**.

To print updates (extended info), select **6. Print updates (extended info)** from the Business Analysis screen for containers (*STRJR > 3*). The Display Application Journal (DSPAPJRN) screen appears with the predefined Output parameter to *PRINT and the Output format parameter to *EXT. Type choices and press Enter.

To work with groups types, select **35. Groups and Items** from the Business Analysis screen for containers (*STRJR > 3*). The Work with Group Types screen appears as shown in "Groups and Items" on page 117.

To work with reports, select **41. Reports** from the Business Analysis screen for containers (*STRJR > 3*). The Work with Reports screen appears as shown in "Working with Reports " on page 95

To work with report scheduler, select **45. Work with Report Scheduler** from the Business Analysis screen for containers (*STRJR > 3*). The Work with Report Scheduler screen appears as shown in "Define Report Schedules " on page 98

To run a report group, select **46. Run a Report Group** from the Business Analysis screen for containers (*STRJR > 3*). The Run Report Group (RUNRPTGRP) screen appears as shown in "Define Report Schedules " on page 98 (Run Report Groups).

To display the action log, select **49. Display Action Log** from the Business Analysis screen for containers (*STRJR > 3*). The Display Messages screen appears.

Working with Applications and BizAlerts

The **Business Analysis** option creates a Journal Application which is based upon the system journal QJRNRCV, that contains activity data on the database files.

The Journal Application information provides the ability to filter the system journal data, sort by the fields' common keys, display changes, and have alerts triggered.

The Journal Application can process data in real-time as well as collect older information, as long as this data is available on the disk.

The data processing can also be done in batch (outside working hours).

To **start working with Applications, BizAlerts - Definitions**, select **11. Applications, BizAlerts etc.** from the main menu (*STRJR*). The **Applications, BizAlerts - Definitions** screen appears.

```
JRWAPP              Applications, BizAlerts - Definitions     iSecurity/Journal
                                                              System:  RLDEV

Applications                              Structure setup
 1. Work with Journal Applications        51. Output Fields per File
 5. Work with Containers                  52. File Structure Modifications
                                          55. Data conversions
 9. Allow applications to users
                                          Journal Objects Care
Process Information                       71. Plan Object Journaling
11. Activation                            72. Check Object Journaling
15. Collect READs by DB Triggers          73. Set Journal As Planned

                                          75. Auto Maintenance of Receivers

                                          77. Auto Start Object journaling
                                          78. Display Auto Start Setting
                                          79. Building Journals, Revoke Changes

Selection or command
===> ____________________________________________________________________________

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

To view field changes in several files, create an application of files that combines information from all the relevant files and fields needed. After creating the application, the first ***Container*** is created automatically. This ***Container*** contains the same logical information from the system's receiver,

in a filtered format from the files and fields users chose. In that way, only the relevant information is kept in the system.

To define a new application, select **1. Work with Journal Applications** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Work with Journaled Applications screen appears as shown in "Work with Journaled Applications" on the next page.

To work with containers from the applications, select **5. Work with Containers** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Work with Application Containers screen appears as shown in "Work with Application Containers" on page 69

To work with Application Autorization, select **9. Allow applications to users** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Work with Application Authorizations screen appears as shown in "Work with Application Autorizations" on page 71.

To activate and start all enabled applications, select **11. Activation** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Collection to Containers screen appears as shown in "Activation" on page 72.

To work with file operations, select **15. Collect READs by DB Triggers** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Work with File Operations screen appears as shown in "Journal DB Operations" on page 76.

To work with file reporting specifications, select **51. Output Fields per File** from the Applications, BizAlerts – Definitions screen (*STRJR > 11*). The Work with File Reporting Specification screen appears as shown in "Output Fields per File" on page 78.

To work with file structure modifications, select **52. File Structure Modifications** from the Applications, BizAlerts- Definitions screen (*STRJR > 11*). The Work with File Structure Modifications screen appears as shown in "File Structure Modifications" on page 80.

To work with data conversions, select **55. Data conversions** from the Applications, BizAlerts- Definitions screen (*STRJR > 11*). The Work with Data Conversions screen appears as shown in "Data Conversions" on page 82.

To **create a journaling plan**, select **`71. Plan Object Journaling`** from the from the Applications, BizAlerts - Definitions (*STRJR > 11*). The **Work with Object Journaling Plan** screen appears as shown in "Plan Object Journaling" on page 84.

To **check object journaling**, select **`72. Check Object Journaling`** from the **Applications, BizAlerts- Definitions** screen (*SRTJR > 11*). The **Work with Object Journaling Status** screen appears as shown in "Check Object Journaling" on page 86.

To **set the journal as planned**, select **`73. Set Journal as Planned`** from the **Applications, BizAlerts- Definitions** screen (**STRJR > 11**). The **Set Journal As Planned (SETJRPLN)** screen appears as shown in "Set Journal as Planned" on page 88.

To **work with IBM Journal Receivers**, select **`75. Auto Maintenance of Receivers`** from the **Applications, BizAlerts – Definitions** screen (*STRJR > 11*). The **Work with Journal Receivers Maintenance** screen appears as shown in "Auto Maintenance of Receivers" on page 89.

To **work with Auto Start**, select **`77. Auto Start Object journaling`**. The **Start Journal Library** screen appears as shown in "Auto Start Object Journaling" on page 91.

To **build and maintain the journal**, select **`79. Building Journals, Revoke Changes`** from the **Applications, BizAlerts – Definitions** screen (*STRJR > 11*). The **Journal Build and Maintain screen** appears as shown in "Building Journals, Revoke Changes" on page 92.

Work with Journaled Applications

To **define a new application**, select **`1. Work with Journal Applications`** from the **Applications, BizAlerts-Definitions** screen (*STRJR > 11*). The **Work with Journaled Applications** screen appears.

```
                        Work with Journaled Applications
 Type options, press Enter.                                        System: RLDEV
   1=Select  3=Copy    4=Delete  5=Display (Receivers)  6=Display (Containers)
   8/9=Enable/Disable application  S/E/D=Start/End/Display real-time collection
   X=Explanation & Classification       Position to  . . . . _____
     = Collecting                       Subset by text . . . _______________
            Enabled        SIEM           by classification. _  A=Agent...
Opt Name  Type   Journal   Only
 _  AUXXJ APP  Y FSJRN        AUXX test Oren AR
 _  DEMO1 APP  Y JRN          Demo Victor
 _  DEMO2 -RPT   JRN          Demo Victor
 _  JELIJ APP  Y ELIJRN       Eli Journal
 _  MFAUS APP  Y SMZO         MFA changes
 _  MONEY -RPT   JRDEMO
 _  RRRRR -RPT   JRDEMO
 _  RRRR1 APP  Y JRDEMO
 _  SMZCJ APP  Y SMZC         test Capture journaling
 _  SMZVJ APP  Y SMZV         SMZV change definitions
 _  TESTU -RPT   JRDEMO       Test Report_Example for User Guide
 _  TEST1 -RPT   JRDEMO
                                                                      More...
 F3=Exit  F5=Refresh  F6=Add  F7=Un/Fold  F8=Collecting  F11=Started  F12=Cancel
```

Adding (Modifying) Application

Press **F6** to add a new set or type **1** by an existing Application and press **Enter**. The **Add Application** screen or **Modify Application** screen appears as appropriate.

```
                              Add Application              System: RLDEV
                                                 Last change date:  0/00/00
                                                          by user:
 Application  . . . . . . . . _____          Name
 Text . . . . . . . . . . . . _____________________________________________
 Type . . . . . . . . . . . . APP            APP=Application, RPT=Report
 Based on journal . . . . . . __________
   Library  . . . . . . . . .   __________       IASP . *NONE      Name, *NONE
 Include all journaled objects  N   Y=Yes, N=Restrict by "Objects to include"

 Select one of the following:
   1. Objects to include
   2. Alerts on data    (before include filters)
   3. Include Filters   (define data to keep in containers)
   4. Alerts on data    (after include filters)

   6. SIEM Support
   7. Define Business Items  (common keys)
   8. Identify Business Items in application files
   9. Configuration
 Selection ===> __

 F3=Exit    F4=Prompt
 Modify data, or press Enter to confirm.
```

Application

An option to specify the five-digit name of the application.

Text

An option to describe the application.

Type

An option to define if this is an application or a report.

APP = Application

RPT = Report

Based on journal

Library

Insert the system's journal file and library name.

IASP

An option to define where the journal is stored.

*NONE = In System ASP

Name = In the specified independent ASP

Include all journaled files

An option to define if all objects recorded in the journal are included in the application.

NOTE: The journal can contain a large number of objects. To isolate some changes, select the objects that are needed.

Y = Yes, all objects in the journal are part of the application

N = No, select in the next option "Objects to include" the objects.

1. Objects to include

Select the objects you want the application to use as shown in "1. Objects to include" on page 53. You can select up to 1,000 objects to use both the header and data of the object. If you select more than 1,000 objects, the application will use only header information for those additional objects.

2. Alerts on data (before include filters)

Alerts based upon the changes in the journal receiver before the include filters are checked as shown in "2. Alerts on data (before include filters)" on page 55.

3. Include Filters (define data to keep in containers)

An option to set filters to extract these changes in databases from the journal that are important and should be kept in the container as shown in "3. Include Filters (define data to keep in containers)" on page 63.

4. Alerts on data (after include filters)

Real-time action based on definitions that are based upon changes in the containers after the included filters were checked as shown in "4. Alerts on data (after include filters)" on page 64

6. SIEM Support

Define SIEM support for the application as shown in "6. SIEM Support" on page 64.

7. Define Business Items (common keys)

Common key fields contain the same information across several files in the application. Usually, these are generic key fields. Such fields can later be used for selections.

For each application, users can select up to 15 fields.

8. Identify Business Items in application files

Build the matching between defined business items and fields in selected files.

9. Configuration

Define some general definitions for your application as shown in "9. Configuration" on page 67.

To **display data for journal receivers**, select **`5=Display (Receivers)`** from the **Work with Journaled Applications** screen (*STRJR > 11 > 1*). The **Display APP Current Journal (DSPAPCRJ)** screen appears as shown in "Business Analysis Journal Receivers" on page 26.

To **display data for containers**, select **`6=Display (Containers)`** from the **Work with Journaled Applications** screen (*STRJR > 11 > 1*). The **Display APP Current Journal (DSPAPCRJ)** screen appears as shown in "Business Analysis Journal Receivers" on page 26.

Activation (Enabling)

After creating and defining the new application, type **8**=Enable to start building the definitions file. The letter **Y** will appear next to the application.

Deactivating (Disabling)

If you want to modify your application, business items, etc., first stop the real-time collection using option **E**=End real-time, then type **9**=Disable. The letter **Y** next to the application will disappear.

Start/End/Display real-time collection

Using AP-Journal, users are able to read database journal receivers in real time and proceed with the journal receiver entries using the definitions of the application. Start and Auto-Start of Applications ensure that all database changes occur in AP-Journal.

You can easily pause the collection and restart it. We work on the technology of remembering the last journal receiver entry and continue with the next (*PRVEND). Therefore, you can pause the collection and resume it without losing data.

To **start collection for a specific application**, type **S** in the **`Opt`** field. The **Activate Application Journal (STRRTAPP)** screen appears. Type choices and press Enter.

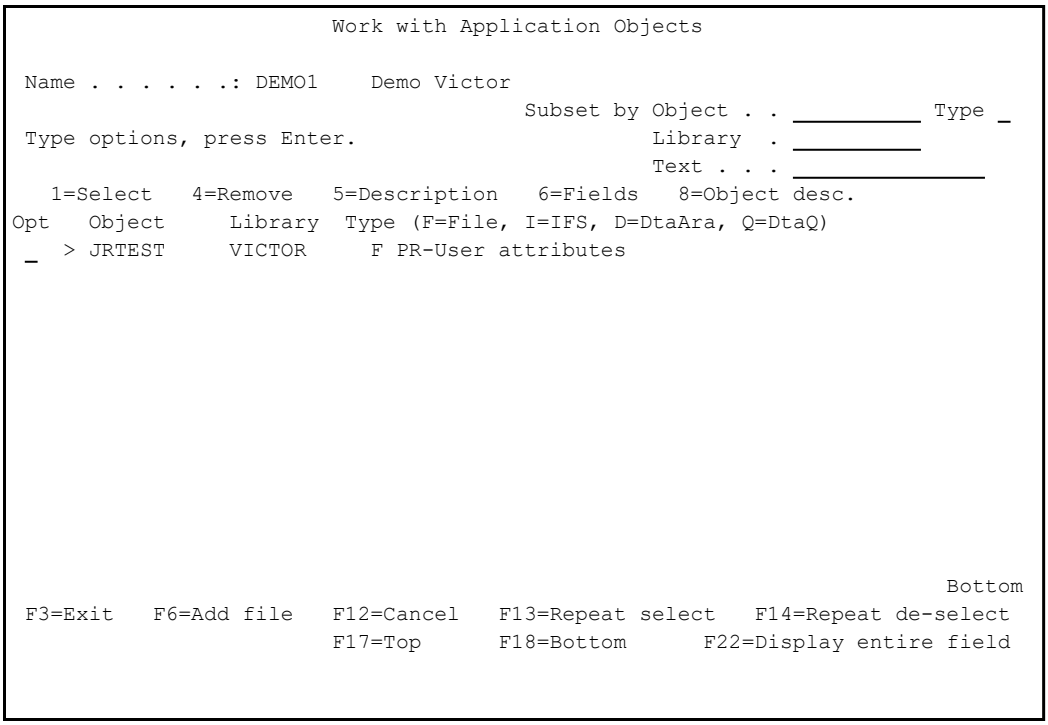
To **end collection for a specific application**, type **E** in the **`Opt`** field. The **Activate Application Journal (STRRTAPP)** screen appears. Type choices and press **Enter**.

Some journals support millions of objects. The **AP-Journal** does support such journals. This includes the functions which list the objects that are journaled, (which will take considerable-equivalent time). **AP-Journal** application supports any number of objects in the following way (restrictions apply):

	Include all Objects = NO	Include all Objects = YES
Number of supported objects	10,000,000	1,000
Select by generic name	Yes	No
Object selection method	By selection over the *ALL entry Consider using the ITEM test and specifying the objects in an external group, with or without generic names.	Use the Objects to include option
Object selection method for work with by fields	Use the Objects to include option	Use the Objects to include option
Objects to refer by fields	1,000	1,000
Maximum objects to use for best performance	N/A	300 The IBM command supports up to 300 named files or *ALL

1. Objects to include

To select objects to work with defining journaled applications, determine the required parameters from the Add Application or Modify Application screen as appropriate (*STRJR > 11 > 1*; F6/1) and type 1 in the **Selection** field. The Work with Application Objects screen appears.



1 = Select

An option to select the file.

4 = Remove

An option to remove the file.

5 = Description

An option to display the description of the object.

6 = Fields

An option to display the File Field Description, including all fields in the file.

8 = Object dec.

An option to display the object description. The Display Object Description - Full screen appears.

F6 = Add file

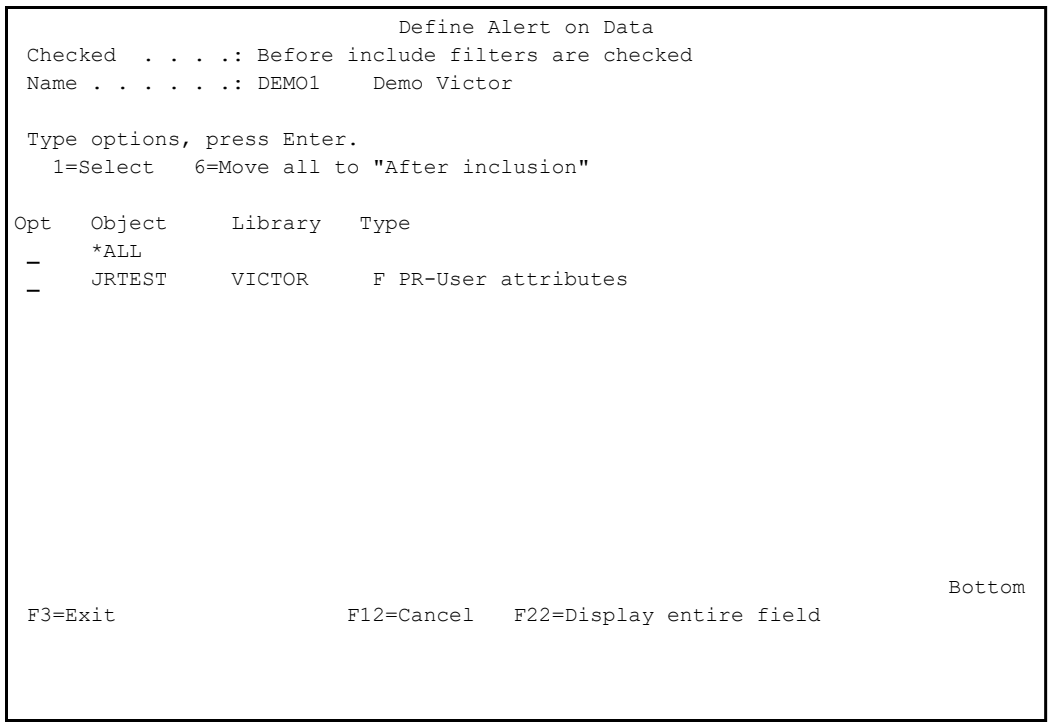
An option to add the file to the selection. The Add Application Object screen appears.

NOTE: The STRJRNPF command should be run to add the recording of the database changes in the journal that is used for this application.

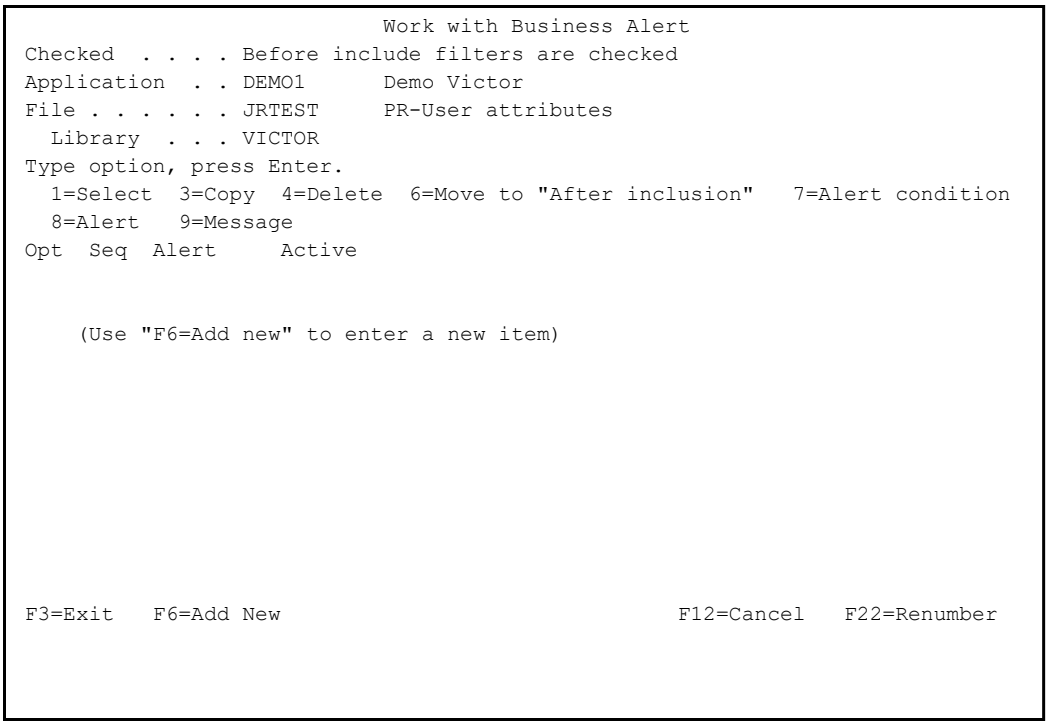
2. Alerts on data (before include filters)

Raw data comes from the database journal that is read from the application job. On this raw data, users can apply alerts.

To **define alert on data defining journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (***STRJR > 11 > 1***; **F6/1**) and type **2** in the **`Selection`** field . The **Define Alert on Data** screen appears.



To **select a file to set an action for**, type **1** in the **`Opt`** field next to the object. The **Work with Business Alert** screen appears.



1=Select

Select an already-defined alert for modification.

3=Copy

Copy an alert to a new one.

4=Delete

Delete an alert.

6=Move to "After inclusion"

Move to “After inclusion”

7=Alert condition

Alert condition for selected entry.

8=Alert

Alert definition

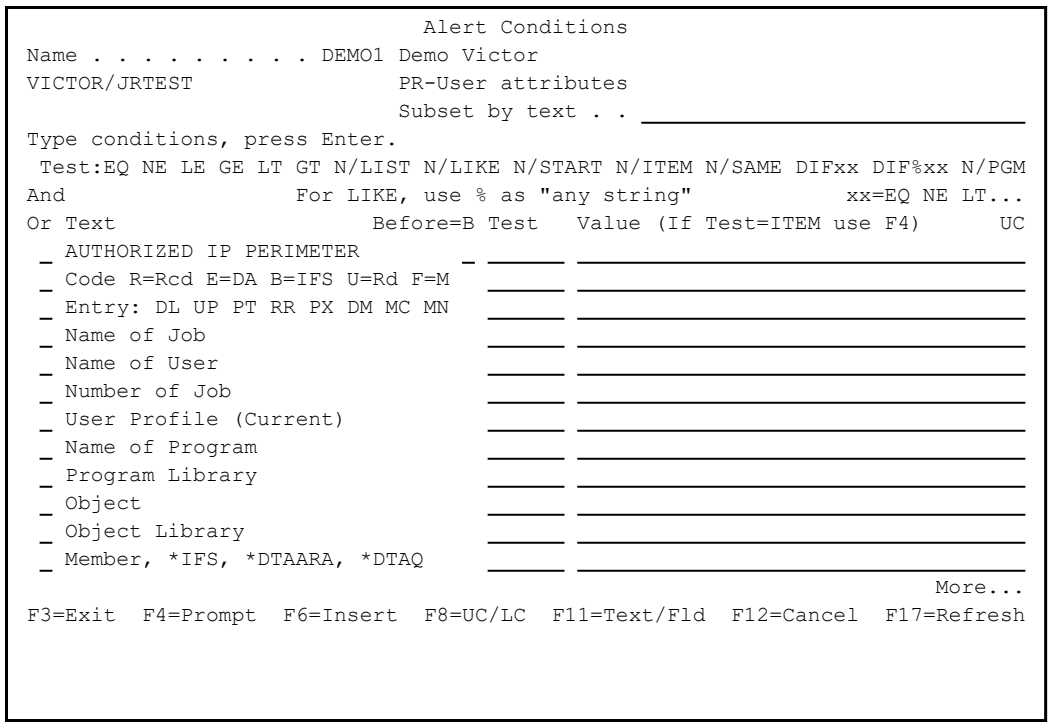
9=Message

Message to be sent.

To **add a new action**, press **F6** from the **Work with Business Alert** screen. The **Add Business Alert** screen appears.

(missing or bad snippet)

Type choices and press **Enter**. The **Alert Conditions** screen appears.



This screen allows users to set filters on events to trigger an alert only in defined cases.

And/Or

An option to combine several tests using and/or.

A - And in addition to previous tests

O - Or alternative to previous tests

Before=B

An option to compare current values to "before" values

Test

The test allows you to filter exactly what you need to use.

EQ = Equal

NE = Not Equal

LE = Less Equal

GE = Greater Equal

LT = Less Than

GT = Greater Than

LIST = on the List

NLIST = Not on the List

LIKE = a pattern (ONLY for character field) NLIKE=Not a pattern (ONLY for character field)

START = a pattern that starts with (ONLY for character field)

NSTART = a pattern that does not start with (ONLY for character field)

ITEM = filter based on group items where the results are members of the defined group

NITEM = filter based on group items where the results are not members of the defined group

SAME = If values are not changed

NSAME = if values are changed

DIF = the update is Different from DIFxx=the update is Different from xx = EQ/NE/LE... (should only be used on a numeric field and computes the numeric difference between the before and after contents of the field.)

DIF%xx = the update is N % Differently xx=EQ/NE/LE... (for numeric field only)

PGM = if the defined program returns a yes

NPGM = if the defined program returns no yes

SAME is a new option which compares between the "before" and "after" field values

Special lines

Code

R = Record

E = Data area operation

B = IFS Object Operation

U = Read records

D = File operation

Entry

DL = Delete

DR = Delete for commit rollback.

PT = Put (write)

PX = Put to a deleted relative record number.

UP = Update (After-image)

UR = After image for commit rollback

DM = Delete member

MC = Change member

MN = Rename member

DT = Delete file

CT = Create file

EA = Data area.

WA = IFS object

RR = Read records.

Value

Specify the comparison value for the field/test here.

F6 = Insert

Insert to insert new lines. Use this to set additional conditions on fields that you already used for test.

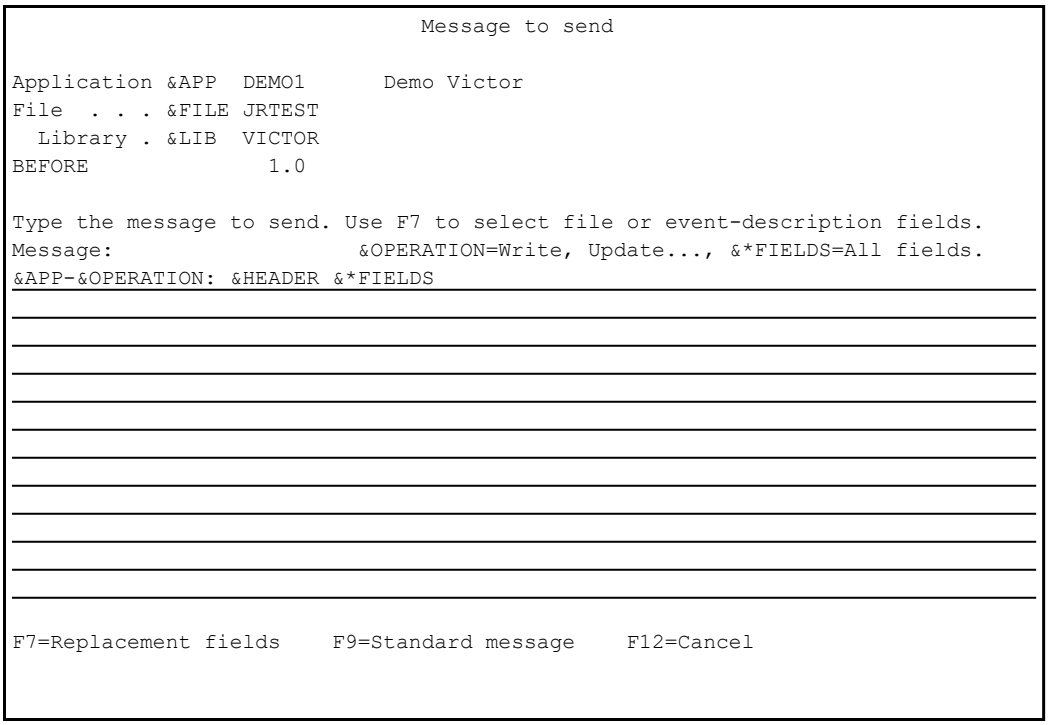
F8 = UC/LC

Toggle between Upper/Lower case.

F11 = Text/Fld

Toggling between field text and field attributes.

Define alert conditions and press Enter to confirm. The Message to send screen appears.



Build your own message or use the default message.

&APP

This is replaced at runtime with the name of your application.

&OPERATION

This is replaced at runtime with the type of operation.

&HEADER

This is replaced at runtime with the header fields.

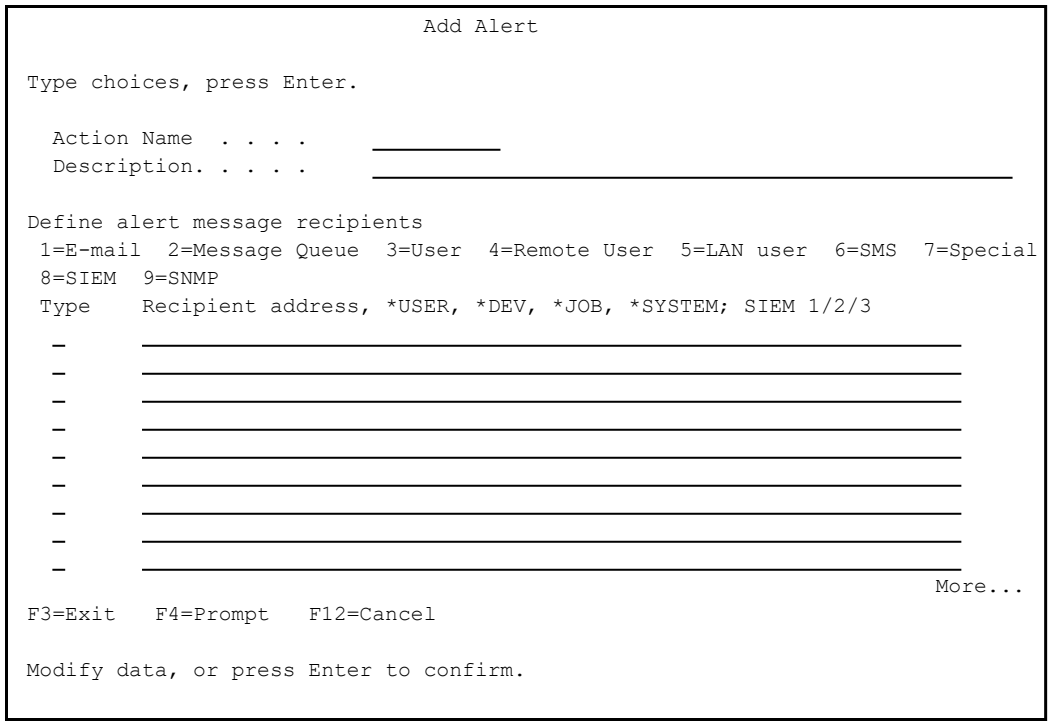
&FIELDS

This is replaced at runtime with the field values.

F7 = Replacement fields

Use F7 to select from available fields those that users need to add between text.

Type message and press Enter. The Add Alert screen appears.



Action Name

Enter a meaningful name for the Action

Description

Enter a free text description of the Action

Type

Recipient type:

1 = E-mail message

2= Message to message queue

3= Message to user

4= Message to remote user

5= Message to LAN user

6= SMS

7= Special

8= SIEM

9= SNMP

Recipient address, *USER, *DEV, *JOB, *SYSTEM; SIEM 1/2/3

Recipient address formatted according to message type:

1 - E-mail address in standard e-mail format (recipient@address)

2 - Fully qualified name of the message queue or *SYSOPR

3 - User profile or IBM i (OS/400) group profile

4 - User profile & SNA address separated by space (for example, USER SYSTEM)

5 - Valid network username or *DOMAIN for all users on your domain

6 - Phone number including country code and area code as necessary

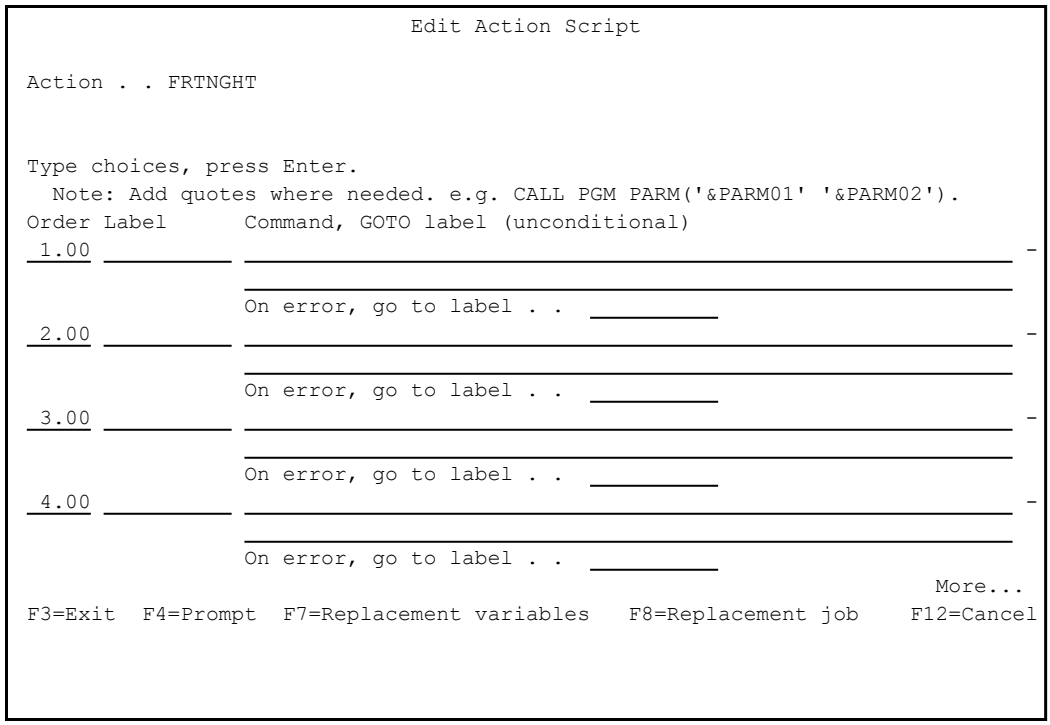
7 - Phone number and access codes for the pager service

8 - E-Mail Address in kind of type 1

*USER in kind of types 1-5

9 - Leave blank; the SNMP message will be sent according to the definitions in option **22. SNMP Definitions** in the System Configuration menu.

Type choices and press Enter. The Edit Action Script screen appears.



Order

Specify the order of the commands here.

Label

Use, if necessary, a label name for jumping to in case of errors.

Command

Type in the command that should be called. Use **F4** to prompt the command and **F7**/**F8** to replace variables.

On error, go to label

Specify here the label name that is used for go to in case of errors.

Define one or more command scripts to be run and press **Enter** to confirm.

3. Include Filters (define data to keep in containers)

To **include filters defining journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; **F6**/1)

and type **3** in the **Selection** field . The **Define Include Filters** screen appears as shown in "Setting Filter Conditions " on page 106.

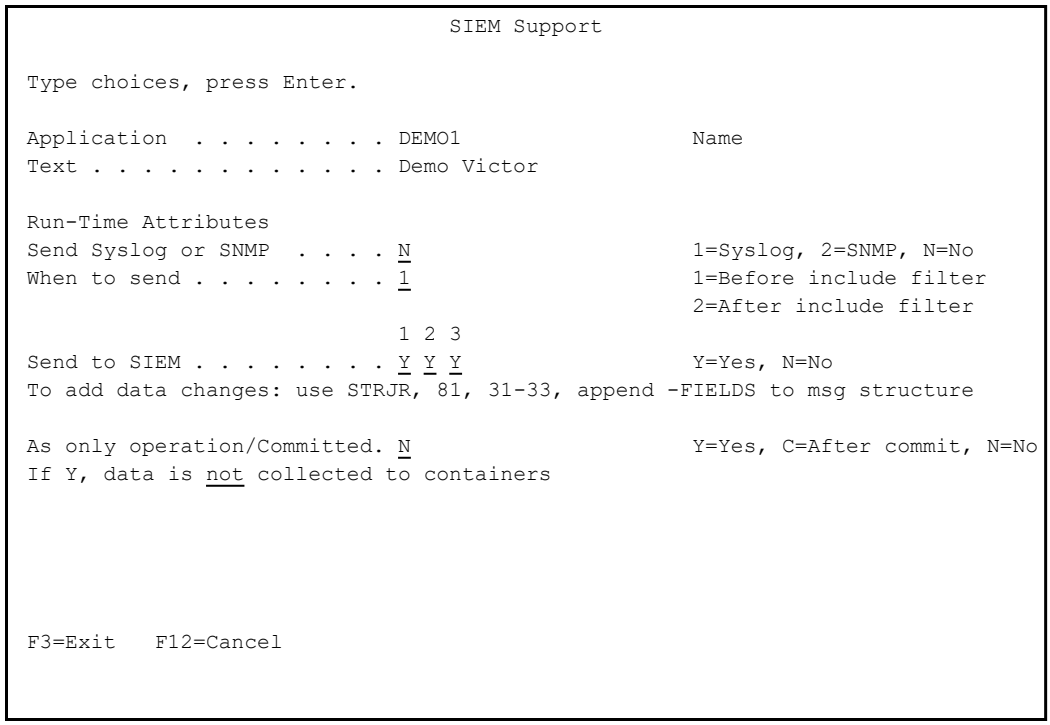
4. Alerts on data (after include filters)

To **to select alerts to work with after the included filters were checked defining journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; F6/1) and type **4** in the **Selection** field . The **Define Alert on Data** screen appears as shown in "2. Alerts on data (before include filters)" on page 55.

6. SIEM Support

Manages the specific application to be sent as a SYSLOG message or as SNMP traps. The advantage of this feature is that the messages are sent as only an operation; the data is not written to the containers, and performance and disk space are not used.

To **define SIEM working with journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; F6/1) and type **6** in the **Selection** field . The **SIEM Support** screen appears.



This screen is used to configure if and how database transactions should be sent.

Send Syslog or SNMP

Select the type of message to be sent, SNMP or Syslog.

When to send

AP-Journal supports sending transactions on raw data or on filtered data.

1 - Send before applying filters on raw data.

2 - Send after applying filters.

Send to SIEM

AP-Journal supports up to three SIEM systems that are used for sending Syslog messages. Select Y for each System that you want to send.

As only operation/Committed

This parameter is used for sending only to SIEM or sending only committed messages.

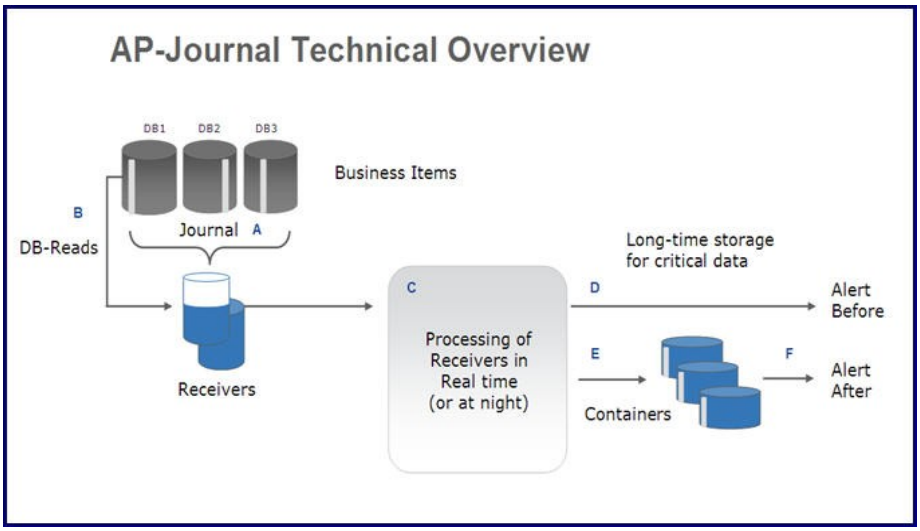
Y - Send only to SIEM, collect not to container.

C - Send only committed transactions to SIEM and collect to container.

N - Send not to SIEM, collect to container.

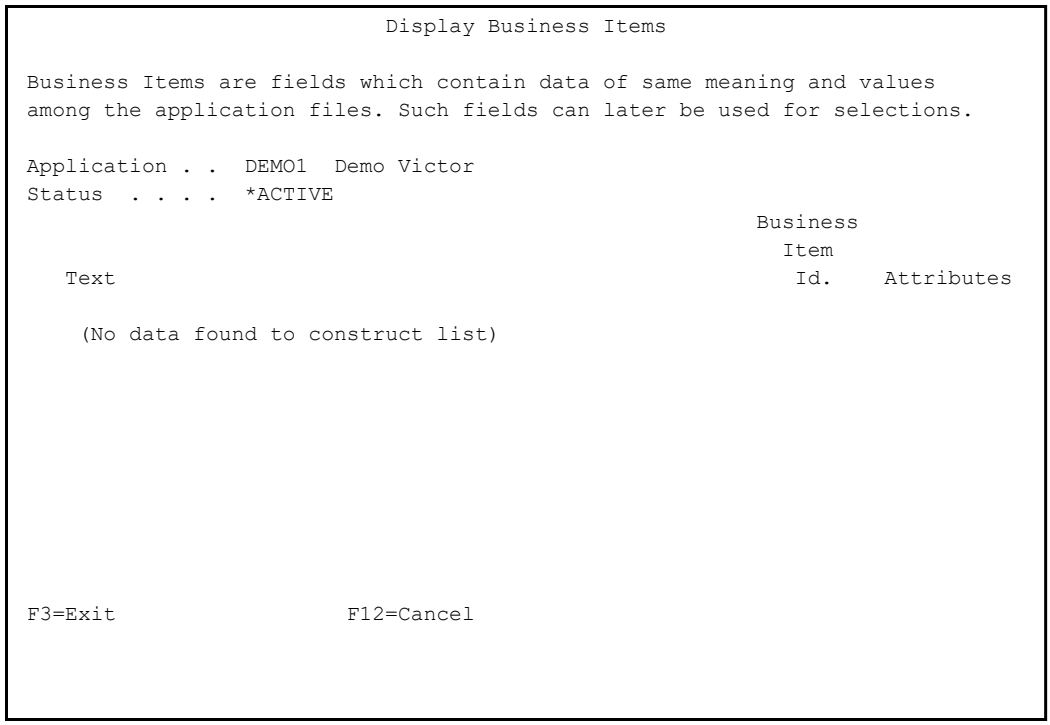
7. Define Business Items (common keys)

Business Items are fields which contain data of the same meaning and values among the application files.



The white strips in the image represent the Business Items. Note that in the Database the Business Items are located on different places in each Database, and after the process procedure the Business Items are organized in the Containers.

To **define Business Items working with journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; F6/1) and type **7** in the **Selection** field . The **Display Business Items** screen appears.

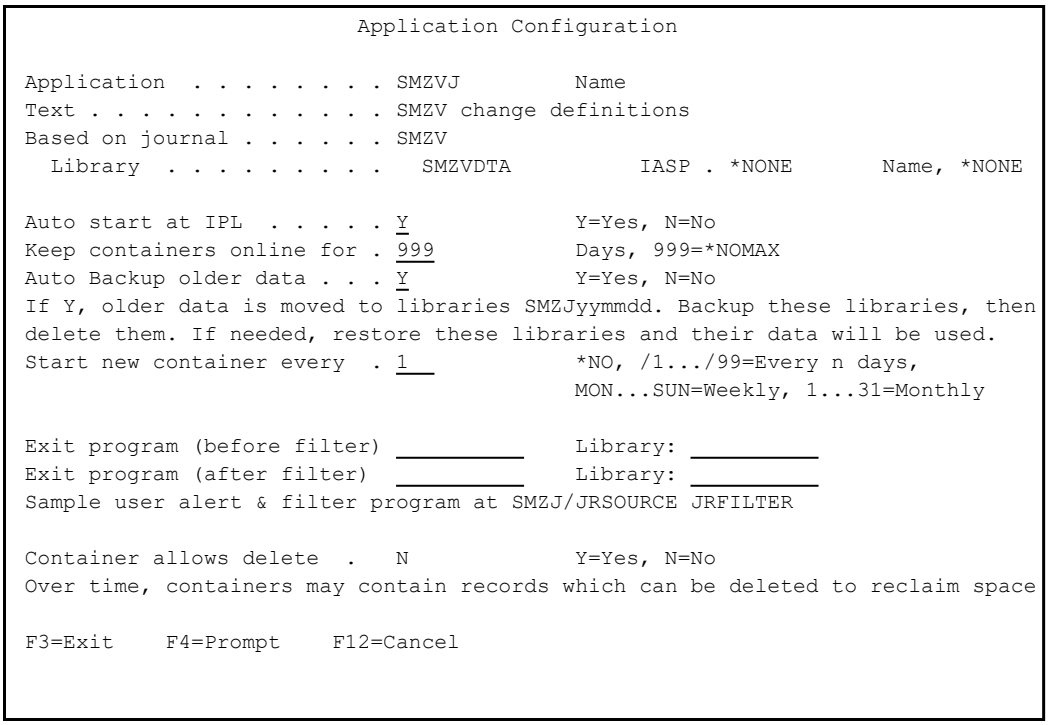


8. Identify Business Items in application files

To **identify Business Items working with journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; F6/1) and type **8** in the **`Selection`** field . The **Work with Application Objects** screen appears.

9. Configuration

To **configure journaled applications**, determine the required parameters from the **Add Application** or **Modify Application** screen as appropriate (*STRJR > 11 > 1*; F6/1) and type **9** in the **`Selection`** field . The **Application Configuration** screen appears.



Auto start at IPL

Y - If AP-Journal is activated at IPL or through Start Real-Time JRN Activities (STRRTJR) screen (STRJR > 11 > 11 > 1: *ALL)

N - If you want to start the application on Demand

Keep containers online for

Specify the days for how long you need to have the data available for analysis using the container solution.

999 = Keep data without limitation

Auto Backup older data

If you specify a number of days for keeping containers online, decide here what should happen after the number of days.

Y = Data that is deleted from Containers are moved in libraries SMZJyymmdd.

N = Only delete from Containers, do not backup

Start new container every

An option to define how often to create a new container. A too-short period results in too many container files, and a too-long period results in too-big container files.

*NO = No new containers should be created. Use this eventually only if you have very few transactions

/1…/99 = Create a new container every specified number of days.

MON…SUN - Create a new container every specified weekday.

1..31 = Create a new container each month on the specified day.

Exit program (before filter) Library

Specify an exit program with the library that should be executed on each transaction (raw data) before applying filters.

Exit program (after filter) Library

Specify an exit program with library that should be executed on each transaction (raw data) after applying filters.

Container allows delete

Y = Yes, you are able to delete data from container (you lose information in the data chain).

N = Nobody can delete data from container files.

Work with Application Containers

To work with containers from the applications, select **5. Work with Containers** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Work with Application Containers screen appears.

```
                      Work with Application Containers

Type options, press Enter.                          Position to . . . _____
  1=Select   6=Change application container

Opt   Name       Text
 _    AUXXJ      AUXX test Oren AR
 _    DEMO1      Demo Victor
 _    DEMO2      Demo Victor
 _    DEMXX      Demo Victor
 _    JELIJ      Eli Journal
 _    MFAUS      MFA changes
 _    MONEY
 _    RRRRR
 _    RRRR1
 _    SMZCJ      test Capture journaling
 _    SMZVJ      SMZV change definitions
 _    TESTU      Test Report_Example for User Guide
 _    TEST1
 _    TEST4      test
                                                                        More...
F3=Exit                  F12=Cancel
```

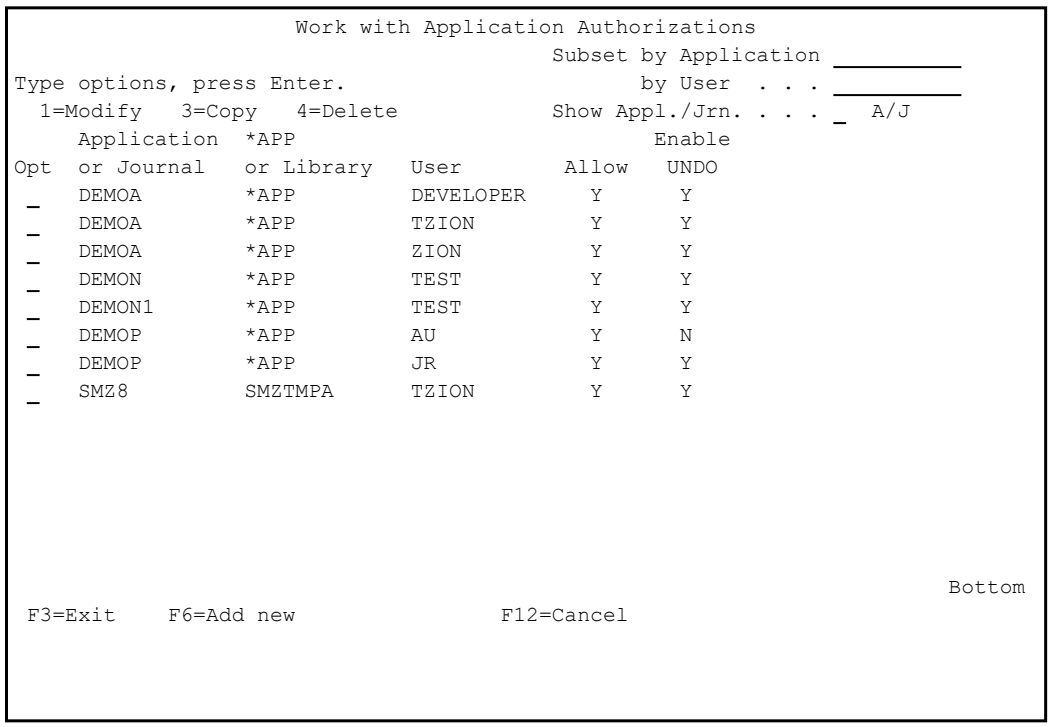
Select an application, type **1,** and press **Enter**. The **Display Application Containers** screen appears.

```
                        Display Application Containers

Type options, press Enter.
  5=Display details

Opt Container Number  From                 To                   Archived to
 _  DEMO1     0006    2025-03-05-10.55.47
 _  DEMO1     0005    2025-02-27-10.51.16  2025-03-05-10.55.46
 _  DEMO1     0004    2025-01-14-10.56.19  2025-02-27-10.51.15
 _  DEMO1     0003    2025-01-14-10.56.19  2025-01-14-10.56.18
 _  DEMO1     0002    2025-01-14-10.54.52  2025-01-14-10.56.18
 _  DEMO1     0001    0001-01-01-00.00.00  2025-01-14-10.54.51

                                                                      Bottom

F3=Exit   F6=Change application container   F12=Cancel
```

Select a container, type **5**, and press **Enter** to display its details or press **F6** to change the application container.

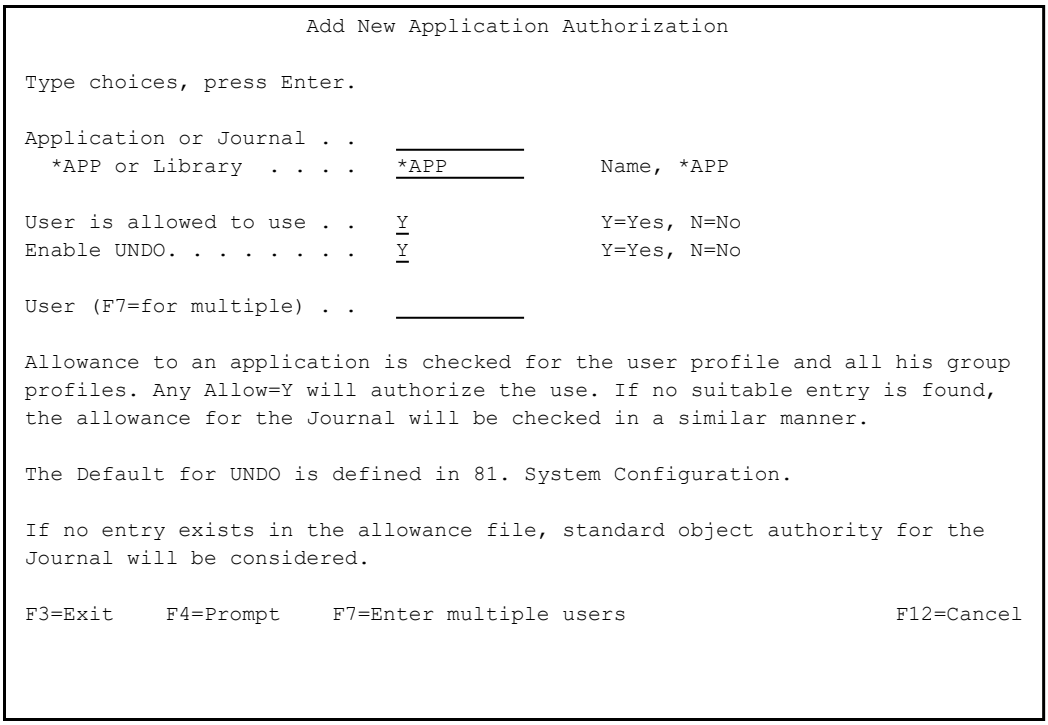
Work with Application Autorizations

To **work with Application Autorization**, select **`9. Allow applications to users`** from the **Applications, BizAlerts-Definitions** screen (***STRJR > 11***). The **Work with Application Authorizations** screen appears.



```
                    Work with Application Authorizations
                                          Subset by Application _________
Type options, press Enter.                       by User  . . . _________
  1=Modify   3=Copy   4=Delete           Show Appl./Jrn. . . . _  A/J
     Application  *APP                          Enable
Opt  or Journal   or Library   User       Allow   UNDO
 _   DEMOA        *APP         DEVELOPER    Y       Y
 _   DEMOA        *APP         TZION        Y       Y
 _   DEMOA        *APP         ZION         Y       Y
 _   DEMON        *APP         TEST         Y       Y
 _   DEMON1       *APP         TEST         Y       Y
 _   DEMOP        *APP         AU           Y       N
 _   DEMOP        *APP         JR           Y       Y
 _   SMZ8         SMZTMPA      TZION        Y       Y
                                                              Bottom
 F3=Exit    F6=Add new              F12=Cancel
```

To **add authorizations**, press **F6** key. The **Add New Application Authorization** screen appears.



Application or Journal

Type the name of the Application or Journal to be authorized.

***APP or library**

Define if you want to authorize an application or the library of a journal.

User is allowed to use

Specify if the user is allowed to use this application.

Enable UNDO

Define if undo should be allowed for the application/user.

User (F7=for multiple)

Specify if a user or a list of users should be allowed for the application/journal.

Activation

To activate and start all enabled applications, select **11. Activation** from the Applications, BizAlerts-Definitions screen (*STRJR > 11*). The Collection to Containers screen appears.

```
JRSETMN                    Collection to Containers          iSecurity/Journal
 System:  RAZLEE3
 Select one of the following:

 Activation
  1. Activate Real-Time Journal Collection
  2. De-activate Real-Time Journal Collection (all applications)
  Use Work with Applications to control collection for a specific application.

  5. Work with Active Jobs

 Auto-Activation
 11. Activate Real-Time Journal Collection at IPL
 12. Do Not Activate Real-Time Journal Collection at IPL




 Selection or command
 ===> ____________________________________________________________________
_
 F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
 F13=Information Assistant  F16=System main menu
```

To **start the application real-time journaling**, select **1 . Activate Real-Time Journal Collection**. The **Start Real-Time JRN Activities (STRRTJR)** screen appears.

```
                    Start Real-Time JRN Activities (STRRTJR)

 Type choices, press Enter.

 Application  . . . . . .  _____          Name, generic*, *ALL
 "Auto Start" Application Only  .  *ALL   *YES, *NO, *ALL
 Starting date and time:
   Starting date  . . . . . .  *PRVEND    Date, *PRVEND, *CURRENT...
   Starting time  . . . . . .  ________   Time, *CURRENT









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

Application

Type in the name of the application.

"Auto Start" Application Only

If you select a generic Application name or *ALL, you can specify whether to include only Auto Start Applications or *ALL Applications.

Starting date and time

Specify the starting point from which journal entries should be collected.

*PRVEND – (Default) Ensures that no journal entry is skipped. For new Applications, the process starts with the oldest available journal receiver.

NOTE: If your system holds more than 2000 journal receivers, the operating system may encounter a problem. In this case, delete older receivers before starting.

*BYRCV – Uses all available journal receivers, starting from the first up to the current one.

You may also use standard date keywords:

*CURRENT

*YESTERDAY

*WEEKSTR

*PRVWEEKS

*MONTHSTR

*PRVMONTHS

*YEARSTR

*PRVYEARS

*MON

*TUE

*WED

*THU

*FRI

*SAT

*SUN

Type choices and press **Enter**.

To **deactivate all applications**, select **2. De-activate Real-Time Journal Collection (all applications)**.

To **work with active jobs**, select **5. Work with Active Jobs**. The **Work with Subsystem Jobs** screen appears. Each application runs in a separate job.

```
                          Work with Subsystem Jobs                   S520
                                                          10/05/20  14:40:08
Subsystem  . . . . . . . . . . . :   ZJOURNAL

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


Opt  Job         User        Type     -----Status-----  Function
__   DEMOP       SECURITY4P  BATCH    ACTIVE            PGM-JRCLCT
__   TIETO       SECURITY4P  BATCH    ACTIVE            PGM-JRCLCT









          Bottom
Parameters or command
===> ____________________________________________________________________________
F3=Exit      F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display schedule data
F12=Cancel   F17=Top     F18=Bottom
```

To **control whether your application starts automatically after an IPL**:

Select **11 – Activate Real-Time Journal Collection at IPL** to enable automatic startup. This adds an AutoStart job entry to the QSYSWRK subsystem, ensuring the Application is active after each IPL.

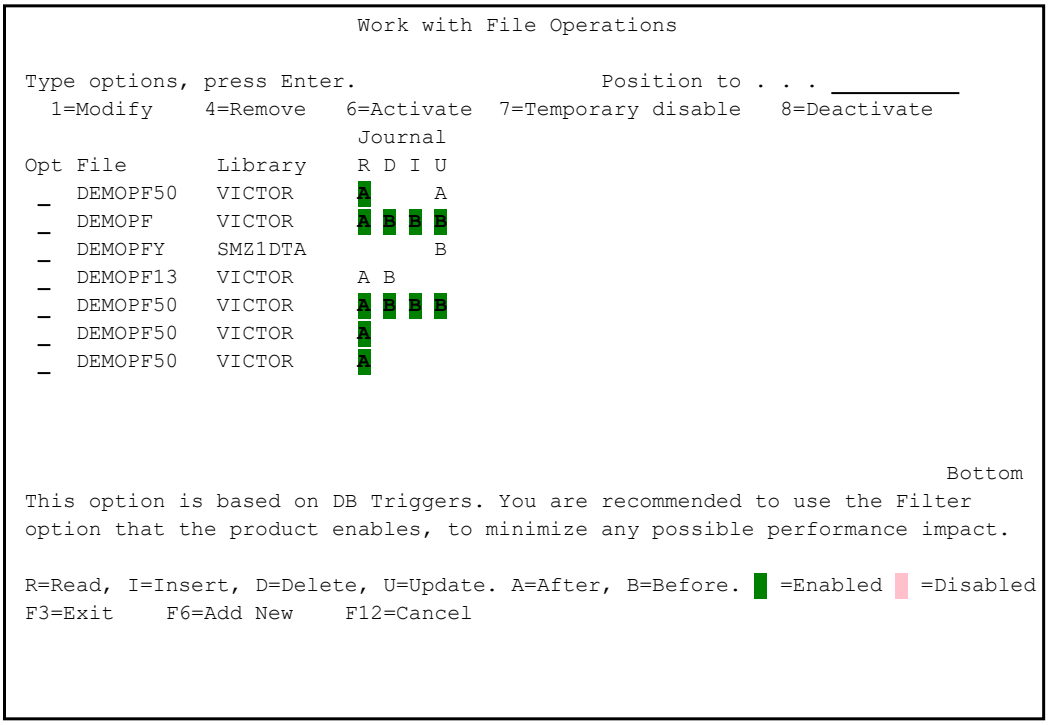
Select **12 – Do Not Activate Real-Time Journal Collection at IPL** to disable automatic

startup. This removes the AutoStart job entry from the QSYSWRK subsystem.

Journal DB Operations

A permanent license key is required in order to use this option.

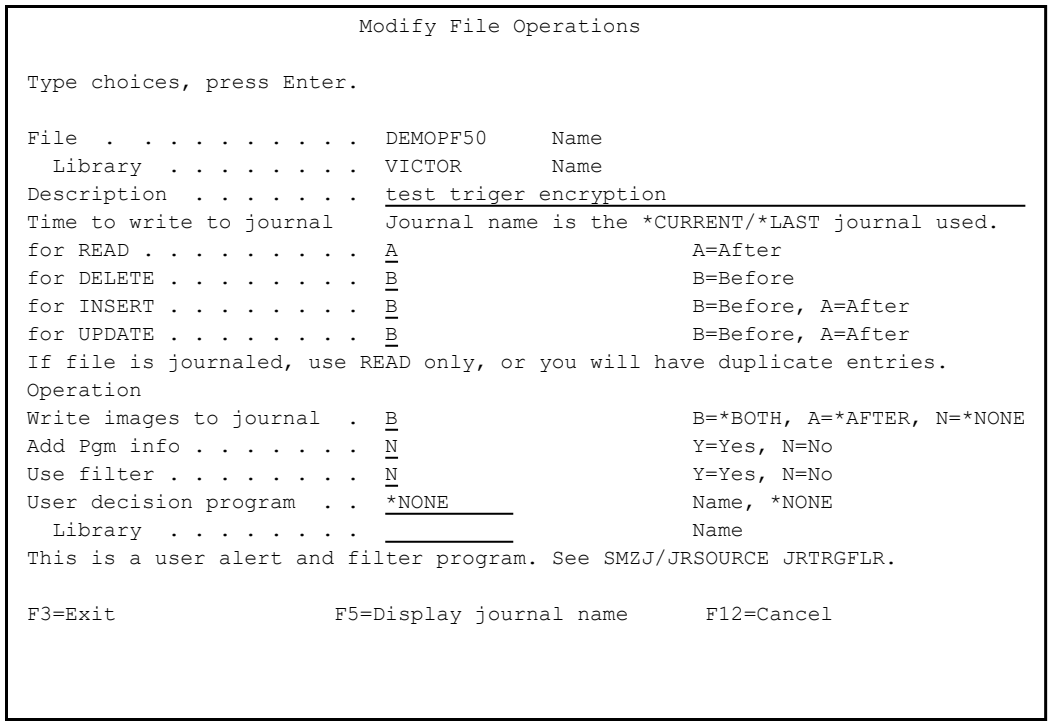
To **work with file operations**, select **`15. Collect READs by DB Triggers`** from the **Applications, BizAlerts-Definitions** screen (*STRJR > 11*). The **Work with File Operations** screen appears.



The activation status of file operations is indicated by the color of the journal definitions on the screen:

- White text on a black background: File operations are activated.
- Black text on a white background: File operations are not activated.
- Pink text: File operations are temporarily disabled.

To **add a new file or to modify an existing one**, press **F6** or type **1** in the **`Opt`** field as appropriate. The **Add File Operations** / **Modify File Operation** screen appears.



File/Library

Define the file and library that you want to add/modify.

Description

You can add a meaningful description for this file.

Time to write to journal

For each of the options, you can write A = After Image or B = Before image.

Operation

Write images to journal. The benefit of the READ feature is that most companies want to know when records have been accessed (read), as that too is a security breach. Supporting READ uses "trigger" technology, not IBM journal receivers, which makes this product unique. **AP-Journal** keeps the information about READs in IBM's journal receivers together with the regular information stored there, so the processing from that point on is the same. Filter can be based upon READs as well. B =*BOTH A =*AFTER N =*NONE

Add Pgm info. Pgm Info is written to the journal

Use filter. Specify Y = Yes if you want to add filters or N= No. In case you select Y, the Filter Conditions screen appears.

User decision program. You can add a program and library for additional calculations.

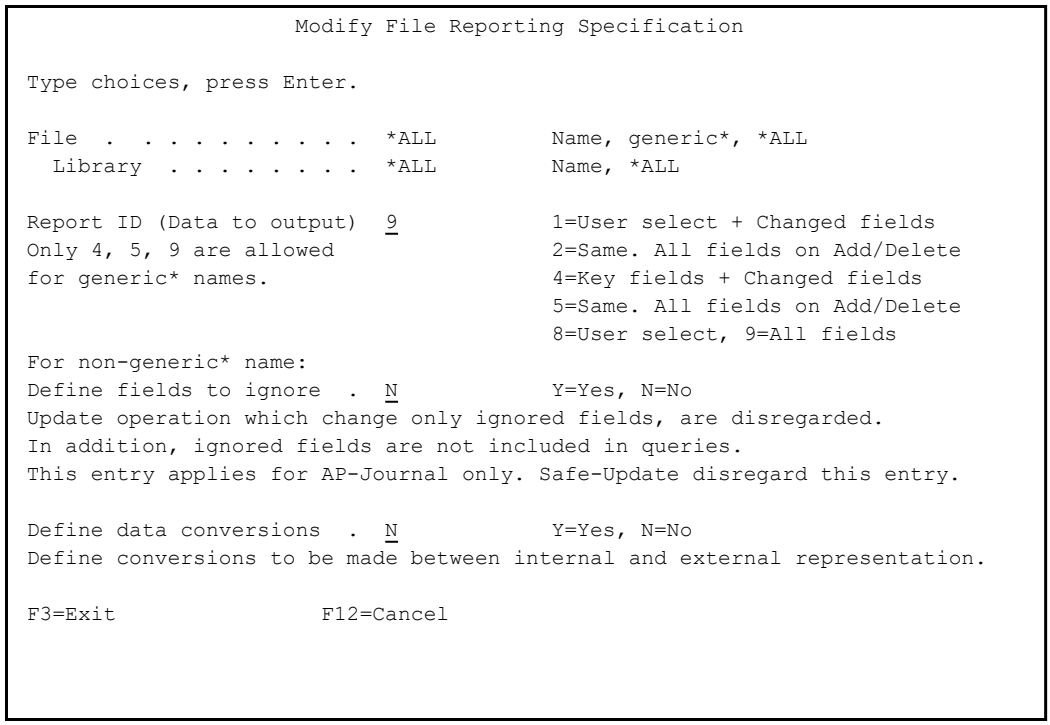
Type choices and press **Enter**.

Output Fields per File

To **work with file reporting specifications**, select **`51. Output Fields per File`** from the **Applications, BizAlerts – Definitions** screen (*STRJR > 11*). The **Work with File Reporting Specification** screen appears.

```
                    Work with File Reporting Specification

Type options, press Enter.
  1=Modify    4=Remove                   Position to file . __________
                         Report                Subset  . . . ________________
Opt File       Library    ID
 _  JRTRGP     SMZJDTA    5  JR Trigger definition
 _  LICENSE    TIFFLIB    4
 _  TESTG      DLT        9
 _  TESTG      FS         9  Output file
 _  TSTSIEM    VICTOR     9  PF for testing many fields
 _  TSTSIEMW   VICTOR     9  PF for testing many fields Wide fields
 _  TSTSYSL    VICTOR     9  Test SYSLOG
 _  YYYY       *ALL       4  Test SYSLOG

                                                                      Bottom
F3=Exit    F6=Add new    F7=Add multiple files    F12=Cancel
```

To **add a new file or to modify an existing one**, press **F6** or type **1** in the **`Opt`** field as appropriate. The **Add File Reporting Specification** / **Modify File Reporting Specification** screen appears.



File/Library

Define the file and library name that you want to add/modify.

Report ID (Data to output)

Select the option to see the defined information from the Receiver or Container:

1 - User selected fields and all changed fields.

2 - User selected fields and all changed fields. All fields are printed after Add/Delete.

4 - Key fields and all changed fields (default).

5 - User selected fields and all changed fields. All fields are printed after Add/Delete.

8 - User selected fields.

9 - All fields.

After pressing **Enter**, the **Select Output Fields** screen appears, where you can specify the order or fields.

Define fields to ignore

If you want to ignore fields, use option Y = Yes. The Fields to Ignore screen appears.

Define data conversions

If you want to define conversions of fields, use option Y = Yes. The Fields to Convert screen appears, where you can select conversion rules using F4.

File Structure Modifications

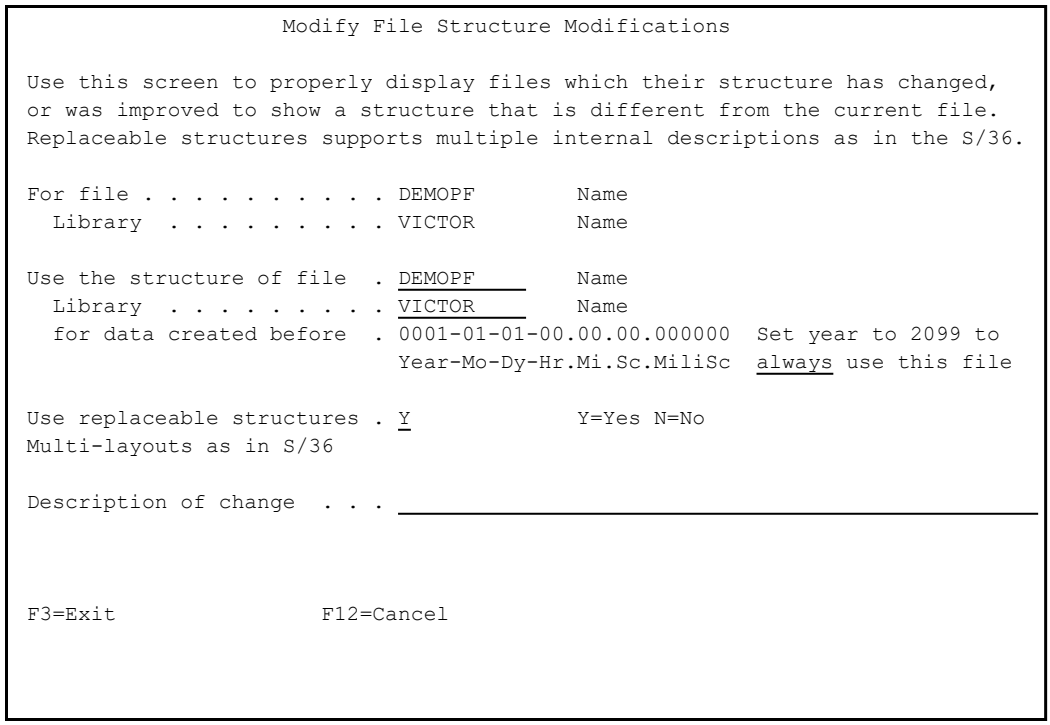
Use this option to properly display files whose structure has changed, or have one or more internal descriptions. Keep each old or different structure as a file. AP-Journal automatically selects the appropriate structure.

You should keep existing reports that have filters for these files to be used with old data kept in either containers or receivers.

To work with file structure modifications, select **52. File Structure Modifications** from the Applications, BizAlerts- Definitions screen (*STRJR > 11*). The Work with File Structure Modifications screen appears.

```
                  Work with File Structure Modifications
                                                Position to .  _________
Type options, press Enter.                      Subset  . . .  _____________
  1=Modify    4=Remove                          Inc. internal  _          Y=Yes
                                                                       Alternate
Opt For editing of file   Use structure of      If date is before  S/36-layout
 _  AUACTNP    SMZJDTA    AUACTNPJ_  SMZJ1      2099-01-01-00.00.00
 _  AUACTNP    SMZ4DTA    AUACTNP_   SMZJ1      2099-01-01-00.00.00
 _  AUIOSP     SMZ4DTA    AUIOSP_    SMZJ1      2099-01-01-00.00.00
 _  AUIOSWP    SMZ4DTA    AUIOSWP_   SMZJ1      2099-01-01-00.00.00
 _  AUNOSLP    SMZ4DTA    AUNOSLP_   SMZJ1      2099-01-01-00.00.00
 _  AUNOSP     SMZ4DTA    AUNOSP_    SMZJ1      2099-01-01-00.00.00
 _  AUNOSWP    SMZ4DTA    AUNOSWP_   SMZJ1      2099-01-01-00.00.00
 _  AUNOSZB    SMZ4DTA    AUNOSZB_   SMZJ1      2099-01-01-00.00.00
 _  AUNOSZC    SMZ4DTA    AUNOSZC_   SMZJ1      2099-01-01-00.00.00
 _  AUNOSZP    SMZ4DTA    AUNOSZP_   SMZJ1      2099-01-01-00.00.00
 _  AURPUS     SMZ4DTA    AURPUS_    SMZJ1      2099-01-01-00.00.00
 _  AUSELCP    SMZ4DTA    AUSELCP_   SMZJ1      2099-01-01-00.00.00
 _  AUUSCZC    SMZ4DTA    AUUSCZC_   SMZJ1      2099-01-01-00.00.00
 _  CMSELCP    SMZTMPA    CMSELCP_   SMZJ1      2099-01-01-00.00.00
                                                                  More...
F3=Exit   F6=Add new   F7=Un/Fold   F12=Cancel
```

To **add a new definition or to modify an existing one**, press **F6** or type **1** in the **Opt** field as appropriate. The **Add File Structure Modifications** / **Modify File Structure Modifications** screen appears.



File/Library

The file to be modified and its library. If you just enter the library, you can use F4 to select from a list of the files in the library.

Use the structure of file

The old structure of the file and its library. If you just enter the library, you can use F4 to select from a list of the files in the library.

for data created before

The date until which this change is valid. Enter the date as: YYYY-MM-DD-hh.mm.ss.milisc

Enter 0001-01-01-00.00.00.000000 for a change that has no expiry date.

Use replaceable structures

Multi-layouts as in S/36, Yes or No.

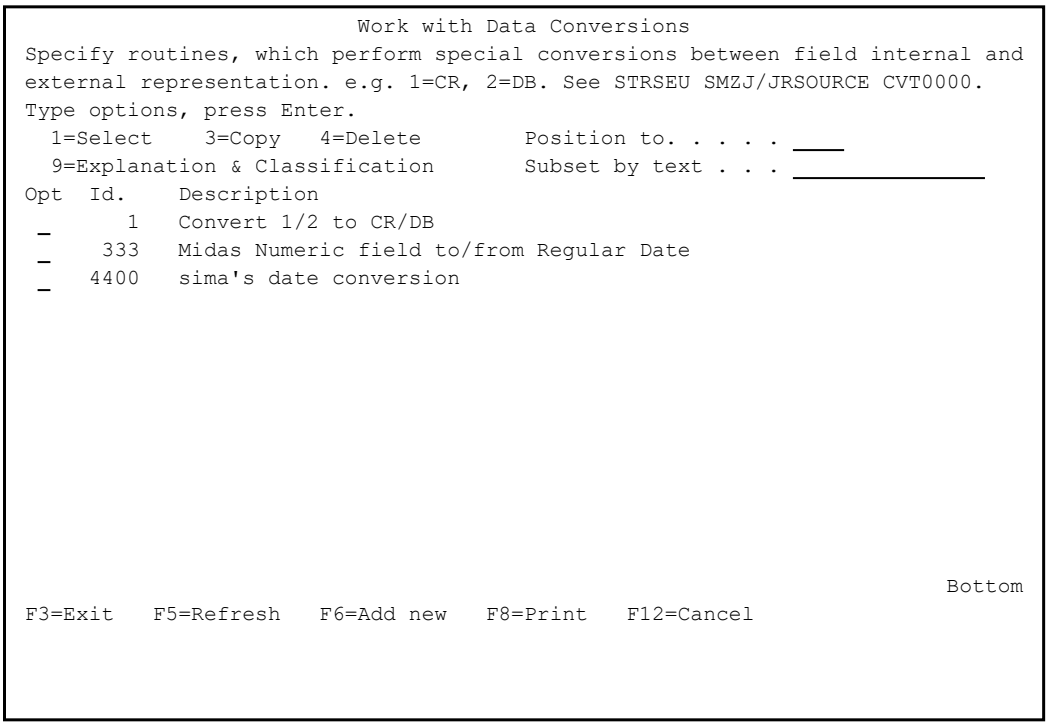
Description of change

Enter a meaningful description of the reason for the file change.

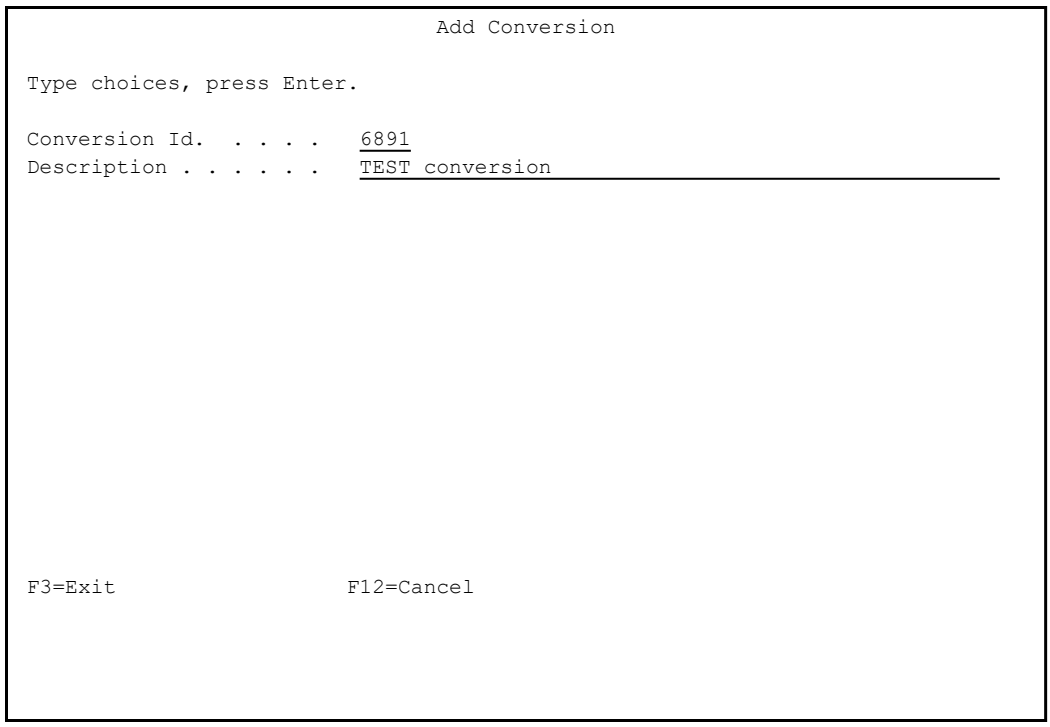
Data Conversions

You can define routines which will convert fields from their internal representation to an acceptable external representation before they are displayed in journals. For example, you might convert a date field that is stored in YYYYMMDD format to be displayed in DD/ MM/YYYY format. The conversion routine must be named *SMZJDTA/CVTnnnn*, where nnnn is the four digit conversion ID.

To work with data conversions, select **55. Data conversions** from the Applications, BizAlerts- Definitions screen (*STRJR > 11*). The Work with Data Conversions screen appears.



To **add a new definition or to modify an existing one**, press **F6** or type **1** in the **Opt** field as appropriate. The **Add Conversion** / **Modify Conversion** screen appears.



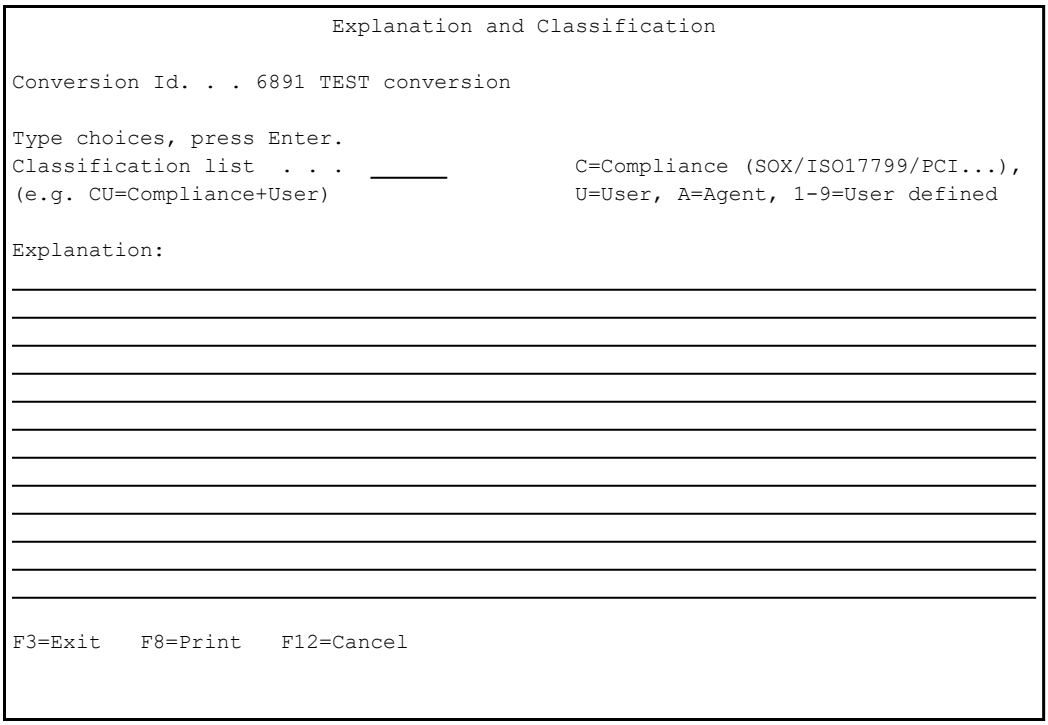
Conversion Id

Enter the four-digit Conversion ID that you used in the conversion routine name.

Description

Enter a meaningful description.

Type choices and press **Enter**. The **Explanation and Classification** screen appears.



Type choices and press **Enter**.

Plan Object Journaling

You can plan journaling for file and data area objects. Use this option to create the plan and also to put the plan into action.

To **create a journaling plan**, select **`71. Plan Object Journaling`** from the from the Applications, BizAlerts - Definitions (***STRJR > 11***). The **Work with Object Journaling Plan** screen appears.

```
                        Work with Object Journaling Plan

Type options, press Enter.                    Position to .  _________
  1=Modify   4=Remove   5=Check library       Subset  . . .  ______________

Opt Library     Type        Object      Journal     Library
 _  ALEX        *FILE       *DTAQ       JRDEMO      SMZJDTA
 _  ALEX        *FILE       A1          JRDEMO      SMZJDTA
 _  ALEX        *FILE       DEMOPF      JRDEMO      SMZJDTA
 _  ALEX        *FILE       DEMOPFFF    *NONE
 _  ROBERT      *FILE       DEMOPF      JRDEMO      SMZJDTA
 _  SMZJDTA     *FILE       *ALL        *ANY
 _  SMZJDTA     *FILE       DDDD*       *ANY
 _  TZION       *FILE       *FILE       JRDEMO      SMZJDTA
 _  TZION       *FILE       DEMOPF      JRDEMO      SMZJDTA
 _  VICTOR      *FILE       DEMOPFV     JRDEMO      SMZJDTA
 _  VICTOR      *FILE       DEMOPF7     JRDEMO      SMZJDTA
 _  VICTOR      *FILE       DEMOVPF     JVICTOR     VICTOR
 _  VICTOR      *FILE       TSTSIEM     JVICTOR     VICTOR
 _  VICTOR      *FILE       TSTSIEM*    JVICTOR     VICTOR
                                                                    More...
F3=Exit    F6=Add new (based on cursor)   F12=Cancel
```

To **add a new definition or to modify an existing one**, press **F6** or type **1** in the **Opt** field as appropriate. The **Add Object journaling Plan** / **Modify Object journaling Plan** screen appears.

```
                        Modify Object journaling Plan

Type choices, press Enter.

Library   . . . . . . . . . ALEX           Name
Object type . . . . . . . . *FILE          *FILE, *DTAARA
Object  . . . . . . . . . . *DTAQ          Name, generic*, *ALL

Journal . . . . . . . . . . JRDEMO         Name, *NOCHK, *ANY, *NONE
  Library . . . . . . . . . SMZJDTA        Name

*NOCHK Do not check journaling status
*ANY   Ensure that the object is journaled
*NONE  Ensure that the object is not journaled




F3=Exit                F12=Cancel
```

Library

The library that contains the object you want to journal.

Object type

*FILE

*DTAARA

Object

Name - The name of the object you want to journal generic* = A group of objects you want to journal. For example, to journal all files that begin with MAS, enter MAS*

*ALL = Journal all the objects of the selected object type in the library.

Journal

Name = The name of the journal to use

*NOCHK = Do not check the journaling status

*ANY = Ensure that the object is journaled

*NONE = Ensure that the object is not journaled

Library

The name of the library that contains the journal.

Type choices and press **Enter**.

Check Object Journaling

After setting the plans, you can check if some objects are not journaled as planned.

To **check object journaling**, select **72. Check Object Journaling** from the **Applications, BizAlerts- Definitions** screen (*SRTJR > 11*). The **Work with Object Journaling Status** screen appears.

```
                    Work with Object Journaling Status

Type options, press Enter.                    Position to .  _________
  1=Check                                     Subset  . . .  _______________

Opt Library
 _  ALEX
 _  ROBERT
 _  SMZJDTA     AP-Journal Temporary lib (A)
 _  TZION       AP-Journal Temporary lib (A)
 _  VICTOR      Victor training
 _  YOEL        Victor training

                                                                        Bottom
F3=Exit                                F12=Cancel
```

Type **1** in the **Opt** field to check the status of objects within the library. The additional Work with Object Journaling Status screen appears.

```
                    Work with Object Journaling Status

Library . . .: ALEX                           Position to .  _________
                                              Subset  . . .  _______________
Type options, press Enter.                    In mismatch .  _          Y, N
  3=Set as planned
                          ----- Actual (Or last) -----    ---- Planned -----
Opt Object     Type       Journaled Journal    Library    Journal    Library
    AA         *FILE         NO
    AAAA       *FILE         NO
    AZFARIZA   *FILE         NO     FSJRN      SMZ1DTA
    A12233353  *FILE         YES    JRDEMO     SMZJDTA
 _  DEMOPF     *FILE         NO     FSJRN      SMZ1DTA    JRDEMO     SMZJDTA
    DEMOPF1    *FILE         NO     FSJRN      SMZ1DTA
    DEMOPF2    *FILE         NO     FSJRN      SMZ1DTA
    DEMOPF55   *FILE         YES    JRDEMO     SMZJDTA
    DSP01      *FILE         NO
    DSP01B     *FILE         NO
    FILE       *FILE         NO
    FSDDSSRC   *FILE         NO
                                                                    More...
F3=Exit    F5=Refresh    F12=Cancel
```

The screen displays a list of objects whose journal status does not match the defined plan. Use Option 3 to update the object's journal status to match the

plan. If an object is currently journaled to the wrong journal, the system will automatically remove it from the incorrect journal and assign it to the correct one as defined in the plan.

Set Journal as Planned

If you know which object you want to set to be journaled as planned, you can do this directly.

To **set the journal as planned**, select **`73. Set Journal as Planned`** from the **Applications, BizAlerts- Definitions** screen (**STRJR > 11**). The **Set Journal As Planned (SETJRPLN)** screen appears.

```
                      Set Journal As Planned (SETJRPLN)

Type choices, press Enter.

Object . . . . . . . . . . . . .   __________     Name, generic*, *ALL
  Library  . . . . . . . . . . .     __________   Name
Object type  . . . . . . . . . .   *FILE         *FILE, *DTAARA, *DTAQ
For planning of *ANY:
  Journal to set to  . . . . . .   *NOSET         Name, *NOSET
    Library  . . . . . . . . . .     __________   Name
  Prefer previous journal  . . .   *NO           *YES, *NO

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

`Object`

The object you chose.

`Library`

The library of the object you chose.

`Object type`

Define the type of object.

*FILE = physical files

*DTAARA = Data area

*DTAQ = data queue

Journal to set to

The journal to receive journal entries.

*NOSET = Use the preferred previous journal parameter

Library

The library that contains the journal.

Prefer previous journal

*YES = use previous journal

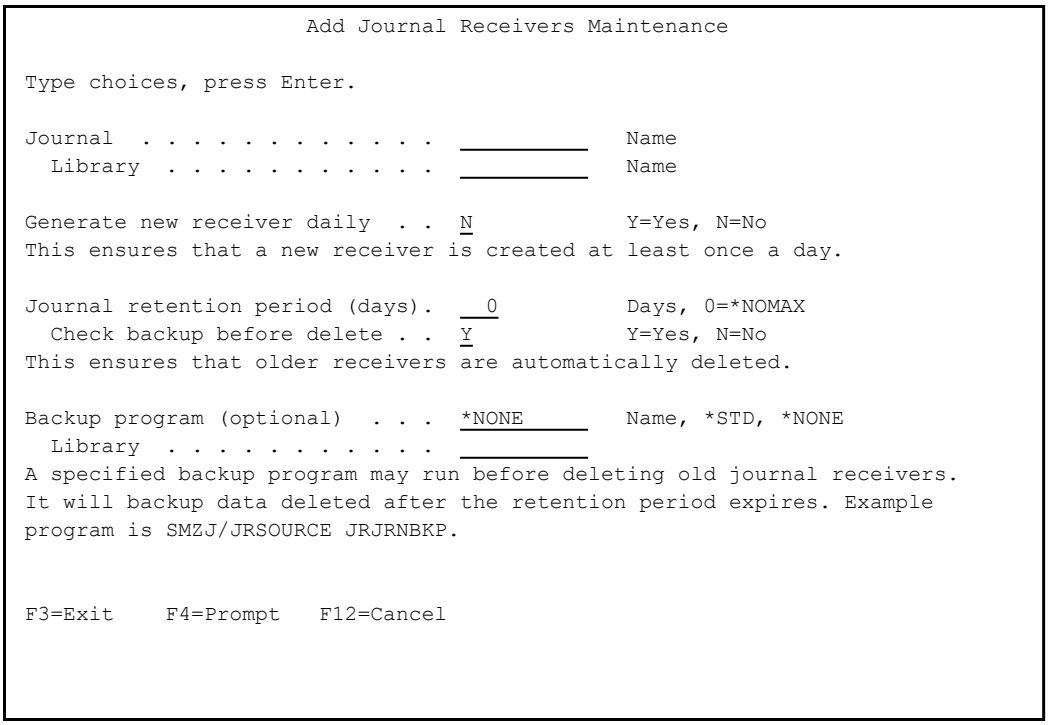
*NO = use the specified journal.

Auto Maintenance of Receivers

To work with IBM Journal Receivers, select **75. Auto Maintenance of Receivers** from the Applications, BizAlerts – Definitions screen (*STRJR > 11*). The Work with Journal Receivers Maintenance screen appears.

```
                  Work with Journal Receivers Maintenance

Type options, press Enter.
  1=Modify   4=Remove   5=Work with journal attributes
  6=Print journal attributes   7=Generate and attach a new receiver
                          Crt  Retain         Position to . . . _________
Opt Journal    Library  Daily  Days
 _  JRN        VICTOR     Y    120
 _  JVICTOR    VICTOR     Y    120
 _  QAOSDIAJRN QUSRSYS    N     30     Journal for DIA files
                                                                  Bottom
F3=Exit    F6=Add New    F12=Cancel
```

To **add a new definition or to modify an existing one**, press **F6** or type **1** in the **Opt** field as appropriate. The **Add Journal Receivers Maintenance** / **Modify Journal Receivers Maintenance** screen appears.



Journal

Specify the name of the journal that should be maintained.

Library

The library that contains the journal.

Generate new receiver daily

Defines whether a new receiver should be generated each day.

• Y = YES – A new journal receiver is created daily, regardless of activity level. This simplifies receiver cleanup and management.

• N = NO – New receivers are only generated when the current one is full, which may occur after hours, days, or weeks, depending on system activity.

Journal retention period (days)

Days = The journal will be kept for the number of specified days.

0 = *NOMAX – Retain journal receivers indefinitely. Manual cleanup is required.

Check backup before delete

Y = Yes check if a journal receiver saved before deleting. If it is not saved, it will not be deleted.

N = No, do not check; delete older journal receivers.

Backup program

A backup program is running before the old journal receivers are running.

Library

The library that contains the backup program.

Auto Start Object Journaling

To work with Auto Start, select **77. Auto Start Object journaling**. The Start Journal Library screen appears.

```
                    Start Journal Library (STRJRNLIB)

Type choices, press Enter.

Library  . . . . . .  _________     Name, generic*
            + for more values  _________
Journal  . . . . . .  _________     Name
  Library  . . . . . .   *LIBL      Name, *LIBL, *CURLIB
Inherit rules:                  _
  Object type  . . . . . .  *ALL        *ALL, *FILE, *DTAARA, *DTAQ
  Operation  . . . . . .  *ALLOPR       *ALLOPR, *CREATE, *MOVE...
  Rule action  . . . . . .  *INCLUDE    *INCLUDE, *OMIT
  Images . . . . . .  *OBJDFT           *OBJDFT, *AFTER, *BOTH
  Omit journal entry . . . . . .  *OBJDFT  *OBJDFT, *NONE, *OPNCLO
  Remote journal filter  . . . .  *OBJDFT  *OBJDFT, *NO, *YES
  Name filter  . . . . . .  *ALL        Name, generic*, *ALL
            + for more values  _
Logging level  . . . . . .  *ERRORS     *ERRORS, *ALL


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

This option allows you to start journaling for all applicable objects within a specified library.

Library

Enter the name of the library containing the objects you want to journal.

Journal/Library

The name of the journal and the library where the journal is stored.

Inherit rules

Define the parameters for starting journaling based on your requirements.

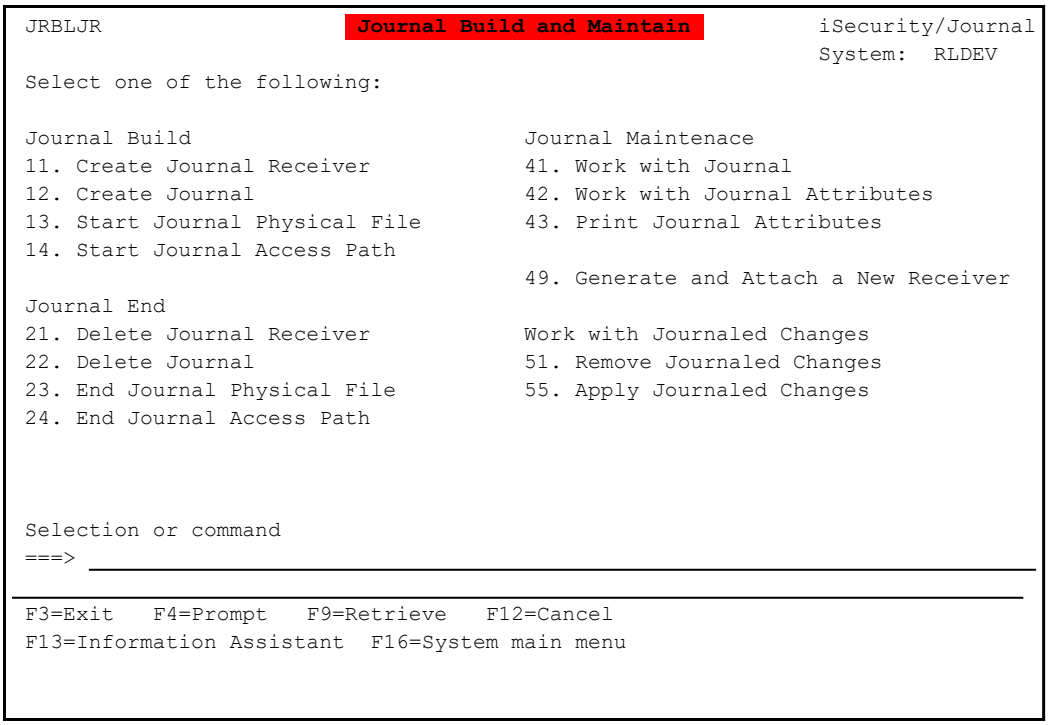
Display Auto Start Settings

To display the Auto Start settings, select **78. Display Auto Start Setting** from the Applications, BizAlerts – Definitions screen (*STRJR > 11*). The Display Library Description (DSPLIBD) screen appears. Define the library and the output type and press Enter.

Building Journals, Revoke Changes

If you start from scratch and do not have any Journals, Journal receivers, or the journaled files, you can start from here to set up the environment.

To build and maintain the journal, select **79. Building Journals, Revoke Changes** from the Applications, BizAlerts – Definitions screen (*STRJR > 11*). The Journal Build and Maintain screen appears.

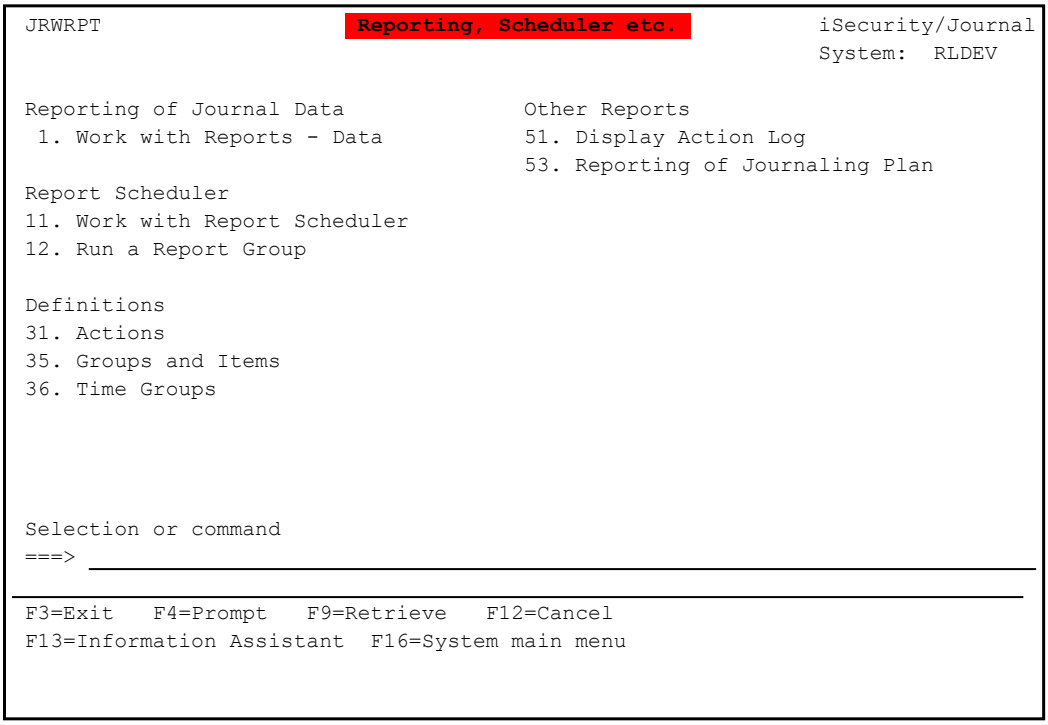

JRBLJR
Journal Build and Maintain
iSecurity/Journal
System: RLDEV
Select one of the following:
Journal Build
11. Create Journal Receiver
12. Create Journal
13. Start Journal Physical File
14. Start Journal Access Path
Journal End
21. Delete Journal Receiver
22. Delete Journal
23. End Journal Physical File
24. End Journal Access Path
Journal Maintenace
41. Work with Journal
42. Work with Journal Attributes
43. Print Journal Attributes
49. Generate and Attach a New Receiver
Work with Journaled Changes
51. Remove Journaled Changes
55. Apply Journaled Changes
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=System main menu

Reporting and Scheduling

Reporting and Scheduling allows you to run pre-defined “report groups” automatically according to a fixed schedule.

A report group is comprised of one or more individual queries, reports, or Activity Log inquiries that are executed together at a designated time. Grouping of reports in this manner is more efficient because the scheduling details and other run-time parameters need only be defined once for the entire group.

To define reports, scheduler, etc., select **12.Reports, Scheduler etc.** from the main menu (*STRJR*). The **Reporting, Scheduler etc.** screen appears.



To work with reports, select **1. Work with Reports - Data** from the Reporting, Scheduler etc. screen (*STRJR > 12*) as shown in "Working with Reports " on the facing page

To work with report scheduler, select **11. Work with Report Scheduler** from the Reporting, Scheduler etc. screen (*STRJR > 12*) as shown in "Define Report Schedules " on page 98.

To **run a report group**, select **`12. Run a Report Group`** from the **Reporting, Scheduler etc.** screen (*STRJR > 12*) as shown in "Define Report Schedules " on page 98.

NOTE: Another way to run a report group is to type **6** in the **`Opt`** field next to the group from the **`Work with Report Scheduler`** screen (*STRJR > 12 > 11*).

Working with Reports

To **work with reports**, select **`1. Work with Reports - Data`** from the **`Reporting, Scheduler etc.`** screen (*STRJR > 12*). The **Work with Reports** screen appears.

```
                          Work with Reports
 Type options, press Enter.                                    System: RLDEV
   1=Modify  3=Copy           4=Delete  5=Run (Receivers)  6=Run (Containers)
   7=Filters                          Position to  . . . . _____
   X=Explanation & Classification     Subset by text . . . _______________
        = Collecting  Enabled           by classification. _  A=Agent...
             Enabled
Opt Name  Type     Journal
 _  AUXXJ APP   Y  FSJRN      AUXX   AR
 _  DEMO1 APP   Y  JRN        Demo
 _  DEMO2 -RPT     JRN        Demo
 _  JELIJ APP   Y  ELIJRN     Eli Journal
 _  MFAUS APP   Y  SMZO       MFA changes
 _  MONEY -RPT     JRDEMO
 _  RRRRR -RPT     JRDEMO
 _  RRRR1 APP   Y  JRDEMO
 _  SMZCJ APP   Y  SMZC        Capture journaling
 _  SMZVJ APP   Y  SMZV       SMZV change definitions
 _  TEST1 -RPT     JRDEMO
 _  TEST4 APP   Y  JRDEMO
                                                              More...
 F3=Exit  F5=Refresh  F6=Add  F7=Un/Fold                  F12=Cancel
```

`1 = Modify`

An option to modify the report.

`3 = Copy`

An option to copy the report.

`5 = Run (Receivers)`

An option to open the **Display APP Current Journal (DSPAPCRJ)** screen.

6 = Run (Container)

An option to open the Display Application Journal (DSPAPJRN) screen.

7 = Filters

An option to open the Define Include Filters screen.

To add a report, press F6. The Add Report screen appears. The following example has been filled in for a TESTU report based on a JRDEMO within an SMZJDTA library.

```
                              Add Report                    System: RLDEV
                                                  Last change date:  0/00/00
                                                           by user:
Report . . . . . . . . . . . . TESTU          Name
Text . . . . . . . . . . . . . Test Report Example for User Guide
Type . . . . . . . . . . . . . RPT            APP=Application, RPT=Report
Based on journal . . . . . . . JRDEMO
  Library  . . . . . . . . . .   SMZJDTA        IASP . *NONE       Name, *NONE
Include all journaled objects  Y    Y=Yes, N=Restrict by "1. Objects"

Select one of the following:
   1. Objects
   3. Filters

Selection ===> 1
About Reports and Applications
Report is a limited application definition, which includes Objects and
Filters. It does not include other definitions such as Business Items (eg.
P/O, Item, Cust.). It is used to define selections over Journaled data or
over prefiltered data that is kept in application containers.

F3=Exit    F4=Prompt

Enter value for a required parameter.
```

Report

Must contain five characters as name.

Text

Insert descriptive text.

Based on journal

Specify the journal name from which the report retrieves data.

Library

Specify the library of the journal.

IASP

*NONE = Journal is in system asp

Name = Journal is in the specified ASP

Include all journaled objects

Y = Report contains all objects in the journal

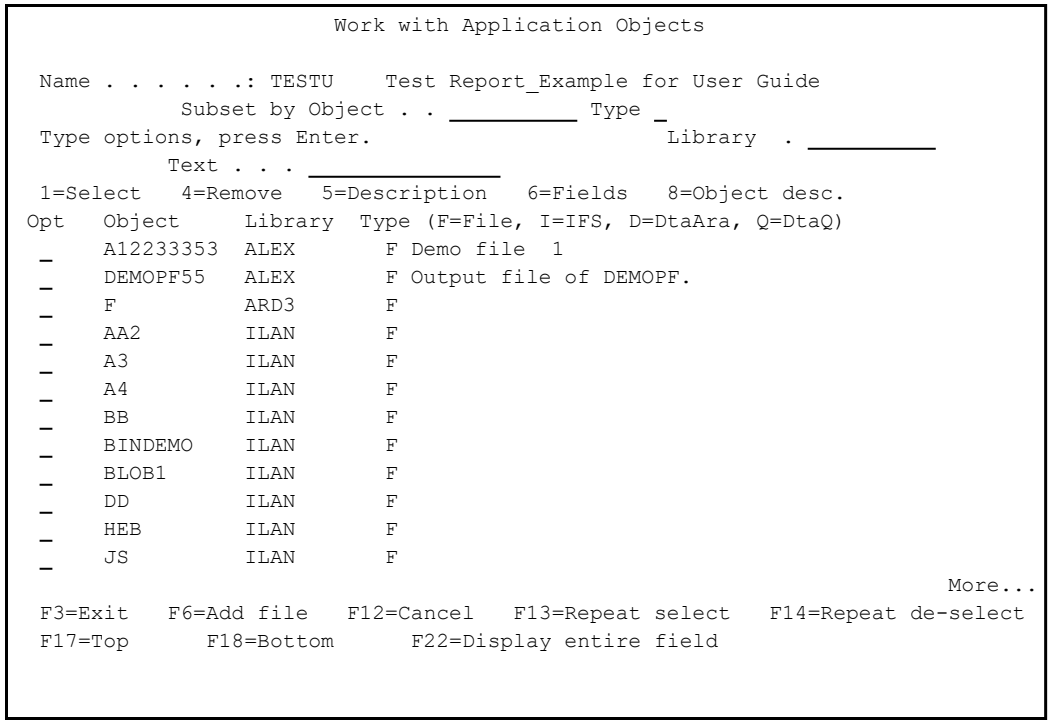
N = Specify the objects in Option 1. Objects

Select one of the following

1 = Objects, define what objects should be included in the report

2 = Filters, set filters to see only desired data in the report

If in **Select one of the following** was selected **1. Objects**, the Work with Application Objects screen appears.



Type options and press Enter twice. The created report appears on the Work with Reports screen.

If in the **Select one of the following** field was selected **2. Filters**, the Define Include Filters screen appears as shown in Setting Filter Conditions.

To **modify the report**, type **1** in the **Opt** field next to the report should be modified. The **Modify Report** screen appears, allowing the modification of either application objects (**1. Objects**) or filters (**3. Filters**) included in the report.

To **display the report**, type either **5** (**5=Run (Receivers)**; the **Display APP Current Journal (DSPAPCRJ)** screen appears; type choices and press **Enter**; the **Display Journal Entries** screen appears) or **6** (**6=Run (Containers)**; the **Display Application Journal (DSPAPJRN)** screen appears; type choices and press **Enter**; the **Display Journal Entries** screen appears).

Define Report Schedules

Working with Report Scheduler

To **work with report scheduler**, select **11. Work with Report Scheduler** from the **Reporting, Scheduler etc.** screen (*STRJR > 12*). The **Work with Report Scheduler** screen appears.

```
                          Work with Report Scheduler
                                      Position to  . . . . _______
                                      Subset by text . . . _________________
Type options, press Enter.
  1=Select   2=Add   3=Copy   4=Delete   5=Run group

Opt Group    Seq                                                    Query
 _  AAAA          victor test empty report
 _           __1.0 Display Application                              DSPAPJRN
 _           __2.0 Display Application                              DEMO1
 _           __3.0 Display Application                              MFAUS
 _  DAILY         Run daily report group
 _  DAILYGU       Daily, for GUI output (EXCEL like, preformatted)
 _  DAILYML       Daily, in HTML, sent by Email
 _  HAIM          TEST report groupe1
 _           __1.0 Display Application                              DEMO1
 _  HATEST        test report group
 _           __1.0 Display Application                              TEST4
 _           __2.0 Display Application                              DEMO1
 _           __3.0 Display Application                              MFAUS
                                                                      More...
F3=Exit    F5=Refresh    F6=Add New Group   F8=Print     F12=Cancel
```

1 = Select

An option to modify a group settings.

2 = Add

An option to add a report to a group.

3 = Copy

An option to copy a group.

4 = Delete

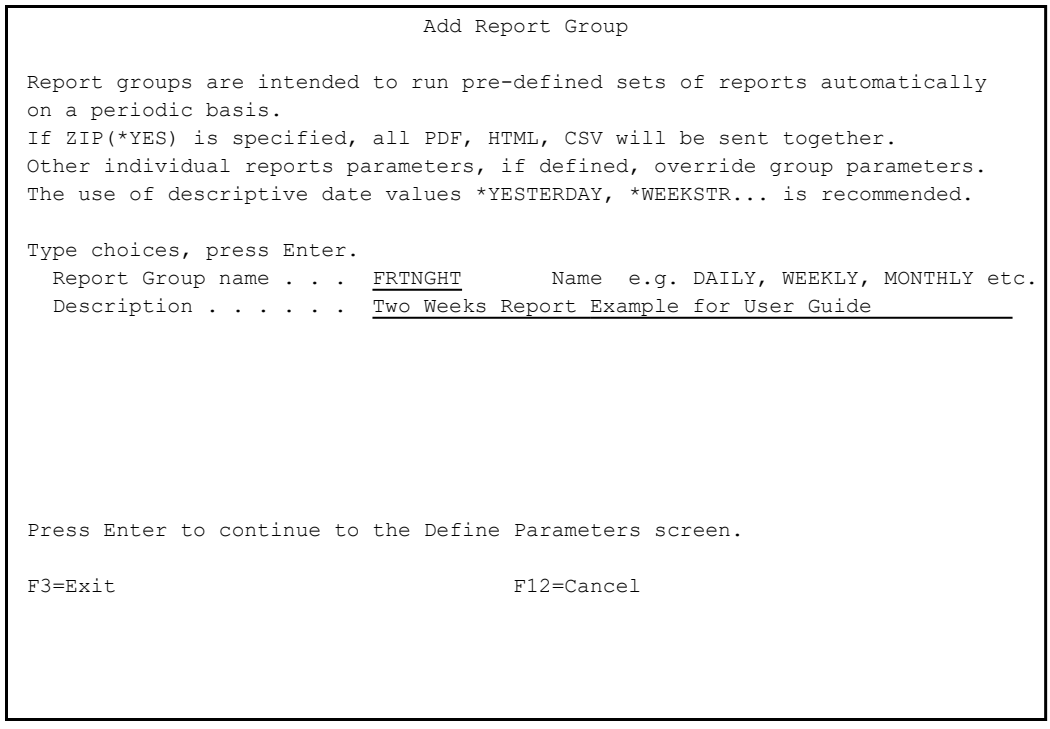
An option to delete a group .

5 = Run

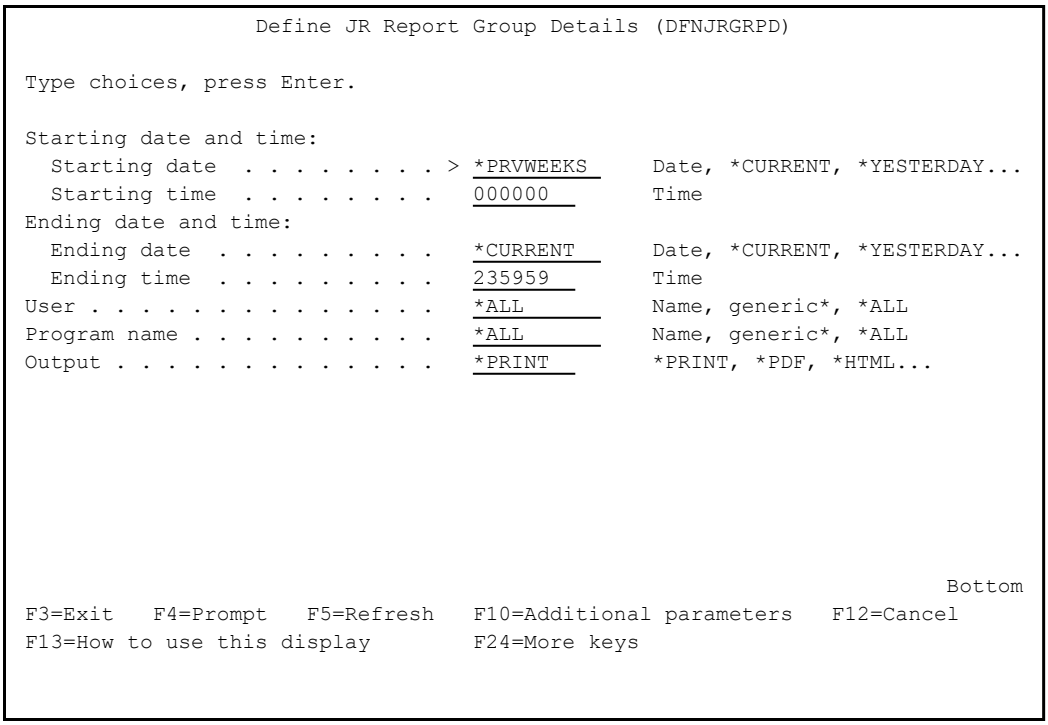
An option to run a group.

To **create a new report group**, type **F6**. The **Add Report Group** screen appears. The following example has been filled in for a FRTNGHT Report Group name.

NOTE: We recommend a meaningful name like DAILY for daily reports, WEDNESD for report groups running every Wednesday, etc.



Press Enter. The **Define JR Report Group Details (DFNJRGRPD)** screen appears.



Starting date and time

Define the start date and time. Press **F4** to select predefined options.

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

Ending date and time

Define the end date and time. Press **F4** to select predefined options.

*CURRENT = The current date (day the report runs)

*YESTERDAY = The day before the current date

*WEEKSTR = Beginning of the current week

*PRVWEEKSTR = Beginning of the previous week

*MONTHSTR = Beginning of the current month

*PRVMONTHSTR = Beginning of the previous month

*YEARSTR = Beginning of the current year

*PRVYEARSTR = Beginning of the previous year

*MON - *SUN = Day of the current (or previous) week

User

Specify the user that should be covered by this report group.

Name = A specific user

Name* = A generic user

*ALL = All users

Program name

Specify the program names that should be covered by this report group.

Name = A specific program name

Name* = A generic program name

*ALL = All program names

Output

Select output format:

*PDF

*HTML

*CSV

*OUTFILE

*PRINT

*PRINT1 - 9

Type choices and press Enter. The Add Job Schedule Entry (ADDJOBSCDE) screen appears.

```
                    Add Job Schedule Entry (ADDJOBSCDE)

 Type choices, press Enter.

 Job name . . . . . . . . . . . . > JR@FRTNGHT    Name, *JOBD
 Frequency  . . . . . . . . . . . > *ONCE         *ONCE, *WEEKLY, *MONTHLY
 Schedule date  . . . . . . . . . > *NONE         Date, *CURRENT, *MONTHSTR...
 Schedule day . . . . . . . . . . > *ALL          *NONE, *ALL, *MON, *TUE...
               + for more values
 Schedule time  . . . . . . . . . > 230000        Time, *CURRENT

                           Additional Parameters

 Job description  . . . . . . . . > *USRPRF       Name, *USRPRF
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB

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

Press **Enter**. A new report group appears on the **Work with Report Scheduler** screen.

To **add reports to the group**, type **2** in the **Opt** field next to the group from the **Work with Report Scheduler** screen (*STRJR > 12 > 11*). The **Add Report Definition screen** appears.

```
                          Add Report Definition

Reports in a group run periodically, as per the group definition.
If ZIP(*YES) is specified for the Group, the mail info is taken from the Group.
All other parameters defined for a report, override group parameters.

Group FRTNGHT    Two Weeks Report_Example for User Guide

Type choices, press Enter.

Report Id.  . . . . . .    1.0
Description . . . . . .  Display Application
Reporting command (F7).  DSPAPJRN       Command, *SELECT/F7=Select from list
                         Display Application
Report parameters (F4).




F3=Exit   F4=Set Parameters   F7=Select Command              F12=Cancel
```

Report ID

Numeric ID automatically assigned by the **AP-Journal**

Description

Type in a meaningful description of your report.

Reporting command

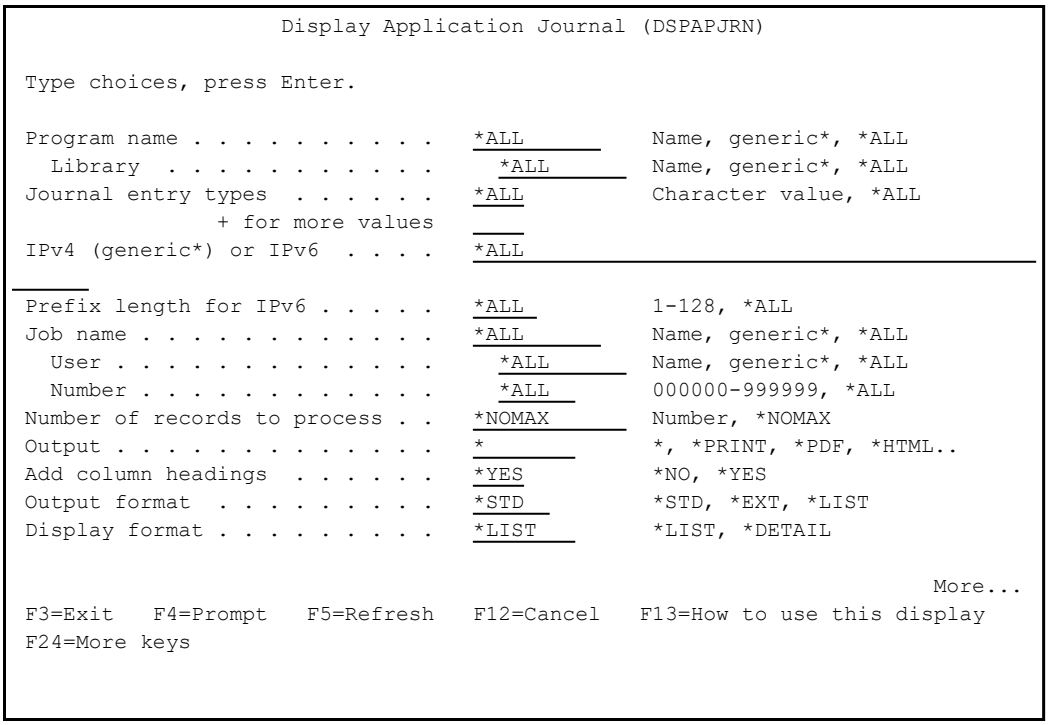
Press F7 to select the available commands from a pop-up window.

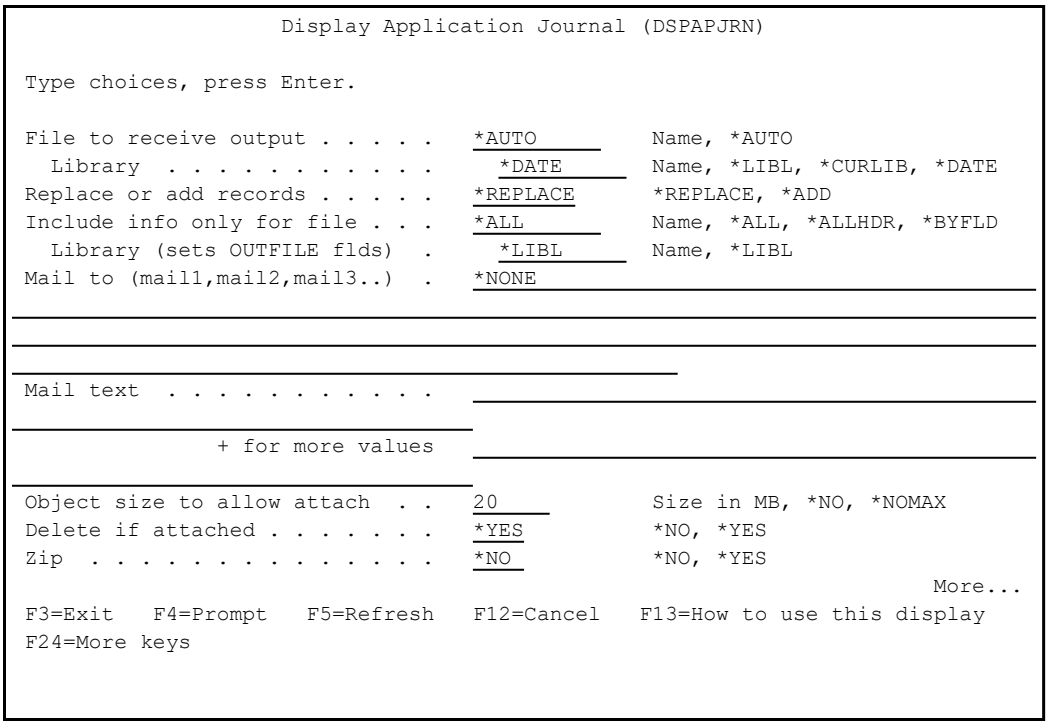
NOTE: There are options to report from Receivers (DSPAPACRJ, DSPAPCRJ), from Containers (DSPAPJRN), or from single-file journals (DSPDBJRN).

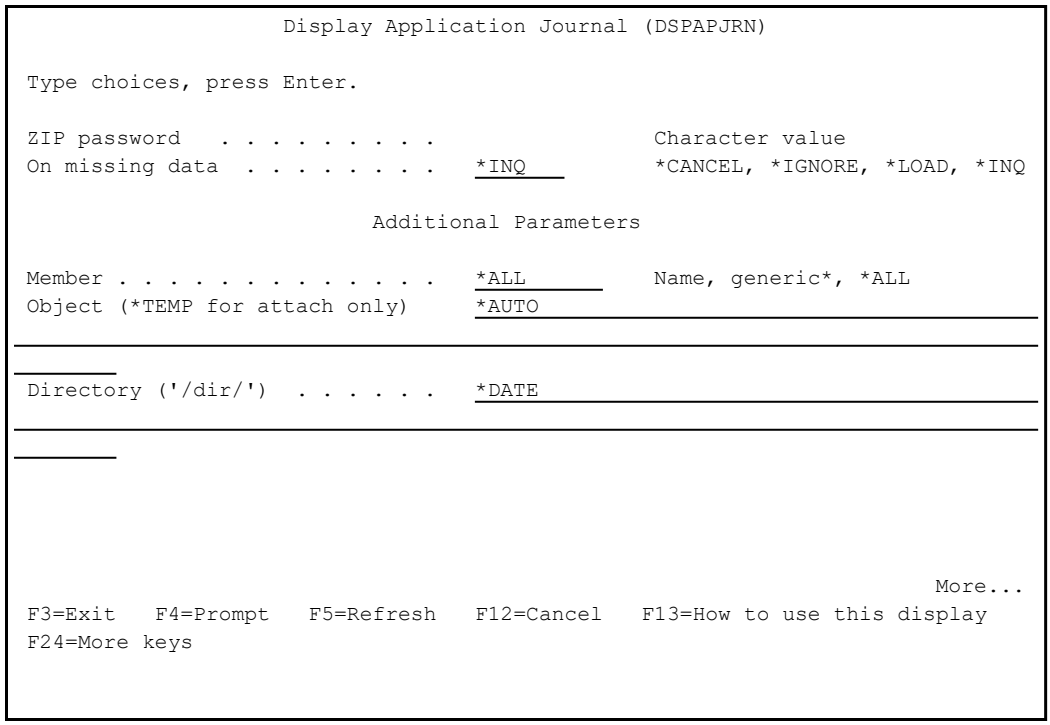
Reporting parameters

Press F4 to select the report parameter. The Display Application Journal (DSPAPJRN) screen appears.

```
                    Display Application Journal (DSPAPJRN)

Type choices, press Enter.

Application           F4=Names      SELECT       Name, *SELECT, AUXXJ, DEMO1...
Report                F4=Names      *NONE        Name, *SELECT, *NONE, AUXXJ...
Display last minutes . . . . . .    *BYTIME      Number, *BYTIME
Starting date and time:
  Starting date  . . . . . .        *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .        000000       Time
Ending date and time:
  Ending date  . . . . . .          *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . .          235959       Time
Analyze business data:              _
  Business item Id.  . . . . . .    *ALL         1-15, *ALL
  Test . . . . . .                  ______       EQ, NE, GT, GE, LT, LE...
  Value  . . . . . .                _____________________________________________
______
                + for more values _
User profile . . . . . .            *ALL         Name, generic*, *ALL
                                                                        More...
F3=Exit    F4=Prompt    F5=Refresh    F10=Additional parameters    F12=Cancel
F13=How to use this display          F24=More keys
```


Display Application Journal (DSPAPJRN)
Type choices, press Enter.
Program name . . . . . *ALL Name, generic*, *ALL
Library . . . . . *ALL Name, generic*, *ALL
Journal entry types . . . . . *ALL Character value, *ALL
+ for more values
IPv4 (generic*) or IPv6 . . . . *ALL
Prefix length for IPv6 . . . . . *ALL 1-128, *ALL
Job name . . . . . *ALL Name, generic*, *ALL
User . . . . . *ALL Name, generic*, *ALL
Number . . . . . *ALL 000000-999999, *ALL
Number of records to process . . *NOMAX Number, *NOMAX
Output . . . . . * *, *PRINT, *PDF, *HTML..
Add column headings . . . . . *YES *NO, *YES
Output format . . . . . *STD *STD, *EXT, *LIST
Display format . . . . . *LIST *LIST, *DETAIL
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

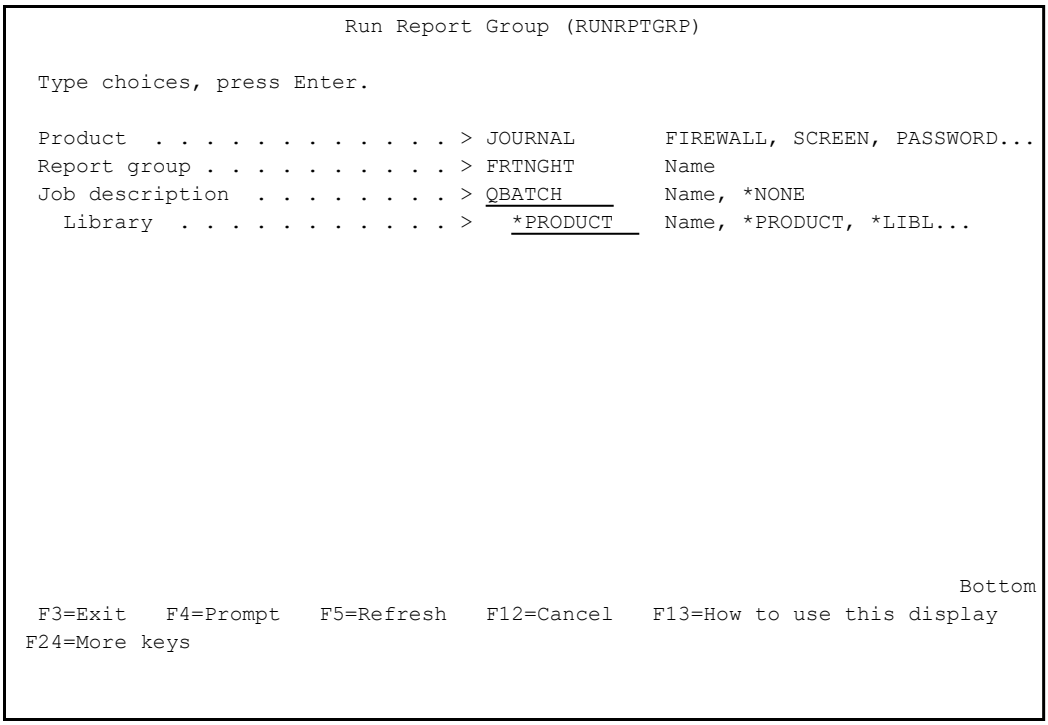

Display Application Journal (DSPAPJRN)
Type choices, press Enter.
File to receive output . . . . . *AUTO Name, *AUTO
Library . . . . . *DATE Name, *LIBL, *CURLIB, *DATE
Replace or add records . . . . . *REPLACE *REPLACE, *ADD
Include info only for file . . . *ALL Name, *ALL, *ALLHDR, *BYFLD
Library (sets OUTFILE flds) . *LIBL Name, *LIBL
Mail to (mail1,mail2,mail3..) . *NONE
Mail text . . . . . .
+ for more values
Object size to allow attach . . 20 Size in MB, *NO, *NOMAX
Delete if attached . . . . . *YES *NO, *YES
Zip . . . . . *NO *NO, *YES
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys



Type choices and press **Enter** to finish the definition and return to the **Work with Report Scheduler** screen.

Run Report Groups

To **run a report group**, type **6** in the **Opt** field next to the group from the **Work with Report Scheduler** screen (***STRJR > 12 > 11***). The **Run Report Group (RUNRPTGRP)** screen appears.

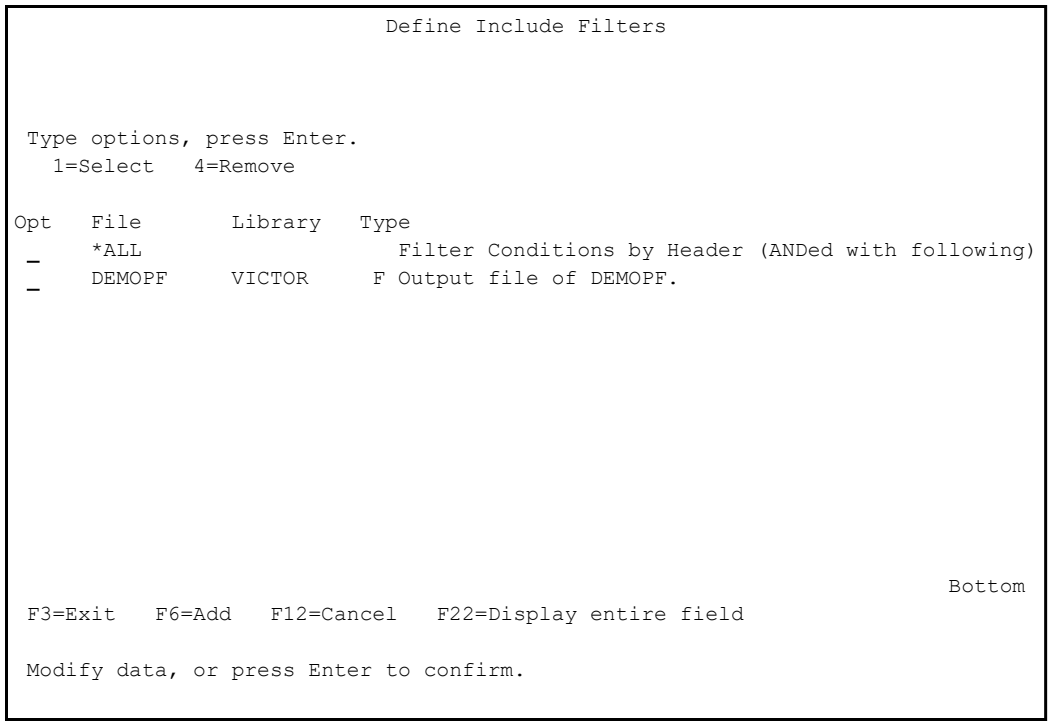


Type choices and press **Enter**.

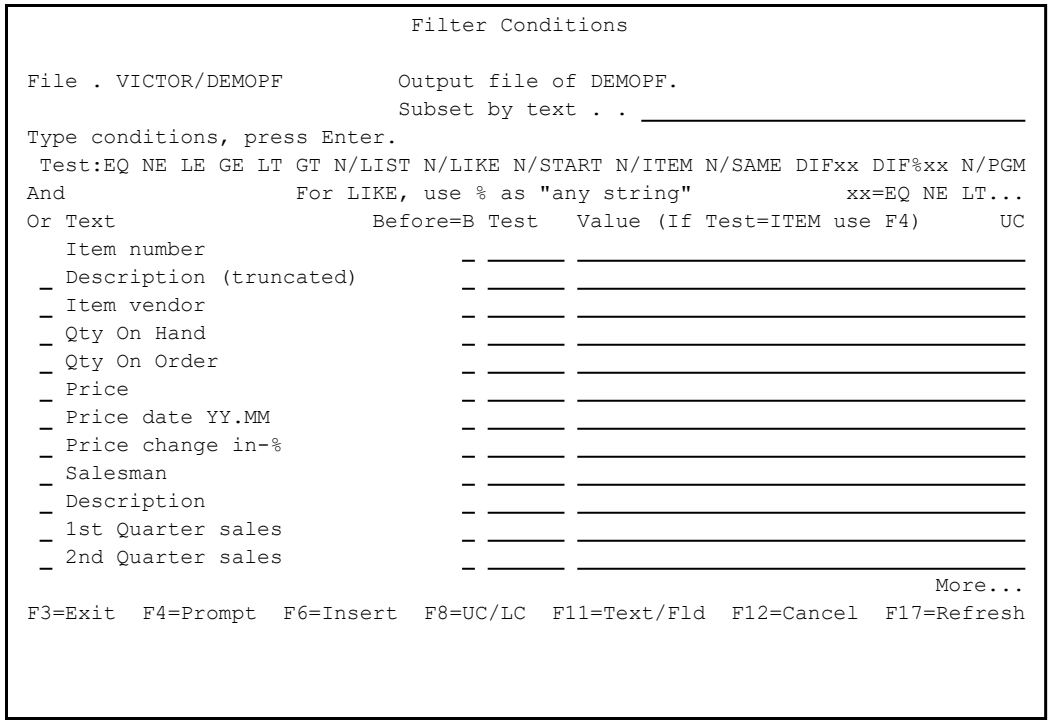
NOTE: Another way to access the **Run Report Group (RUNRPTGRP)** screen is *STRJR > 12 > 12.*

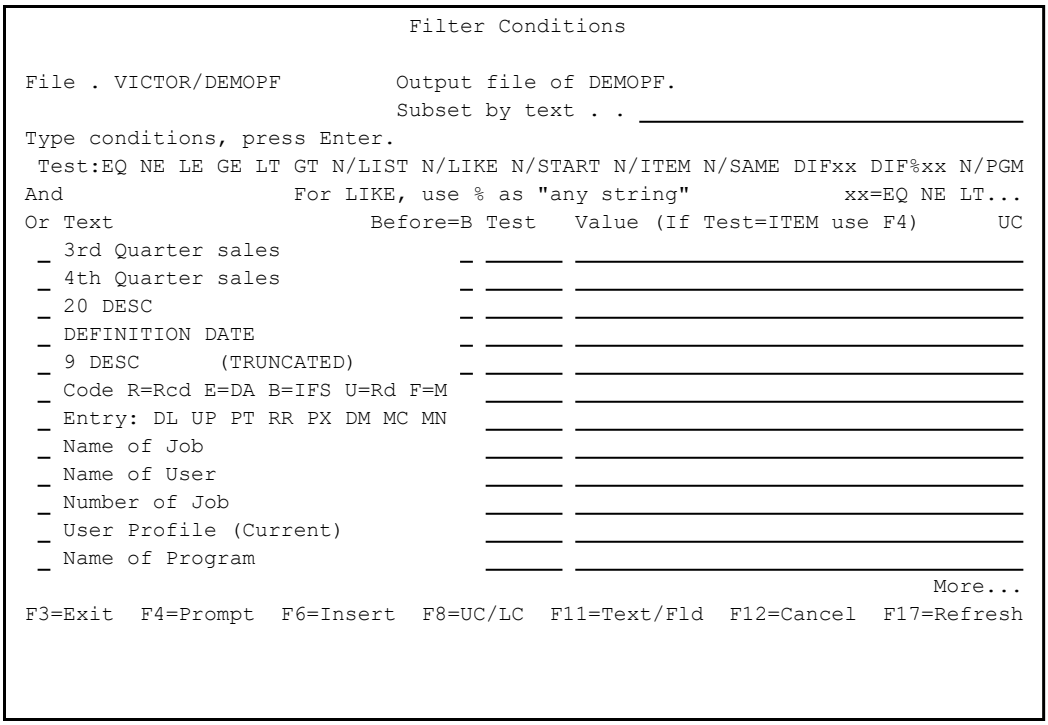
Setting Filter Conditions

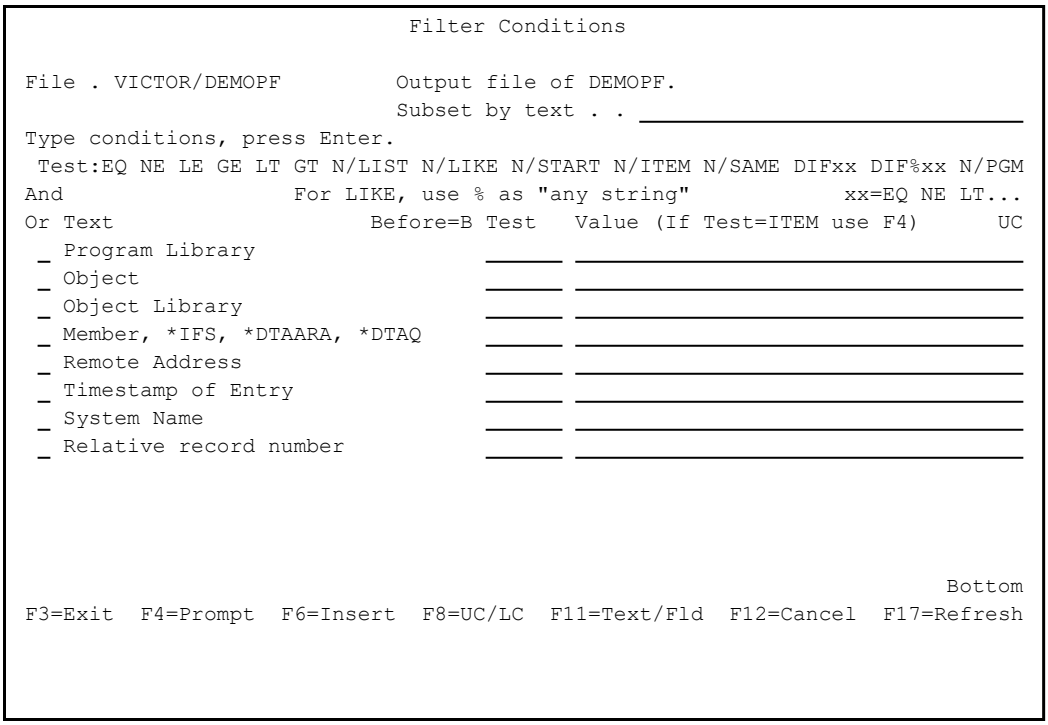
Using the **Filter Conditions** screen, user can combine tests on any number of fields in a record to determine the system's response.



Type **1** in the **Opt** field next to the existing filter condition to change and press **Enter**. The **Filter Conditions** screen appears.







Each line on the body of the screen shows a single test to be done on the record or request being checked. They include four fields:

And/Or

How this test connects to the ones above it, as described below. (This field does not appear on the first line, since no test precedes it.)

Text

The name of the field within the record or request being checked.

Test

How the Field is compared to the Value, using comparators shown below.

Value

The value against which the Field is tested.

This field is case sensitive, unless the **Test** field is set to **LIKE** or **NLIKE**. The two characters shown in a black-on-green field at the right end of the line of field labels about the first line of the body of the screen shows the Caps-Lock state. If the field shows "UC", typed characters are entered as uppercase. If it shows "LC", typed characters are entered as lowercase. To toggle between them, press the F8 key.

Setting the Order of Rules

Tests are run in the order that they appear in the list, from the top down. Tests that you have defined appear at the top of the list. Lines without tests appear below them and are ignored by the filter.

To insert a test above a line showing a defined test, place the cursor on the line containing that test and press the F6 key. The Select Multiple Fields/Conditions for Insert window appears, showing the list of generic fields and fields known to the server. To select the field to test, type **1** in its **Opt** field and press Enter. A line for a test based on the field appears on the Filter Conditions screen above the line on which you had placed the cursor.

To **insert a test after the last defined test**, place the cursor on a line below that test and press the **F6** key. The **Select Multiple Fields** window appears, showing the list of generic fields and fields known to the server. To select the field to test, type **1** in its **Opt** field and press **Enter**. The window closes and a line for a test based on the field appears on the **Filter Conditions** screen below the last of the defined tests.

To **delete a test**, clear the Test and Value fields from the line showing the test. The line is removed when the screen refreshes.

To **move a test**, insert an identical test in the new position then clear the original test.

Test Comparison Operators

The **Test** field can be set to the following values:

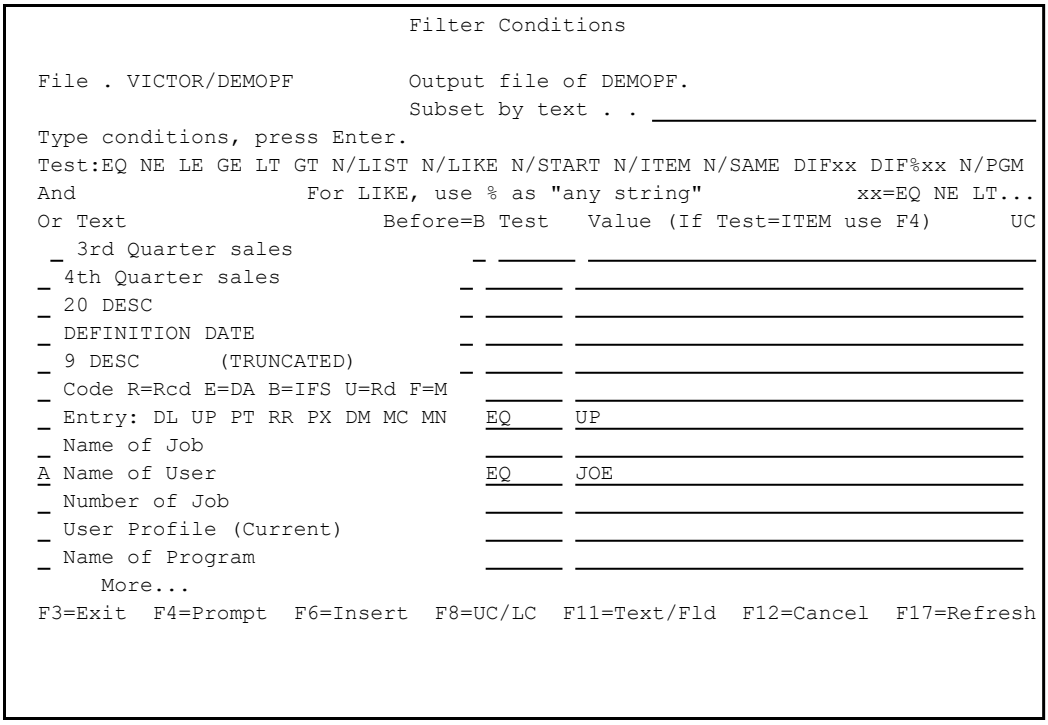
- **EQ**: **Equal to**. The field contents are identical to those of the **Value** field.
- **NE**: **Not equal to**. The field contents are not identical to those of the **Value** field.
- **LT**: **Less than**. The field contents are less than those of the **Value** field. To select all instances in which a field is empty, use the **LT** operator, and set the **Value** operator to "**.**" (a single dot).
- **LE**: **Less than or equal to**. The field contents are less than or equal to those of the **Value** field.
- **GT**: **Greater than**. The field contents are greater than those of the **Value** field.
- **GE**: **Greater than or equal to**. The field contents are greater than or equal to those of the **Value** field. To select all instances in which a field is not empty, use the **GE** operator, and set the **Value** operator to "**.**" (a single dot).
- **LIST**: **Included in list**. The field contents are included in a space-separated list in the **Value** field. For example, "BLUE" is included in the list "RED BLUE GREEN". (**LIST** is not effective if you might be checking values that contain spaces, such as "NEW YORK" or "VAN HALEN". To check those, either create a group to be used with **ITEM** or combine a set of **EQ** tests.)

- **NLIST**: Not included in list. The field contents are not included in a space-separated list in the **Value** field. For example, "YELLOW" is not included in the list "RED BLUE GREEN". (Like **LIST**, **NLIST** is not effective if you might be checking values that contain spaces.)
- **LIKE**: Matches a substring search. The field contents match the string in the Value field. The "%" character can be used as a wild card in the **Value** field. For example, if the field contents consists of the string "PURPLE", it would be **LIKE** the **Value** field string "%URP%".
- **NLIKE**: Does not match a substring search. The field contents do not match the string in the **Value** field. The "%" character can be used as a wild card in the **Value** field. For example, if the field contents consists of the string "ORANGE", it would be **NLIKE** the **Value** field string "%URP%".
- **ITEM**: True if the value of the **Field** field is a member of a group named in the **Value** field. After entering **ITEM** in the **Test** field, place the cursor in the Value field and press the F4 key. The Select Subject window appears, containing a list of groups known to the system. To select a group from this list, type **1** in the **Opt** field for that group and press the Enter key. To work with the groups, including editing or removing them, press the F6 key.
- **NITEM**: True if the value of the **Field** field is not a member of a group named in the **Value** field. You can select a group from a list as shown for the **ITEM** operator.
- **START**: True if the value of the **Field** field begins with the characters in the **Value** field.
- **NSTART**: True if the value of the **Field** field does not begin with the characters in the **Value** field.
- **PGM**:True if a specific user program, run against the **Field** contents, returns a value of True. Indicate the program in the **Value** field as "LIBRARY/PROGRAM".
- **NPGM**: True if a specific user program, run against the **Field** contents, returns a value of False. Indicate the program in the **Value** field as "LIBRARY/PROGRAM".

Combining Tests with the And/Or Field

By default, consecutive tests on the screen are combined. The result is True only if the result of each of the tests is True.

If the line for a test contains the letter "**O**" (for "Or") in its **And/Or** field, it causes the filter to consider the tests included on the screen as two distinct groups. If either the group of tests before the line with the "**O**" or the group of tests beginning with and following that line are all True, the result is True.



In this example the filter conditions are true if the Entry is UP and the Name of User is JOE.

NOTE: AND has precedence over OR, as shown in IBM documentation at https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.f54dg00/ispdg170.htm

To **filter by fields in one of the files**, type **1** in the **Opt** field for that file and press **Enter**. The **Filter Conditions** screen appears.

Actions

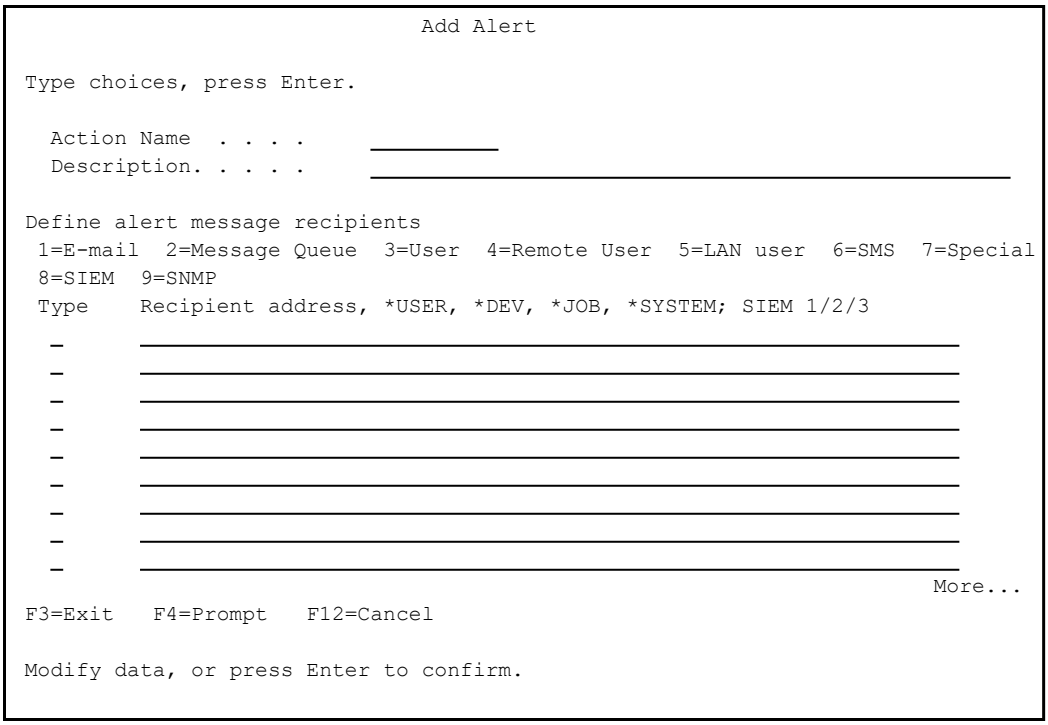
This section discusses the steps necessary to define the actions that are triggered by a rule. Actions can consist of alert messages and/or command scripts that perform one or more specific activities.

To **work with actions**, select **`31. Actions`** from the main screen (*STRJR*).
The **Work with Actions** screen appears.

```
                          Work with Actions
                                                    Position to:  _________
Type options, press Enter.
  1=Select   3=Copy   4=Delete   7=Rename   8=Where used

Opt Action        Description
 _  ALERT01       Alert via EMail - SMS - User
 _  ALEX122148    Created by Action
 _  ALEX140856    Created by Action
 _  ALEX174143    Created by Action
 _  ALEX195321    Created by Action
 _  GS212548QP    Created by Action
 _  JR085909QP    Created by Action
 _  TEST          test
 _  TZIO124013    Created by Action
 _  TZIO143541    Created by Action
 _  VICT134148    Created by Action
 _  VICT150248    Created by Action
 _  VICT164050    Created by Action
 _  VICT165231    Created by Action
                                                                   More...
F3=Exit    F6=Add new               F12=Cancel
```

NOTE: The **Work with Actions** screen is also accessible from the **Reporting, Scheduler etc.** screen (*STRJR > 12*).

To **add a new alert**, press **F6** from the **Work with Actions** screen. The **Add Alert** screen appears.



Action Name

Enter a meaningful name for the Action

Description

Enter a free text description of the Action

Type

Recipient type:

1 = E-mail message

2= Message to message queue

3= Message to user

4= Message to remote user

5= Message to LAN user

6= SMS

7= Special

8= SIEM

9= SNMP

Recipient address, *USER, *DEV, *JOB, *SYSTEM; SIEM 1/2/3

Recipient address formatted according to message type:

1 - E-mail address in standard e-mail format (recipient@address)

2 - Fully qualified name of the message queue or *SYSOPR

3 - User profile or IBM i (OS/400) group profile

4 - User profile & SNA address separated by space (for example, USER SYSTEM)

5 - Valid network username or *DOMAIN for all users on your domain

6 - Phone number including country code and area code as necessary

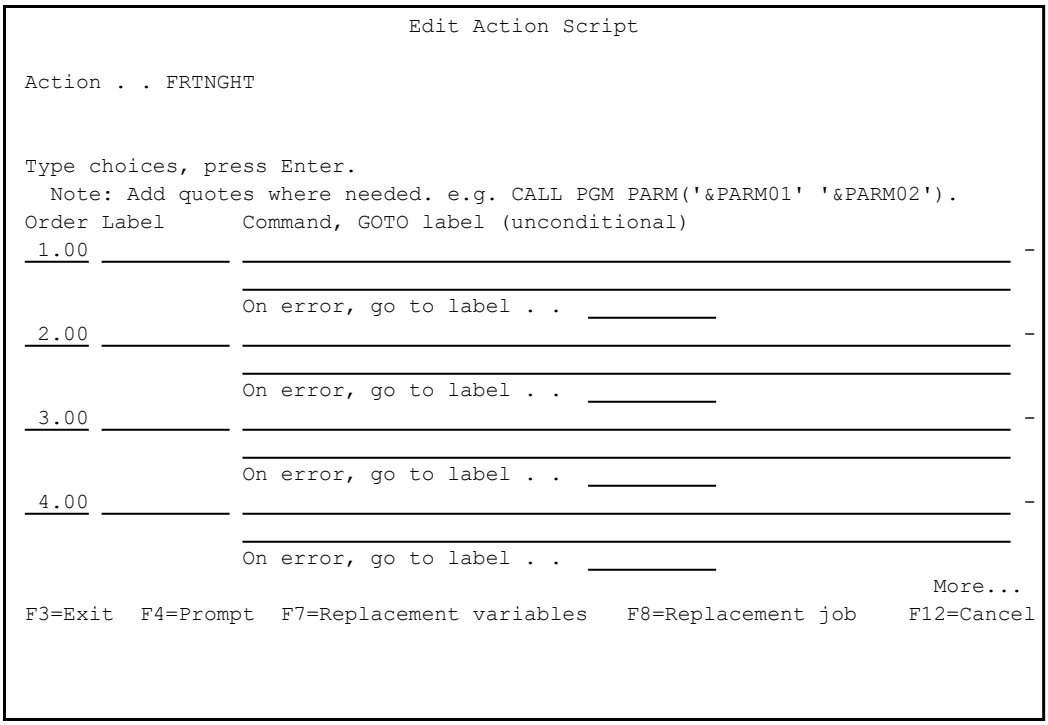
7 - Phone number and access codes for the pager service

8 - E-Mail Address in kind of type 1

*USER in kind of types 1-5

9 - Leave blank; the SNMP message will be sent according to the definitions in option **22. SNMP Definitions** in the System Configuration menu.

Type choices and press Enter. The Edit Action Script screen appears.



Order

Specify the order of the commands here.

Label

Use, if necessary, a label name for jumping to in case of errors.

Command

Type in the command that should be called. Use **F4** to prompt the command and **F7**/**F8** to replace variables.

On error, go to label

Specify here the label name that is used for go to in case of errors.

Define one or more command scripts to be run and press **Enter** to confirm.

Groups and Items

Define assorted groups of reports in line with your requirements, to schedule a particular group of reports to run as one unit sometime in the future.

The %GROUP is used for defining a group of user-profiles that all share the same authorities.

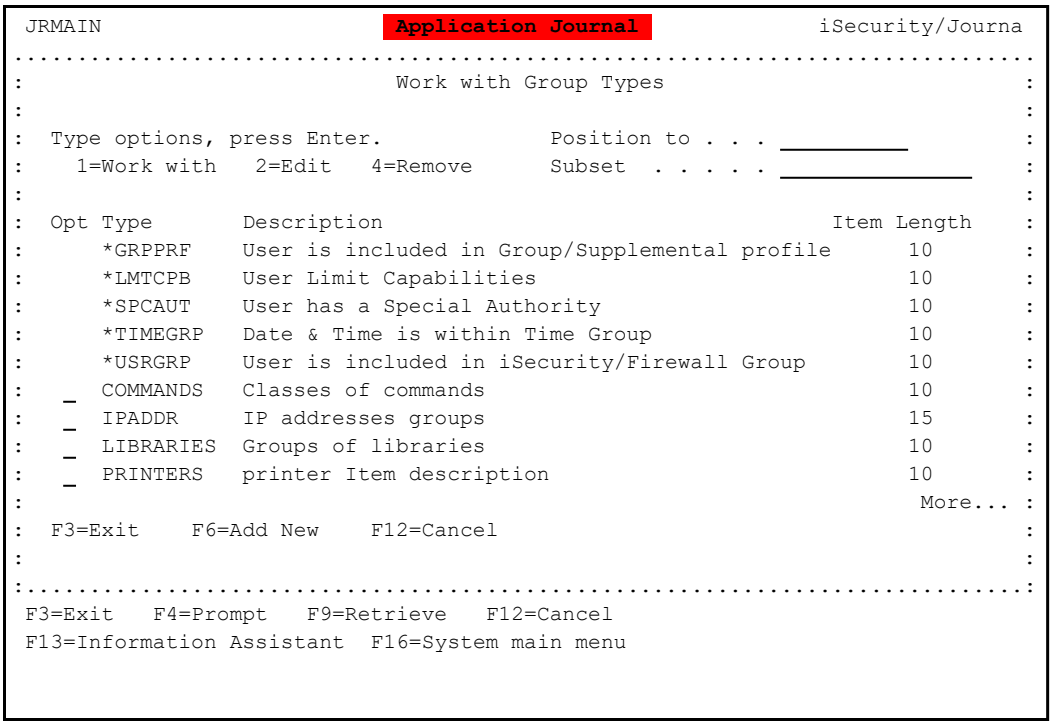
This solution enables defining GROUPS by GROUP-TYPES. These GROUP-TYPES can be any system entity such as files, libraries, applications, identification numbers, and so on.

For each GROUP-TYPE, you can define an unlimited number of GROUPS and within the GROUPS, any number of items can be defined. For example, you can define all identification numbers of the PCs in the organization as one group in the GROUP-TYPE defined as MACHINE_ADDRESS. Another group in MACHINE_ADDRESS may contain all the identification numbers of the PCs in a sister organization.

In all comparison tables, for defining rules, for generating and selecting queries, or for defining the items in reports, the ITEM GROUP-TYPE/GROUP syntax can be used to include only those transactions which contain the GROUP-TYPE/GROUP specified. Like- wise, NITEM GROUP-TYPE/GROUP can be used to include only those transactions which do not contain the GROUP-TYPE/GROUP defined.

In addition, there are special GROUPS available to you, such as groups of users already defined on the system, all of which have a common identifying characteristic. For example, the group profile of the system, group profiles defined in Firewall, and virtual groups of users named *SECADM, *SAVESYS and so on, which are the users who have this particular privilege defined in their special authority.

To work with group types, select **`35. Groups and Items`** from the main menu (*STRJR*). The Work with Group Types screen appears:



NOTE: Predefined groups are started with *****. You can use these groups for nearly unlimited filtering.

***GRPPRF**

Use this group to filter users belonging to a group or supplementary group profiles.

***LMTCPB**

Use this group to filter users depending on the ability to access the command line.

***SPCAUT**

Use this group to filter users depending on the special authorities of a user.

***TIMEGRP**

Use this group to filter date and time within the Time Group.

***USRGRP**

Use this group to filter users depending on the user group of Firewall where the user is included.

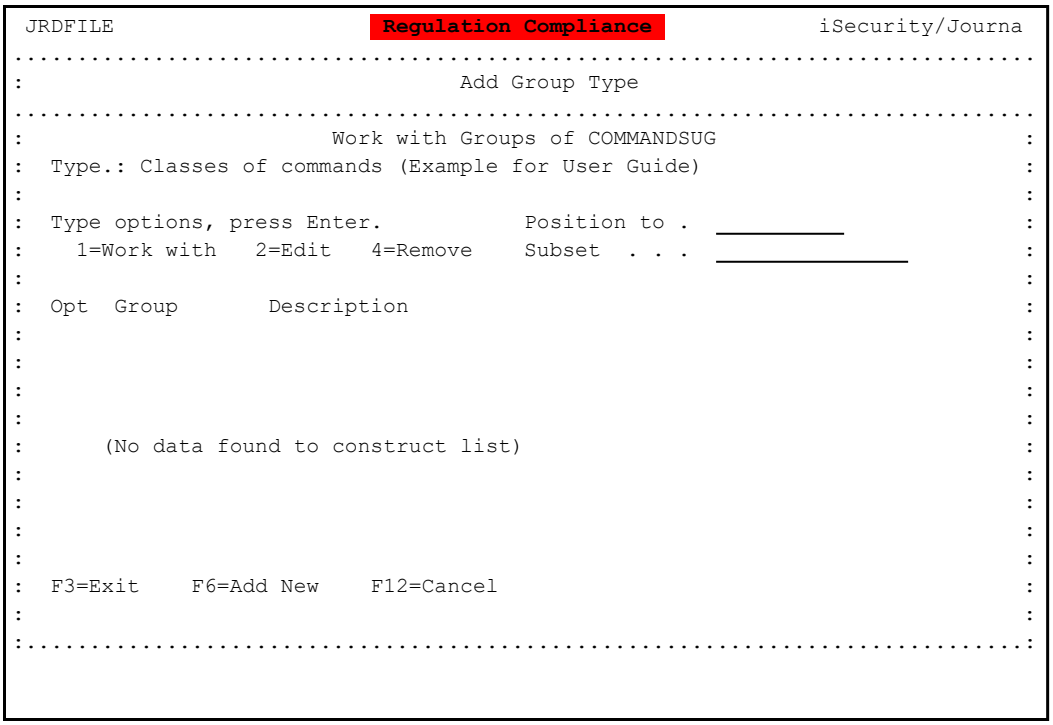
NOTE: Since the grouping options are nearly unlimited, you can specify all types of groups you need based on IP addresses, job names, JOBQ names, libraries, programs, system values, and more.

NOTE: The Work with Group Types screen is also accessible from other screens, e.g., the **Regulation Compliance** screen (*STRJR > 1*), **Business Analysis** screen (*STRJR > 2*).

To **add a new group type**, press **F6** from the **Work with Group Types** screen. The **Add Group Type** screen appears. Define Group type, Text and Maximum item lenght. The following example has been filled in for a group of classes of commands.

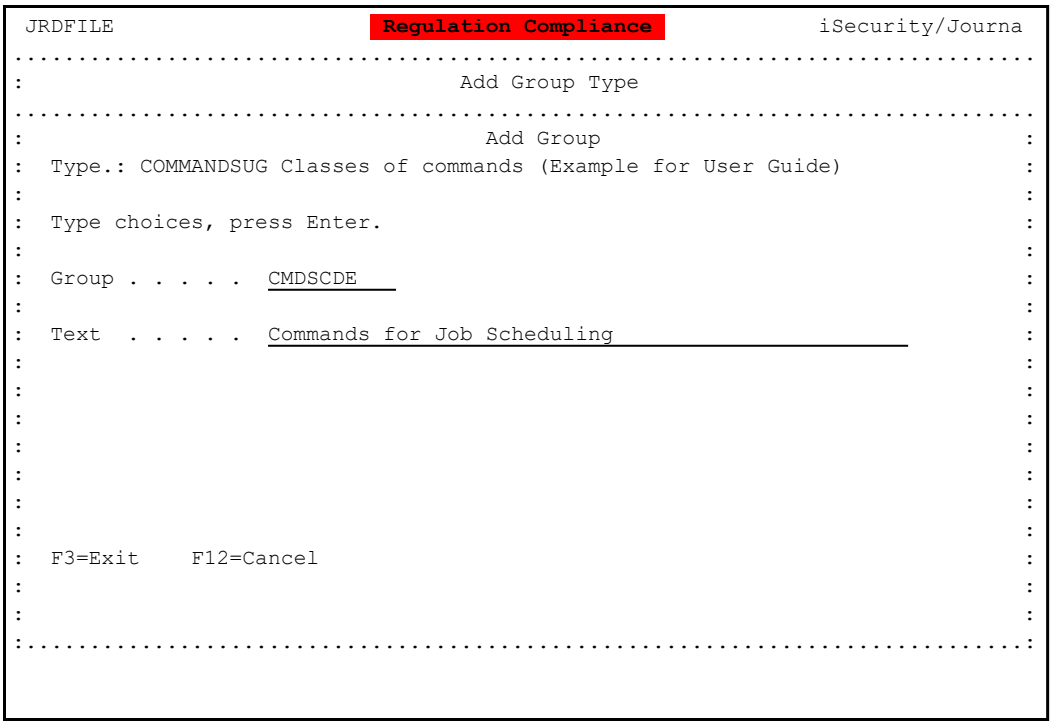
```
 JRDFILE                      Regulation Compliance              iSecurity/Journa
.....................................................................................
:                                  Add Group Type                                   :
:                                                                                   :
:  Type choices, press Enter.                                                       :
:                                                                                   :
:    Group type. . . . . .  COMMANDSUG                                              :
:                                                                                   :
:    Text  . . . . . . . .  Classes of commands (Example for User Guide)            :
:                                                                                   :
:    Maximum item length .  20                        1 - 20                        :
:                                                                                   :
:                                                                                   :
:                                                                                   :
:                                                                                   :
:                                                                                   :
:                                                                                   :
:                                                                                   :
:  F3=Exit                 F12=Cancel                                               :
:                                                                                   :
:...................................................................................:
 F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
 F13=Information Assistant  F16=System main menu
```

Press **Enter**. The **Work with Groups of** [Name of the Group] screen appears.

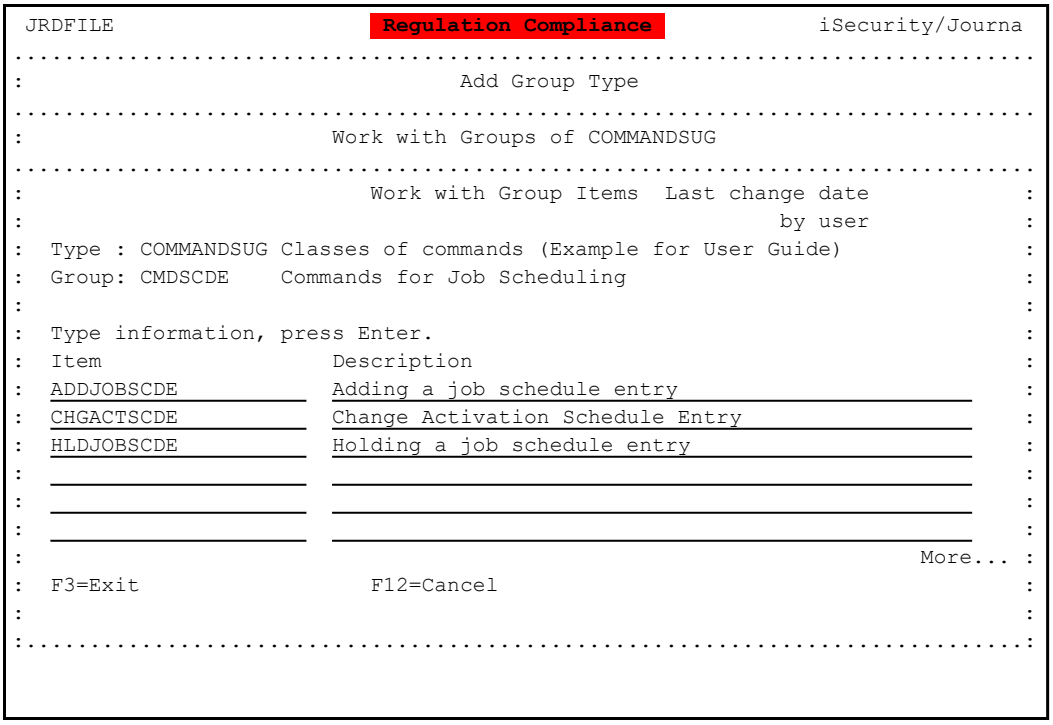


Press **F6** to add a new group. The **Add Group** screen appears.

Define **Group** and **Text**. The following example has been filled in for a group of commands for Job Scheduling.



Press **Enter**. A new group appears on the **Work with Groups of** [Name of the Group] screen. Type **1** in the **Opt** field to work with group items. The **Work with Group Items** screen appears. Define **Item** and **Description**. The following example has been filled in for a group of commands for Job Scheduling.



Press **Enter**.

To **modify items in the existing group**, type **1** in the **Opt** field. **Work with Groups of** [Name of the Group] screen appears.

To work with items and their descriptions within the group, type option **1=Work with** in the **Opt** field.

To edit the group name and its description, type option **2=Edit** in the **Opt** field.

To remove the group, type option **4=Edit** in the **Opt** field.

Time Groups

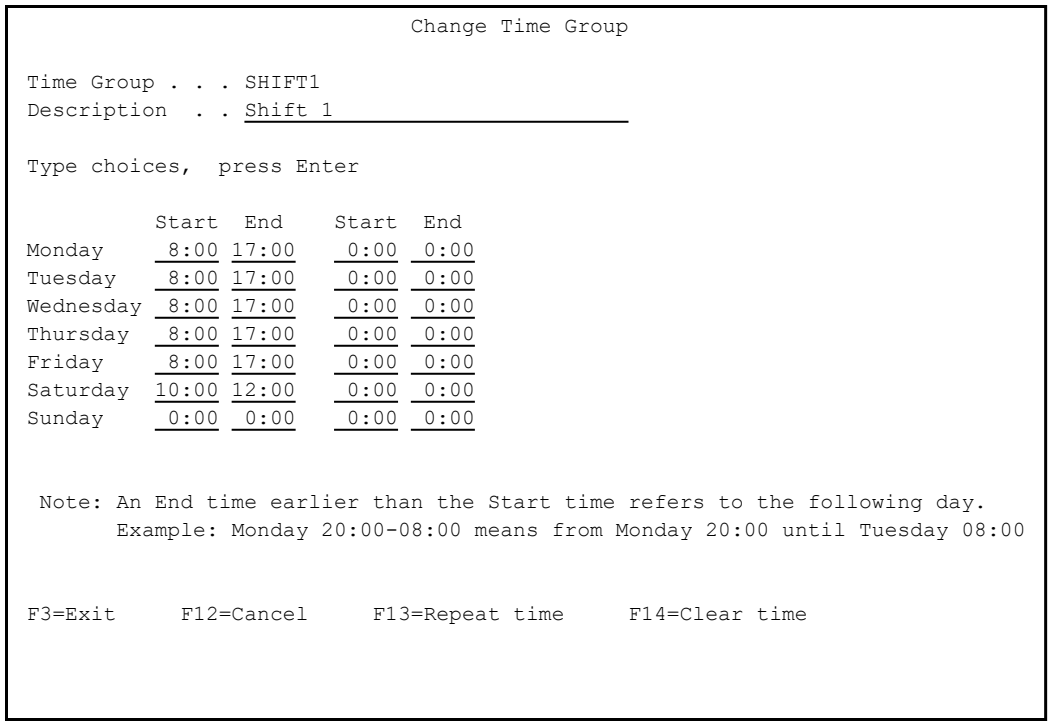
Time groups are user-defined sets of time and day of the week parameters that you can use as filter criteria for queries and reports. Time group filters can be either:

- Inclusive - Include activities that occur only during the time group periods
- Exclusive - Exclude all activities that occur during the time group periods.

To **define a time group**, select **`36. Time Groups`** from the main menu (*STRJR*). The **Define Time Groups** screen appears.

```
                              Define Time Groups

Type options, press Enter.
  1=Select    4=Delete

Opt Time Group    Description
 _  SHIFT1        Shift 1
 _  WORKHOURS     Regular work hours

                                                                      Bottom
F3=Exit    F6=Add new    F8=Print list    F12=Cancel
```

Press **F6** to create a new time group or type **1** in the **`Opt`** field to select an existing time group to modify it.



Time Group

Enter a meaningful name for the Time Group. This field is mandatory.

Description

Enter a meaningful description of the Time Group.

Start and End

For each relevant day of the week, enter Start and End Times in the format HH:MM, using the 24-hour clock. Midnight is 00:00.

NOTE: An End time earlier than the Start time refers to the following day. For example, Monday 20:00-08:00 means from Monday 20:00 until Tuesday 08:00.

F13

Copies the starting and ending times from the cursor line to all subsequent lines

F14

Erases the starting and ending lines from the cursor line and below

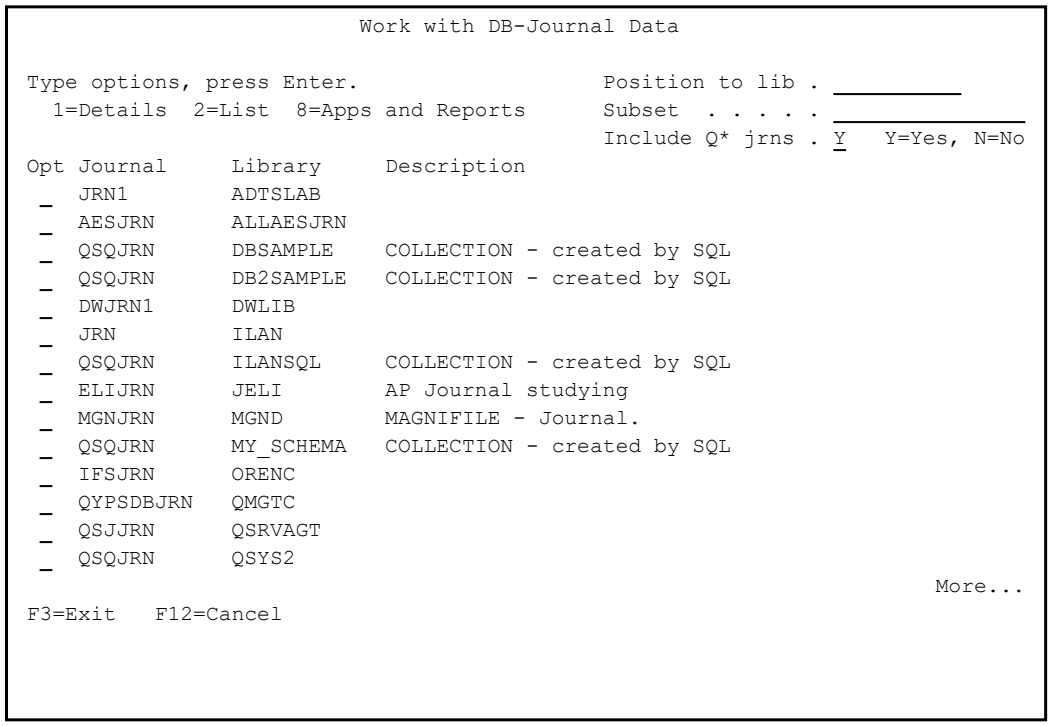
Type choices and press **Enter**.

NOTE: The **Define Time Groups** screen is also accessible from **Reporting, Scheduler etc.** screen (*STRJR > 12*).

Reviewing Database Changes

You can see all the journals that exist on your organization's computers, work with the journals of a specific database and you can also check the changes performed on a specific file.

To **work with database journals**, select **`51. Work with DB-Journals`** from the Application Journal main menu (*STRJR*). The **Work with DB-Journal Data** screen appears.



```
                          Work with DB-Journal Data

Type options, press Enter.                    Position to lib . _________
  1=Details  2=List  8=Apps and Reports       Subset  . . . . . _________
                                              Include Q* jrns . Y   Y=Yes, N=No
Opt Journal     Library     Description
 _  JRN1        ADTSLAB
 _  AESJRN      ALLAESJRN
 _  QSQJRN      DBSAMPLE    COLLECTION - created by SQL
 _  QSQJRN      DB2SAMPLE   COLLECTION - created by SQL
 _  DWJRN1      DWLIB
 _  JRN         ILAN
 _  QSQJRN      ILANSQL     COLLECTION - created by SQL
 _  ELIJRN      JELI        AP Journal studying
 _  MGNJRN      MGND        MAGNIFILE - Journal.
 _  QSQJRN      MY_SCHEMA   COLLECTION - created by SQL
 _  IFSJRN      ORENC
 _  QYPSDBJRN   QMGTC
 _  QSJJRN      QSRVAGT
 _  QSQJRN      QSYS2
                                                                      More...
F3=Exit   F12=Cancel
```

`1=Details`

Type **1** in the **`Opt`** field to display the journal details. The **Display APP Current Journal (DSPAPCRJ)** screen appears. Type choices and press **Enter**.

`2=List`

Type **2** in the **`Opt`** field to list the journal details. The **Display APP Current Journal (DSPAPCRJ)** screen appears. Type choices and press **Enter**.

8=Apps and Reports

Type 8 in the **Opt** field to work with applications and reports. The Applications and Reports for Journal screen appears. Type choices and press Enter.

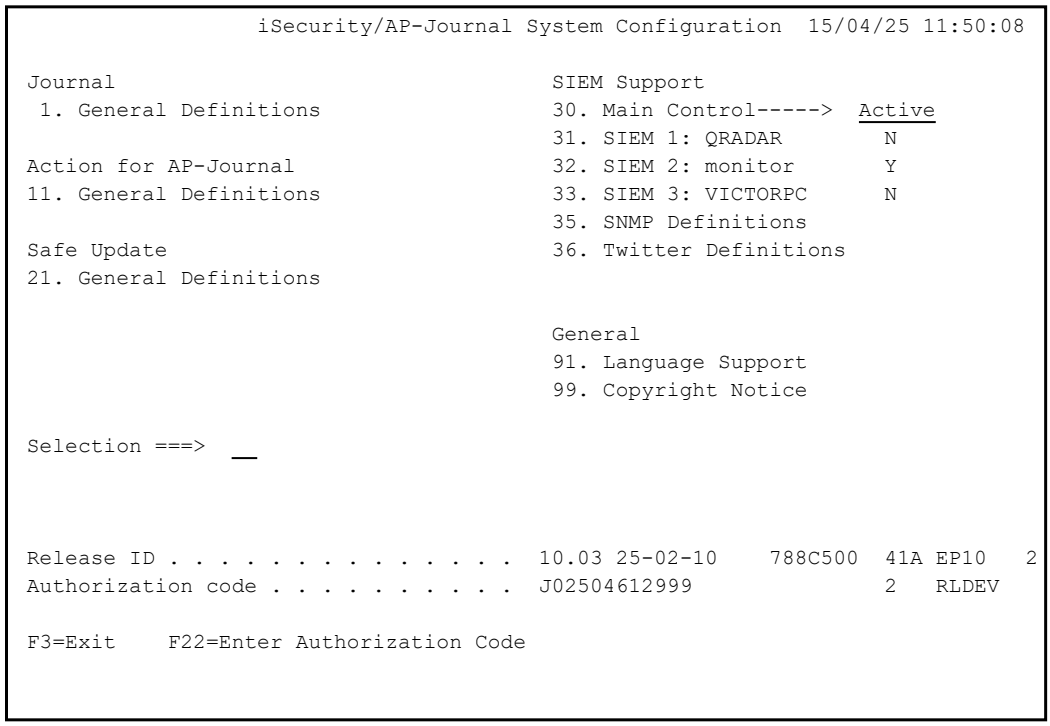
To display the list of changes, select **52. Display File Journal-List Journals** from the main menu (*STRJR*). The Display File Journal (DSPDBJRN) screen appears with the predefined **Display format** field to *LIST. Type choices and press Enter. The Display Journal Entries screen appears.

To display changes details, select **53. Display File Journal-Details** from the main menu (*STRJR*). The Display File Journal (DSPDBJRN) screen appears with the predefined **Display format** field to *DETAIL. Type choices and press Enter. The Display Database Updates screen appears.

Configuration and Maintenance

The system configuration option presents general definitions relating to marking the changed field, SMS and E-mail definitions, SEM definitions, and language support.

To **work with system configuration**, select **81. System Configuration** from the main menu (*STRJR*). The **iSecurity/AP-Journal System Configuration** screen appears.



To **enter the authorization code**, press **F22**.

To **define the general preferences of the file appearance**, select **1. General Definitions** from the **iSecurity/AP-Journal System Configuration** screen (*STRJR > 81*). The **Define Journal global defaults** screen appears as shown in "Journal General Definitions" on page 130.

To **define the action general definition**, select **11. General Definitions** from the **iSecurity/AP-Journal System Configuration** screen. The **Action General Definitions**

screen appears as shown in "Action Definitions" on page 131.

To **define SIEM Support**, select as appropriate, as shown in "SIEM Support" on page 132

To **work with Language Support**, select **91. Language Support** from the **iSecurity/AP-Journal System Configuration** screen (*STRJR > 81*). The **Journal Language Definitions** screen appears as shown in "Language Support" on page 135.

The **Maintenance Menu** enables you to set and display global definitions for **AP-Journal**.

To **access the Maintenance Menu**, select **82. Maintenance Menu** from the main menu (*STRJR*). The **Maintenance Menu** screen appears.

```
JRMINTM                          Maintenance Menu                iSecurity/Journal
                                                                 System:  RLDEV
Select one of the following:

Global                                   Trace Definition Modifications
 1. Export Definitions                   71. Add Journal
 2. Import Definitions                   72. Remove Journal
 3. Delete Statistics Data               78. Real-Time Definition Change Alerts
                                         79. Display Journal
Journal Specific
21. Set *CSV Output Fields Order
25. Faster Access to Existing Data




                                         Uninstall
                                         98. Uninstall

Selection or command
===> ____________________________________________________________________________

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

To **export definitions**, select **1. Export Definitions** from the **Maintenance Menu** screen (*STRJR > 82*). The **Export iSecurity/Part 4 Defns. (EXPS4DFN)** screen appears as shown in "Export Definitions" on page 136.

To **import definitions**, select **2. Import Definitions** from the **Maintenance Menu** screen (*STRJR > 82*). The **Import**

iSecurity/Part 4 Defns. (IMPS4DFN) screen appears as shown in "Import Definitions" on page 138.

To delete statistics data, select **3. Delete Statistics Data** from the Maintenance Menu screen (*STRJR > 82*). The Delete AP-Journal Statistic (DLTJRSTT) screen appears as shown in "Delete Statistics Data" on page 139.

To customize the *CSV output by re-ordering fields, removing fields, and changing column headings, select **21. Set *CSV Output Fields Order** from the Maintenance Menu screen (*STRJR > 82*) . The SEU Edit screen appears showing the SMZJDTA/JRSOURCE JRCSV member as shown in "Customize *CSV Output Fields" on page 140.

To work faster for applications generated before **AP-Journal Release 9.12**, select **25. Faster Access to Existing Data** from the Maintenance Menu screen (*STRJR > 82*). The Faster Access To Application Data screen appears.

To add a journal, select **71. Add Journal** from the Maintenance Menu screen (*STRJR > 82*). The Create Journal - Confirmation pop-up window appears. When you are ready to start journaling, press Enter.

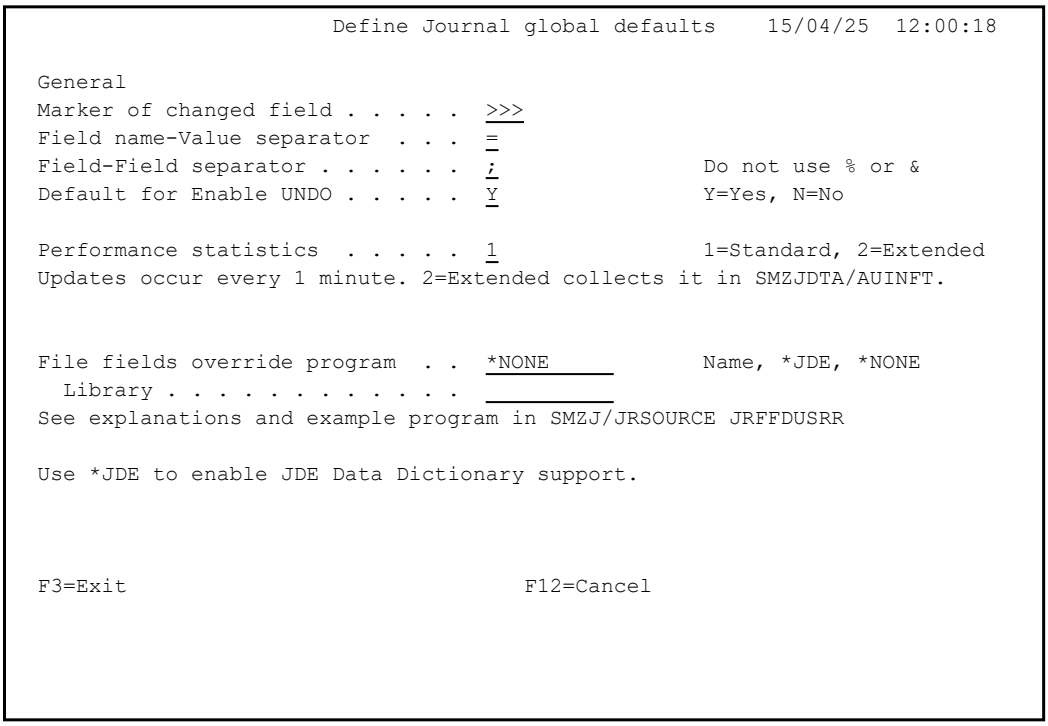
To remove the journal, select **72. Remove Journal** from the Maintenance Menu screen (*STRJR > 82*). The End Journal - Confirmation pop-up window appears. When you are ready to end journaling, press Enter.

To display the journal, select **79. Display Journal** from the Maintenance Menu screen (*STRJR > 82*). The Display APP Current Journal (DSPAPCRJ) screen appears. Type choices and press Enter. When you are ready to end journaling, press Enter. The Display Journal Entries screen appears.

To **uninstall the product**, select **98. Uninstall** from the **Maintenance Menu** screen (*STRJR > 82*). The **Uninstall SECURITY4P** screen appears.

Journal General Definitions

To **define the general preferences of the file appearance**, select **1. General Definitions** from the **iSecurity/AP-Journal System Configuration** screen (*STRJR > 81*). The **Define Journal global defaults** screen appears.



Marker of changed field

The character you want to use to indicate changed fields.

Field name-value separator

The character you want to use to separate the field name from its value.

Field-Field separator

Specify a specific character (or leave field empty).

Default for Enable UNDO

An option to undo changes in database files using the journal.

Y = Yes, UNDO enabled by default

N = No, UNDO not enabled by default.

Performance statistics

The updates occur every 60 seconds. Extended performances are collected in SMZJDTA/AUINFT.

File fields override program and library

You can use a program to replace the TEXT of the fields or even provide a non-DDS record structure. An example program source is available at SMZJ/JRSOURCE JRFFDUSRR.

If you want to enable JDE Data Dictionary support, enter *JDE

Type choices and press **Enter**.

Action Definitions

To **define the action general definition**, select **11. General Definitions** from the **iSecurity/AP-Journal System Configuration** screen. The **Action General Definitions** screen appears.

```
                          Action General Definitions         15/04/25 12:24:34

Type options, press Enter.

Log Action activity . . . . . . . . . . Y          N=No, Y=Yes
Use DSPMSG SMZJDTA/JRACTLOG to display activity.

Log CL script commands  . . . . . . . . 1          1=No, 2=Fails, 3=All

Send message only if within . . . . . .  60        Minutes
Run scripts only if within  . . . . . .  60        Minutes
Do not perform actions for events if the time passed since they have
occured, passed the specified limits.









 F3=Exit  F12=Previous
```

Log Action activity

Y = Yes

N = No

Use DSPMSG SMZJDTA/JRACTLOG to display activity.

Log CL script commands

1 = No - do not log any CL script commands

2 = Fails - log only CL script commands that fail

3 = All - log all CL script commands

Send message only if within

To avoid too many actions, you can specify a number of minutes.

Run scripts only if within

To avoid too many scripts, you can specify a number of minutes.

Type options and press Enter.

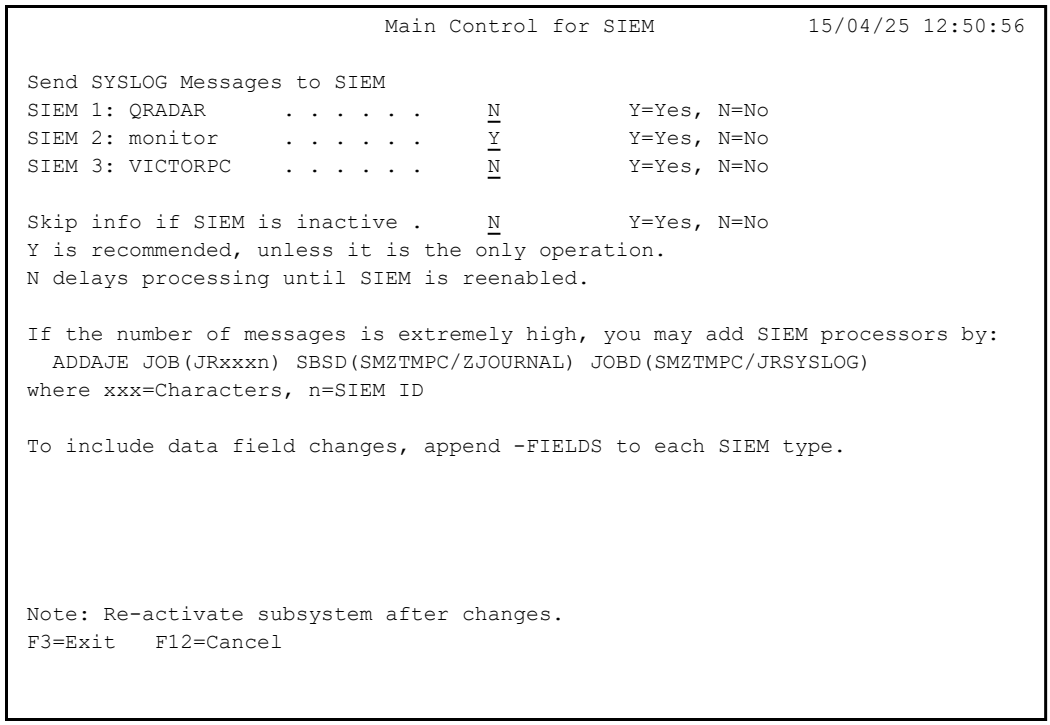
SIEM Support

SIEM can transmit up to 1000 lines per second. Message alerts contain detailed event information about application data changes, deletions or readings of objects and files, emergency changes in user authorities, detection of IFS viruses, malicious network access to the IBM i, and more.

This feature sends events from the IBM i different Audit entry types to a remote SYSLOG server according to a range of severities such as emergencies, alerts, critical, error, warning and more.

If Send SYSLOG messages is set to Yes in the SIEM definitions, the product will automatically send all events according to the Severity range to auto send parameter (list below); the message structure parameter is used to set the format of the message.

Select **30. Main Control** from the iSecurity/BaseSystem Configuration screen (*STRJR > 81*). The Main Control for SIEM screen appears.



Send SYSLOG Messages to SIEM

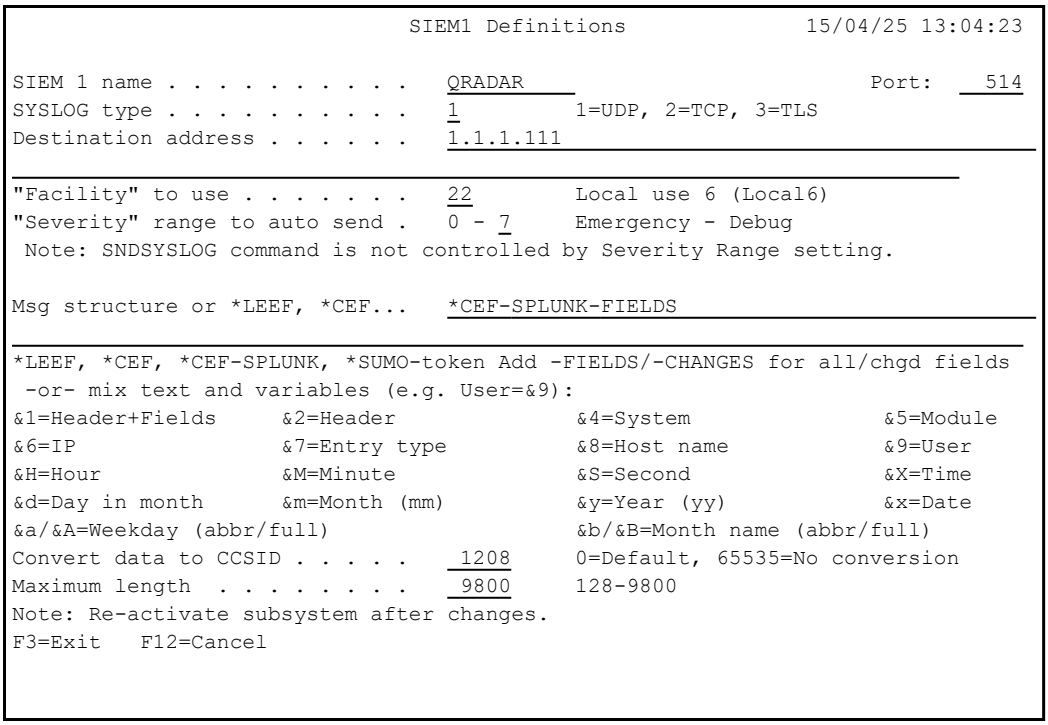
Specify whether the SIEM server is active or not.

Skip info if SIEM is inactive

Y = Yes – Recommended, unless it is the only operation

N = No - Delays processing until SIEM is re-enabled.

To define SIEM definitions, select **31. SIEM 1**, **32. SIEM 2**, **33. SIEM 3** as appropriate from the iSecurity/BaseSystem Configuration screen (*STRJR > 81*). The SIEM Definitions screen appears.



SIEM name

Enter a short name for the SIEM, e.g., SPLUNK, QRADAR, etc.

Syslog type

1 = UDP (send and forget)

2 = TCP (verify receiver before sending, slower)

3 = TLS (verify receiver before sending, encrypted and slower)

Destination address

Enter the IP address of the SIEM server.

Facility to use

Specify the facility based on the SIEM's requirements. For IBM i, it is usually set to "22."

Severity range to auto send

Severities range from 0 (Emergency) to 7 (Debug). Specify which severity levels you want to send to the SIEM.

Msg structure

You can define a pre-existing format or create your own message structure. Predefined formats include *LEEF, *CEF, *CEF-SPLUNK,

and *SUMO-token. You can add more as needed.

Convert data to CCSID

If requested by the SIEM department, specify the desired CCSID.

Maximum length

You can specify the maximum length of a message, which can range from 128 to 9800 characters.

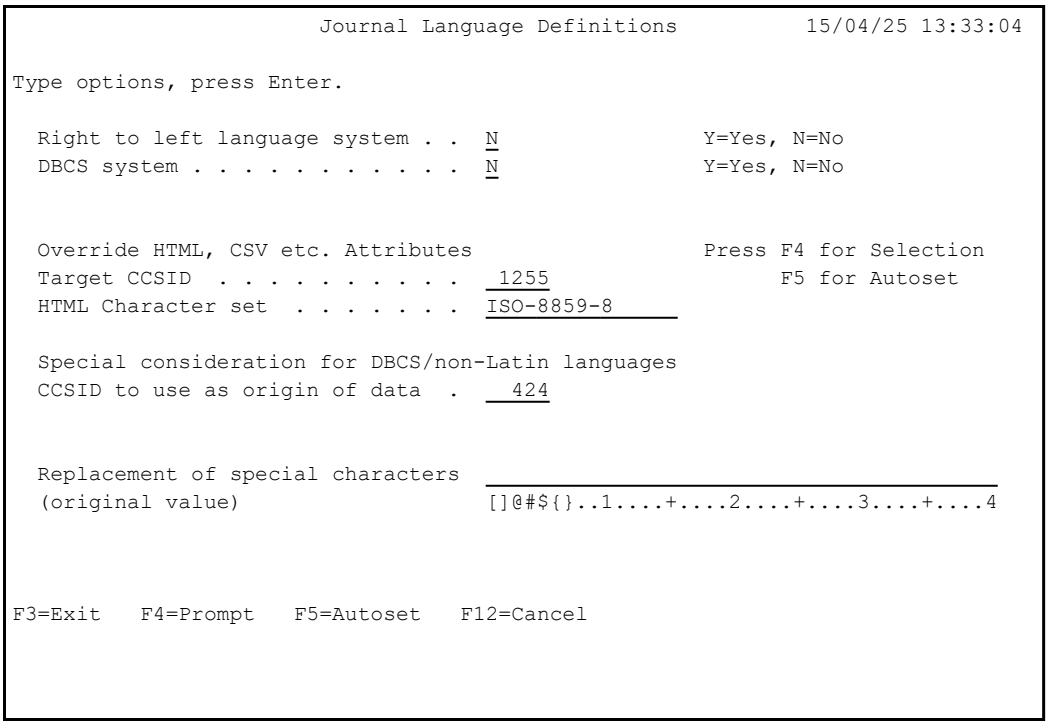
To generate SNMP traps, select **35. SNMP Definitions** from the iSecurity/BaseSystem Configuration screen (*STRJR > 81*). The SNMP Definitions screen appears. Type choices and press Enter.

Language Support

Double-Byte Character Set (DBCS) is a set of characters in which each character is represented by two bytes. These character sets are commonly used by national languages, such as Japanese and Chinese, which have more symbols than can be represented by a single byte.

There are two option: the default setting of 'N' (do not support DBCS), and 'Y' (support DBCS). Choose an option based on the relevant national language.

To work with Language Support, select **91. Language Support** from the iSecurity/AP-Journal System Configuration screen (*STRJR > 81*). The Journal Language Definitions screen appears.

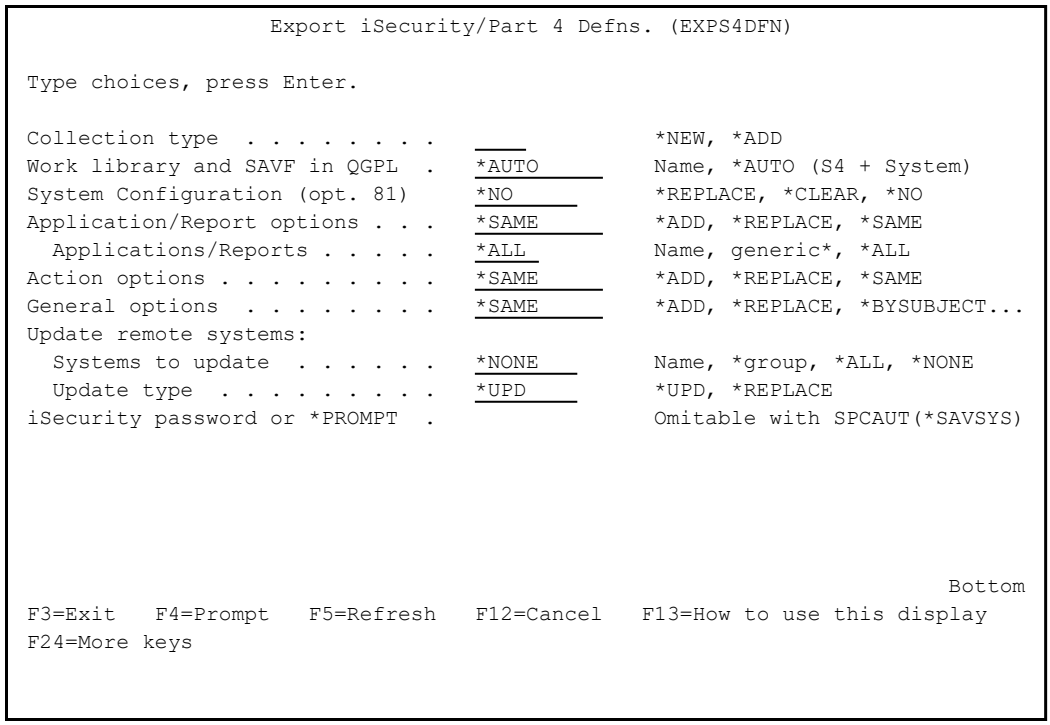


Type choices and press **Enter**.

Export Definitions

Create an SAVF file containing the definitions and settings you want to import:

To **export definitions**, select **`1. Export Definitions`** from the **Maintenance Menu** screen (*STRJR > 82*). The **Export iSecurity/Part 4 Defns. (EXPS4DFN)** screen appears.



Collection type

*NEW = Build a new set of export

*ADD = Add some exported information to the export

Work library and SAVF in QGPL

Specify the name of the save file that contains the export.

*AUTO = S4 + System name

System Configuration

*REPLACE = replaces the previously exported information

*CLEAR = Clears the configuration in the export save file

*NO = Do not export system configuration

Application/Report options

*ADD = add to a previously imported/exported rule

*REPLACE = replace a previously imported/exported rule

*SAME = do not make any changes

Applications/Reports

*ALL = All Applications/Reports

Name = only Application/Reports with this name will be exported

Generic* = all Applications/Reports starting with this will be exported

Action options

*ADD = add to a previously imported/exported rule

*REPLACE = replace a previously imported/exported rule

*SAME = do not make any changes

General options

*ADD = add to a previously imported/exported rule

*REPLACE = replace a previously imported/exported rule

*SAME = do not make any changes

*BYSUBJECT = specify what should be exported

Update remote systems

*NONE = Do not update remote systems

Name = Update specified system

*group = Update all systems in specified group

*ALL = Update all defined systems

Update type

*UPD = Update systems

*REPLACE = Replace configuration on remote systems

iSecurity password or *PROMPT

This parameter can be omitted if SPCAUT (*SAVSYS) is defined.

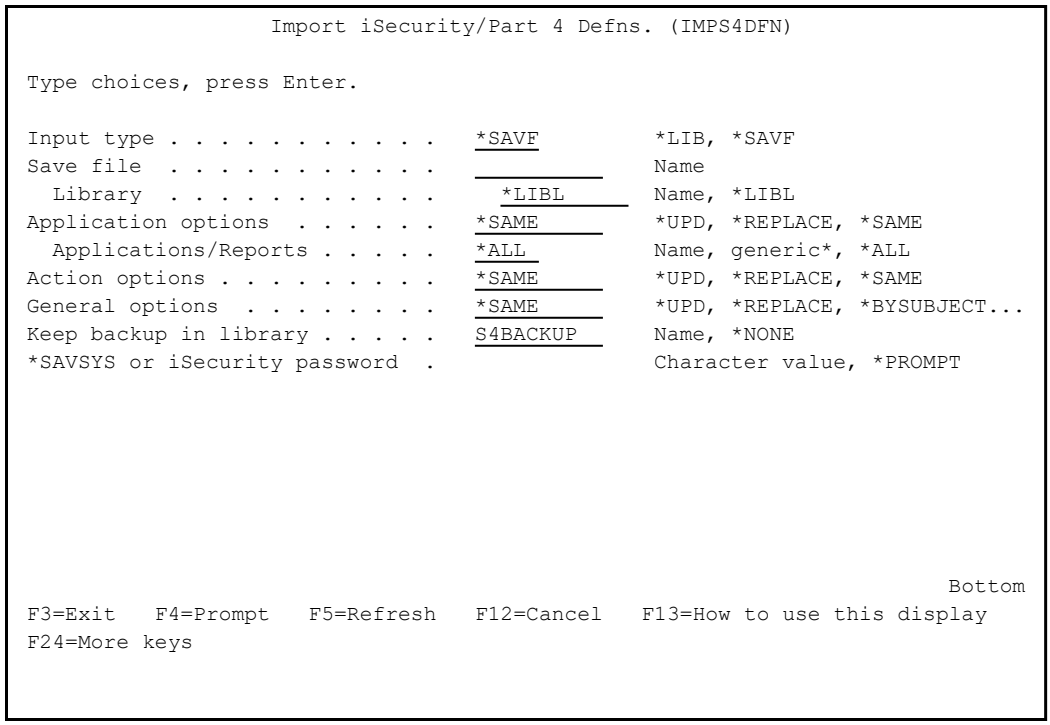
Set your desired parameters and press Enter to confirm.

Type choices and press **Enter**.

Import Definitions

Import the SAVF file containing the exported definitions and settings to another computer or LPAR.

To **import definitions**, select **2. Import Definitions** from the **Maintenance Menu** screen (*STRJR > 82*). The **Import iSecurity/Part 4 Defns. (IMPS4DFN)** screen appears. Define if you want to import from the saved file or the library and press **Enter**. The extended **Import iSecurity/Part 4 Defns. (IMPS4DFN) Defns. (EXPS4DFN)** screen appears.

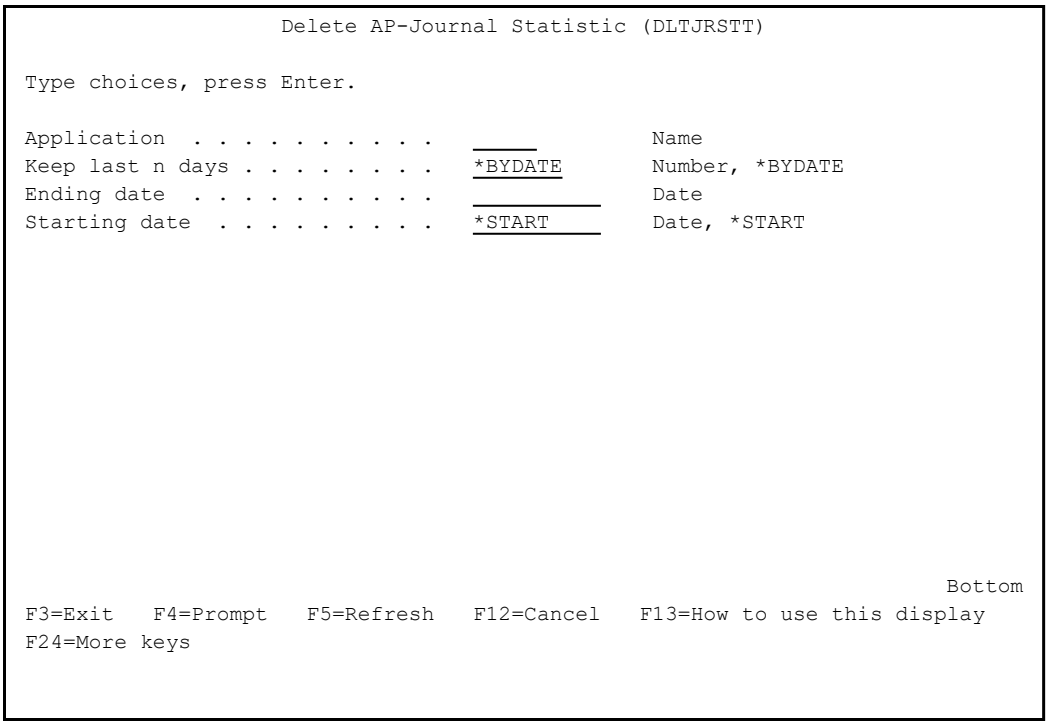


Type choices and press **Enter**.

Delete Statistics Data

You can delete the statistical data used in the GUI version of the product. Before you delete any data, you should ensure that it is backed up and that, if necessary, you have a way to restore all deleted data.

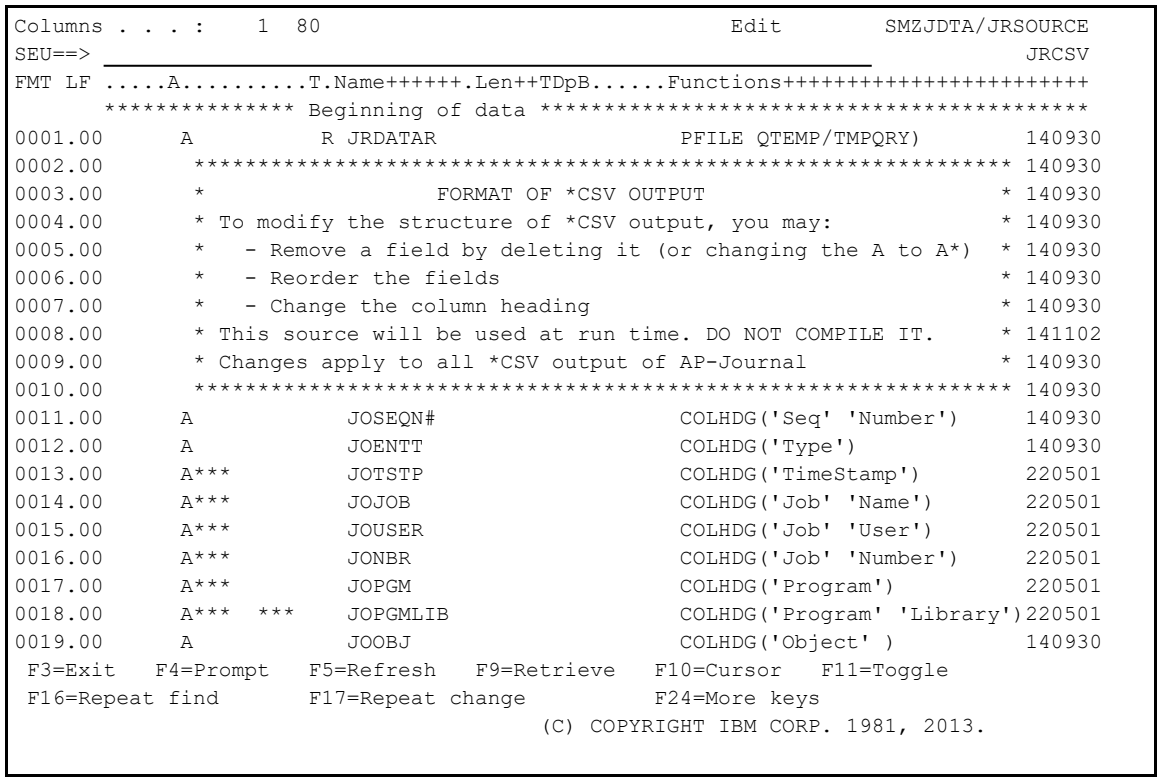
To **delete statistics data**, select **3. Delete Statistics Data** from the **Maintenance Menu** screen (*STRJR > 82*). The **Delete AP-Journal Statistic (DLTJRSTT)** screen appears.



Type choices and press **Enter**.

Customize *CSV Output Fields

To customize the *CSV output by re-ordering fields, removing fields, and changing column headings, select **`21. Set *CSV Output Fields Order`** from the Maintenance Menu screen (*STRJR > 82*) . The **SEU Edit** screen appears showing the SMZJDTA/JRSOURCE JRCSV member.

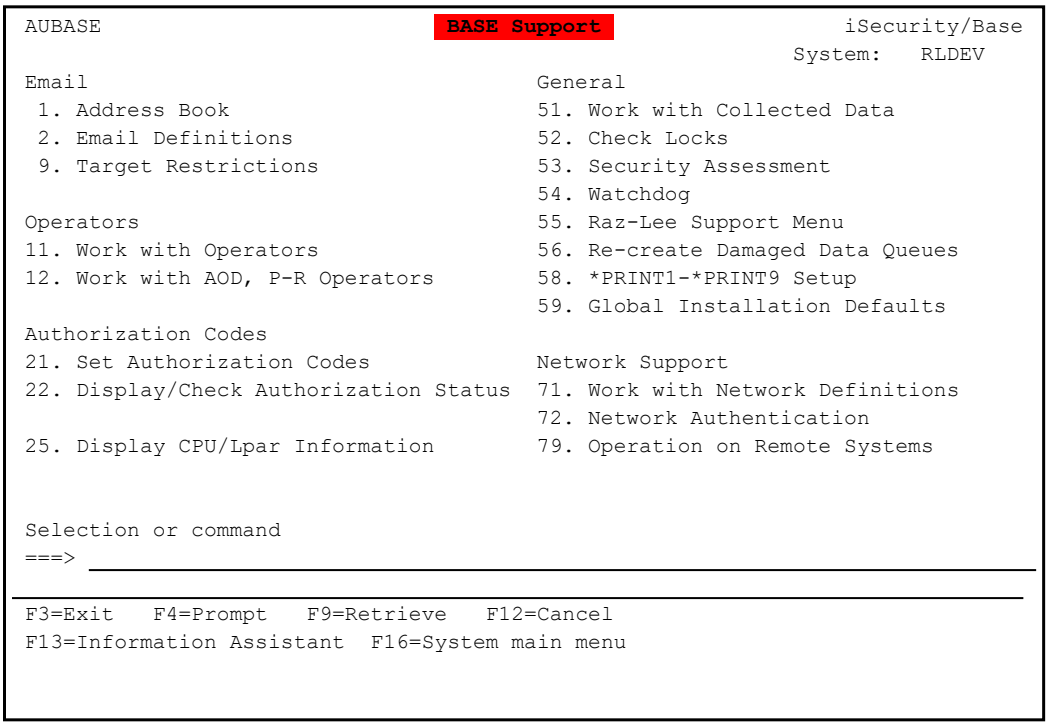


Customize the output by following the instructions within the JRCSV member.

BASE Support

Using the **BASE Support** menu, you can view and modify settings that are common to all modules of iSecurity. This menu, with all its options, is in all iSecurity major modules.

To **access the BASE Support menu**, select **89. BASE Support** in the product's main menu (*SRTJR*> **89**).



For detailed instructions, please refer to the [iSecurity Installation and Base Support.]