iSecurity AP Journal

User Guide
Version 9.1

www.razlee.com

Contents

Contents 2
About this Manual 10
Chapter 1: Introducing AP-Journal 15
Start working with AP-Journal 22
Chapter 2: Working with Single Files 23
Journal Analysis 23
Setting the Order of Rules 31
Test Comparison Operators 31
Combining Tests with the And/Or Field 33
Retrieving Data-Base Journals 35
Work with Classes of Groups 38
Work with Group Items 39
Chapter 3: Analyze Business 40
Business Analysis Menu 40
Work with Reports 41
Add Report 41
Work with Application Files 42
Define Include Filters 43
Filter Conditions 44
Display APP Current Journal 46
Display Journal Entries 49
Display Database Updates 50
Display JR-Receivers Report 51
Display APP Current Journal (DSPAPCRJ) 53
Display Journal Entries 55
Display Database Updates 56
Chapter 4: Work with Business Analysis 58
Applications, BizAlerts - Definitions 58
Creating a new set of files 60
Work with Journaled Applications 60
Modify Application 61

Files to include 65
Work with Application Files 65
Alerts on data (before include filters) 66
Define Alert on Data 66
Work with Business Alert 67
Add Business Alert 68
Alert Conditions 68
Message to send 69
Add Alert 70
Edit Action Script 70
Include Filters 71
Define Include Filters 71
Filter Conditions 72
Alerts on data (after include filters) 73
Define Alert on Data 73
SIEM Support 74
SIEM Support 74
Define Business Items 75
Work with Business Items 76
Add Business Items 76
Identify Business Items in application files 78
Work with Application Objects 78
Select Field with Same Data 78
Configuration 79
Application Configuration 80
Days to keep data on line to 999 and Auto replace container to NO. 81
Work with Journaled Applications 81
Start Real-Time JRN Activities (STRRTJR) 81
Work with Application Containers 83
Display Application Containers 83
Work with Application Authorizations 84
Add New Application Authorization 85
NOTE: 85
Collection to Containers 86
Journal DB Operations 87

Work with File Operations 87
Modify File Operations 88
Output Fields per File 90
Work with File Reporting Specification 90
Add File Reporting Specification 92
Select Output Field 93
Select Fields to Ignore 93
File Structure Modifications 94
Work with File Structure Modifications 94
Add File Structure Modifications 95
Data Conversions 97
Work with Data Conversions 97
Add Conversion 98
Plan Object Journaling 99
Create Plan 100
Work with Object Journaling Plan 100
Add Object Journaling Plan 101
Set Actual as Planned 102
Work with Object Journaling Status 102
Start Journal Physical File 103
Start Journal Object 104
Check Object Journaling 105
Set Journal As Planned 106
Set Journal As Planned 106
Receiver Auto Maintenance 107
Work with Journal Receivers Maintenance 107
Add Journal Receivers Maintenance 108
Building Journals and Receivers 109
21. Work with Journal 110
Chapter 5: Working with Report Scheduler 111
Define Report Schedules 112
Reporting, Scheduler etc. Menu 112
Work with Report Scheduler 113
Add Report Group 113

Define JR Group Details 114
Add Job Schedule Entry 114
Add Report Definition 115
Add Report Definition 116
Run Report Groups 117
Run Report Group 117
Actions 118
Work with Actions 118
Add Alert 119
Edit Action Script 122
Groups and Items 123
Work with Classes of Groups 124
Add Class 124
Work with Groups 125
Time Groups 126
File Journal Lists 129
Display File Journal 129
Chapter 6: Reviewing Database Changes 132
Work with Database Journals 133
Work with DB-Journal Data 133
Journal Details 134
Journal Lists 137
Applications and Reports 138
Applications and Reports for Journal 138
File Journal Details 139
Chapter 7: Configuration and Maintenance 140
System Configuration 140
Journal General Definitions 141
Define Journal global defaults 141
Action Definitions 143
General Definitions 144
Action General Definitions 144
SMSDefinitions 145
SMS Definitions 146

Security Event Management 147
Syslog Definitions 148
Syslog Definitions 149
SNMP Definitions 150
Twitter Definitions 151
Twitter Definitions 151
Language Support 153
Journal Language Definitions 153
Global Definitions 155
Maintenance Menu 155
Export Definitions 156
Export iSecurity/Part 4 Defns. (EXPS4DFN) 156
Import Definitions 159
Import iSecurity/Part 4 Defns. (IMPS4DFN) 159
Delete Statistics Data 160
Journal Specific Maintenance 161
Customize *CSV Output Fields 162
Trace Definition Modifications 163
Add Journal 164
Create Journal - Confirmation 164
Remove Journal 165
End Journal 165
Display Journal 166
Display Journal Entries 166
Display Journal Entry 167
Uninstall 168
Uninstall 168
BASE Support menu 169
Other 170
Email Address Book 171
Work with Email Address Book 171
Add Email Name 172
Enter. 172
Email Definitions 173
Email Definitions 174

Operators and Authority Codes 175
Work with Operators 176
CRTDTAARA SMZTMPC/DFTPWD *char 10 176
Work with Operators 177
Modify Operator 178
Work with AOD, P-R Operators 180
Work with Operators - AOD 180
Modify Operator - AOD 181
Work with Authorization 183
Add iSecurity Authorization (ADDISAUT) 183
Authorization Status 184
Status of iSecurity Authorization 184
General 185
Work with Collected Data 186
Work with Collected Data 186
Work with Collected Data - Journal 187
Check Locks 188
Check Locks 189
Printer Files Setup 190
*PRINT1-*PRINT9 Setup 191
CHGOUTQ OUTQ('local outq/library') RMTSYS (*INTNETADR) 192
+ RMTPRTQ('outq on remote') AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO) 193
+ INTNETADR('IP of remote') 194
CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS (*INTNETADR) 195
+ RMTPRTQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE (*IP) TRANS- FORM(*NO) 196
+ INTNETADR(1.1.1.100) 197
PDF Setup 198
Printer Files Setup 198
*PDF Setup 199
Global Installation Defaults 200
Global Installation Defaults 200
Network Support 203

Work with Network Definitions 204
Work with Network Systems 204
Add Network System 205
Network Authentication 207
Network Authentication 207
Check Authorization Status 208
Check Raz-Lee Authorization 208
Send PTF 210
iSecurity Send PTF 211
Run CL Scripts 214
iSecurity Remote Command 215
Current Job CntAdm Log 217
All Job CntAdm Log 218
Changing run attribute to further improve performance ... 219
CHGCLS CLS(SMZJDTA/ZJOURNAL) TIMESLICE(1000) 219
CHGSBSD SBSD(SMZJDTA/ZJOURNAL) POOLS ((1*SHRPOOLnn)) 219
CHGSBSD SBSD(SMZJDTA/ZJOURNAL) POOLS((1*BASE)) 219
Retrieve Data-Base Journal (RTVDBJRN) 219

Software Version: 9.1

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

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

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

Native IBM i (OS/400) User Interface

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

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all

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.

2020 © Copyright Raz-Lee Security Inc. All rights reserved.

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)

Chapter 1: 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.

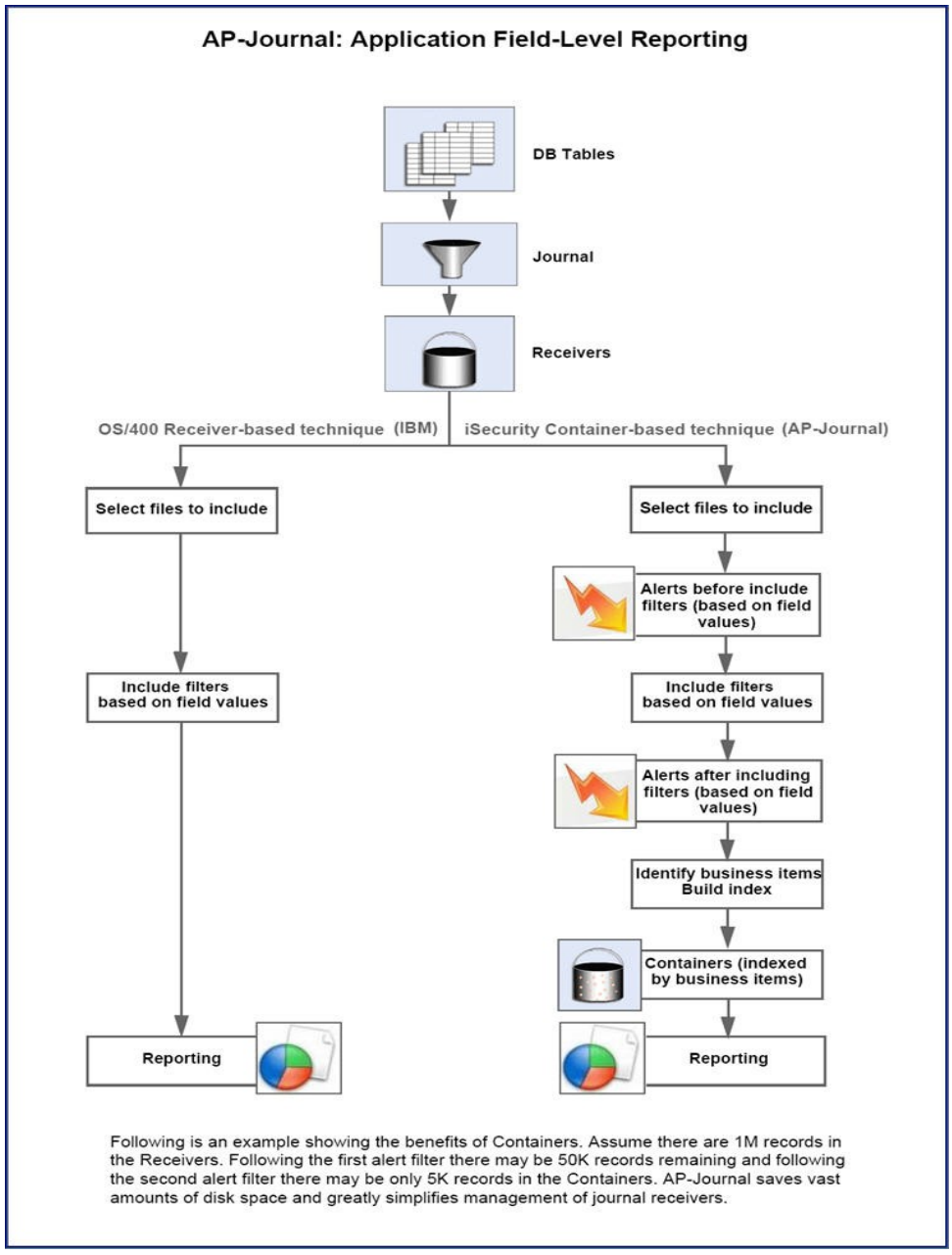
AP-Journal is fed by the IBM receiver, therefore it is enough to install AP-Journal in the machine where the receiver is located.

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.

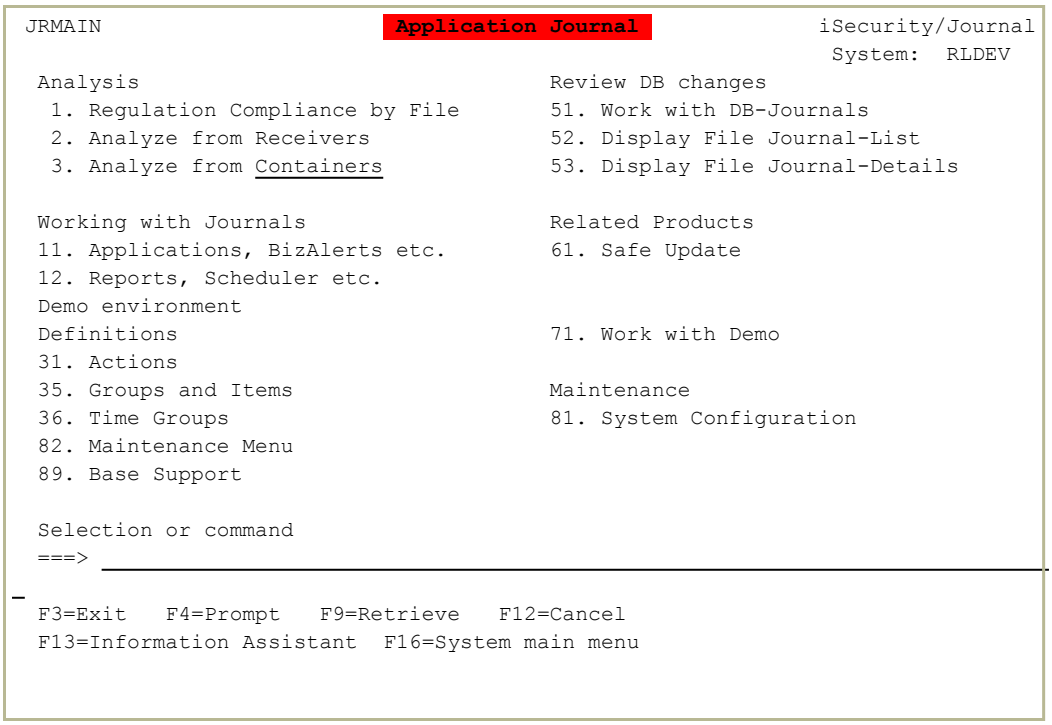
Many features are also accessible via the command line, for the convenience of experienced users.

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.



Chapter 2: Working with Single Files

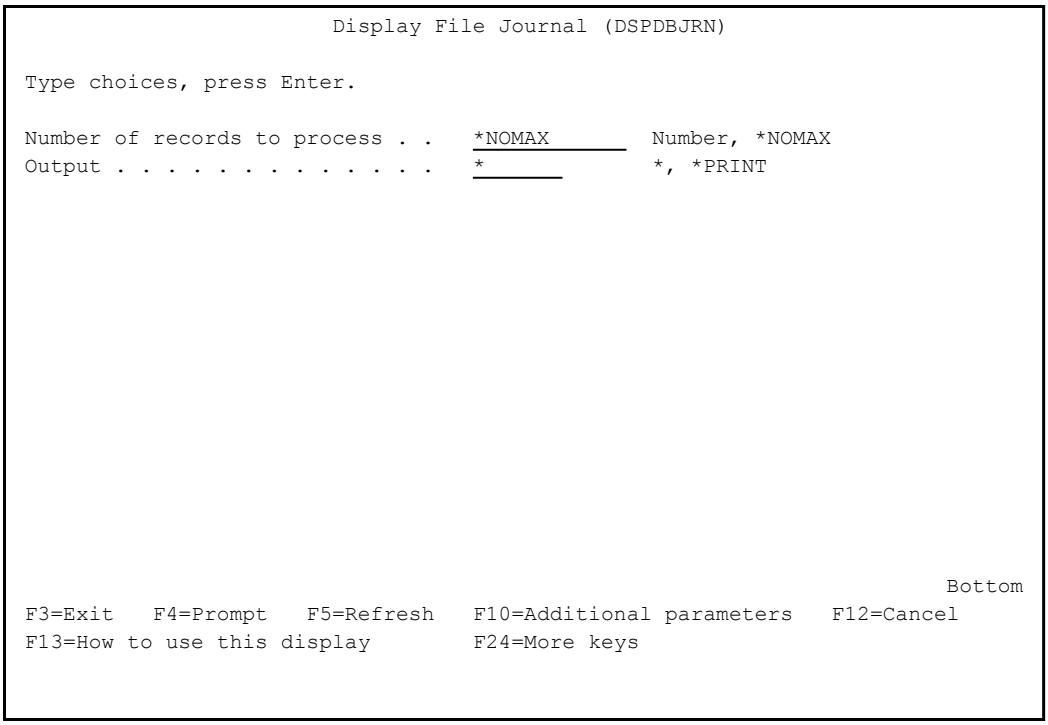
Journal Analysis

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 90. [[? Fix this link ?]]

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.

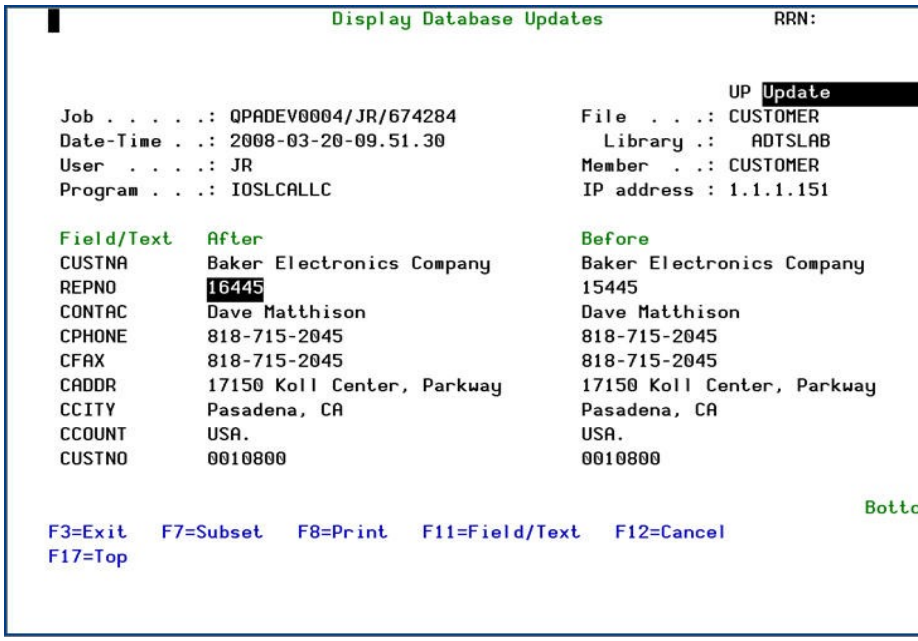
Include ticket # as

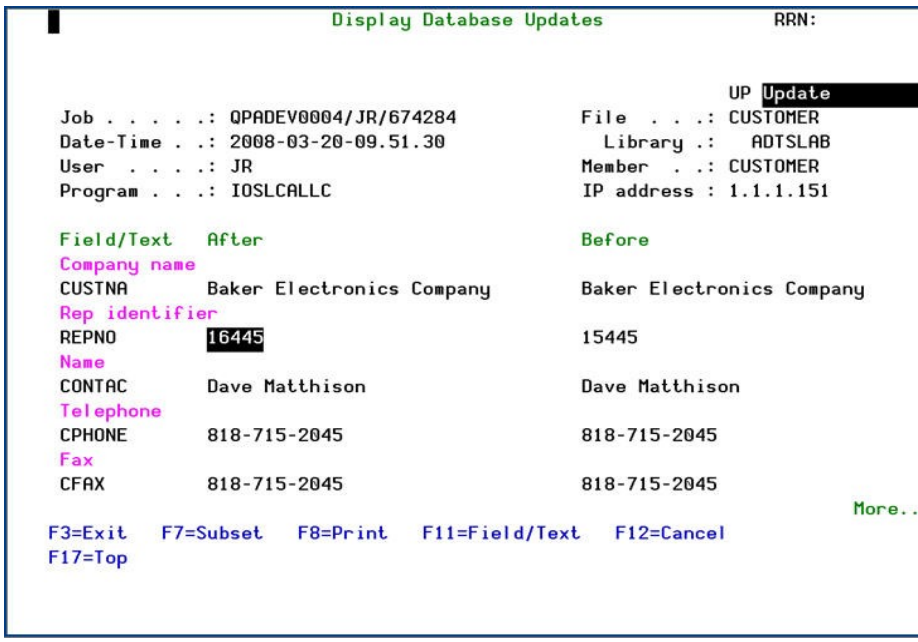
NOTE: This field only appears if you set the **Output** field to ***PRINT**.

[[? Need to find out ?]]

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

Type the file and library name, set 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 purple. [[? Need valid file/library to show example data ?]]





The screen contains these fields:

Job

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

Date/Time

The date and time of the update.

User

The user who updated the file.

Program

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

File

The file that was updated.

Library

The library containing the file.

Member

The member that was updated.

IP Address

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

To **filter the results** of the reports, press the **F7=Subset** key. The **Define Include Filters** screen appears.

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

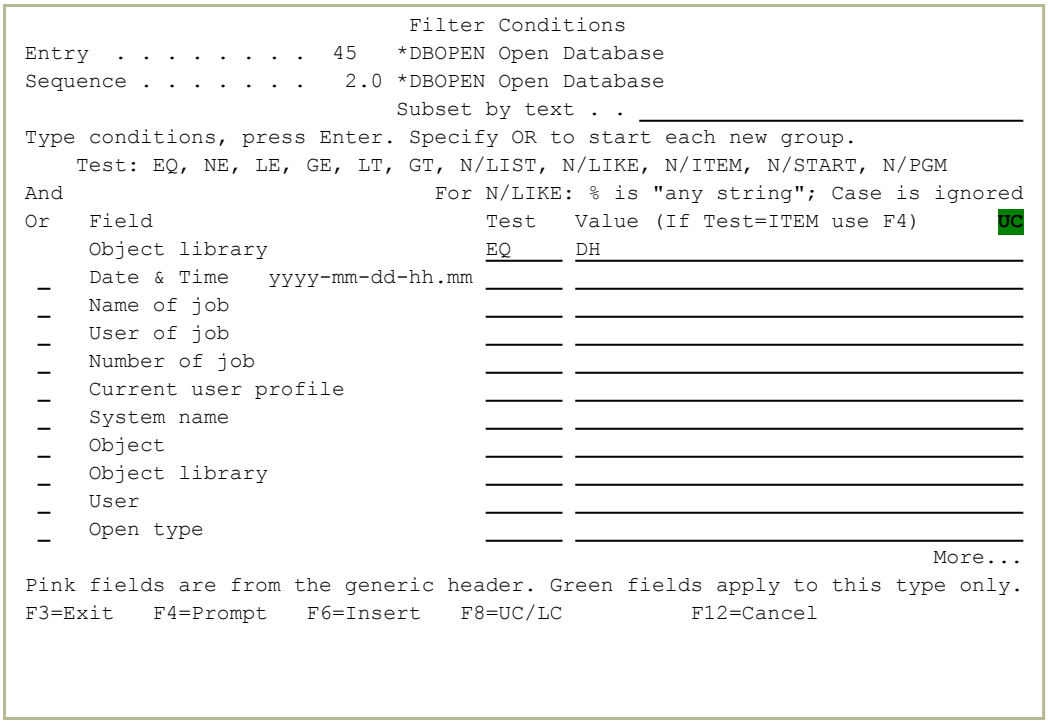
To **filter by fields in one of the files**, type **1** in the **Opt** field for that file and press **Enter**. The **Filter Conditions** screen appears, as shown in "Setting the Order of Rules" on page 31.

To print the file changes, select **2. Print File Updates** from the Regulation Compliance menu (*STRJR* > **1**). The Display File Journal (DSPDBJRN) screen appears as described above, 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**).

Setting Filter Conditions

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



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.)

Field

The name of the field within the record or request being checked. The items in this field are read-only. If they appear in green, they are the names of fields defined for files on that server or entry type. If they appear in pink, they are generic fields referring to the event or request being tested.

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 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:

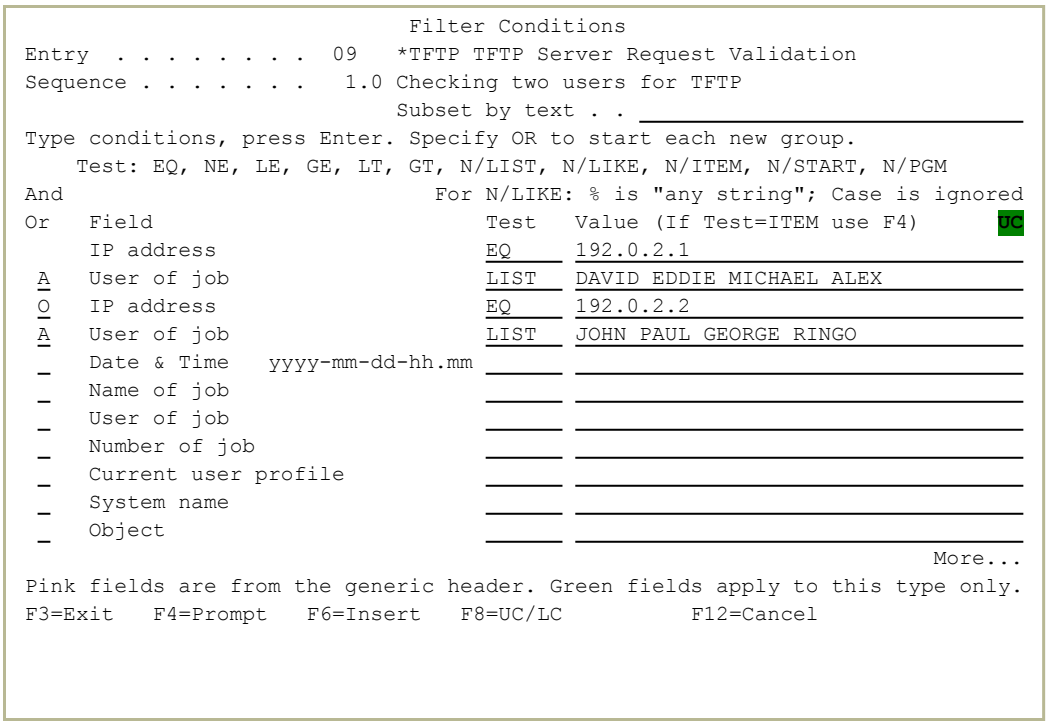
- **EQ**: Equal to. The field contents are identical to those of the **Value** field.
- **NE**: Not equal to. The field contents are not identical to those of the **Value** field.
- **LT**: Less than. The field contents are less than those of the **Value** field.
- **LE**: Less than or equal to. The 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.
- **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.



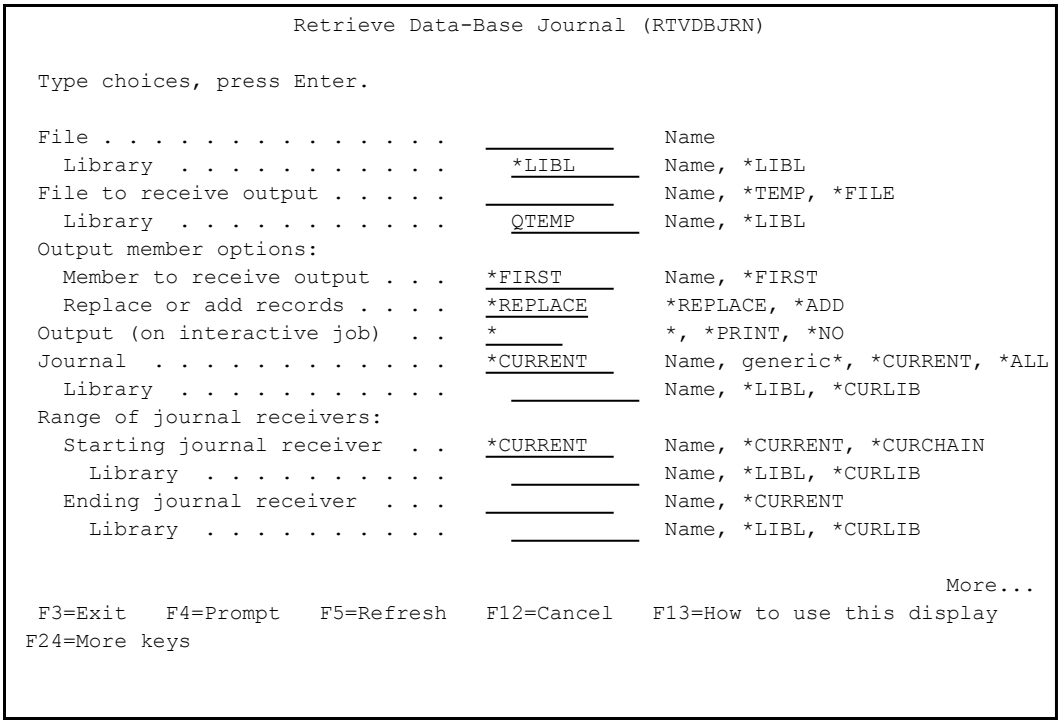
In this example, using values for iSecurity/Firewall, the filter conditions are true if either

- The IP address is 192.0.2.1 and the user is any of DAVID, EDDIE, MICHAEL, or ALEX, or
- The IP address is 192.0.2.2 and the user is any of JOHN, PAUL, GEORGE, or RINGO.

This follows standard logic operations, where 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

Retrieving Data-Base Journals

To **build a new output file** from updates that were done to a single database file, using the fields of the journal's headers its records' fields, 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.

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
```

```
                    Retrieve Data-Base Journal (RTVDBJRN)

Type choices, press Enter.

User profile . . . . . . . . . .   *ALL_______    Name, *ALL
Dependent entries  . . . . . . .   *ALL_         *ALL, *NONE

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

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.

%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.

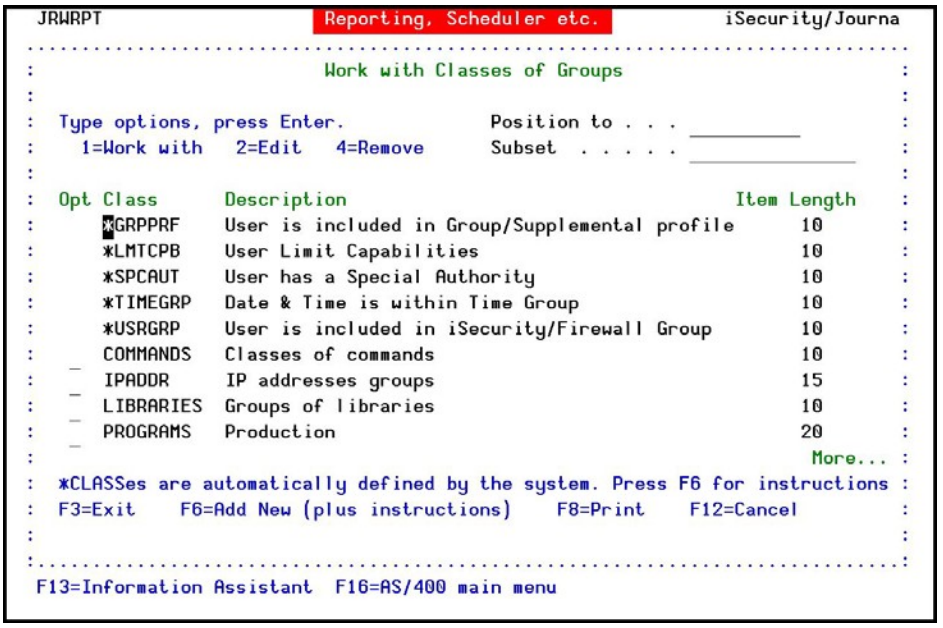
For each GROUP-TYPE, you can define an unlimited number of GROUPS and within GROUPS any number of items. For example, all identification numbers of the PCs in the organization can be defined as one group in the GROUP-TYPE defined as MACHINE_AD- DRESS. Another group in MACHINE_ADDRESS may contain all 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, special GROUPS 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 sys- tem, group profiles defined in Firewall, and virtual groups of users named *SECADM,

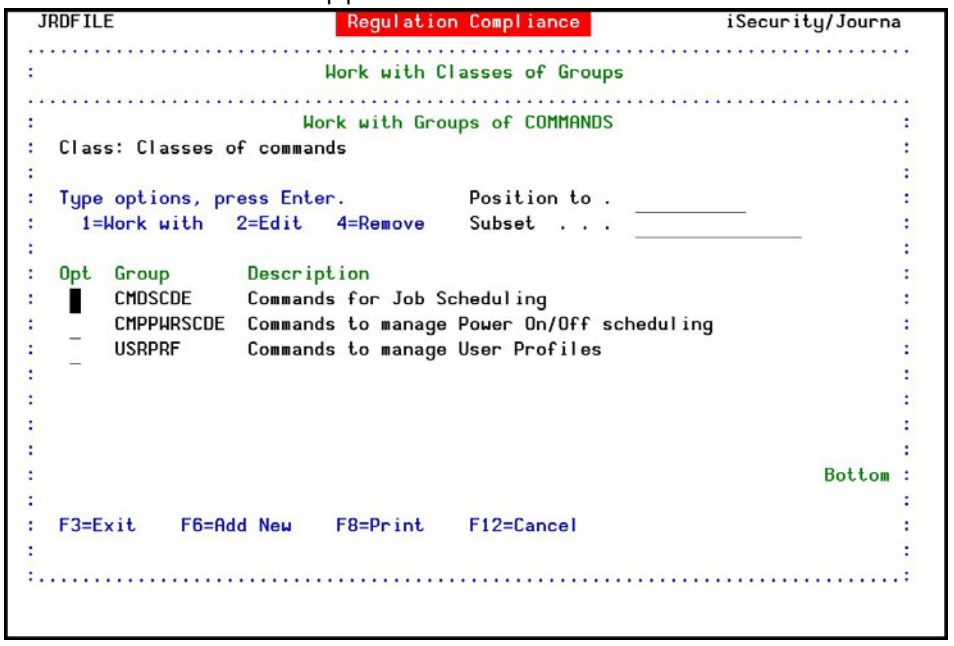
*SAVESYS and so on which are the users who have this particular privilege defined in their special authority.

1. Do one of the following:
    - Select 1.RegulationCompliance from the ApplicationJournal main menu. The Regulation Compliance menu appears.
    - Select 2. Analyze from Receivers from the Application Journal main menu. The Business Analysis menu appears.
    - Select 3. Analyze from Containers from the Application Journal main menu. The Business Analysis menu appears.
2. Select 35.GroupsandItems from the chosen menu. The WorkwithClasses of Groups screen appears.



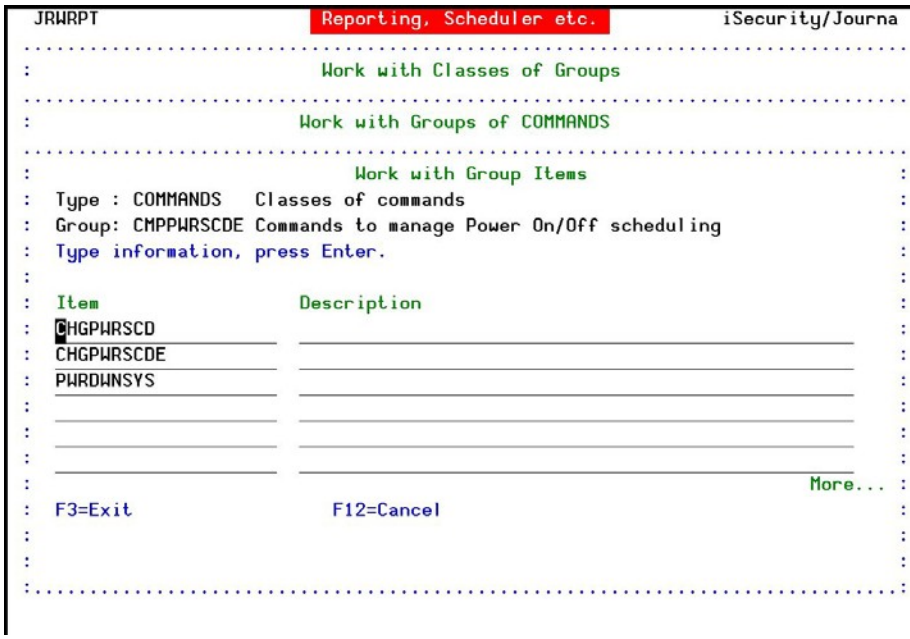
Work with Classes of Groups

3. Type 1 to modify a group type or press F6 to add a new one. The Workwith Groups of <ClassName> screen appears.



Work with Groups of <ClassName>

4. Type 1 to modify a group or press F6 to add a new one. The Work withGroup Items screen appears.



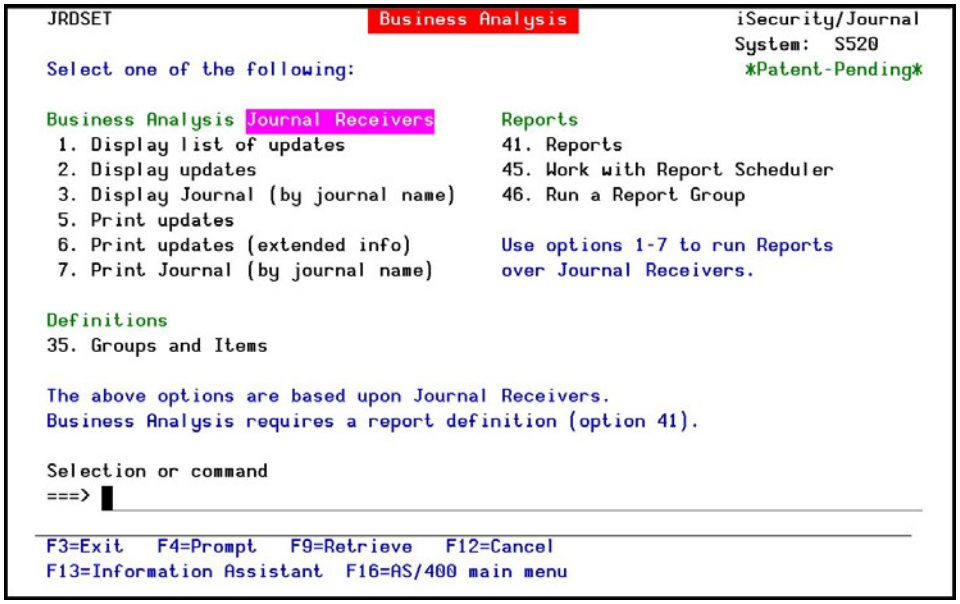
Work with Group Items

5. To add a new Item, simply type the command and a description on the first free line.

Chapter 3: Analyze Business

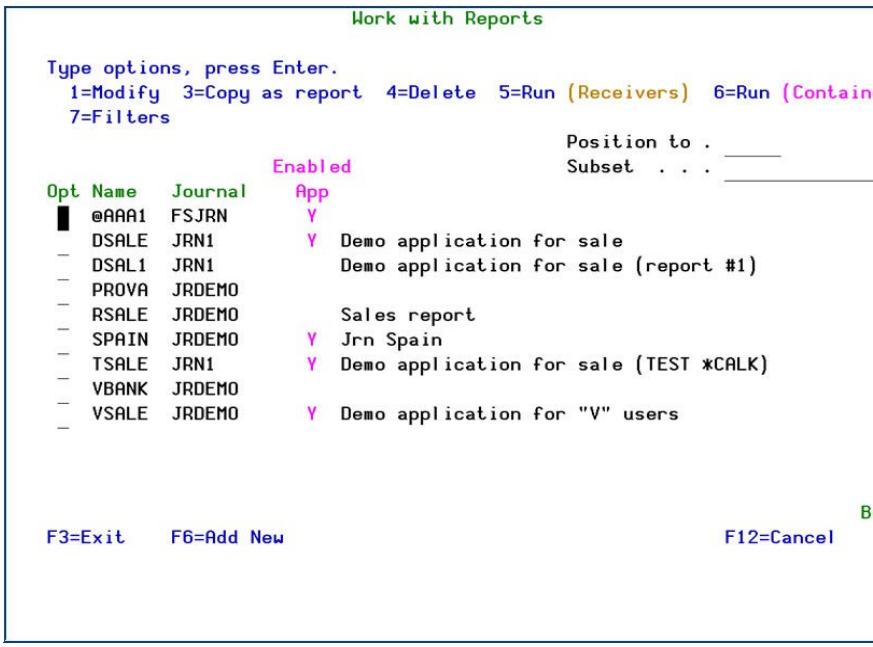
Analyze Business
To view changes that were done on a single file, follow this procedure:

1. Select 2.AnalyzefromReceivers or 3.AnalyzefromContainers from the Application Journal main menu. The Business Analysis menu appears.



Business Analysis Menu

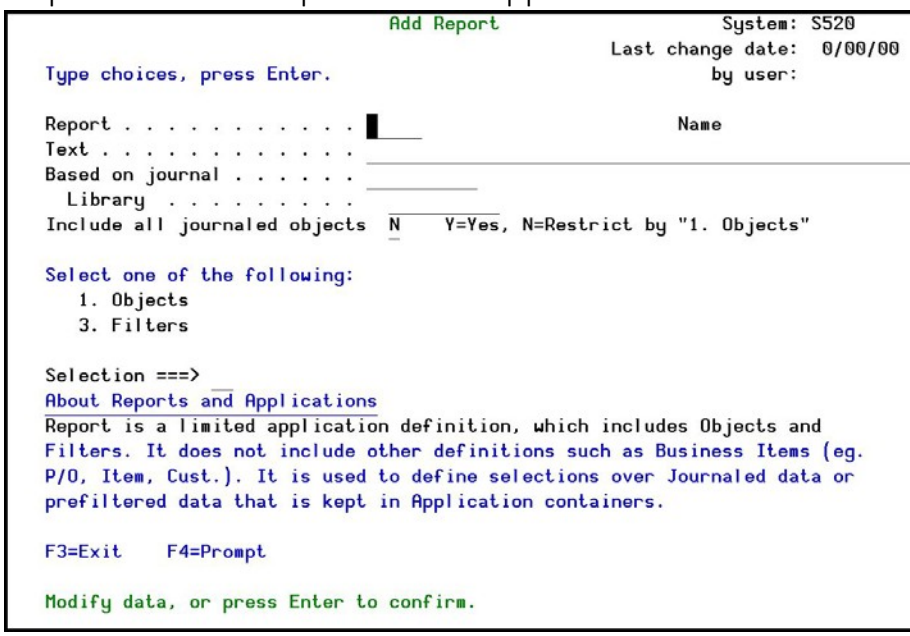
2. Select 41. Reports. The Work with Reports screen appears.



Work with Reports

Defining Set of Files

3. Press F6 to add a new report. The Add Report screen appears.



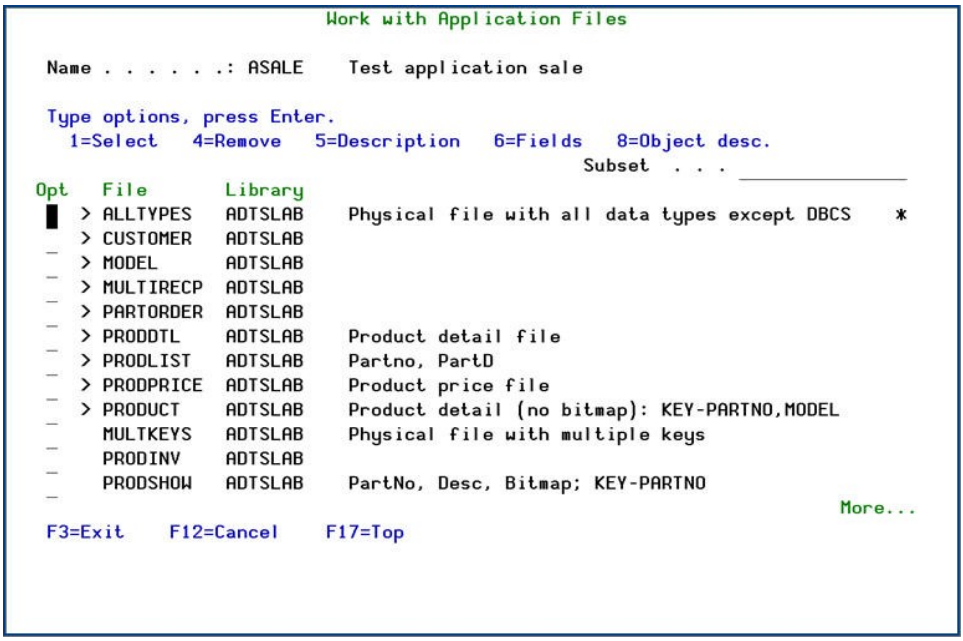
Add Report

The following table explains the options:

Option	Description
Set	Insert five character set name
Text	Insert descriptive text
Based on journal	Insert the system's journal name
Library	Insert the system's journal library name
Include all journaled objects	Y =Yes N =No, restrict by 1. Objects
Selection	1. Files: Select the files you want the set to use. If no file was selected, the set will contain all the files in the journal. 3. Filters: Select a predefined filter

NOTE: If Raz-Lee's FileScope in installed, its journal file can be used. The file name is: FSJRN at library: SMZ1DTA.

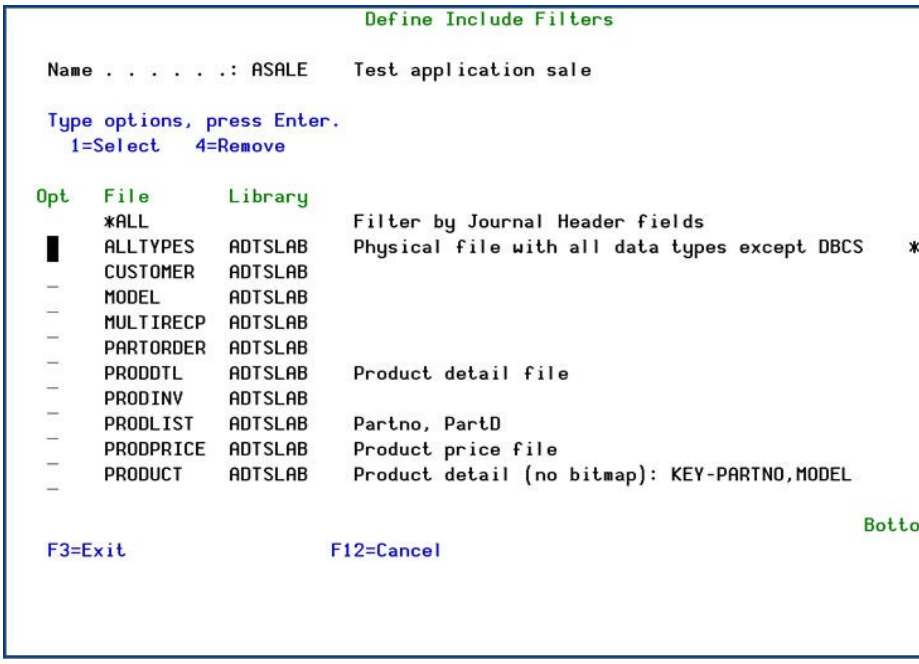
4. Type 1 at the selection field to select files to work with. A list of files appears.



Work with Application Files

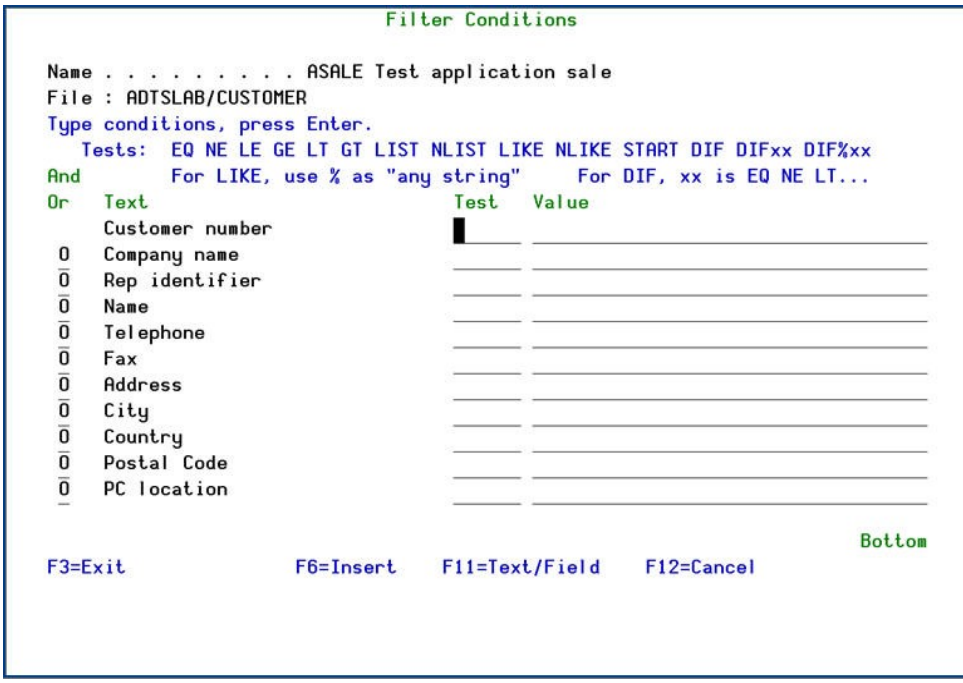
5. Type 1=Select to select the files. Press Enter to confirm the files selected and return to the Add Report screen.

6. Type 3. Filters in the selection field of the Add Report screen to select predefined filters for the selected files. Also select one general filter for the record's headers.



Define Include Filters

7. Type 1 to select *ALL or the file's name to filter according to the fields name. The
Filter Conditions screen appears, allows to set filter for the results by header.



Filter Conditions

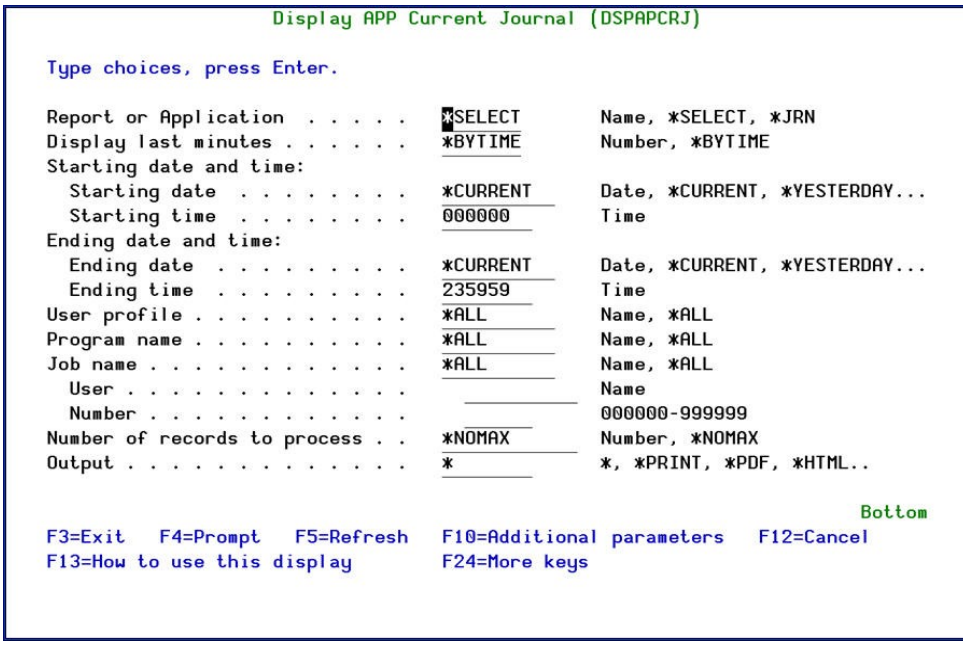
Option	Description
And/Or	Select A =And/ O =Or operators to display All or Any of the conditions

Option	Description
Test	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) 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)
F6=Insert	Insert a another row to add more filter conditions for the same field

8. Press Enter to confirm and Enter to confirm these definitions.

Set of Files Analysis

1. To view the changes that were done on a set of files, select 1. Display list of updates .



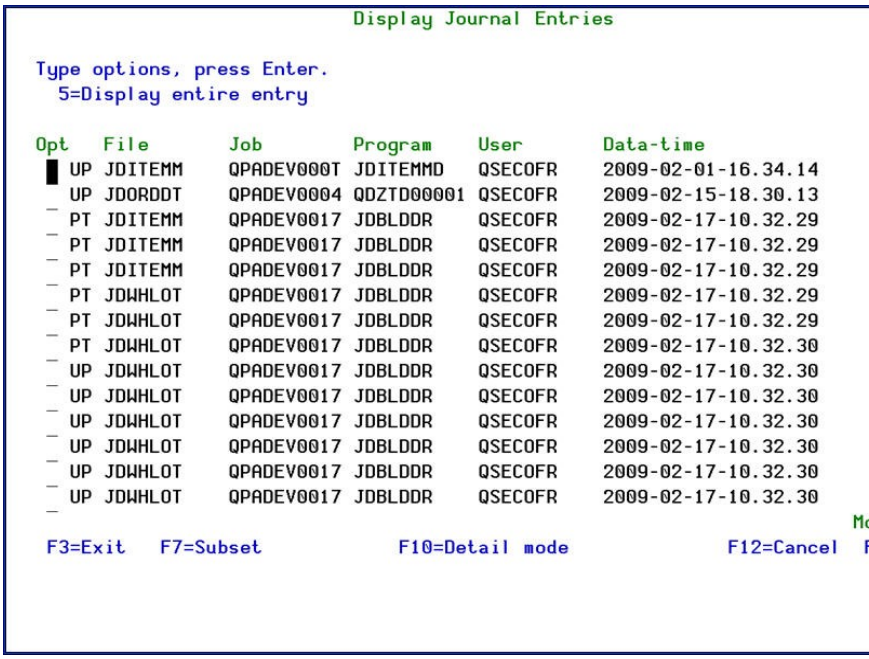
Display APP Current Journal

Option	Description
Report or Application	Set of file 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.
Display last minutes	Last N minutes to display
Starting/Ending date and time	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

Option	Description
User Profile	User profile who conduct the file's update
Program name	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	Insert a number or *NOMAX
Output	* = to display only *PRINT = to print *PDF = PDF file *HTML = HTML file *OUTFILE *PRINT1-*PRINT9 = Select correct print option. Read more about the setup at chapter 6 for details.
On missing data (in Containers)	*CANCEL = cancel the missing data search *IGNORE = ignore the missing data *LOAD = search for the missing data in external data storage *INQ = inquiry for which the user should answer

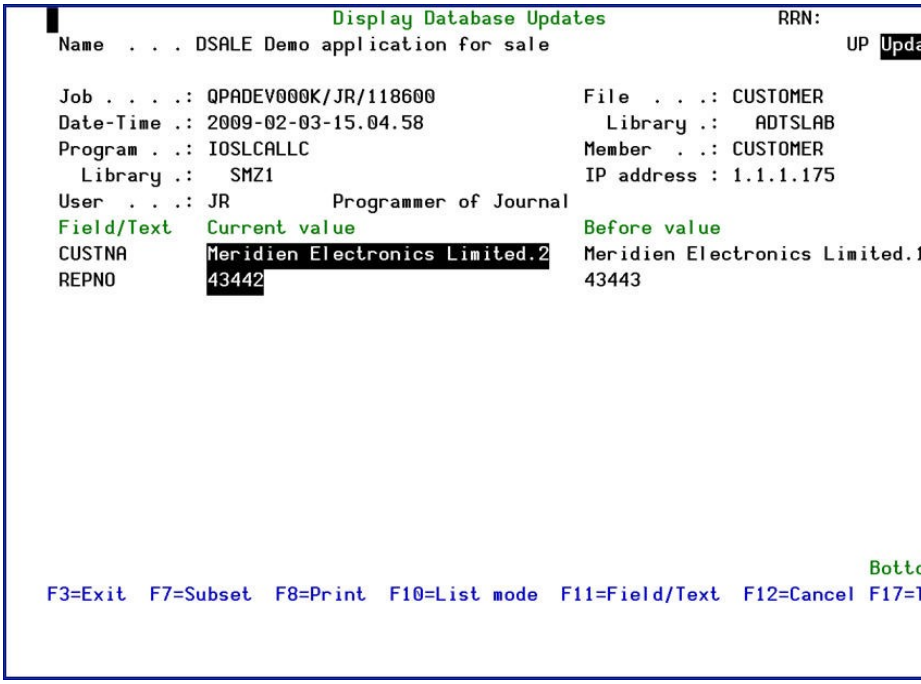
2. Type the report/application name, define criteria and press Enter .

3. The Display Journal Entries screen appears, showing a list of journal entries according to the filter conditions selected.



Display Journal Entries

4. Type 5 to display the entry details with the information before and after the changes. The fields that were changed will appear with a black background.



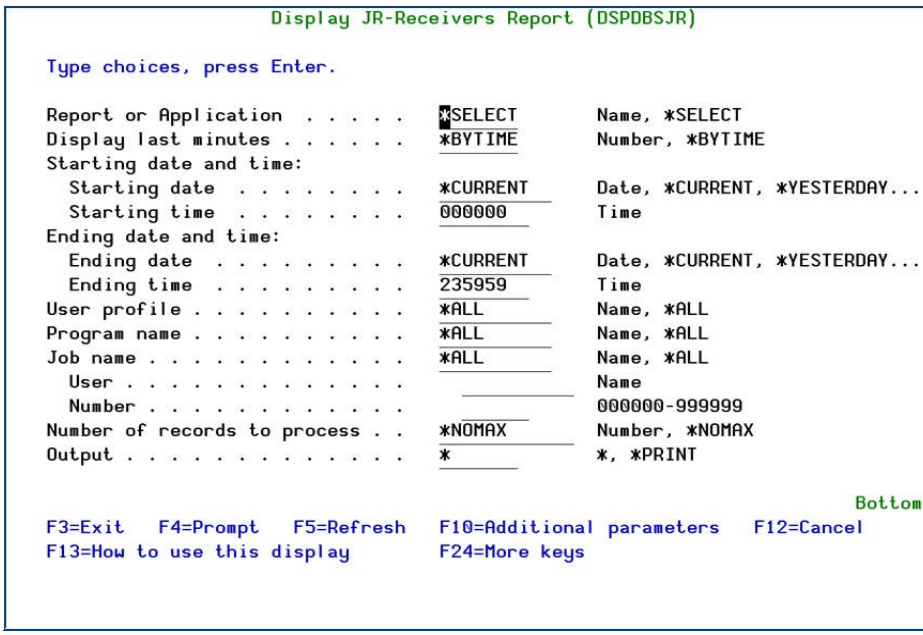
Display Database Updates

Field	Description
Job	Name of the job that changed the file's information
Date-Time	Date and time of the update
User	User profile name
Program	Name of the program used to change the file's information
File	The updated file
Library	Library's name
Member	The updated member
IP Address	The IP address that the change was set from. From V5R3 and higher.
F7=Subset	Search the file for specific information All = Filter according to the fields title FIle name = Filter according to the fields name

Field	Description
F8=Print	Print from the current position or from the beginning of the set, and select how many records to print
F11=Field/Text	Display the field's descriptive text

Printing the Set changes

1. Select 5. Print Updates . The Display JR-Receivers Report screen appears.



Display JR-Receivers Report

Option	Description
Set	Name of set to display
Display last minutes	Last N minutes to display
Starting/Ending date and time	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 conduct the file's update
Program name	Name of the program used to change the file's information

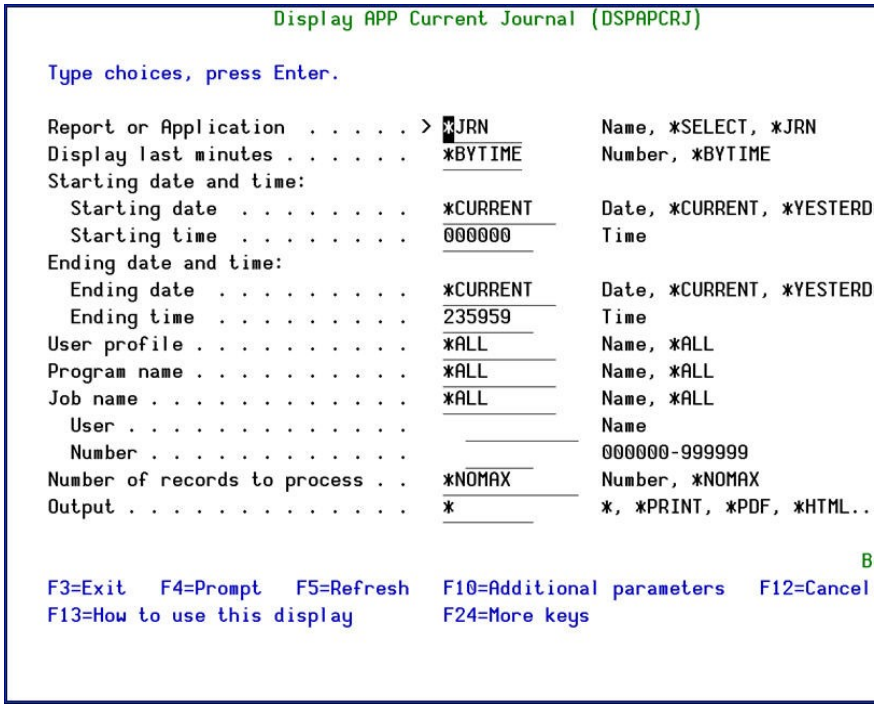
Option	Description
Job name	Name of the job that changed the file's information
Number of records to process	Insert a number or *NOMAX
Output	*PRINT - to print * - to display only

NOTE:Attheoutputprintnexttothefieldsthatwerechanged,aspecialmarkwill appear. This can be modified from option 81. System Configuration off the main menu: Marker of changedfield

Display Immediate

NOTE: See chapter 3 - Work with Single File for information regarding options 31, 32 and 39.

1. Select 3 and/or 7 to display/print directly from the journal receivers. These options do not require an application to be pre-defined.



Display APP Current Journal (DSPAPCRJ)

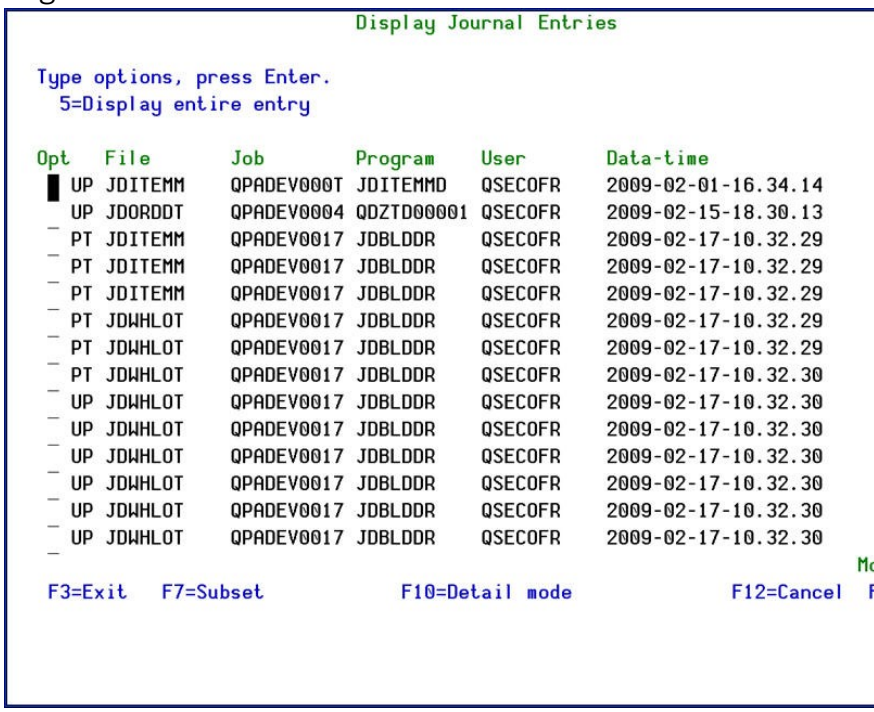
Option	Description
Report or Application	*JRN = Press F9 and Page Down twice, then enter a name in the "For APP(*JRN) - Journal" field as well as a library name.
Display last minutes	Last N minutes to display
Starting/Ending date and time	Select only those records occurring within the range specified 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 conduct the file's update
Program name	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	Insert a number or *NOMAX

process

Output

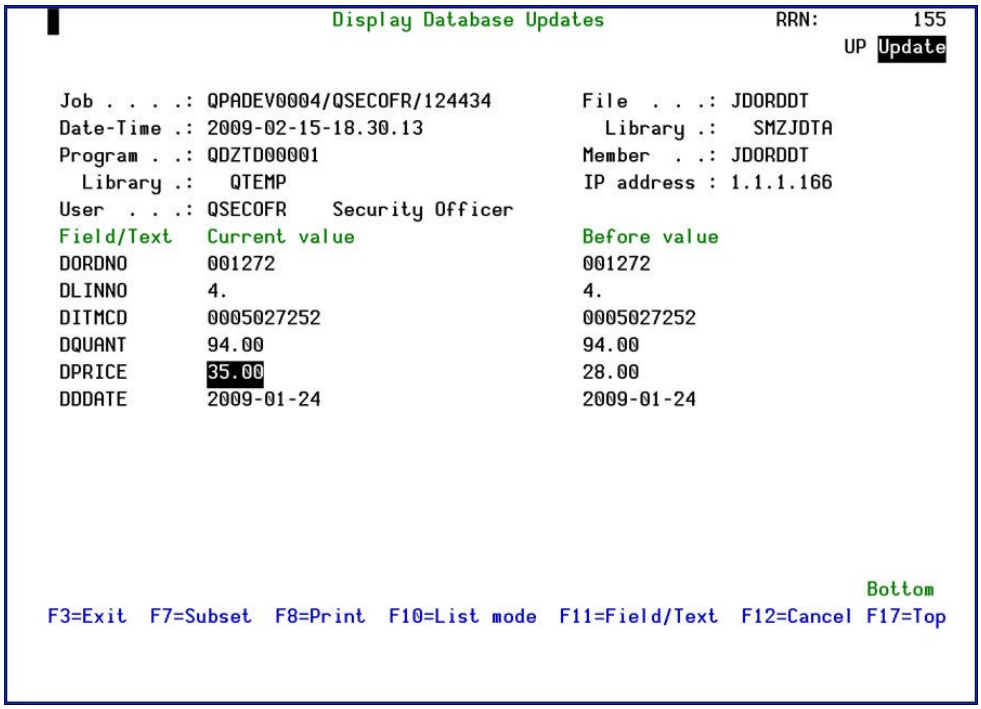
* = to display only
*PRINT = to print
*PDF = PDF file
*HTML = HTML file
*OUTFILE
*PRINT1-*PRINT9 = Select correct print option. Read more about the setup at chapter 6 for details.

2. The Display Journal Entries screen appears, showing a list of journal entries according to the filter condition selected.



Display Journal Entries

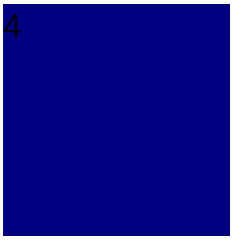
3. Type 5 to display the entry details with the information before and after the changes. The fields that were changed will appear with black background.



Display Database Updates

Field	Description
Job	Name of the job that changed the file's information
Date-Time	Date and time of the update
User	User profile name
Program	Name of the program used to change the file's information
File	The updated file
Library	Library's name
Member	The updated member
IP Address	The IP address that the change was set from. From V5R3 and higher.

Field	Description
F7=Subset	Search the file for specific information All = Filter according to the fields title FIle name = Filter according to the fields name
F8=Print	Print from the current position or from the beginning of the set, and select how many records to print.
F11=Field/Text	Display the field's descriptive text



Work with Business Analysis

Chapter 4: Work with Business Analysis

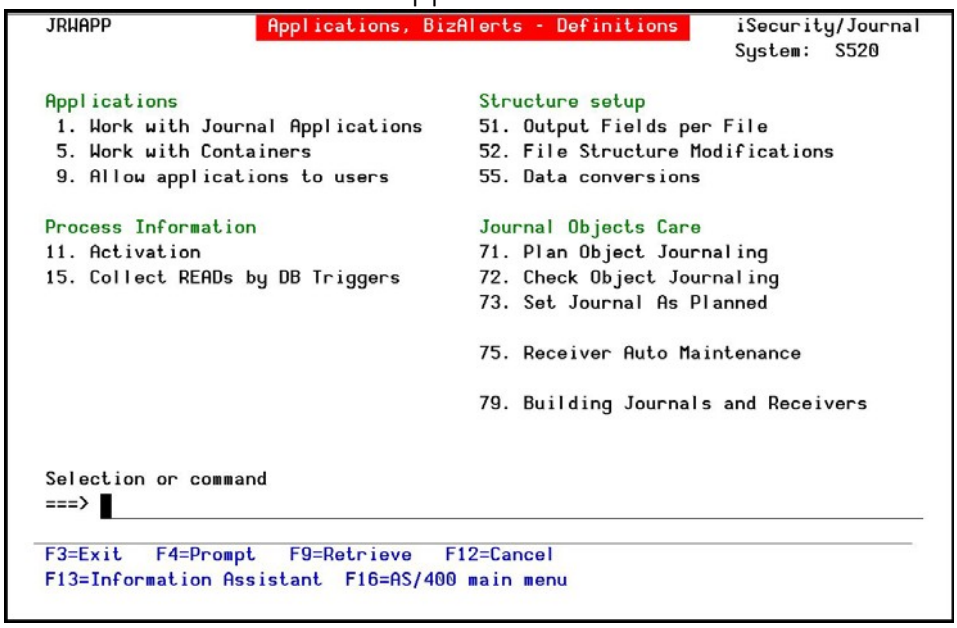
Business Analysis option creates Journal Application which is based upon the system journal QJRNRCV, that contains activity data on the database files.

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 (off-working hours). To build, define and work with Journal Applications:

1. Select 11. Applications,BizAlertsetc. from the ApplicationJournal main menu. The Applications, BizAlerts - Definitions menu appears.



Defining Application

Applications, BizAlerts - Definitions

To view field changes in several files, create an application of files combines information from all the relevant files and fields needed. After creating the

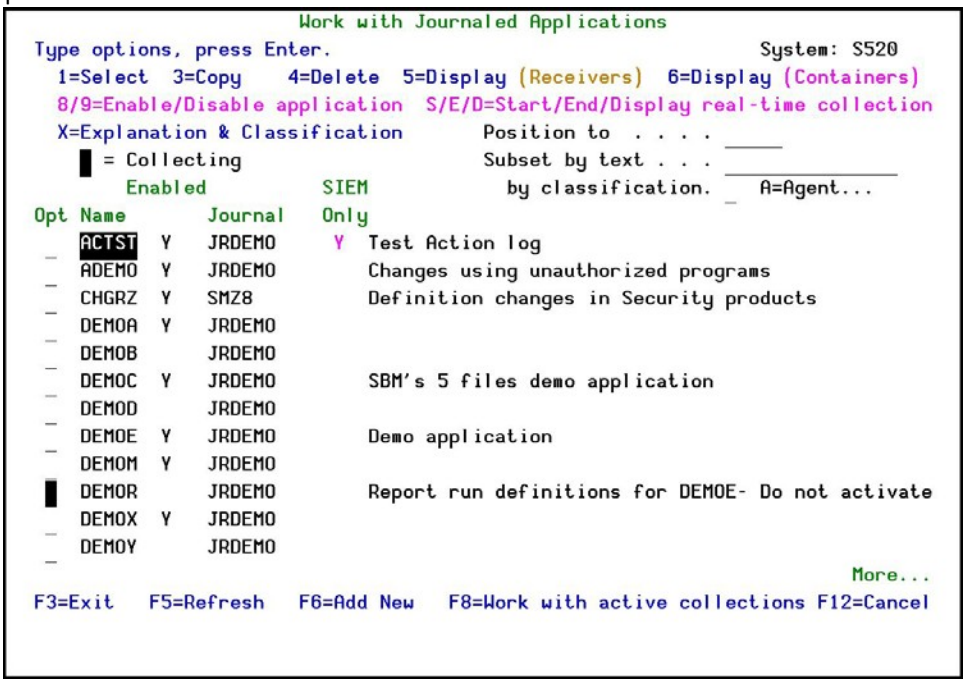
application, the first

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 you chose. In that way, only the relevant information is kept in the system.

Creating a new set of files

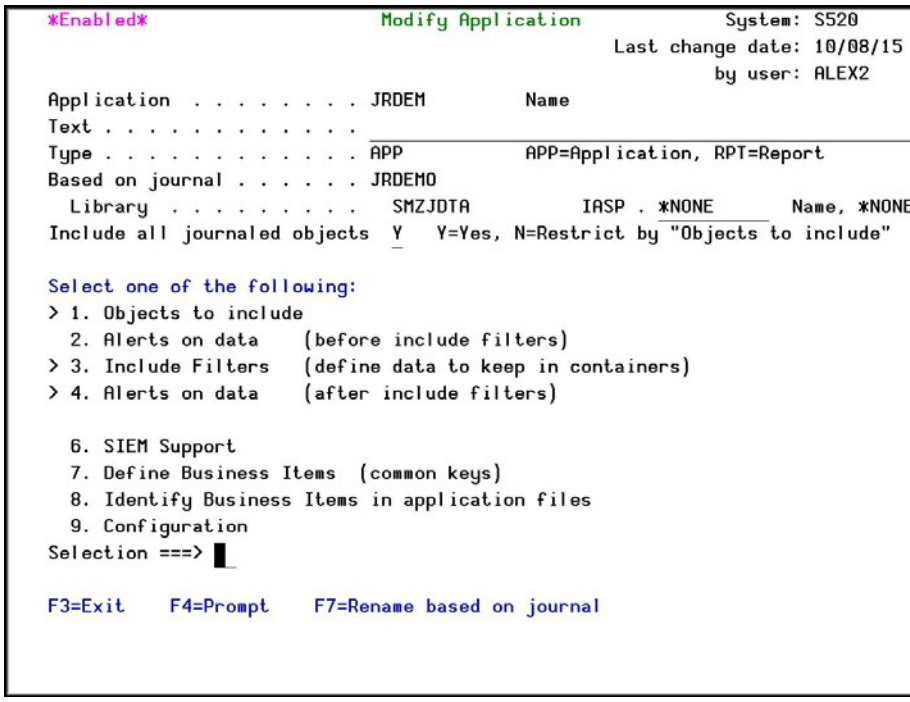
To define a new application:

1. Select 1. Work with Journal Applications from the Applications, BizAlerts-Definitions menu. The WorkwithJournaledApplications screen appears.



Work with Journaled Applications

2. 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.



Modify Application

NOTE: If Raz-Lee's FileScope is installed, you can use its journal file FSJRN in library SMZ1DTA as a base journal.
The table below describes the parameters:

Parameter	Description
Application	Insert a five character application name
Text	Insert a meaningful description
Type	Define if this is an application or a report APP = Application RPT = Report
Based on journal	Insert the system's journal file and library name

Parameter	Description
IASP	Name *NONE
Include all journalled files	Type ‘ Y ’ to include all the journaled files or ‘ N ’ to select specific files to include using option 1. Objects to include below.
Selection	1. Objects to include: Select the objects you want the applica- tion to use. 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. Alertsondata: Alerts based upon the changes in the journal receiver before the include filters are checked. 3. Include Filters: Select a predefined filter. 4. Alerts on data: Real- time action based on definitions that are based upon changes in the containers after the include fil- ters were checked. 6. SIEM Support: Define SIEM support for the application. 7. Define Business Items: Common key fields which 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 you can select up to 15 fields.

8. Identify Business Items in application files Select the Application Objects to be used in the application.
9. Configuration: Define the application configuration.

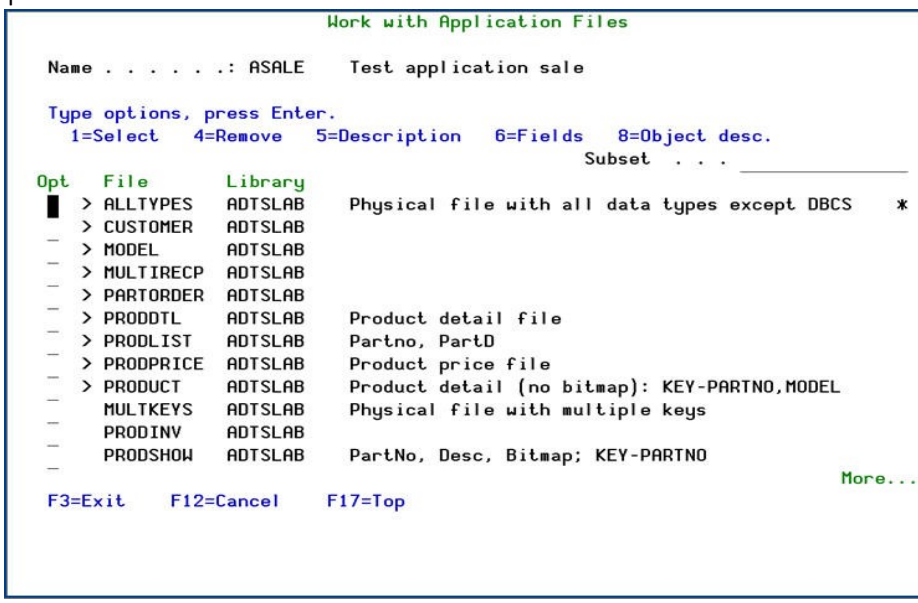
Some journals support millions of objects. The AP-Journal does support such journals. This includes the functions which list the objects that are journaled, (which will take considerable-equivalent time). AP-Journal application supports any number of objects in the following way (restrictions apply):

	Include all Objects = NO	Include all Objects = YES
Number of supported objects	10,000,000	1,000
Select by generic name	Yes	No

	Include all Objects = NO	Include all Objects = YES
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

Files to include

1. Enter parameters as described above and type 1 in the Selection field to select objects to work with. The Work with Application Objects screen appears.

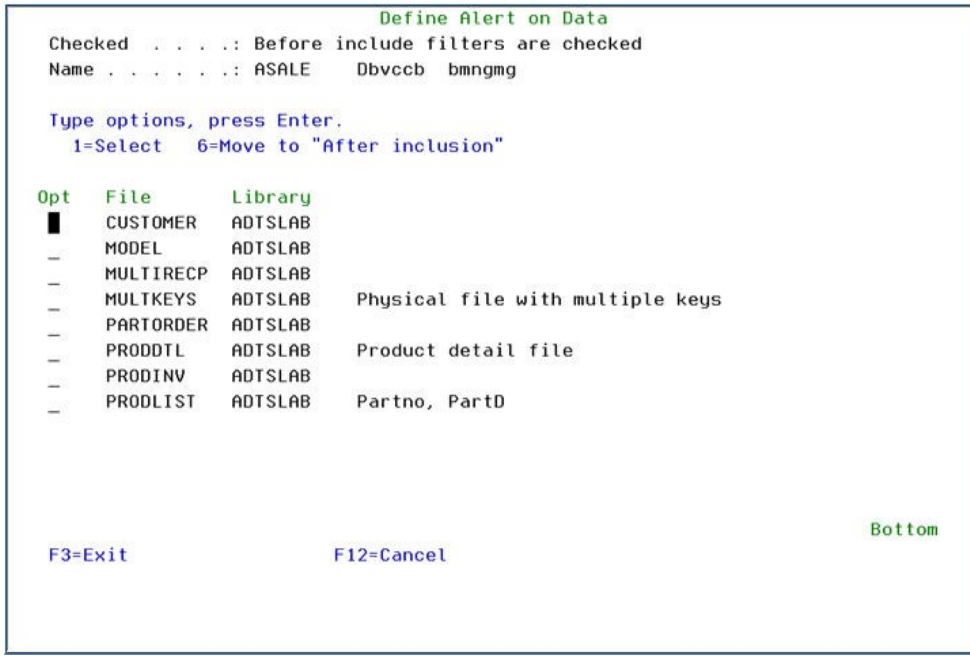


Work with Application Files

2. Type 1=Select to select the files. Press Enter to confirm the selected files. The Add Application screen appears.

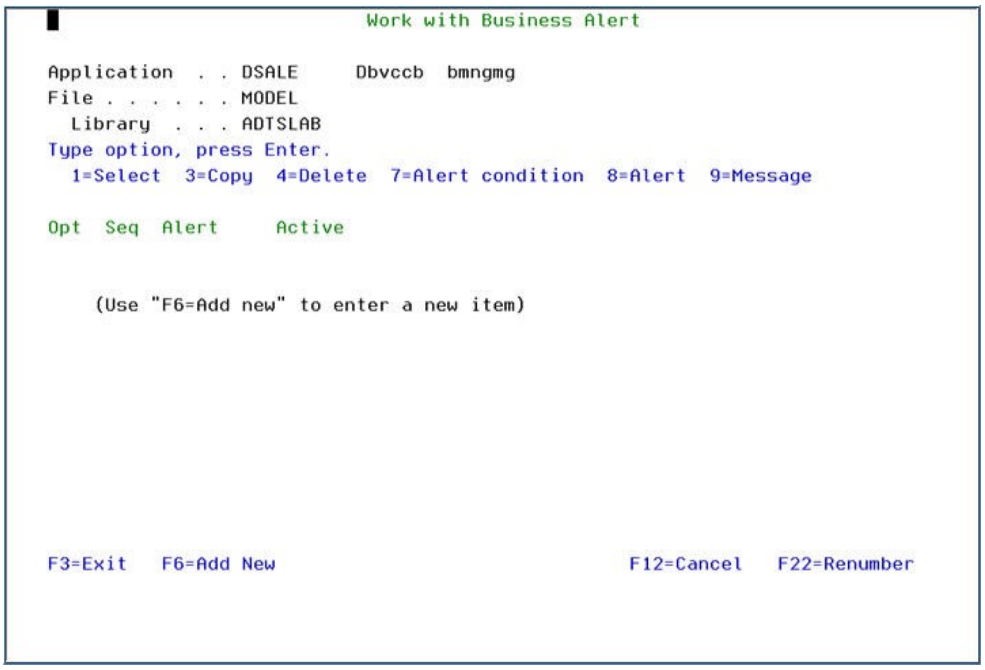
Alerts on data (before include filters)

1. Type 2 in the Selection field to select alerts to work with. The Define Alerton Data screen appears.



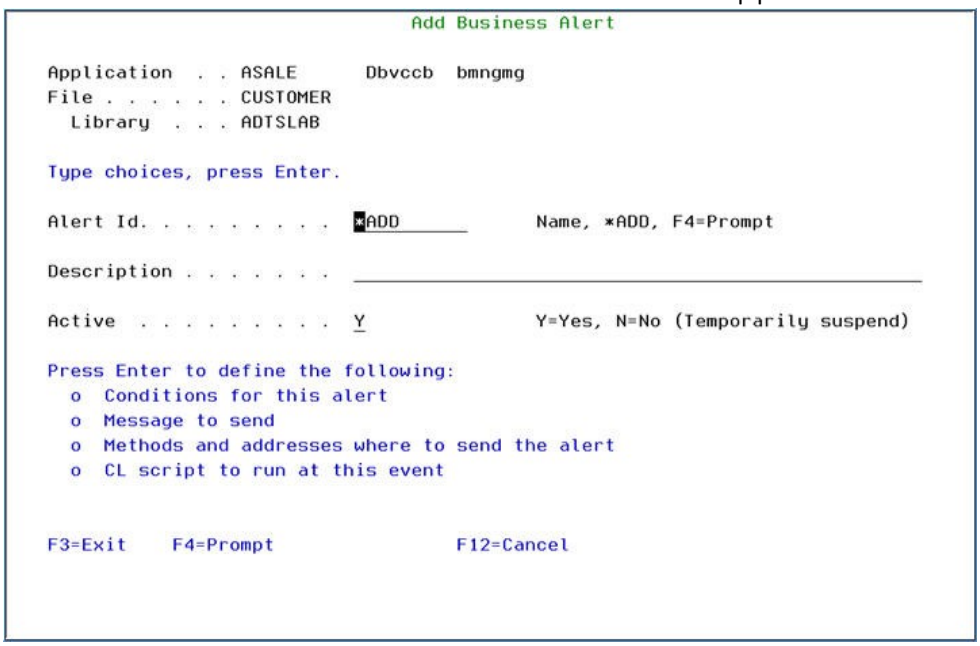
Define Alert on Data

2. Type 1 to select a file to set an action for and press Enter . The Workwith Business Alert screen appears.



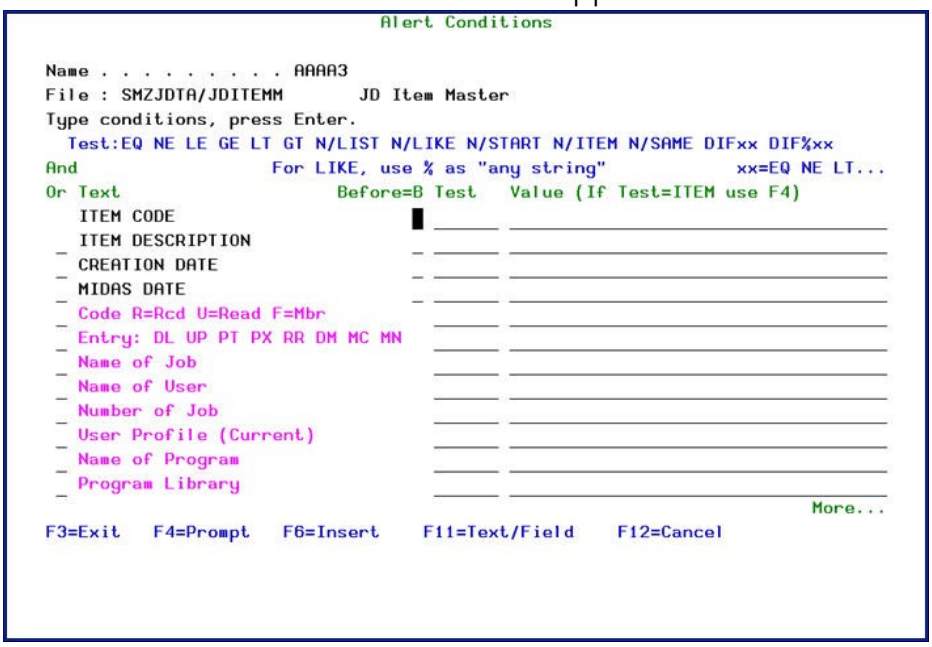
Work with Business Alert

3. Press F6 to add a new action. The Add Business Alert screen appears.



Add Business Alert

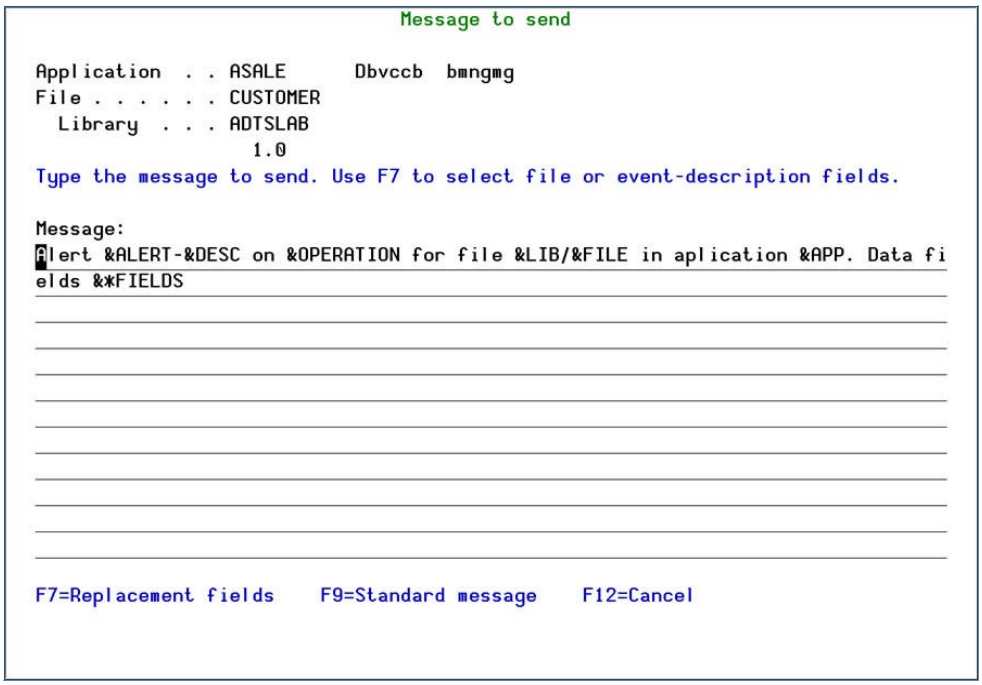
4. Type a name for the new action and a description and press Enter . The Alert Conditions screen appears.



Alert Conditions

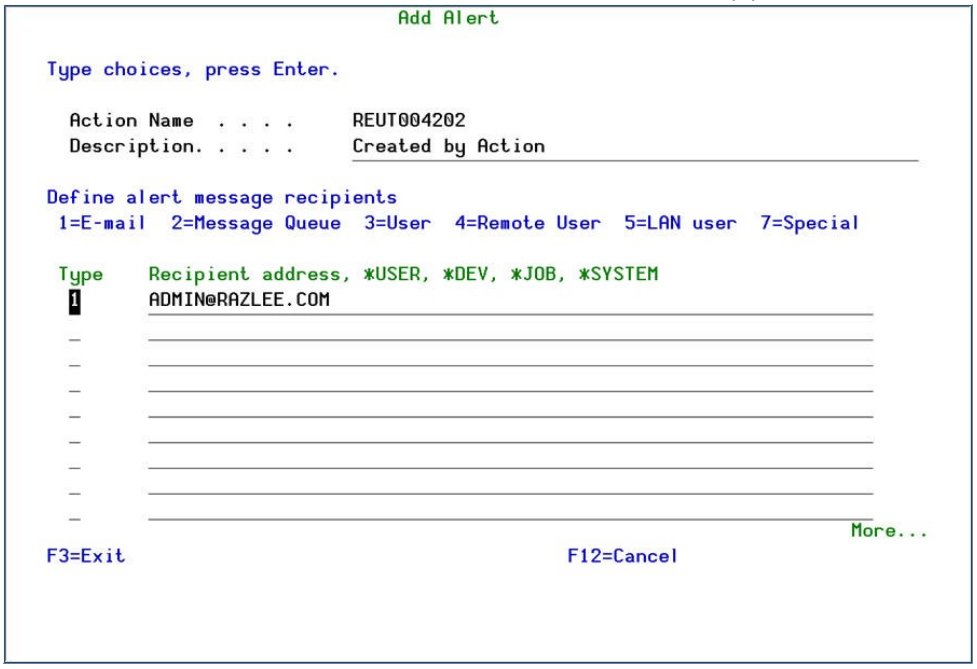
- NSTART is a new option which checks that the "before" or "after" values do not start with the characters entered
- SAME is a new option which compares between the "before"and "after-"field values
- NSAME (replaces DIF which can also be specified) is a new option which compares between the "before"and "after"field values
- Before=B can be used to compare current values to "before" values
- Code R =Rcd U =Read F =Mbr
- Entry: DL =delete UP =update PT = PX = RR= DM =delete member MC =member change MN =member rename

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



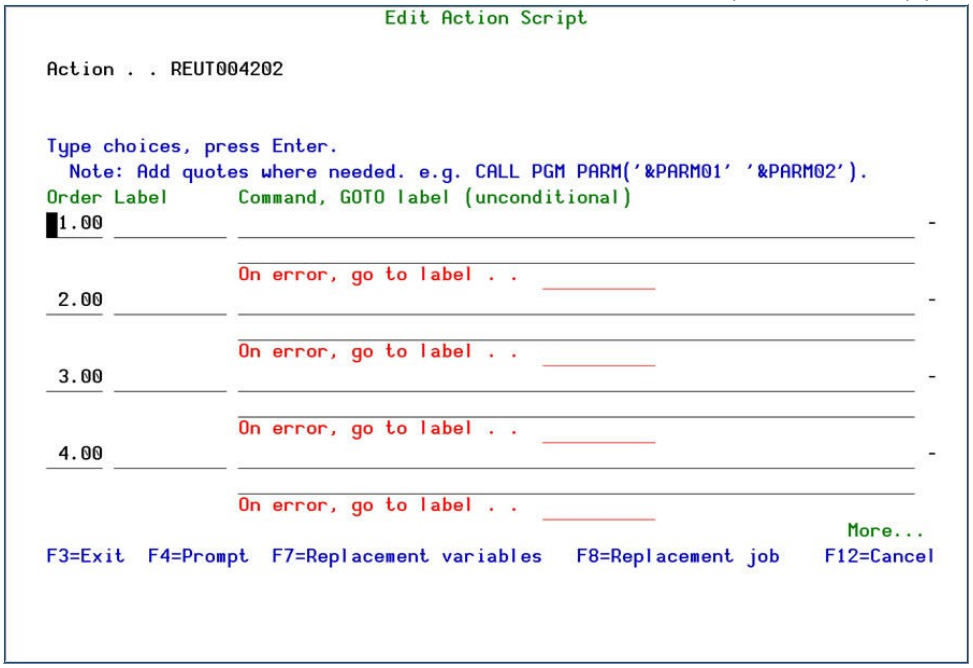
Message to send

6. Type a message to send and press Enter . The Add Alert screen appears.



Add Alert

7. Define a methods and addresses where to send the alert message. Press Enter to confirm, the Edit Action Script screen appears.

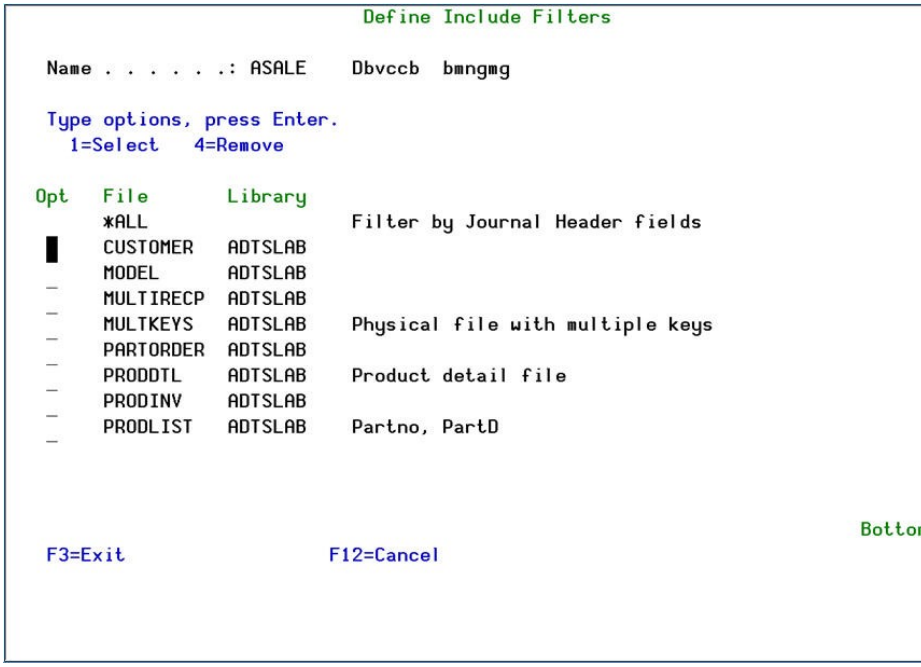


Edit Action Script

8. Type a CL command to issue in real-time and press Enter to confirm. The Add Application screen appears.

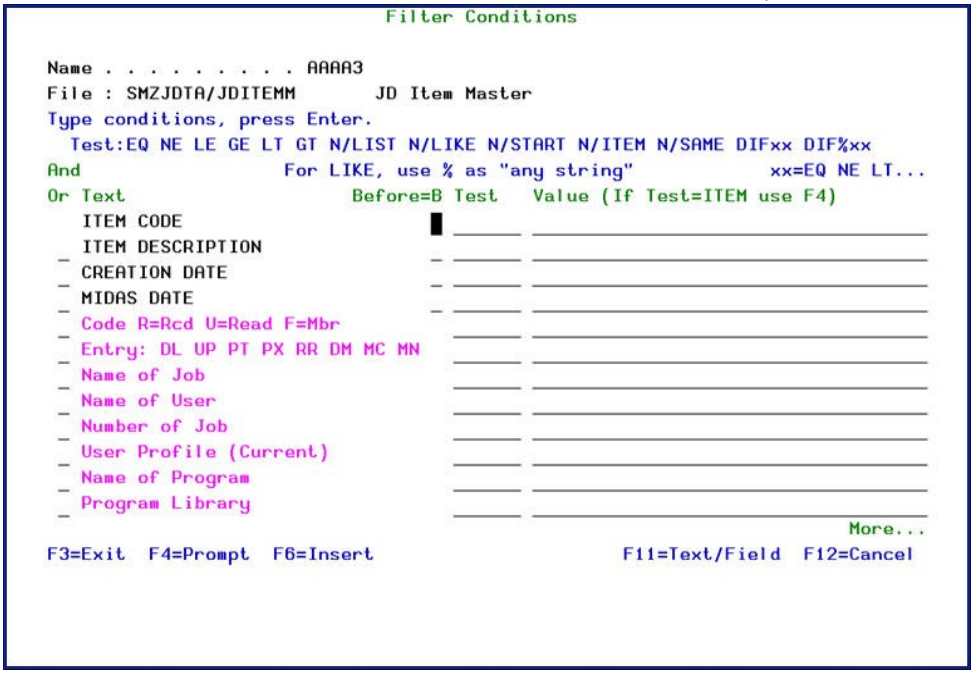
Include Filters

1. Type 3 in the Selection field to define filters to work with. The Define Include Filters screen appears..



Define Include Filters

2. Type 1=Select to select a file of a list and set a filter to define data to keep in containers.

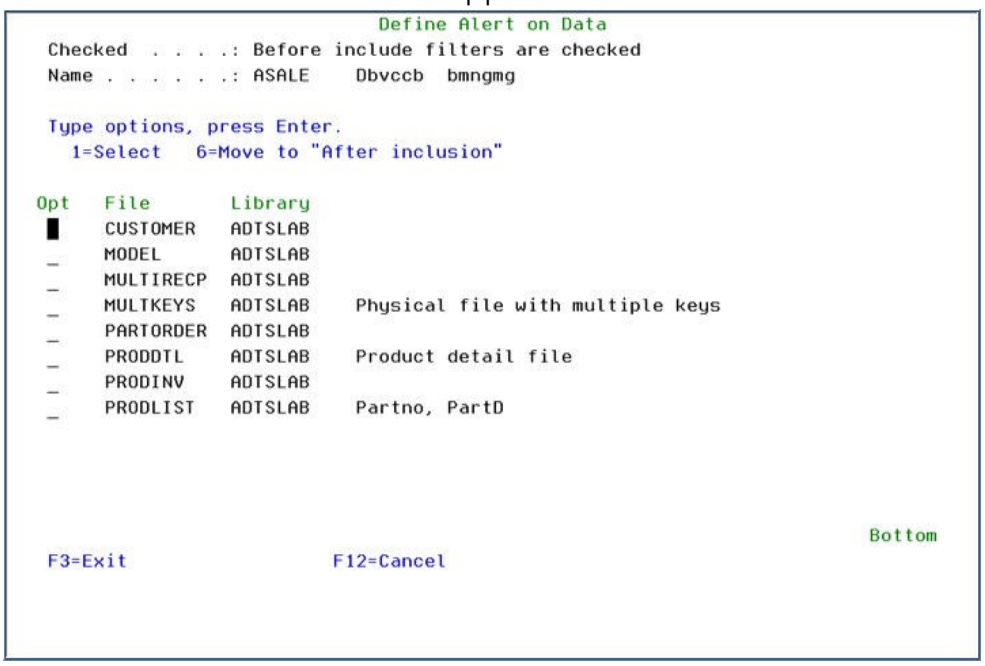


Filter Conditions

3. Set filter conditions and press Enter to confirm. The Add Application screen appears.

Alerts on data (after include filters)

1. Type 4 in the Selection field to select alerts to work with after the include filters were checked. The Define Alert on Data screen appears.

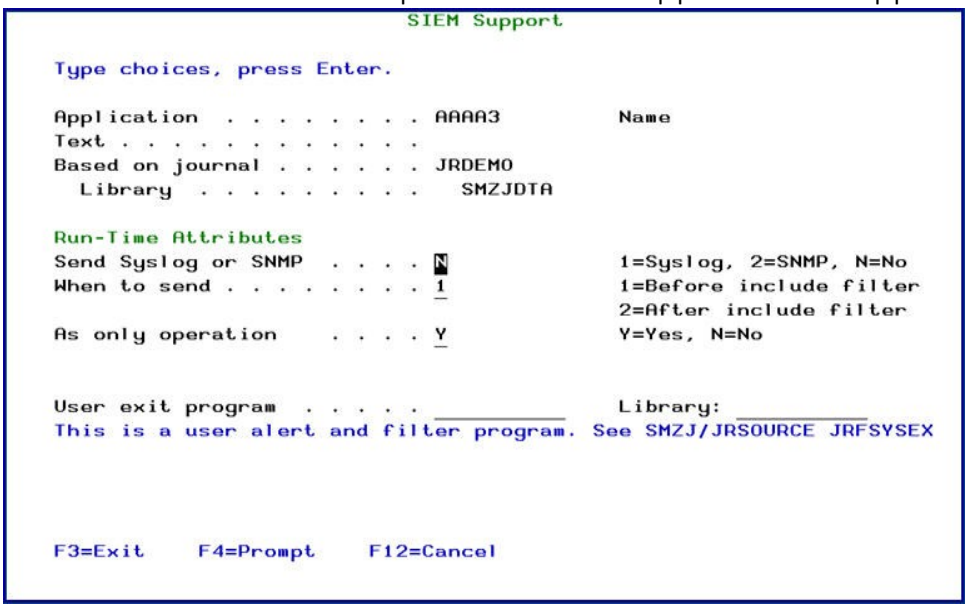


Define Alert on Data

2. Continue with the same steps as described in Alerts on data (before include filters) on page 57 .

Manages the specific application to be sent as a SYSLOG message or as SNMP traps (to define from where to send the messages, use option **21. Syslog Definitions** in the **iSecurity/Journal System Configuration** menu). The advantage of this feature is that the messages are sent as only as an operation; the data is not written to the containers and performance and disk space are not used.

1. Type6 in the Selection field to define SIEM support. The SIEMSupport screen appears.

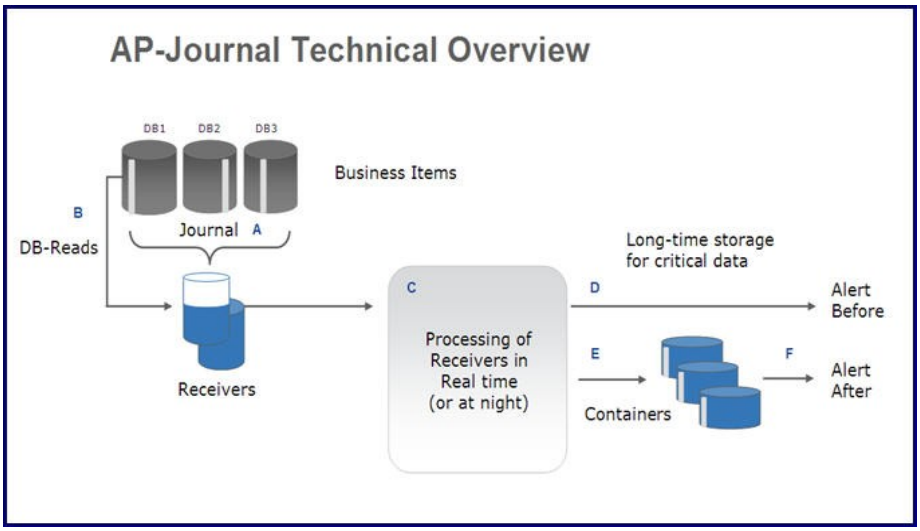


SIEM Support

2. Select the type of message to be sent, SNMP or Syslog.
3. Define whether to send the message before or after checking the include filter.
4. Define whether or not to send the message as an operation.
5. Define a User Exit Program to use.
6. Press Enter . The Add Application screen appears.

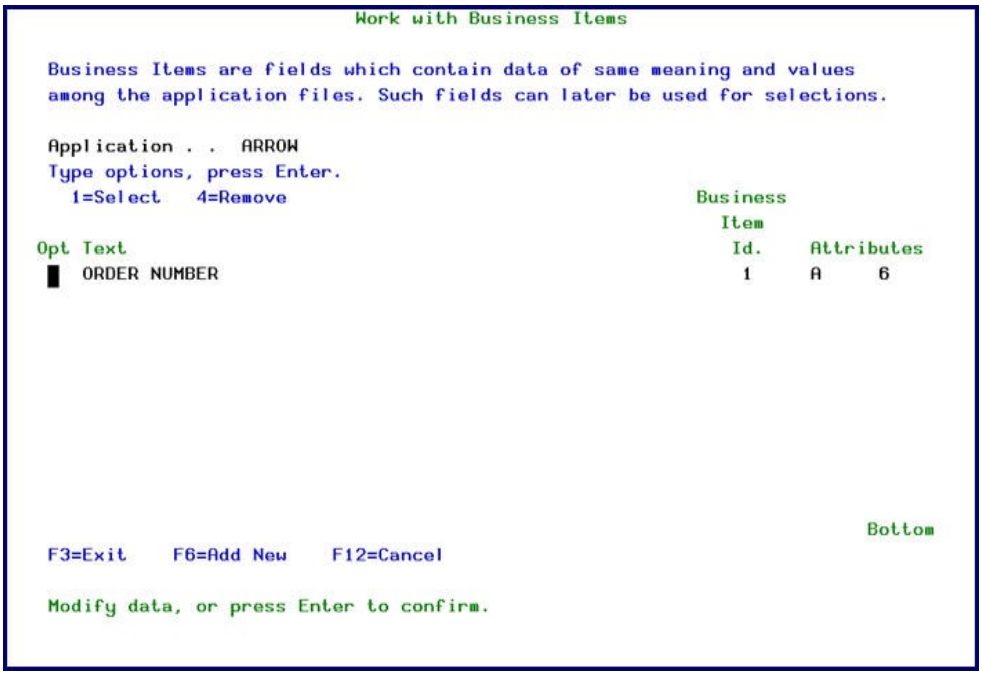
Define Business Items

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



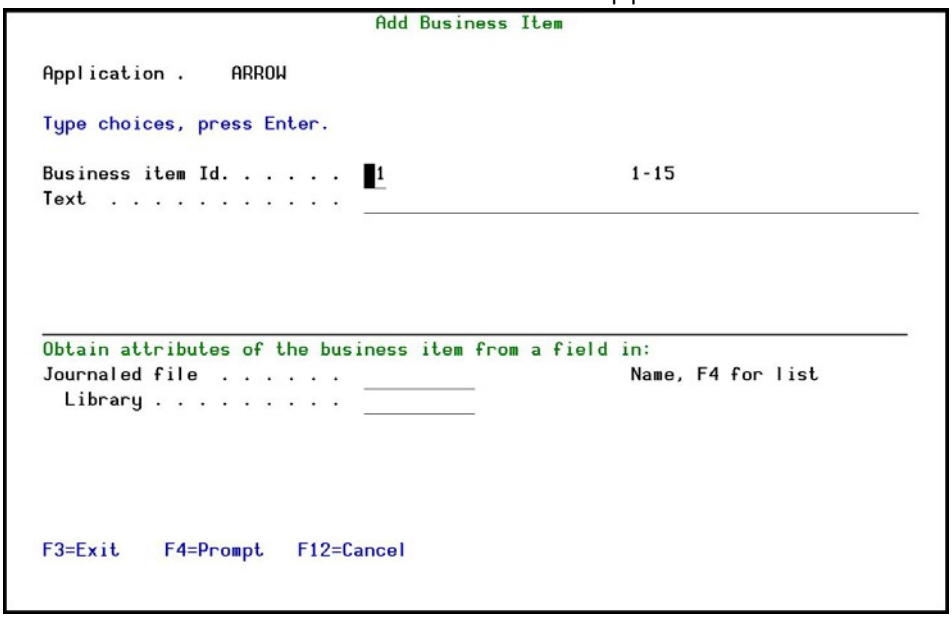
The white strips in the image represent the Business Items. Note that in the Database the Business Items are located on different places in each Database, and after the process procedure the Business Items are organized in the Containers.

1. Type 7 in the Selection field to select Business Items to work with. The Work with Business Items screen appears.



Work with Business Items

2. Press F6 to add a new action. The Add Business Item screen appears



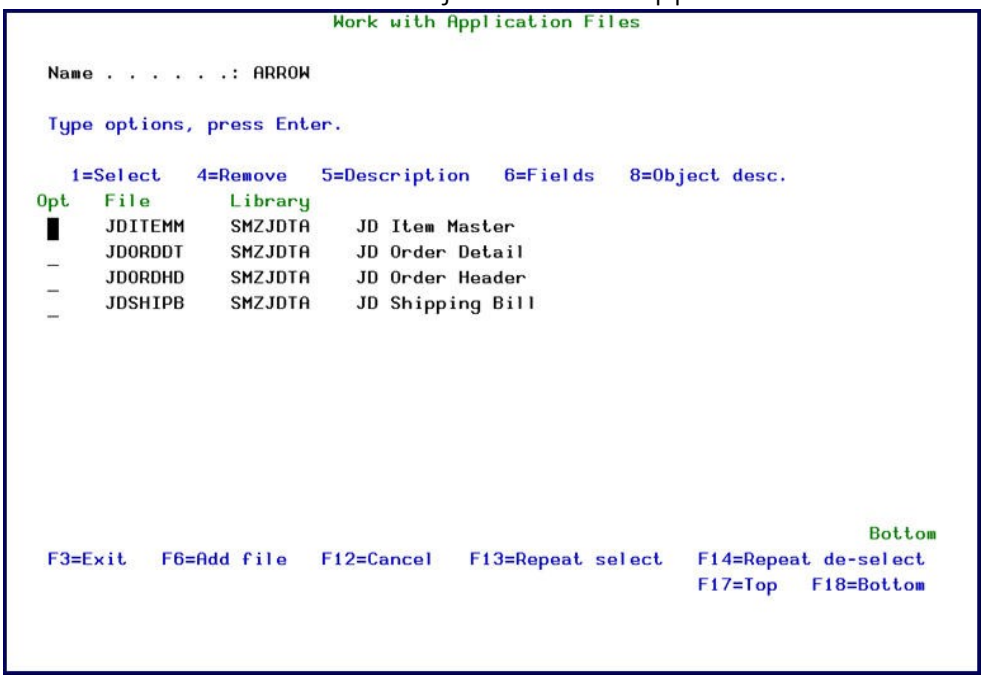
Add Business Items

3. Enter a unique Business Item ID for this Business Item in this application.

4. Enter a meaningful description Text for this Business Item.
5. Enter the File and Library from which attributes of the Business Item can be taken.
6. Press Enter . The Add Application screen appears.

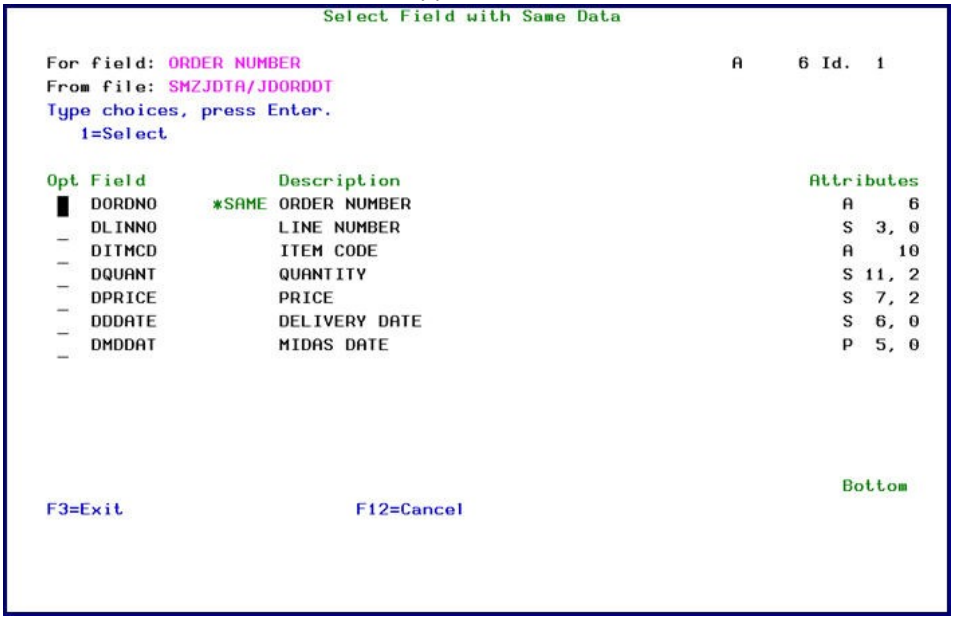
Identify Business Items in application files

1. Type 8 in the Selection field to identify Business Items to work with. The Work with Application Objects screen appears.



Work with Application Objects

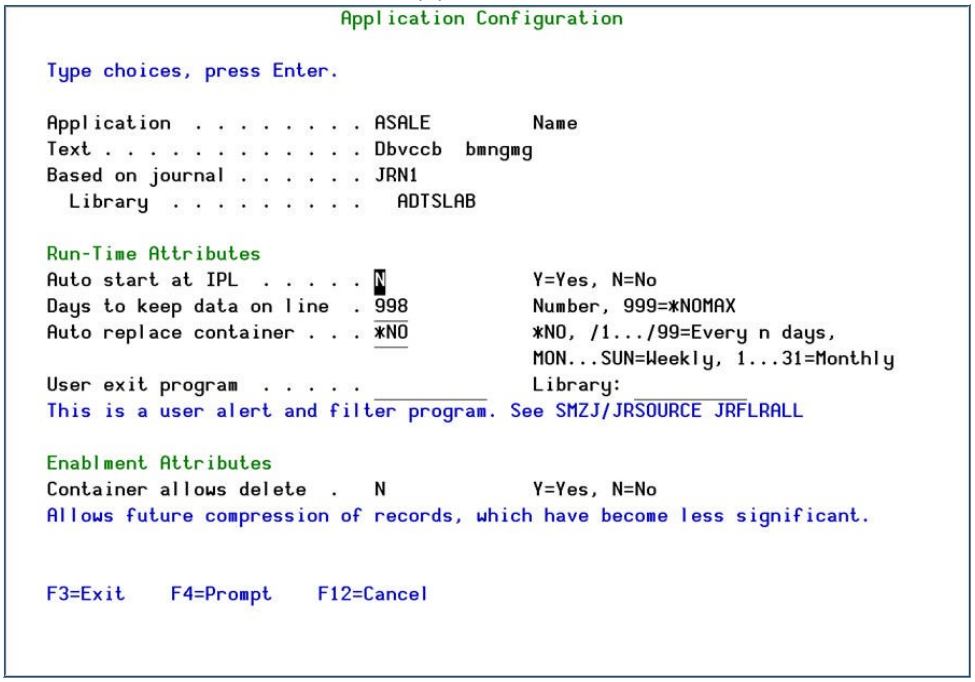
2. Type 1=Select to select files for the application



Select Field with Same Data

Configuration

1. Type 9 in the Selection field to configure the application. The Application Configuration screen appears.



Application Configuration

Parameter	Description
Auto start at IPL	Y=Yes N=No
Days to keep data on line	Define a retention period in days for the application data. 999 = *NOMAX
Auto replace container	Define when a container will be automatically replaced with a new one. *NO = no automatic replacement of the container /1 ... /99 = replace the container every nn days MON ... SUN = Replace the container weekly on the given day of the week 1 ... 31 = Replace the container monthly on the given day of the month
User exit program	Define a path to an alert and filter program.

Parameter	Description
Container allows delete	Y=Yes N=No

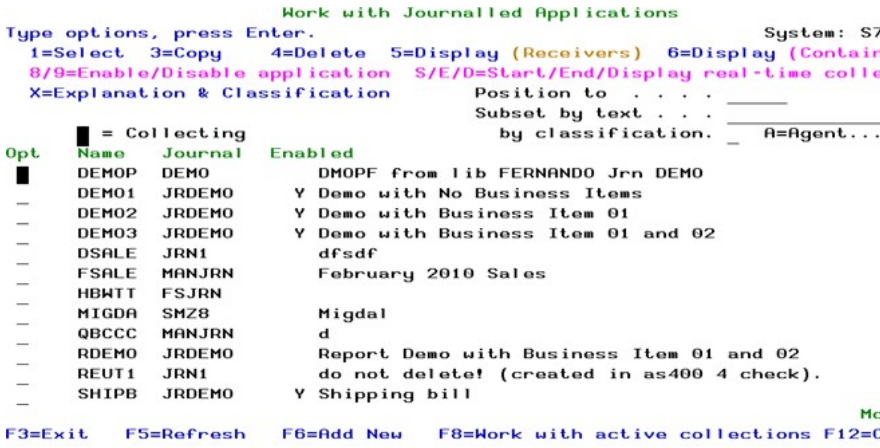
2. Enter your configuration parameters and press Enter . The AddApplication screen appears.

NOTE: Based on the Days to keep data on line and Auto replace container parameters, the AP-Journal daily maintenance program (JR#MNT) builds the SMZJYYMMDD libraries (one for each calendar date), and excess Data files (excess containers) are MOVED into it. It is the customer's responsibility to backup/delete these libraries; Raz-Lee provides a template program for the backup.

If you do not want containers to be replaced or libraries to be built, set

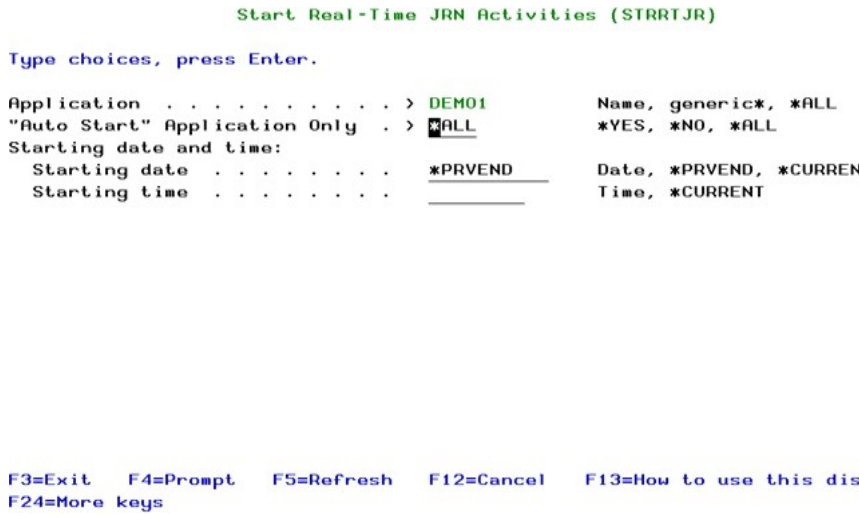
Days to keep data on line to 999 and Auto replace container to NO.

Activation 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.



Work with Journaled Applications

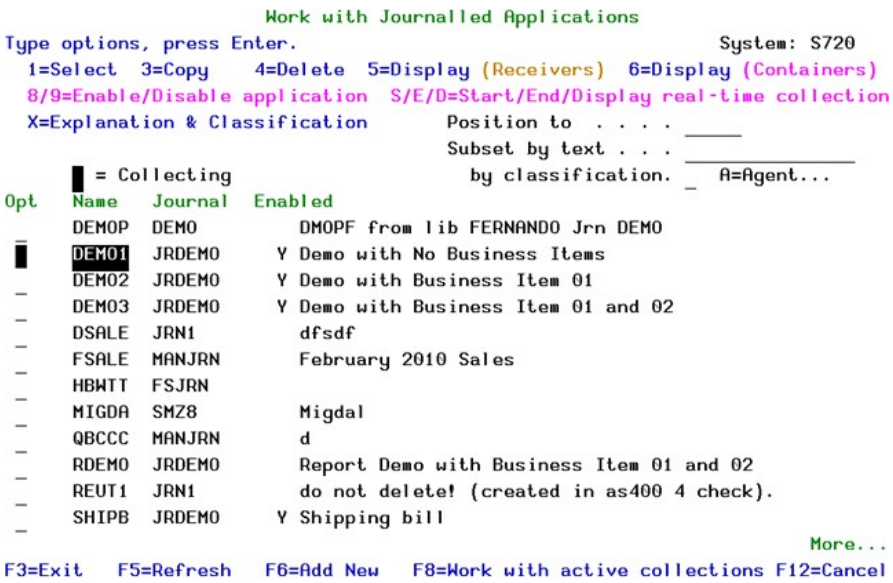
Type S to Start a specific application. The application reads the definition file and builds a subsystem which collects the data. The Start Real-Time JRN Activities (STRRTJR) screen appears.



Start Real-Time JRN Activities (STRRTJR)

NOTE: *prvend = from beginning of available data or from today
Select a starting date and time and press **Enter** to confirm.

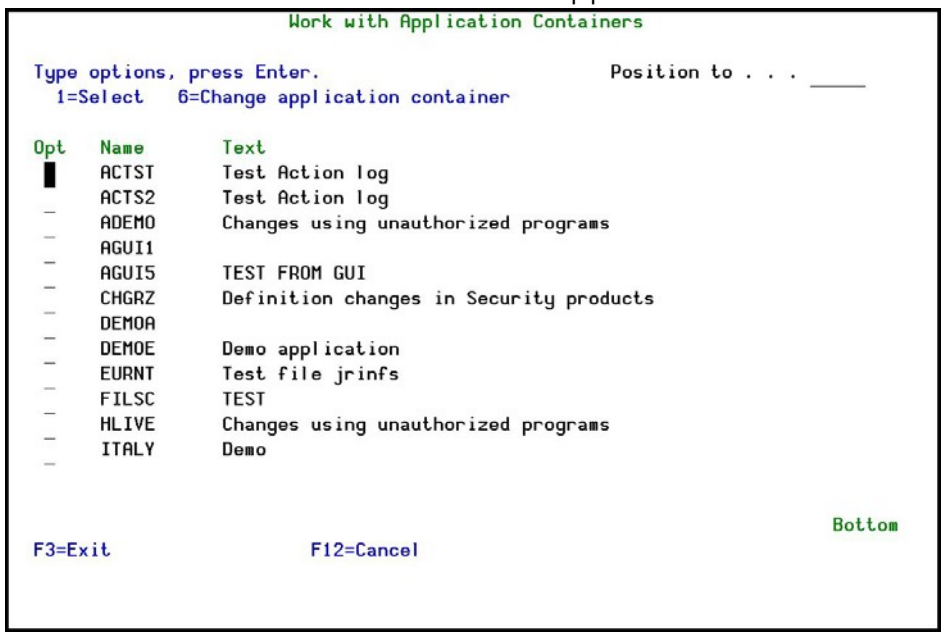
The application will appear activated with a highlighted background.



Work with Containers

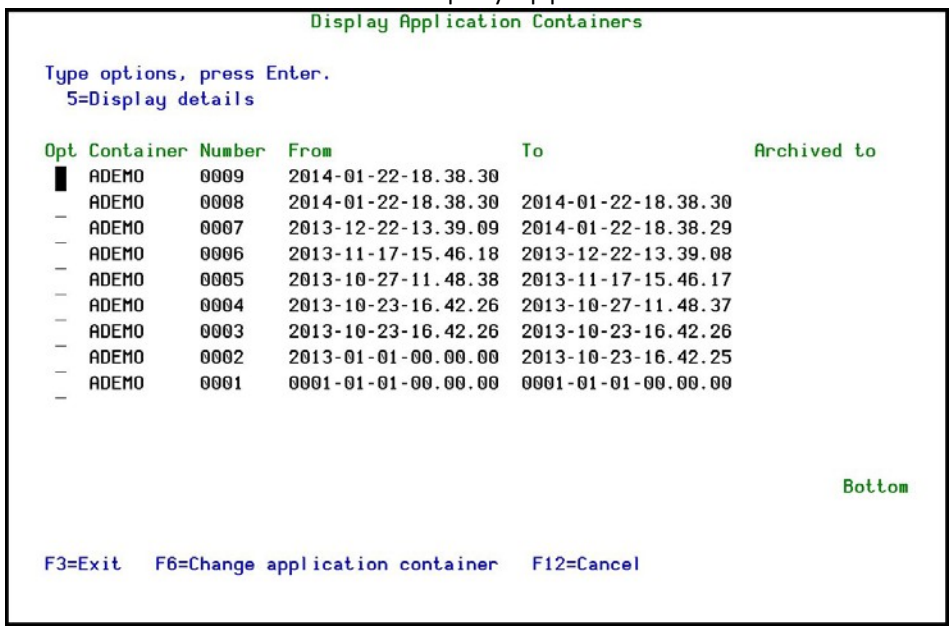
The journal information is stored in containers. This option allows you to manipulate the containers.

1. Select 5. Work with Containers from the Applications, BizAlerts - Definitions menu. The WorkwithApplicationContainers screen appears.



Work with Application Containers

2. Select an application, type 1 and press Enter . The DisplayApplication Containers screen appears.



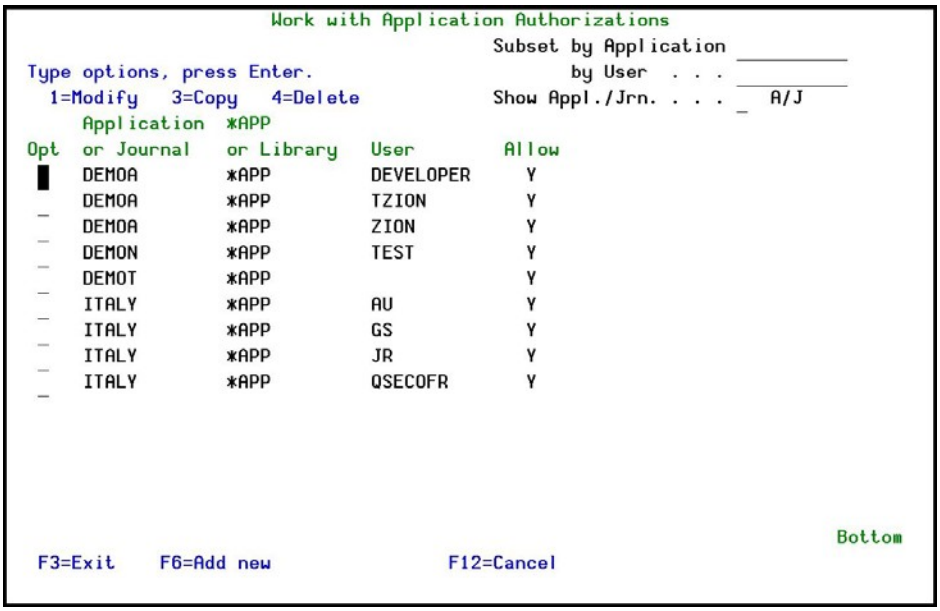
Display Application Containers

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

Allow applications to users

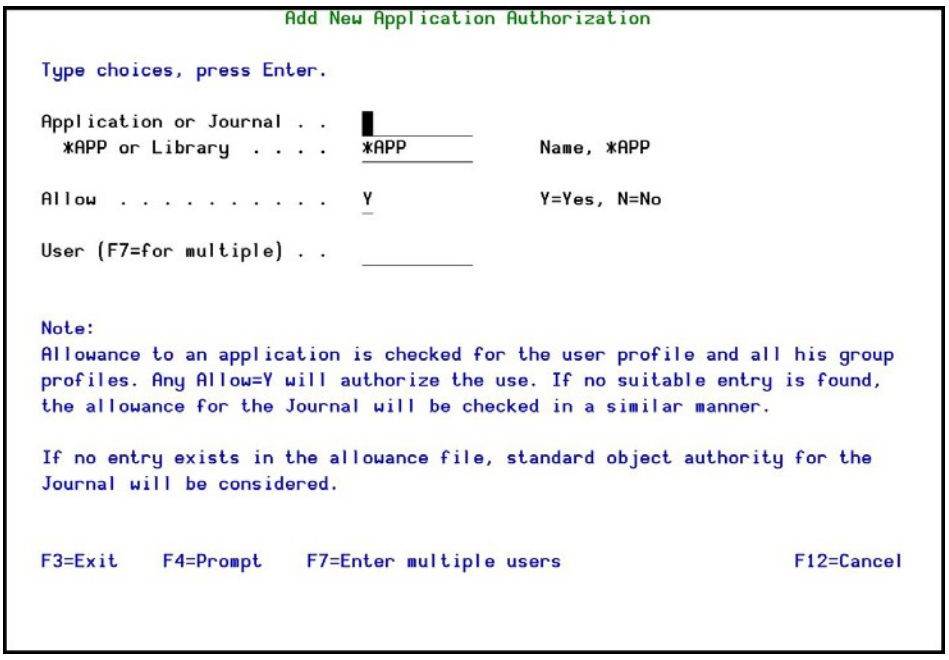
Use this option to authorize your journal applications to specific users.

1. Select 9. Allow applications to users from the Applications, BizAlerts- Definitions menu. The Work with Application Authorizations screen appears.



Work with Application Authorizations

2. Press F6 to add authorizations. The Add New ApplicationAuthorization screen appears.



Add New Application Authorization

Parameter	Description
Application or Journal	Type the name of the Application or Journal to be authorized.
*APP or Library	Name *APP =
Allow	Y = Yes N = No
User	Enter the name of the user. Use F7 to enter multiple users.

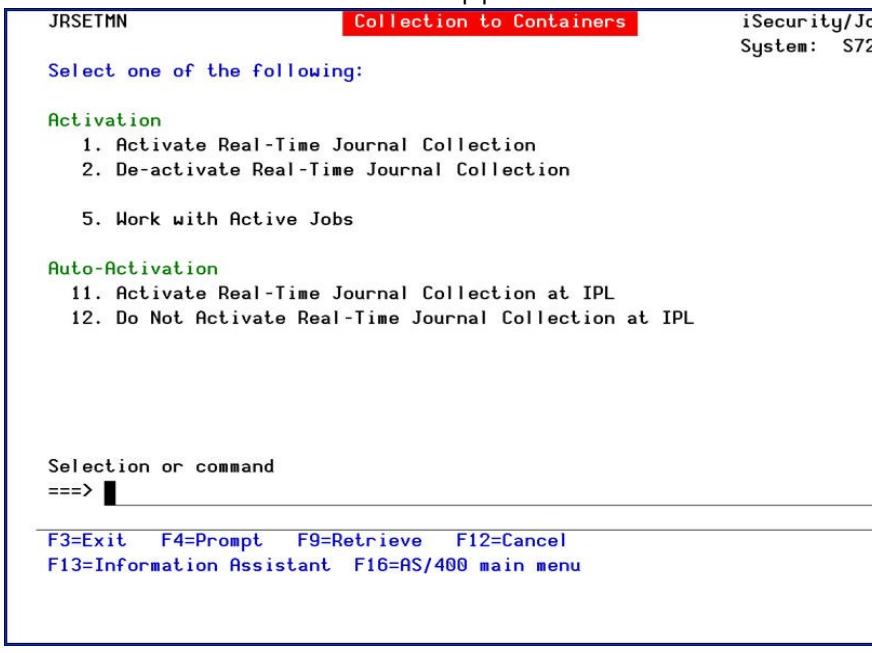
3. Enter your parameters and press Enter .

Process Information

NOTE:

Activation
This option activates and starts all enabled applications.

1. Select 11. Activation from the Applications,BizAlerts-Definitions menu. The Collection to Containers menu appears.

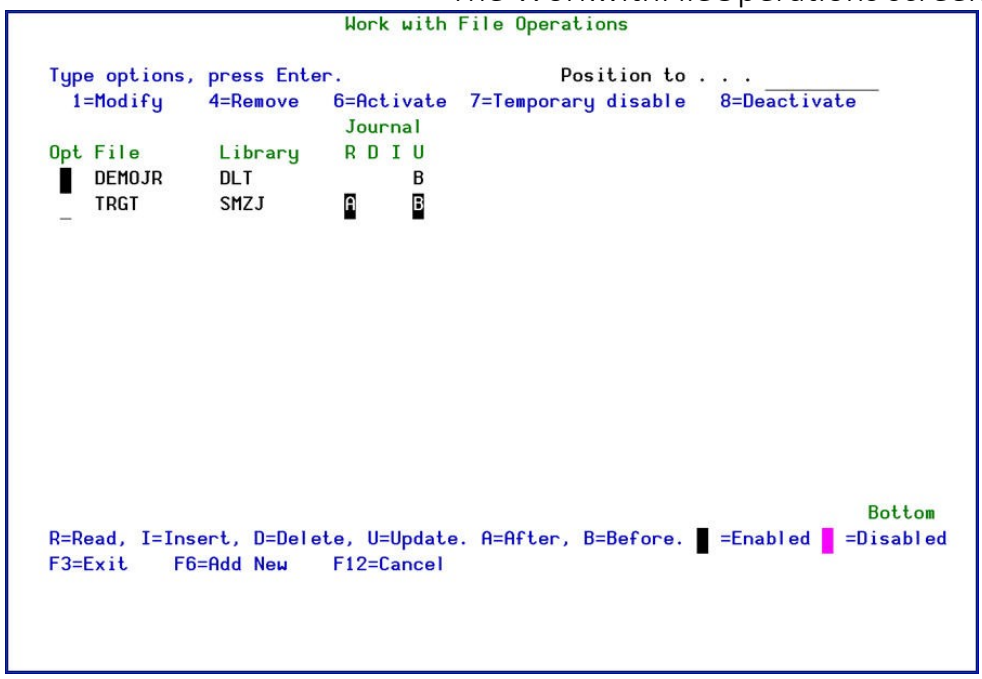


Collection to Containers

2. Select 1. Activate Real-Time Journal Collection to start the application real- time journaling, and press Enter .
3. Select 11. Activate Real-Time Journal Collection at IPL and press Enter .
4. Select 5. Work with Active Jobs and make sure the job is active.Each applica- tion will appear in a different job.

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

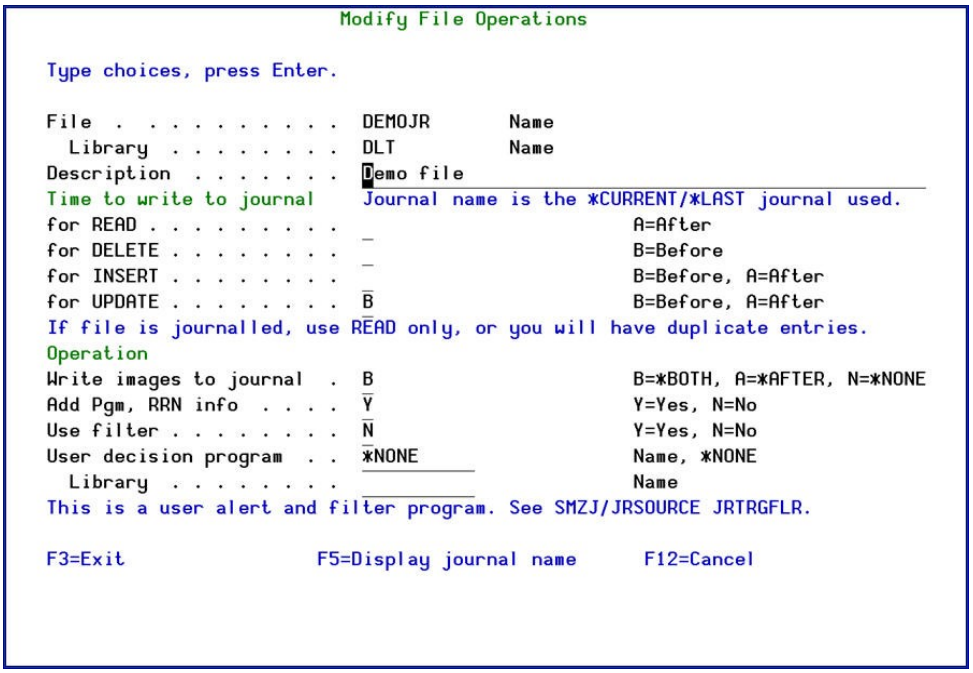
1. Select 15. Collect READs by DB Triggers from the Applications, BizAlerts-Definitions menu. The WorkwithFileOperations screen appears.



Work with File Operations

The file operations are activate if the journal definitions in the screen are white on a black background (as in the second row), and not activate if the definitions are black on a white box (as in the first row). If the letters are pink, the file operations are temporarily disabled.

2. Press F6 to add a new file or type 1 to modify an existing one. The ModifyFile Operation screen appears.



Modify File Operations

Option	Parameters
File	Name of file
Library	Name of file's library
Description	Descriptive text
Time to write to Journal	For each type of change (Read, Delete, Insert, Update) A =After change B =Before change

Option	Parameters
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, RRN info	Y =Yes N =No
Use filter	Y =Yes N =No
User decision program	Name=Name of program *NONE
Library	Library of program

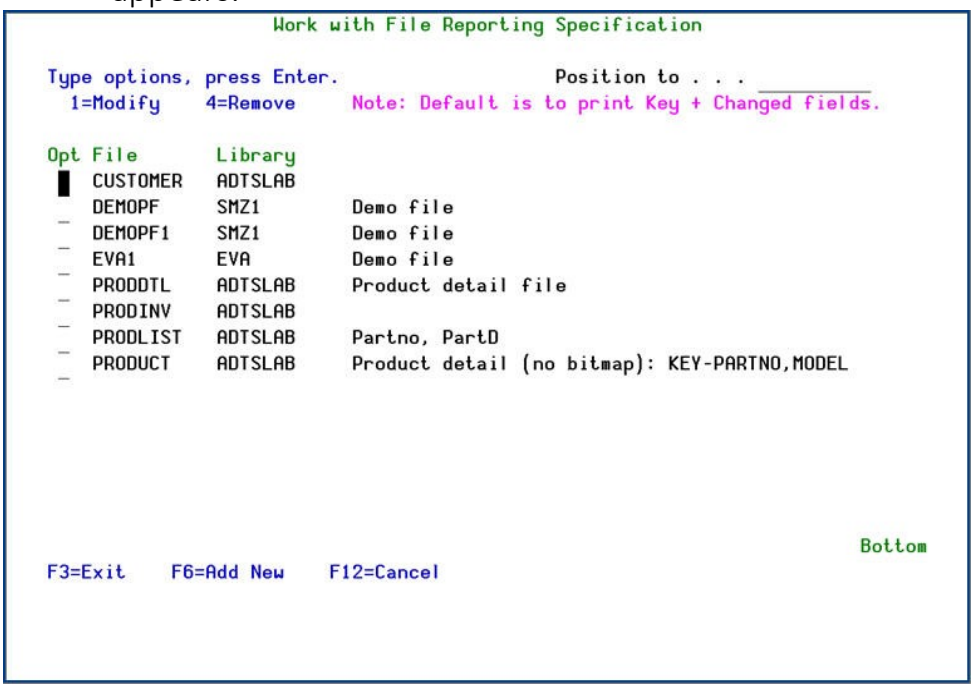
Structure Setup

Define the fields you want to see in reports and how to display them

Output Fields per File

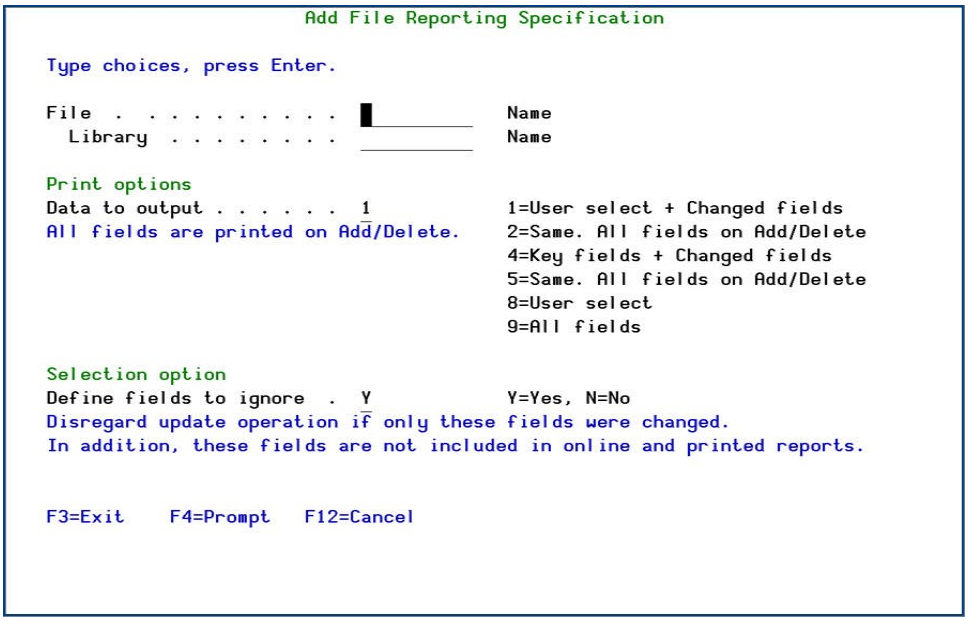
Select which fields you want to display in the report.

1. Select 51. Output Fields per File from the Applications, BizAlerts - Definitions menu. The WorkwithFileReportingSpecification screen appears.



Work with File Reporting Specification

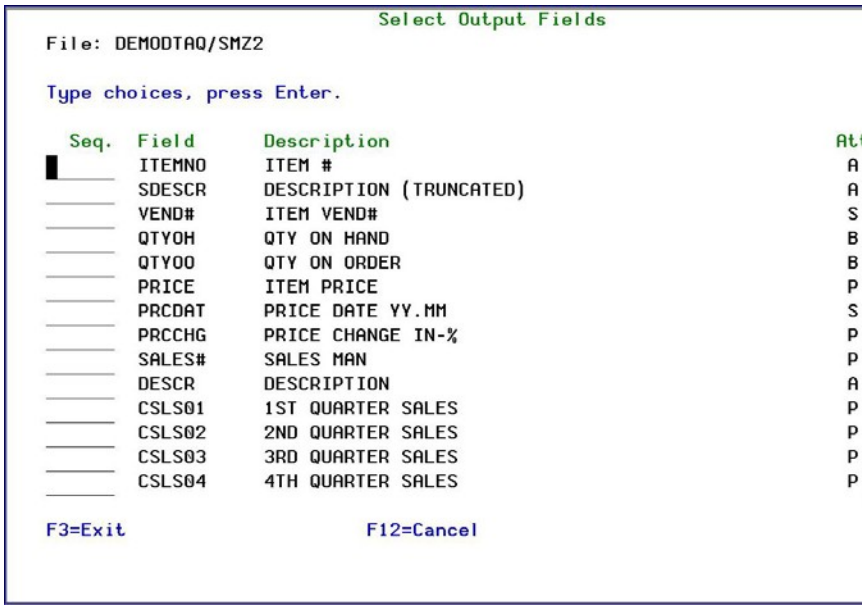
2. Press F6 to add a new file. The AddFileReportingSpecification screen appears.


Add File Reporting Specification
Type choices, press Enter.
File . . . . . Name
Library . . . . . Name
Print options
Data to output 1
1=User select + Changed fields
All fields are printed on Add/Delete.
2=Same. All fields on Add/Delete
4=Key fields + Changed fields
5=Same. All fields on Add/Delete
8=User select
9=All fields
Selection option
Define fields to ignore . Y
Y=Yes, N=No
Disregard update operation if only these fields were changed.
In addition, these fields are not included in online and printed reports.
F3=Exit
F4=Prompt
F12=Cancel

Add File Reporting Specification

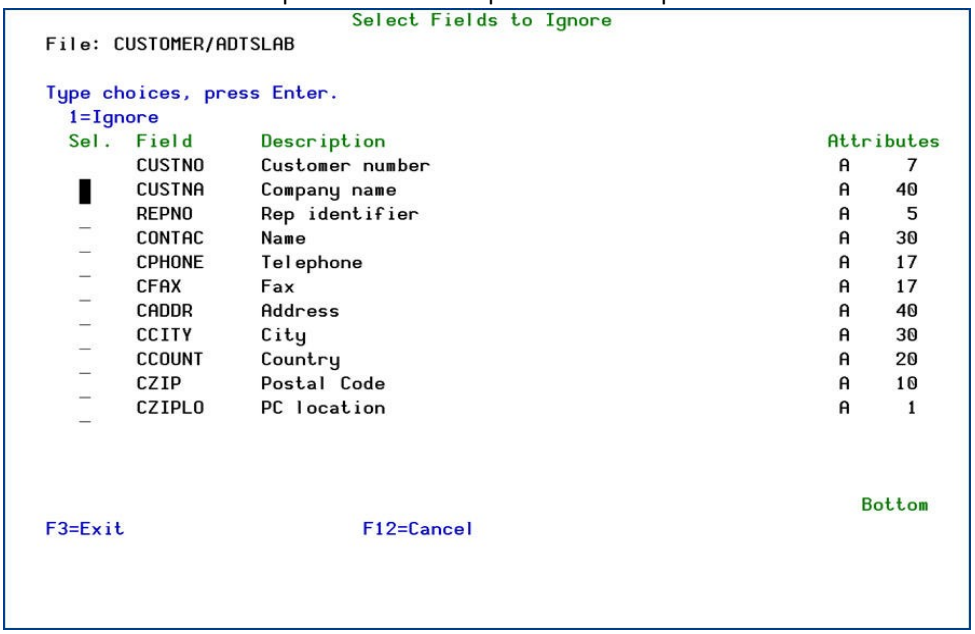
Option	Description
File/Library	The file to be reported and its library. If you just enter the library, you can use F4 to select from a list of the files in the library.
Data to output	Select fields to output: 1 =User selected fields and all changed fields. 2 =User selected fields and all changed fields. 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
Define fields to ignore	Y =Define fields whose changes will be ignored N = No ignore fields are defined
Define data conversions	Y =Define fields which should be converted for external display N =No fields are converted

3. Define your parameters and press Enter to continue. If relevant, the Select Output Fields screen appears.



Select Output Field

4. Set the Output Fields sequence and press Enter to confirm.



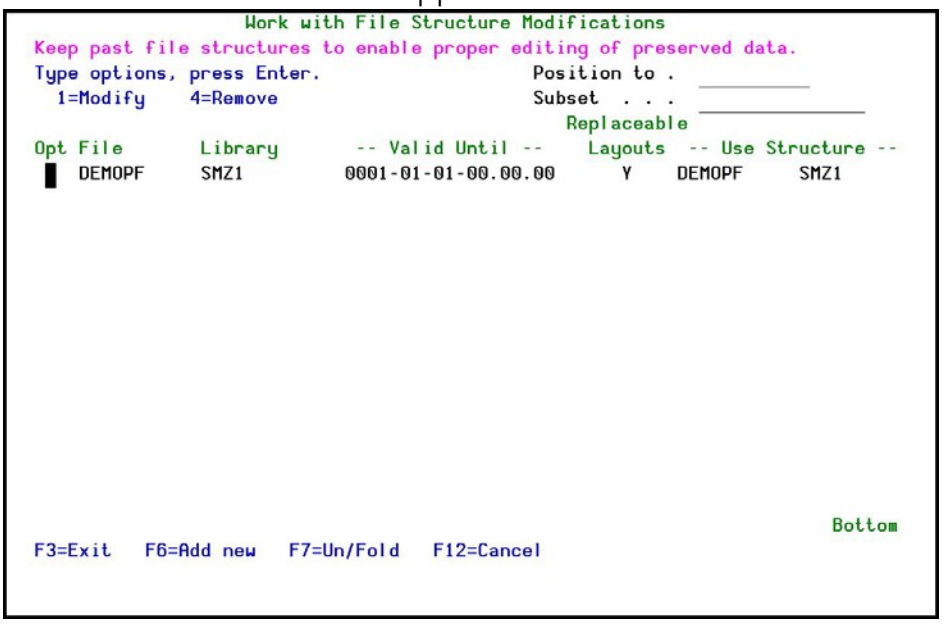
Select Fields to Ignore

5. If relevant, define fields to be ignored and press Enter to confirm.
6. If relevant, define the Data Conversion fields and press Enter to confirm.

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.

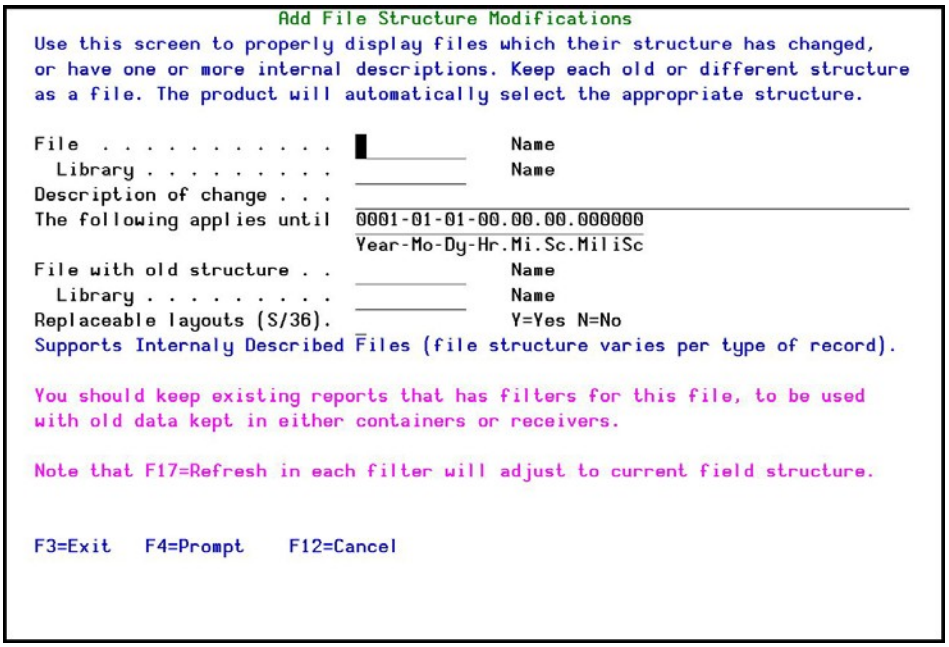
You should keep existing reports that have filters for these files, to be used with old data kept in either containers or receivers.

1. Select 52.FileStructureModifications from the Applications,BizAlerts- Definitions menu. The Work with File Structure Modifications screen appears.



Work with File Structure Modifications

2. Type 1 to modify an existing definition or press F6 to add a new one. The Add File Structure Modifications screen appears.



Add File Structure Modifications

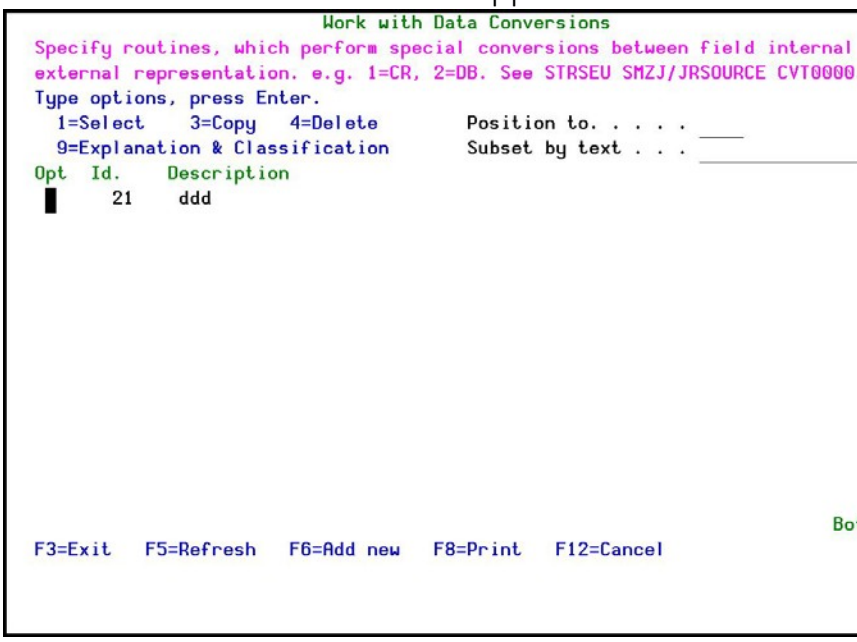
Option	Description
File/Library	The file to be modified and its library. If you just enter the library, you can use F4 to select from a list of the files in the library.
Description of change	Enter a meaningful description of the reason the file changed
The following applies until	The date until which 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 which has no expiry date
File/Library with old structure	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.

Option	Description
Replaceable layouts (S/36)	Y = Yes N = No

3. Enter your parameters and press Enter .

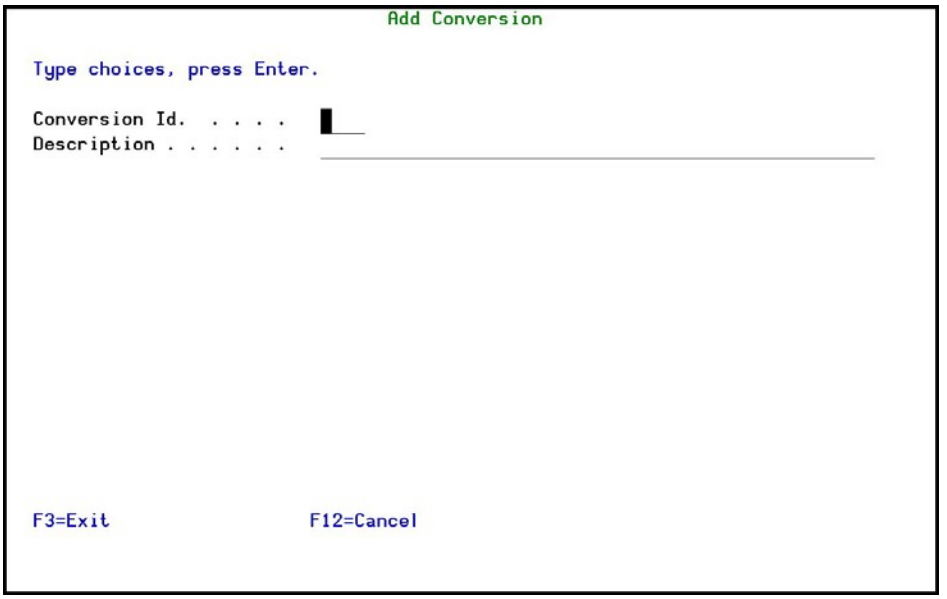
You can define routines which will convert fields from their internal representation to an acceptable external representation before they are displayed in journals. For example, you might convert a date field that is stored in YYYYMMDD format to be displayed in DD/ MM/YYYY format. The conversion routine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

1. Select 55. Data conversions from the Applications, BizAlerts - Definitions menu. The WorkwithDataConversions screen appears.



Work with Data Conversions

2. Type 1 to modify an existing definition or press F6 to add a new one. The Add Conversion screen appears.



Journal Objects Care

Add Conversion

3. Enter the four digit ConversionID that you used in the conversion routine name, a meaningful Description and press Enter .
4. You can also use option 9 in the WorkwithDataConversions screen to add an Audit Explanation andClassification .

Plan how to journal files and libraries.

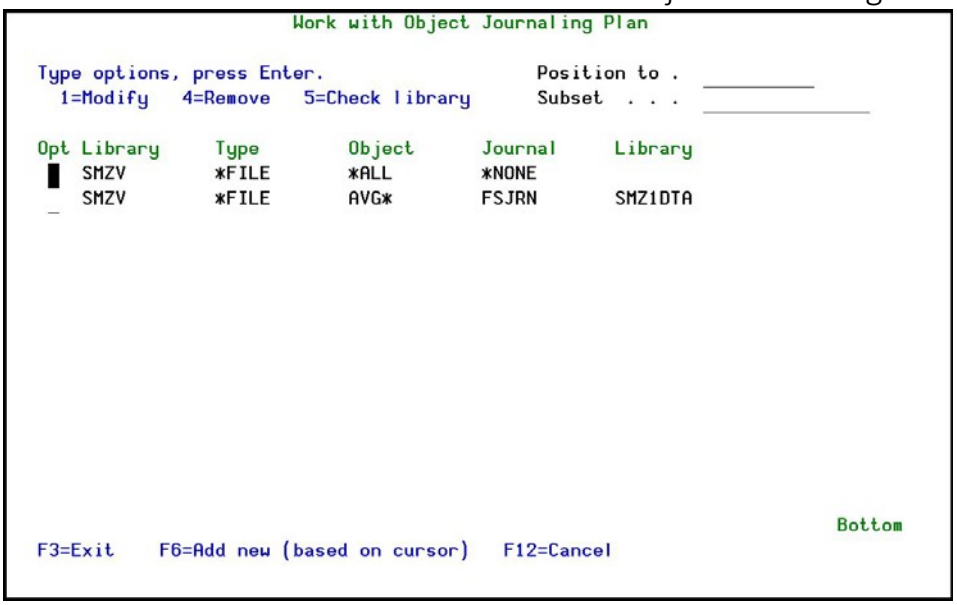
Plan Object Journaling

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.

Create Plan

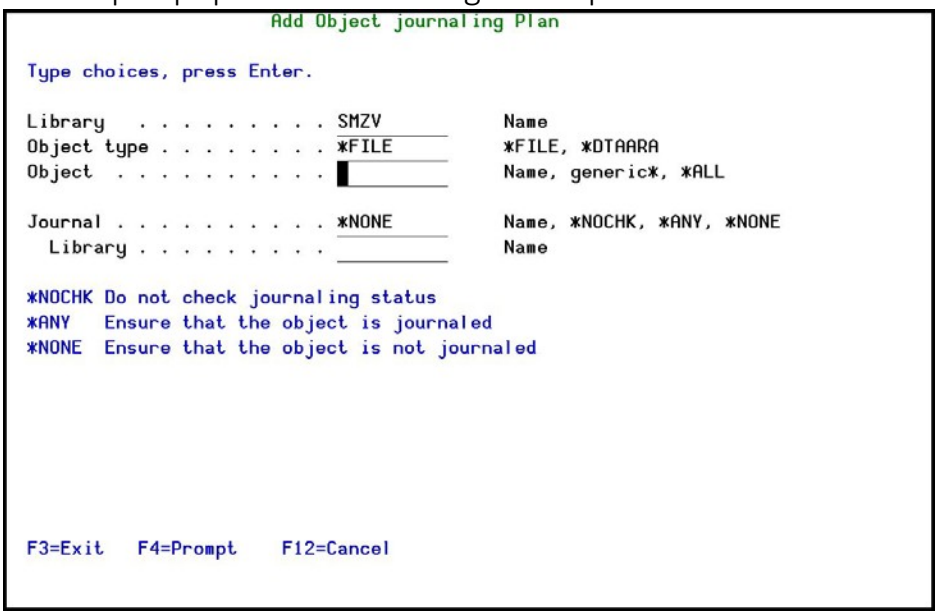
To create a journaling plan:

1. Select 71. Plan Object Journaling from the Applications, BizAlerts-Definitions menu. The Work with Object Journaling screen appears.



Work with Object Journaling Plan

2. Type 1 to modify an existing definition or press F6 to add a new one. The Add Object Journaling Plan screen appears. Some fields will be pre-populated according to the position of the cursor.



Add Object Journaling Plan

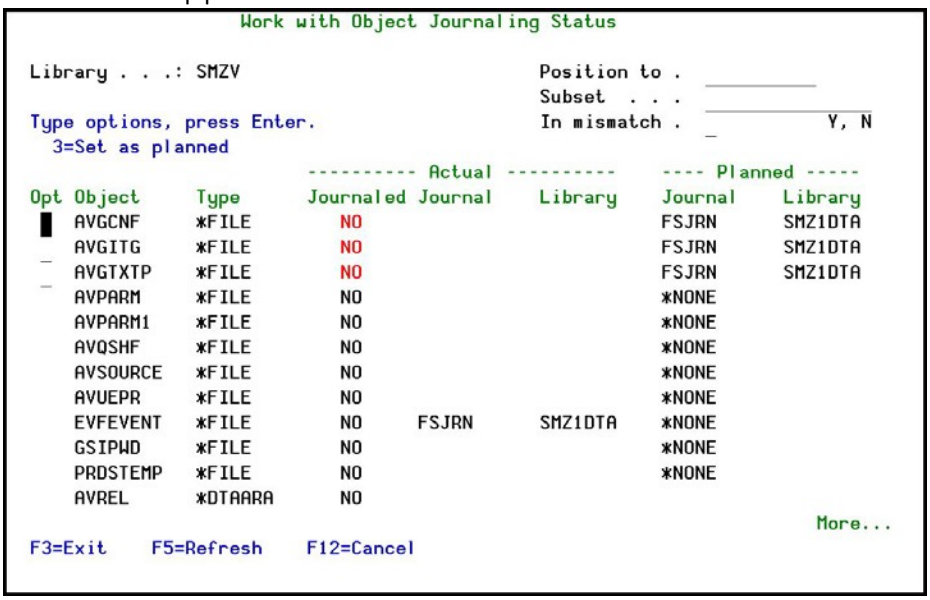
Option	Description
Library	The file that contains the object you want to journal.
Object Type	*FILE *DTAARA
Object	Name = The name of the object you want to journal generic* = A group of objects you want to journal. For example, to journal all files that begin with MAS, enter MAS* *ALL = Journal all 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

3. Enter your parameters and press Enter .

Set Actual as Planned

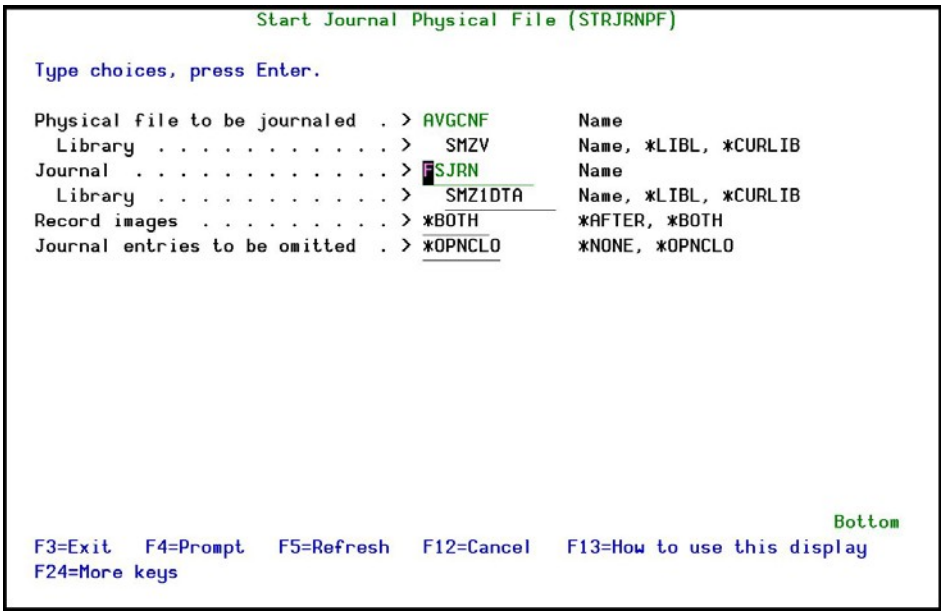
To set a journaling plan to actual for a given library:

1. Select 71. Plan Object Journaling from the Applications, BizAlerts- Definitions menu. The Work with Object Journaling screen appears.
2. Type 5 by any of the plan entries for the selected library. The WorkwithObject Journaling Status screen appears.



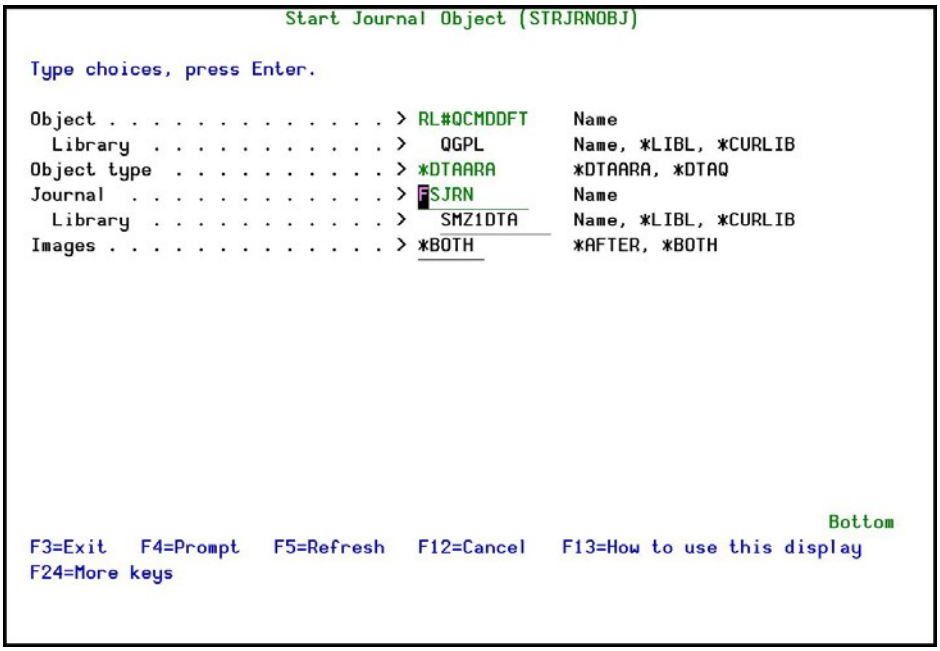
Work with Object Journaling Status

3. Type 3 by the object to be journaled. The Start Journal Physical File screen appears for files and the Start Journal Object screens for data areas.



Start Journal Physical File

Option	Description
Physical file to be journaled	The file you chose
Library	The library of the file you chose
Journal	The journal to receive the journal entries
Library	The library that contains the journal
Record images	*AFTER = Only record the after images *BOTH = Record both the before and after images
Journal entries to be omitted	*OPNCLO = Do not record the file opening and closing actions. *NONE = All actions are recorded.



Start Journal Object

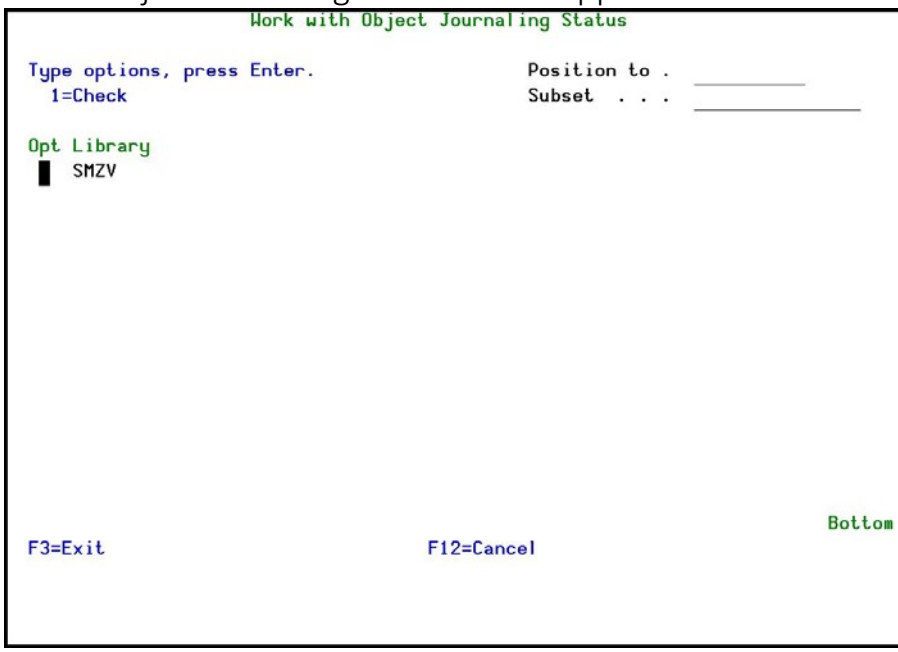
Option	Description
Object	The object you chose
Library	The library of the object you chose
Object type	Always *DTAARA
Journal	The journal to receive the journal entries
Library	The library that contains the journal
Images	*AFTER = Only record the after images *BOTH = Record both the before and after images

4. Enter your parameters and press Enter .
5. Repeat this procedure for every object to be journalled.

Check Object Journaling

You can check which libraries have objects with journal plans.

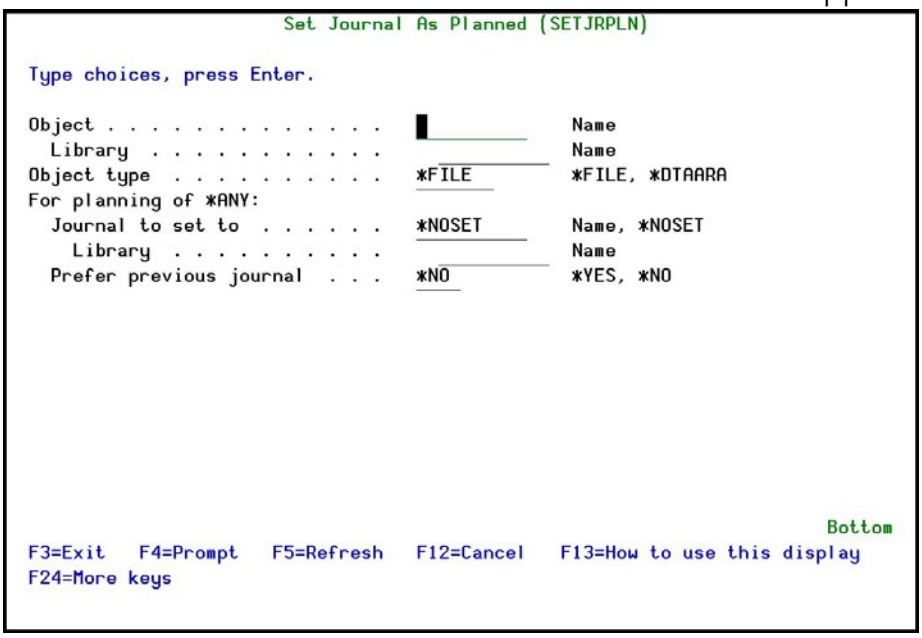
1. Select 72. Check Object Journaling from the Applications, BizAlerts - Definitions menu. The WorkwithObjectJournalingStatus screen appears.



2. Type 1 to check the status of the objects of a specific library. The Work with Object Journaling Status screen appears, (see Work with Object Journaling Status).
   You can set the actual journal status of objects on this screen to be the planned status, as described from Step 3 onwards in procedure Set Actual as Planned on page 95.

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

1. Select 73. Set Journal As Planned from the Applications, BizAlerts- Definitions menu. The Set Journal As Planned screen appears.



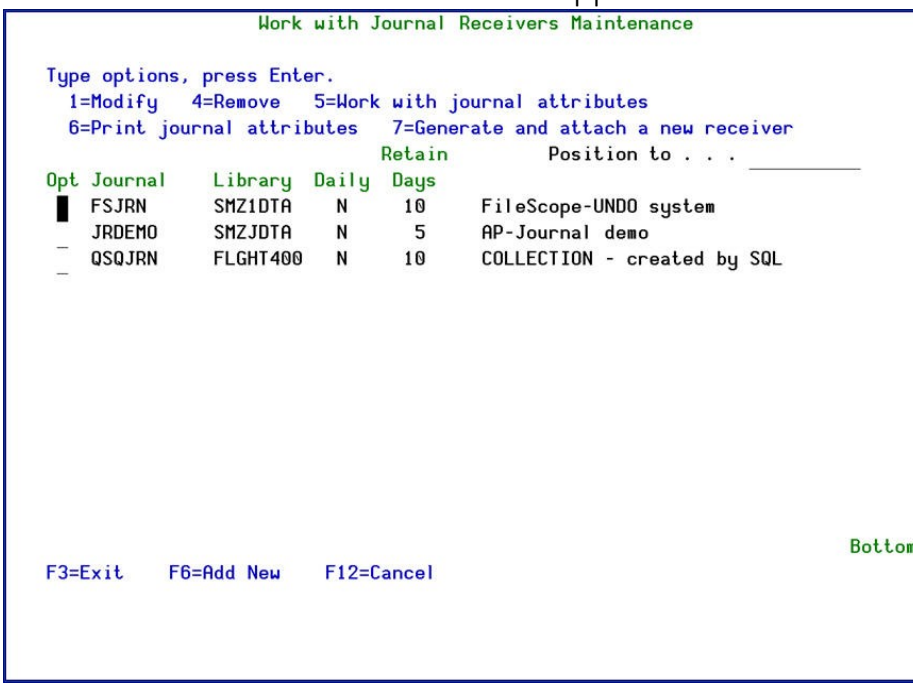
Set Journal As Planned

Option	Description
Object	The object you chose
Library	The library of the object you chose
Object type	Always *DTAARA
Journal to set to	The journal to receive the journal entries
Library	The library that contains the journal
Prefer previous journal	*YES *NO

2. Enter your parameters and press Enter .

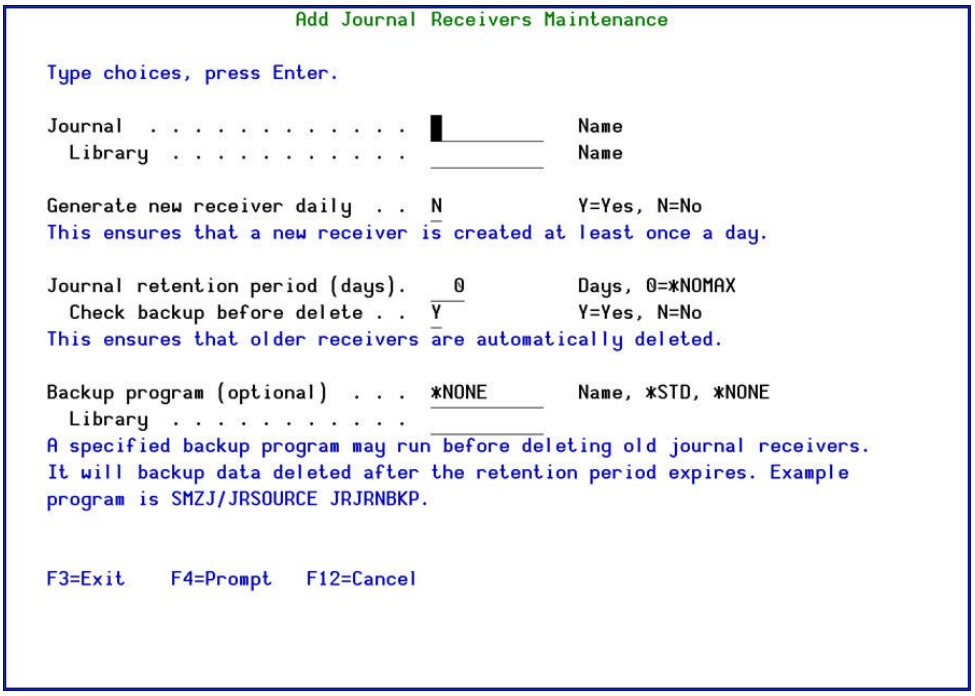
Receiver Auto Maintenance

1. To work with IBM Journal Receivers, select 75. Receiver Auto Maintenance . The Work with Journal Receivers Maintenance screen appears.



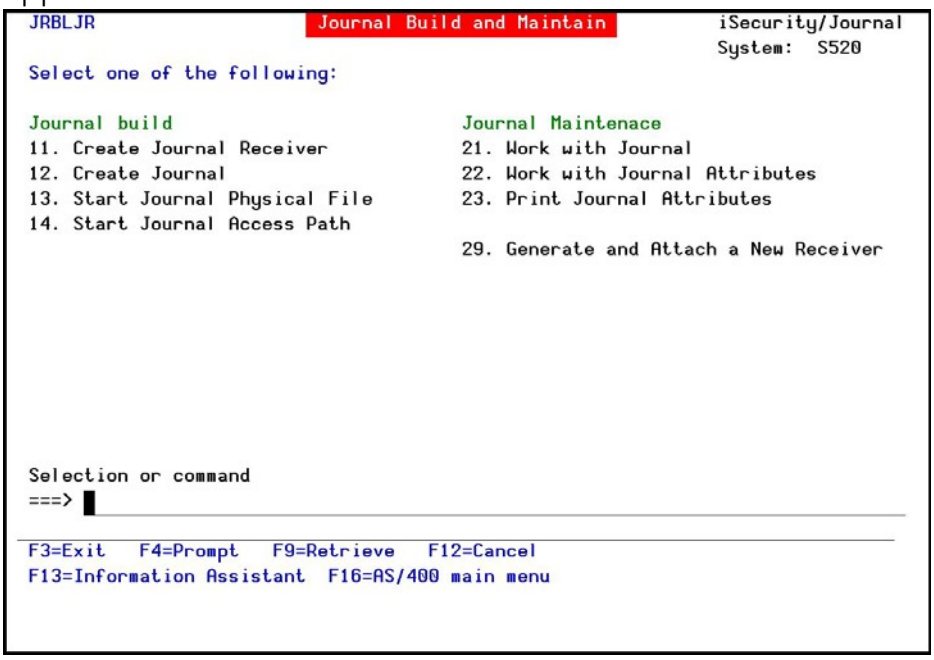
Work with Journal Receivers Maintenance

2. If this screen is empty, press F6 to add new Journal Receivers to the maintenance.



Add Journal Receivers Maintenance

You can use this option to access a number of standard journal commands all from the same menu. To access the menu, select 79.BuildingJournalsandReceivers . The Journal Build and Maintain menu appears.

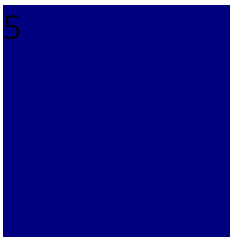


The following options are available:

- Journal Build
  - 11. Create Journal Receiver - runs the Create Journal Receiver (CRTJRNRCV) command
  - 12. Create Journal - runs the Create Journal (CRTJRN) command
  - 13. Start Journal Physical File - runs the Start Journal Physical File (STRJRNPF) command
  - 14. Start Journal Access Path - runs the Start Journal Access Path (STRJRNAP) command

- Journal Maintenance
    - 21. Work with Journal
    - 22. Work with Journal Attributes - runs the Work with Journal Attributes (WRKJRNA) command
    - 23. Print Journal Attributes - runs the Work with Journal Attributes (WRKJRNA) command
    - 29. Generate and Attach a New Receiver- runs the Change Journal (CHGJRN) command

For full details of the available parameters for each command, see the appropriate IBM documentation.



Working with Report Schedule

Chapter 5: Working with Report Scheduler

Report Scheduler

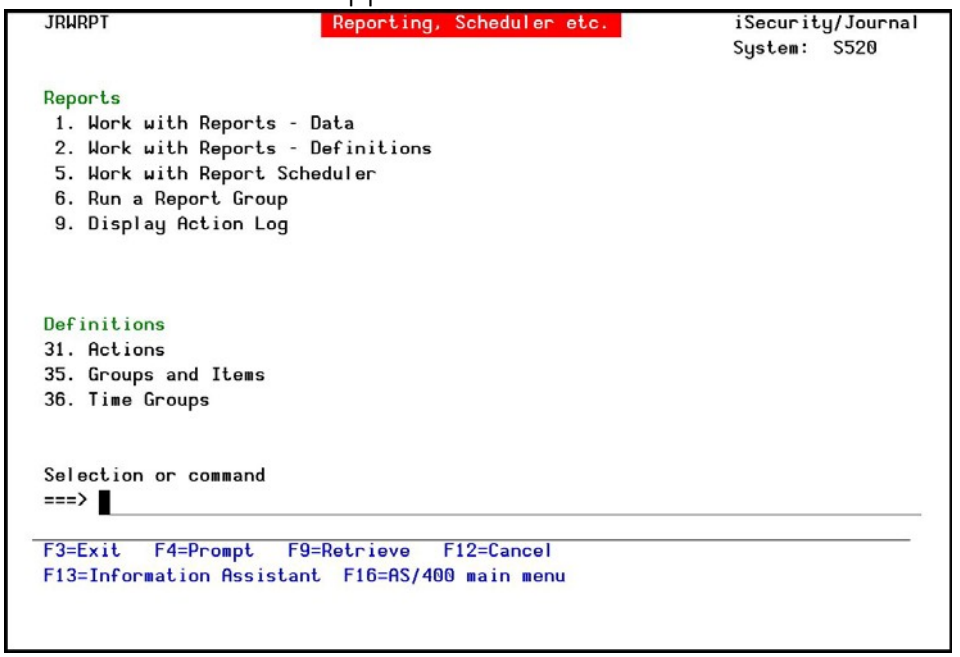
The Report Scheduler allows you to run pre-defined “report groups” automatically according to a fixed schedule.

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.

The first step in the Report Scheduler definition process is to define the report group. The report group definition consists of a group name, description and several run time parameters that apply to each report in the group.

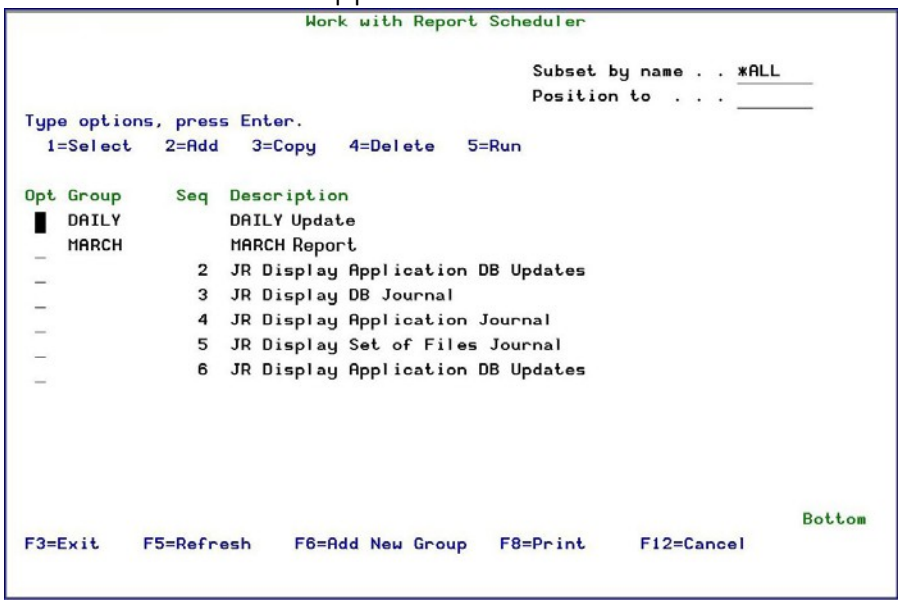
Define Report Schedules

1. Select 12.Reports,Scheduleretc. from the ApplicationJournal main menu. The Reporting, Scheduler etc. menu appears.



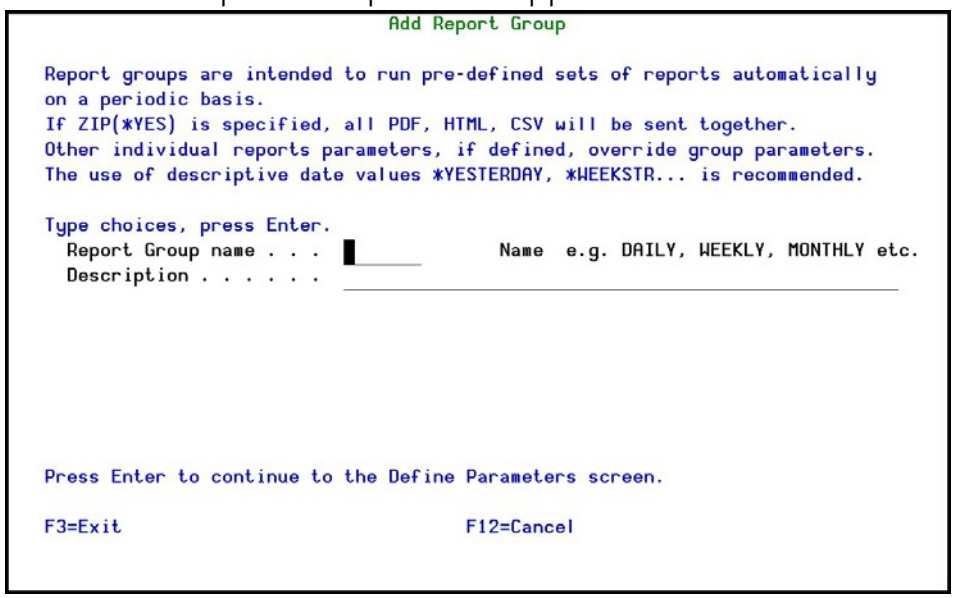
Reporting, Scheduler etc. Menu

2. Select 5.WorkwithReportScheduler from the Reporting,Scheduleretc. menu. The Work with Report Scheduler screen appears.



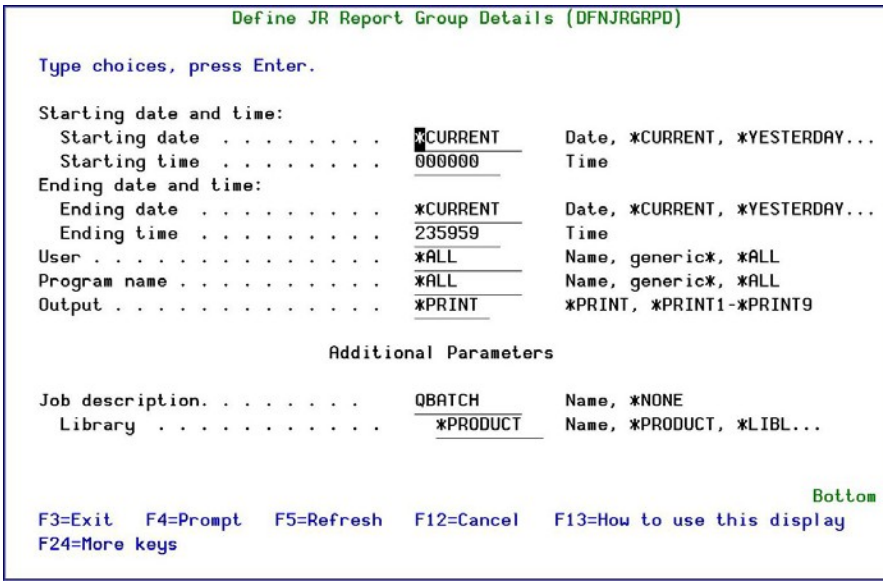
Work with Report Scheduler

3. Press F6 to create a new report group or type 1 to select an existing group. The
   Add Report Group screen appears.



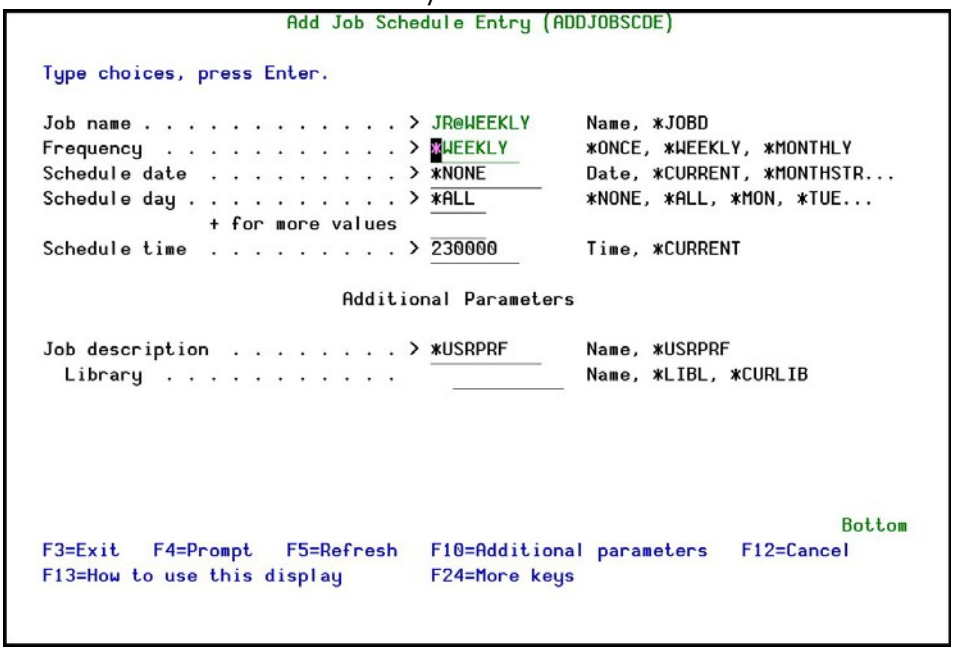
Add Report Group

4. Press Enter to continue to the Define JR Report Group Details screen.



Define JR Group Details

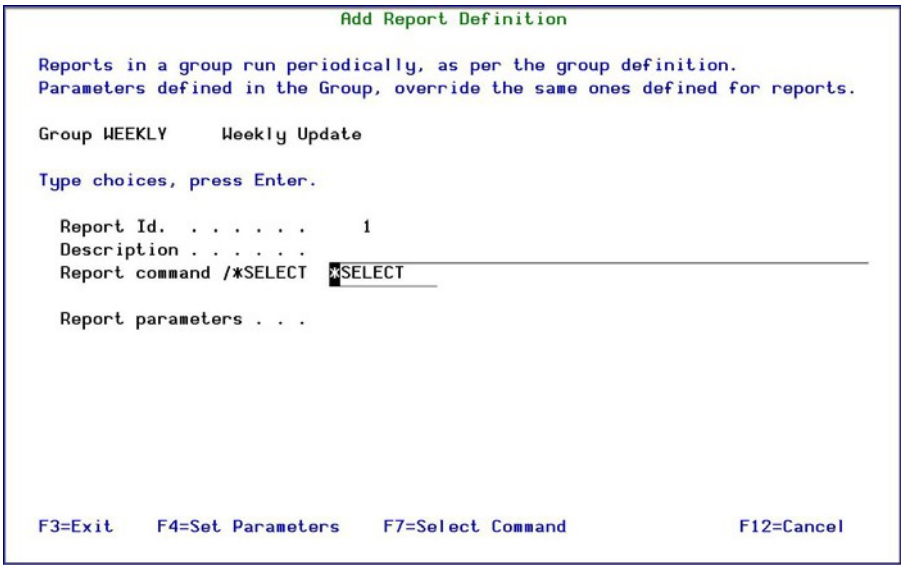
5. Press Enter to continue to the Add Job Schedule Entry screen.



Add Job Schedule Entry

NOTE: The Schedule Date and Schedule Day fields are mutually exclusive. If you use one, you must set the other to the value '*NONE'. Other fields may appear on this screen, which is associated with the IBM i (OS/400) CHGJOBSCDE command. These fields are not relevant under most circumstances.

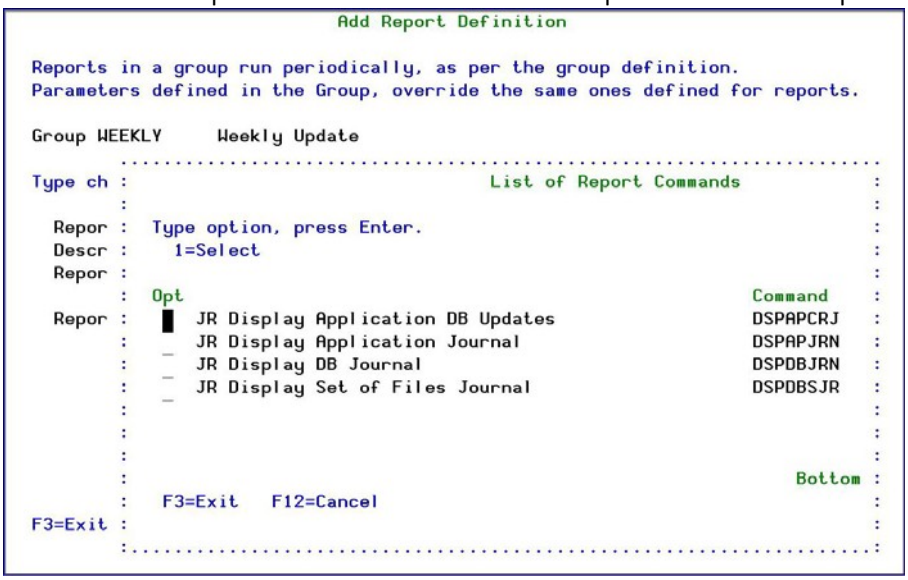
6. Press Enter to complete the definition and return to the Work withReport Scheduler screen.
7. Type 2=Add to add reports to the new group.



Add Report Definition

Option	Description
Report ID	Numeric ID automatically assigned by the AP-Journal
Description	Free text description of the report
Report Command (F4)	Press F4 to select report type from a pop-up window

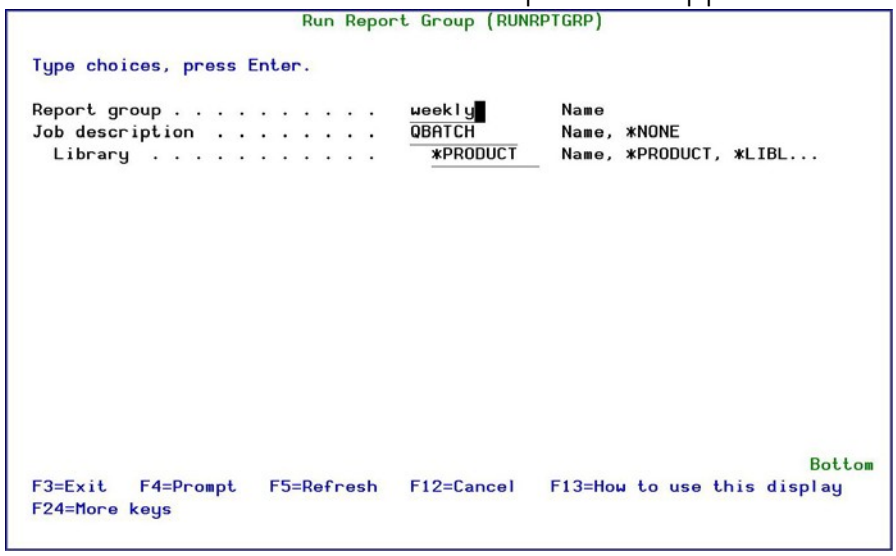
8. Define run time parameters for the report and press Enter . The actual parameters available are specific to the report type.



Add Report Definition

9. Press Enter to finish the definition and return to the Work withReport Scheduler screen.

1. Select 6. Run a Report Group from the Reporting, Scheduler etc. menu. The Run Report Group screen appears.



Run Report Group

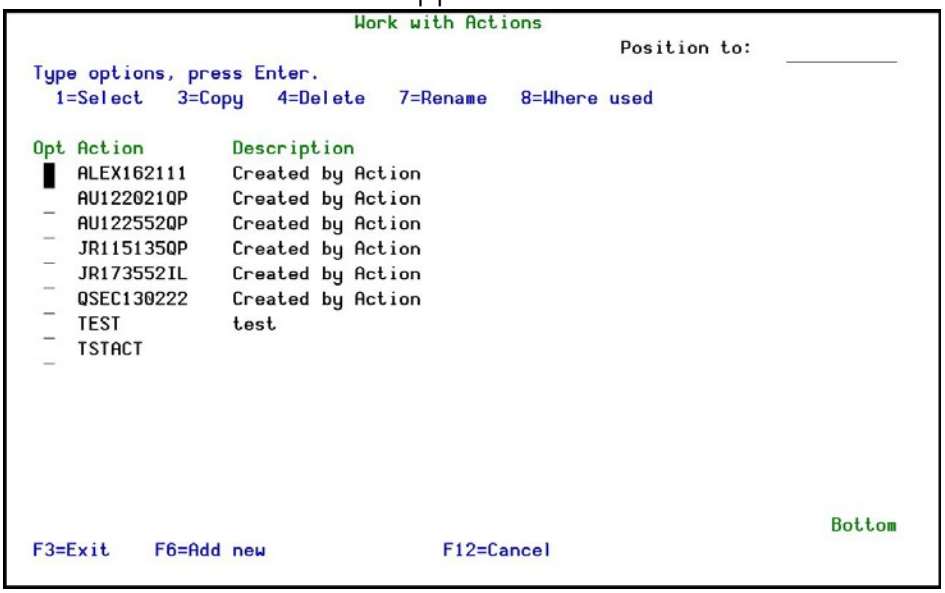
2. Enter the ReportGroup , the JobDescription and Library for the reports to be run and press Enter . Your chosen reports will be run.

Definitions You can define specific actions to be performed every time a Journal report is produced, Groups of reports to run together, and Time Groups to be used to schedule reports.

Actions

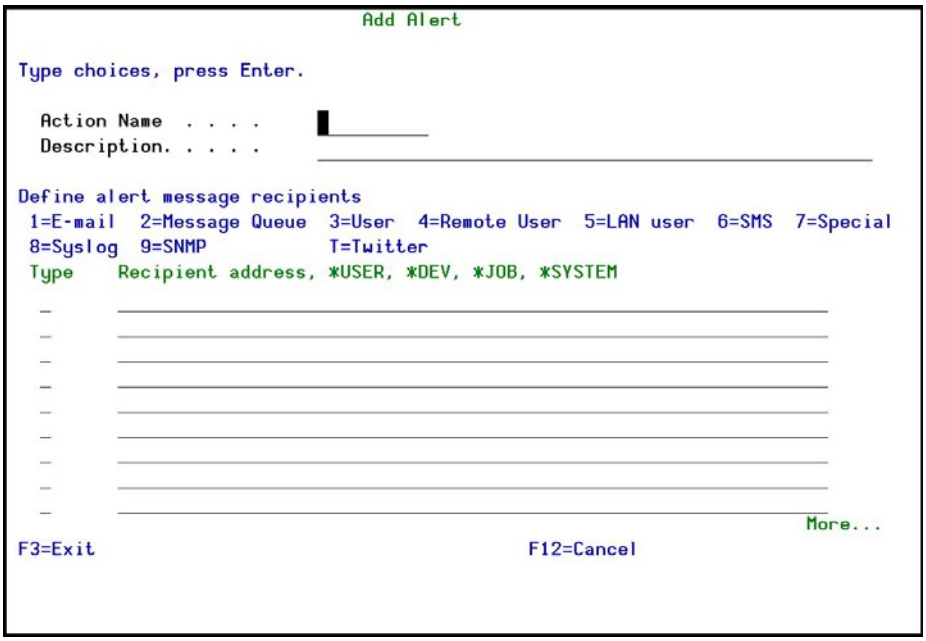
This section discusses the steps necessary in order to define the actions that are triggered by a rule. Actions can consist of alert messages and/or command scripts that perform one or more specific activities.

1. Select 31. Actions from the Reporting, Scheduler etc. menu. The Work with Actions screen appears.



Work with Actions

2. Press F6 to create a new action or type 1 to select an existing action. The Add Alert screen appears.



Add Alert

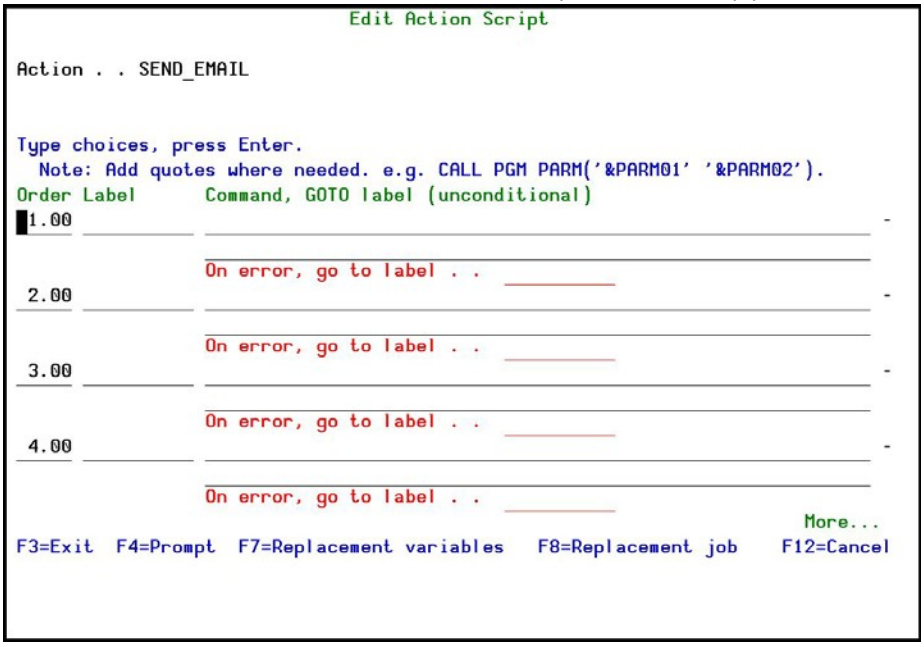
Option	Description
Action Name	Enter a meaningful name for the Action
Description	Enter a free text description of the Action
Type	Recipient type 1. - E-mail message 2. - Any specific message queue (SNDMSGTOMSGQ) 3 - User message queue (SNDMSGTOUSR) 4. - Remote system user (SNDNETMSG) 5. - Users or workstations on a LAN (SNDNWSMSG) 6. - SMS message to cellular telephone 7. - Message to beeper or pager 8. - Syslog 9. - SNMP T - Twitter

Option	Description
Recipient Address	Recipient address formatted according to message type (See following table)

-

Message Type	Recipient Address Format
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 a space (for example, USER SYSTEM)
5	Valid network user name or *DOMAIN for all users on your domain
6	Phone number including country code and area code as neces- sary
7	Phone number and access codes for the pager service
8	Leave blank; the SYSLOG message will be sent according to the definitions in option 21. Syslog Definitions in the System Configuration menu (see Syslog Definitions onpage 139 for more details).
9	Leave blank; the SNMP message will be sent according to the definitions in option 22. SNMP Definitions in the System Configuration menu (see SNMP Definitions on page 140 for more details).
T	Leave blank, the Twitter message will be sent according to the definitions in option 23. Twitter Definitions in the System Configuration menu (see Twitter Definitions on page 141 for more details).

3. Enter your parameters and press Enter. The Edit Action Script screen appears.



Edit Action Script

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

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.

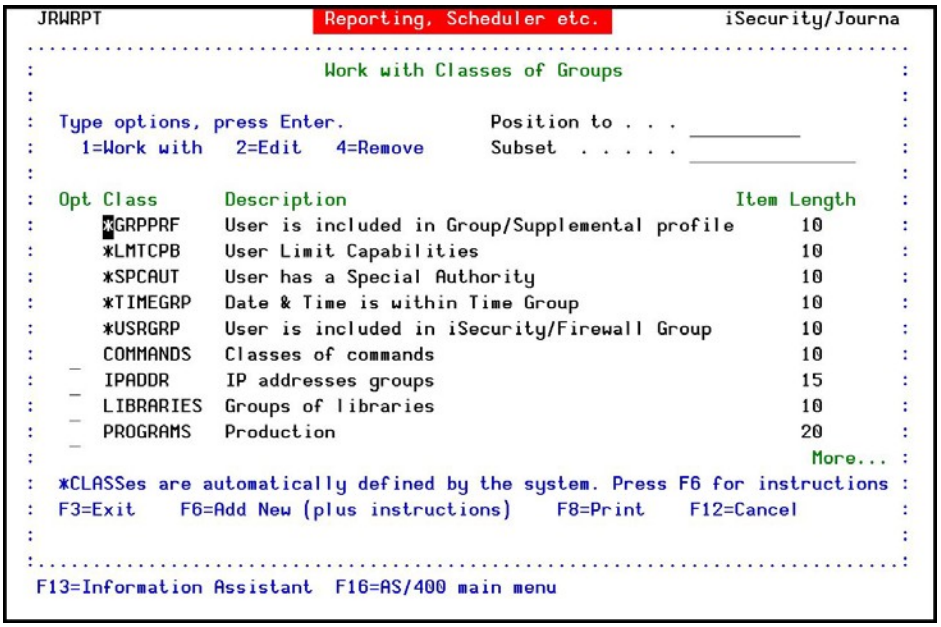
In all comparison tables, for defining rules, for generating and selecting queries, or for defining the items in reports, you can use the ITEM GROUP-TYPE/GROUP syntax to

include only those transactions that contain the GROUP-TYPE/GROUP specified. Likewise, you can use the NITEM GROUP-TYPE/GROUP to include only those transactions that 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.

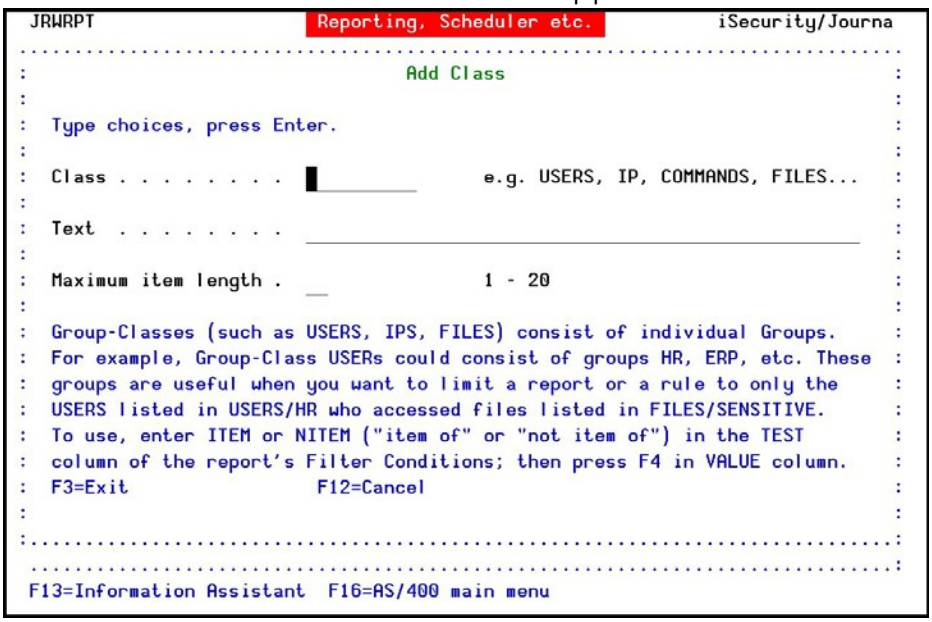
To define Groups and Items:

1. Select 35. Groups and Items from the Report-ing, Scheduler etc. menu. The Work with Classes of Groups screen appears.



Work with Classes of Groups

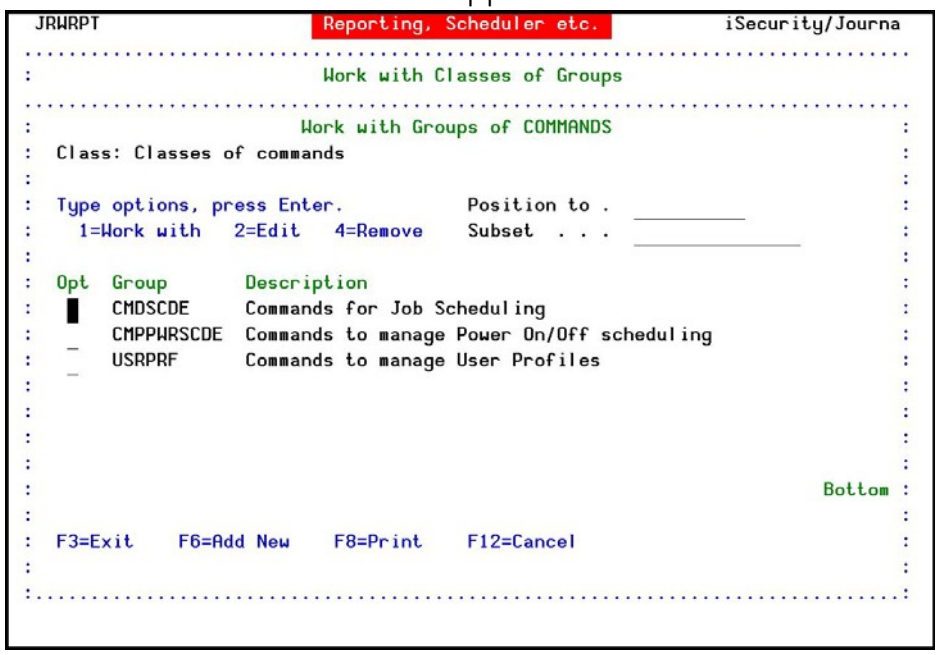
2. Press F6 to add a new class or type 1 to modify an existing class to your needs. The Add Class screen appears.



Add Class

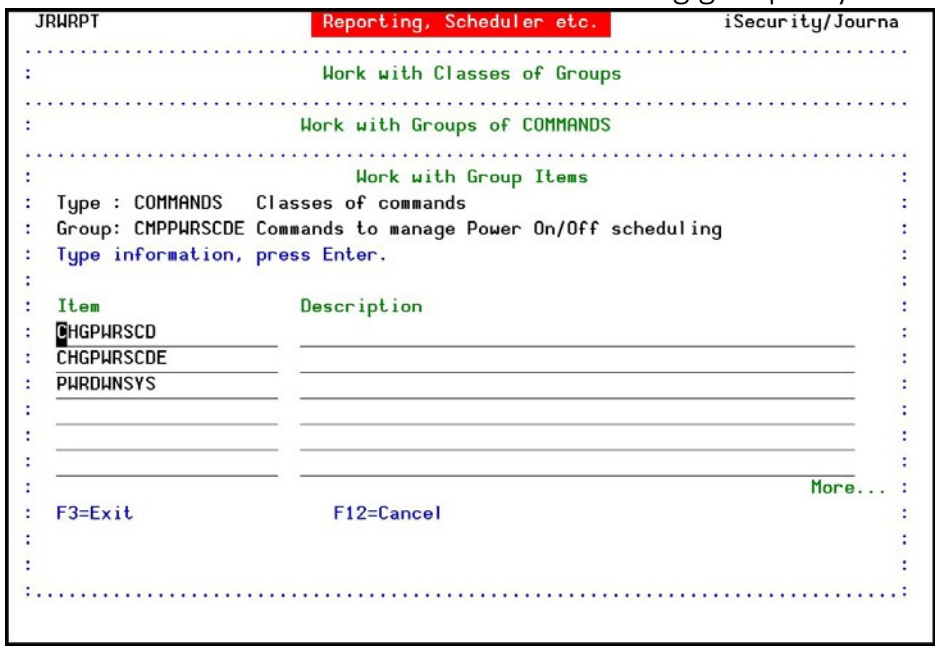
3. Enter a Class , Text and the Maximum itemlength .

4. Press Enter . The WorkwithGroups screen appears.



Work with Groups

5. Press F6 to add a new Group or 1 to modify items in existing group to your needs.

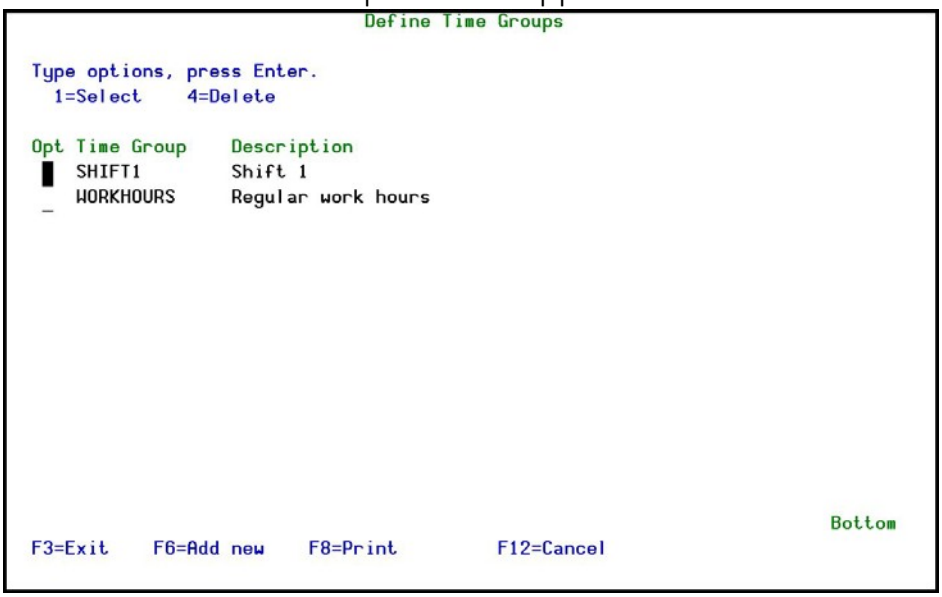


Time Groups

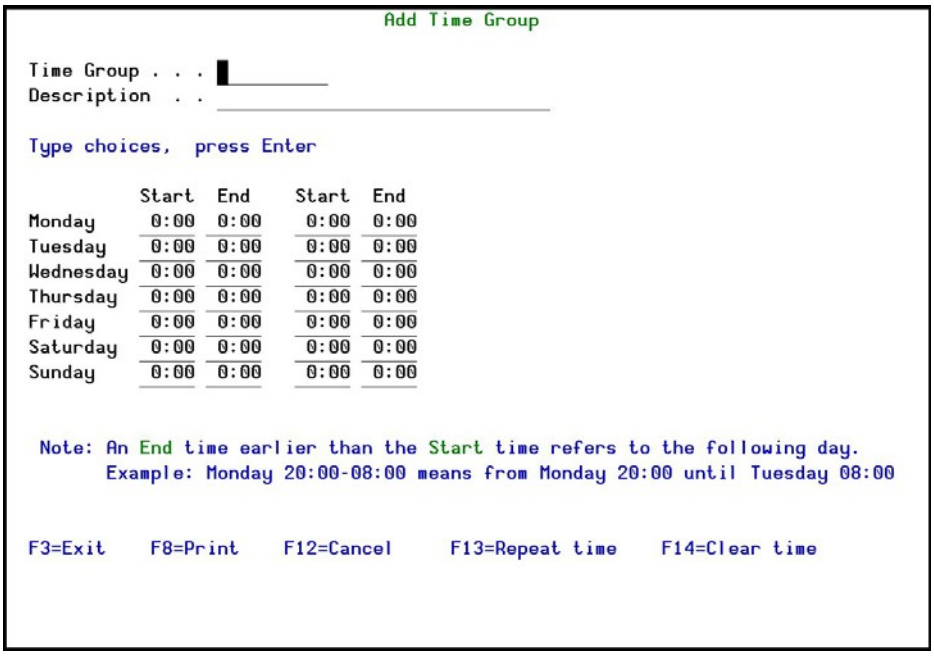
Time groups are user-defined sets of time and day of the week parameters that you can use as filter criteria for queries and reports. Time group filters can be either:

- 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:

1. Select 36. Time Groups from the Reporting, Scheduler etc. menu. The Define Time Groups screen appears.

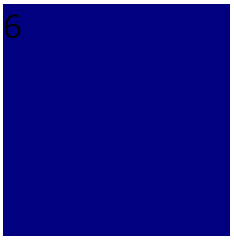


2. Type 1 to select an existing time group to modify or press F6 to create a new time group.



Parameter/Option	Description
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 fol- lowing 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

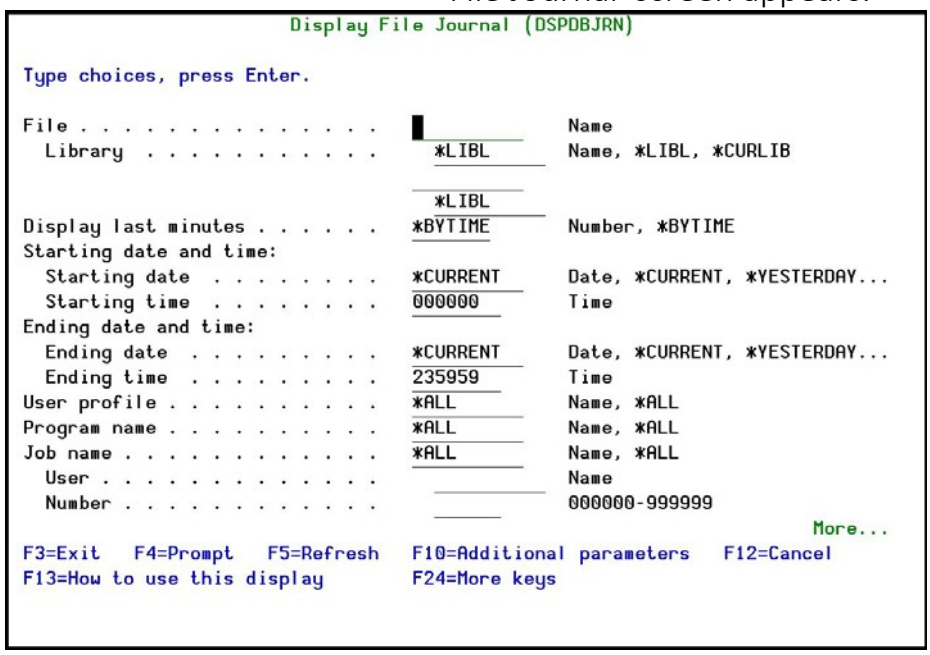
3. Enter parameters as described in the table and press Enter .



Review Database Changes

To produce a list of changes:

1. Select 52. Display File Journal - List from the Application Journal main menu. The Display File Journal screen appears.



Display File Journal

Option	Description
File	Name of file to display
Library	Name of library to display
Display last minutes	Last N minutes to display

Option	Description
Starting/Ending date and time	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 updated the file.
Program name	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	Insert a number or *NOMAX
Output	*PRINT - to print *PRINT1 - *PRINT9 *PDF *HTML *CSV *OUTFILE

* - to display only

2. Enter your parameters and press Enter . The report is sent to the selected output format.

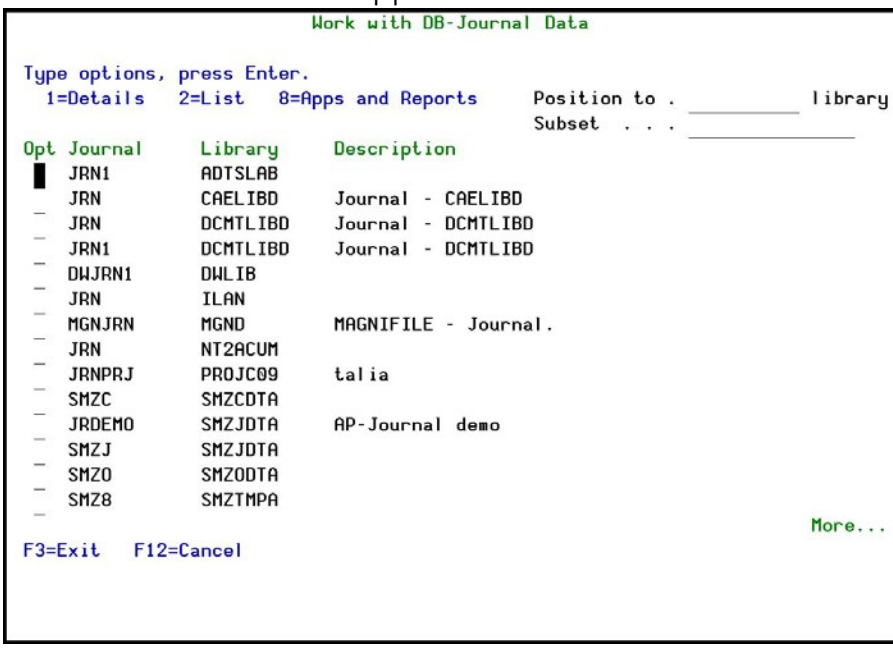
Chapter 6: Reviewing Database Changes

Database Journals
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.

Work with Database Journals

To work with Database Journals:

1. Select 51. Work with DB-Journals from the Application Journal main menu. The Work with DB-Journal Data screen appears.



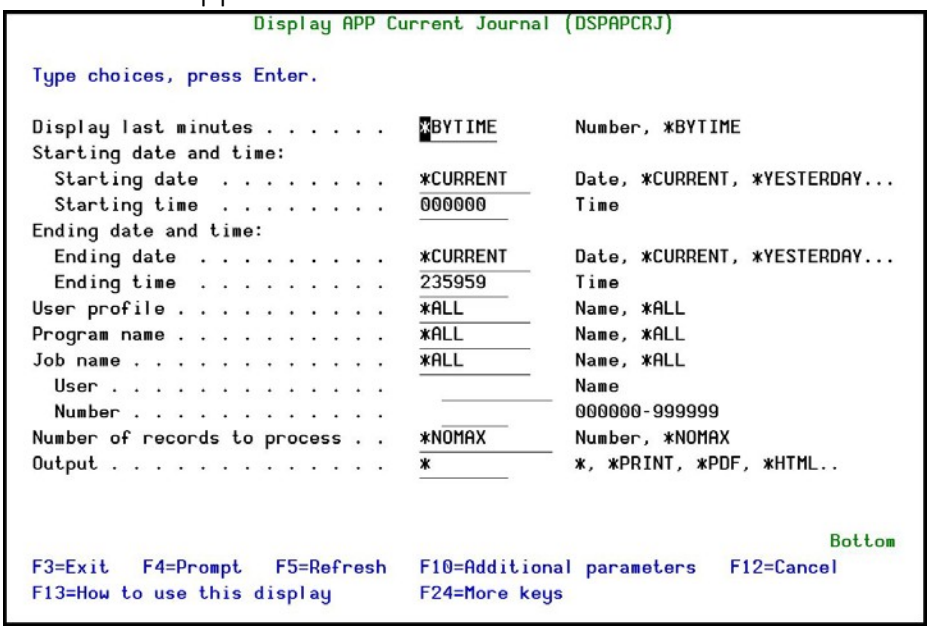
Work with DB-Journal Data

2. Select 1 to work with Journal Details , 2 to work with Journal Lists , or 8 to work with Applications and Reports .

Journal Details

To work with Journal Details:

1. Select the Journal you want to work with in the Work with DB-JournalData screen and type 1 . The Display APP Current Journal screen appears.



Option	Description
File	Name of file to display
Library	Name of library to display
Display last minutes	Last N minutes to display

Option	Description
Starting/Ending date and time	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 updated the file.
Program name	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	Insert a number or *NOMAX
Output	*PRINT - to print *PRINT1 - *PRINT9 *PDF *HTML *CSV *OUTFILE

* - to display only

2. Enter your parameters and press Enter . The report is sent to the selected output format.

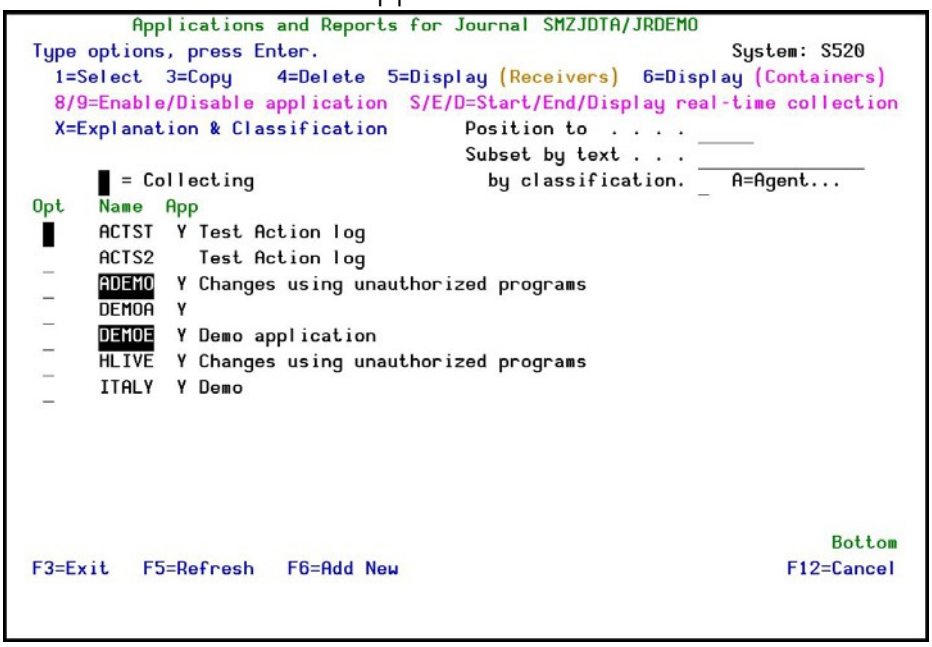
Journal Lists

To work with Journal Lists:

1. Select the Journal you want to work with in the Work with DB-JournalData screen and type 2 . The Display APP Current Journal screen appears (see Journal Details for screenshot and parameter details).
2. Enter your parameters and press Enter . The report is sent to the selected output format.

To work with Applications and Reports:

1. Select the Journal you want to work with in the Work with DB-JournalData screen and type 8 . The Applications and Reports for Journal screen appears.



Applications and Reports for Journal

2. See Creating a new set of files on page 53 for details on working with this screen.

File Journals You can produce a list of changes performed on a specific file and also a full detailed report of the changes.

File Journal Details

To produce a list of change details:

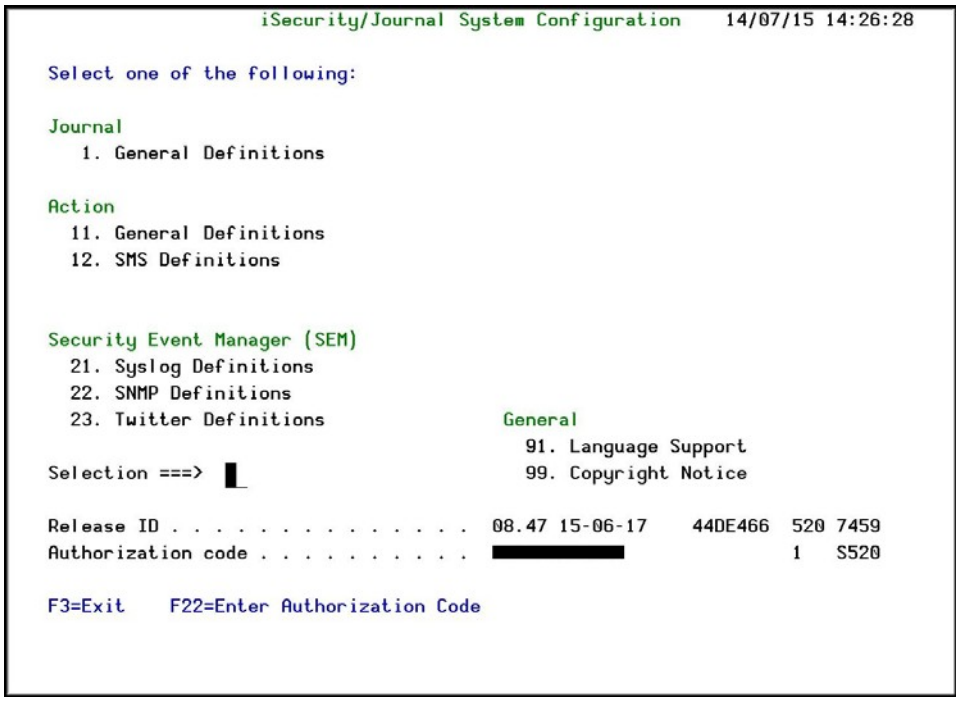
1. Select 53. Display File Journal - Details from the Application Journal main menu. The DisplayFileJournal screen appears (see File Journal Lists for screenshot and parameter details).
2. Enter your parameters and press Enter . The report is sent to the selected output format.

System Configuration and Maintenance

Chapter 7: Configuration and Maintenance

System Configuration

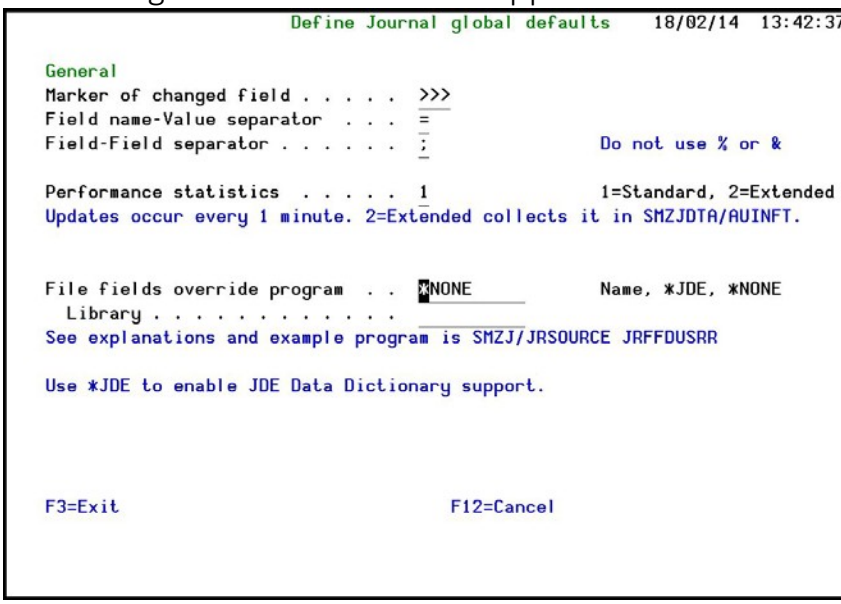
This option presents general definitions relating to marking of the changed field, SMS and E-mail definitions, SEM definitions, and language support. You access System configuration by selecting **81. System Configuration** from the AP-Journal main menu. The **System Configuration** menu appears. Press **F22** to enter the authorization code.



System Configuration

Journal General Definitions

1. Select 1. General Definitions from the System Configuration menu to define the general preferences of the file appearance. The DefineJournalglobal defaults screen appears.



Define Journal global defaults

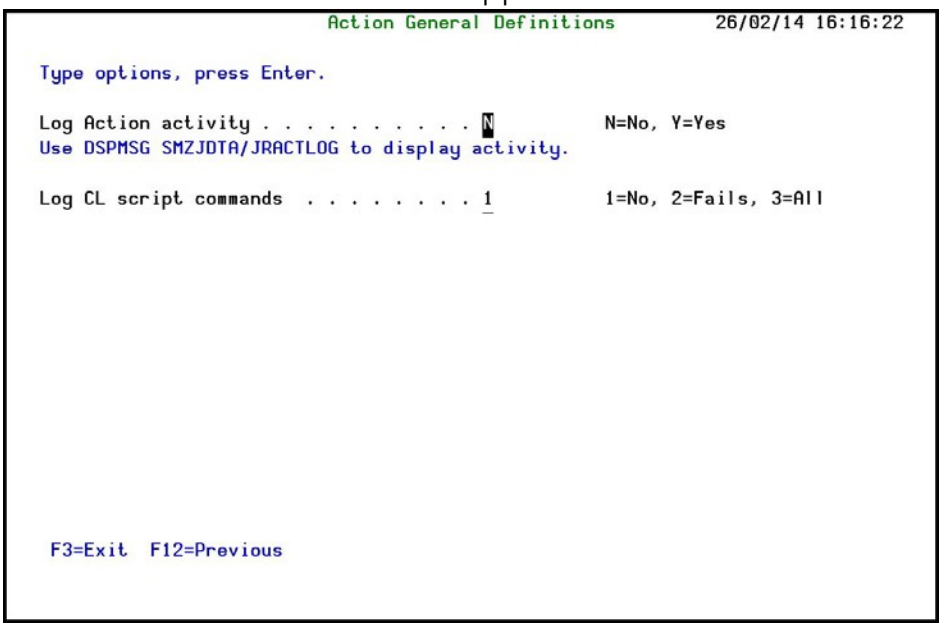
Option	Description
Marker of changed field	The character you want to use to indicate changed fields.
Field name-value separator	The character you want to use to separate the field name from its value.
Field-Field separator	The character you want to use to separate one field from another. You should not use % or & .
Performance statistics	1 =Standard 2 =Extended The updates occur every 60 seconds. Extended performances are collected in SMZJDTA/AUINFT .

Option	Description
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/JRSOURCEJRFFDUSRR . If you want to enable JDE Data Dictionary support, enter *JDE .

2. Enter your required parameters and then press Enter to confirm.

General Definitions

1. Select 11. General Definitions from the iSecurity/Base System Configuration menu. The Action General Definitions screen appears.



Action General Definitions

Option	Description
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

2. Enter your required parameters and press Enter .

SMSDefinitions

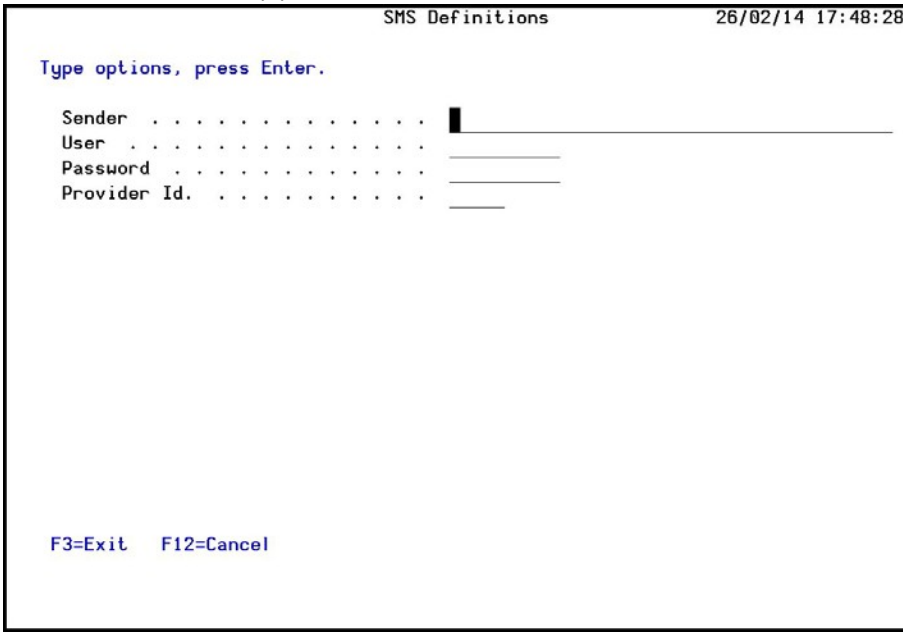
SMS messages are supported in real-time actions and will work in different ways for different suppliers.

NOTE: SMS support requires configuration together with a local SMS supplier before use.

Every supplier carries its own restrictions and modality. The current interface was developed according to a certain supplier. Users can develop their own interfaces according to the local suppliers. The interface should be developed in a program named XXALR6R and receives two parameters:

- 64 Alpha = destination
- 1000 Alpha = message

1. Select 12. SMS Definitions from the iSecurity/BaseSystem Configuration menu. The SMS Definitions screen appears.



SMS Definitions

Option	Description
Sender	Type the SMS Supplier description. This information will be available for the agent/customer and will be encrypted and not displayed in the screen.
User	Enter user name in case that authentication is needed. This field is encrypted and will not be displayed in the message.
Password	Enter a password in case that authentication is needed. This field is encrypted and will not be displayed in the message.
Provider Id	This field is used in order to individualize the supplier

2. Enter your required parameters and press Enter .

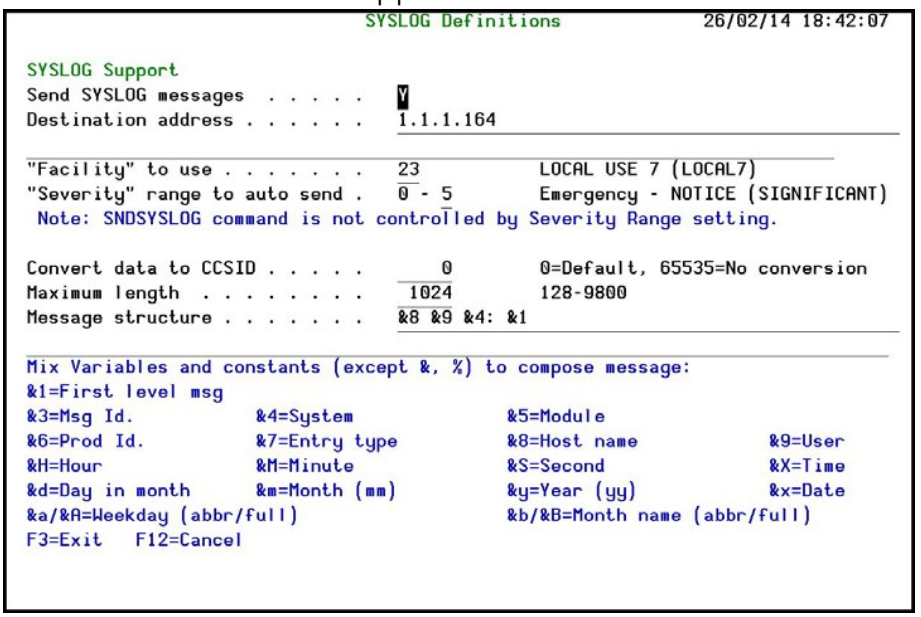
Numerous iSecurity products integrate with SEM/SIEM systems by sending security alertsinstantaneously to these systems; web-based alerts are supported using Twitter https://twitter.com/ (can transmits up to 1000 lines per second). Message alerts contain detailed event information about application data changes, deletes or reads of objects and files, emergency changes in user authorities, IFS viruses detected, malicious network access to the System i, and more.

Syslog Definitions

This feature sends events from the IBM i different Audit entry types to a remote SYSLOG server according to range of severities such as emergency, alert, 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.

1. Select 21. Syslog Definitions from the iSecurity/BaseSystem Configuration menu. The SYSLOG Definitions screen appears.



Syslog Definitions

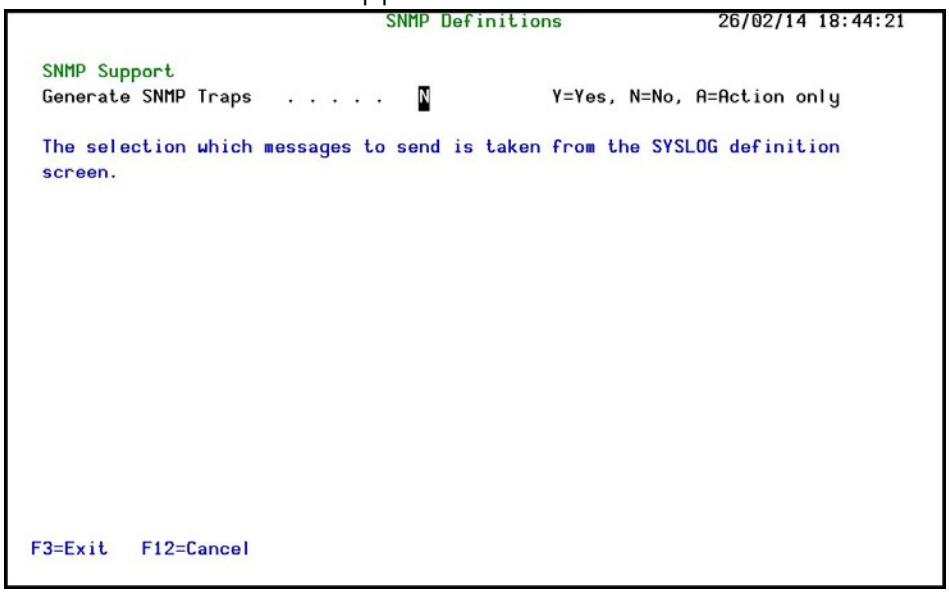
Option	Description
E-mail Method	1 =Advanced 2 =Native 3 =Secured 9 =None The Advanced or Secured mode is recommended for simplicity and performance reasons. If using 2 =native, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the WRKDIRE command. This option does not support attached files.
Mail (SMTP) server name	The name of the STMP server or *LOCALHOST
Reply to mail address	The e-mail address to receive replies.
E-mail user and password	If you chose 1 = Advanced or 3 =Secured for the E-mail method, enter the email user that will be used to send the emails and the password of that user
E-mail User ID and Address	If you chose 2 =Native for the E-mail method, enter the user ID and address that will be used to send the emails.
User Profile	If you chose 2 =Native for the E-mail method, enter the user profile that will be used to send the emails.

2. Enter your required parameters and then press Enter to confirm.

SNMP Definitions

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

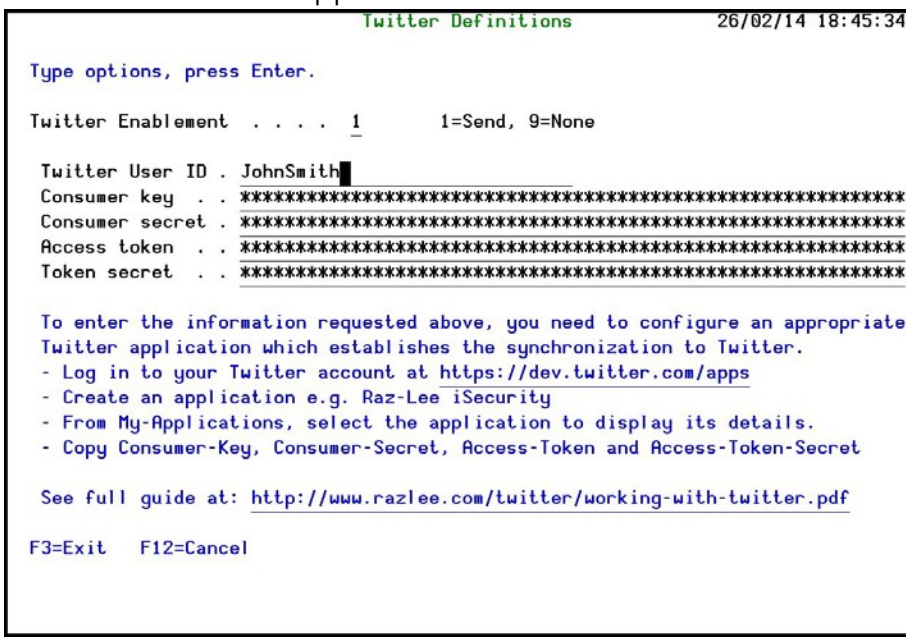
1. Select 22. SNMP Definitions from the iSecurity/BaseSystem Configuration menu. The SNMP Definitions screen appears.



Option	Description
Generate SNMP Traps	Y = Yes N = No A = Actions Only The selection of which messages to send is taken from the Syslog definitions (see Syslog Definitions on page 139 for more details).

2. TypeY to generate SNMP traps to monitor network attached devices for conditions that warrant administrative attention.
3. Enter your required parameters and then press Enter to confirm.

1. Select 23. Twitter Definitions from the iSecurity/Base System Configuration menu. The Twitter Definitions screen appears.



Twitter Definitions

Option	Description
Twitter Enablement	1 = Send 9 = None
Twitter User ID	The Twitter account you use to send messages.
Consumer Key Consumer Secret Access Token Access Secret	Use the value you received when you created the application.

2. Enter your required parameters and then press Enter to confirm.
   To enter the information requested above, you need to configure an appropriate Twitter application that establishes the synchronization to Twitter.

1. If necessary, create a Twitter account.
2. Log in to your Twitter account at https://dev.twitter.com/apps .
3. Create an application.
4. From My applications , select the application to display its details.
5. Copy the Consumer-Key , Consumer-Secret , Access-Token , and Access- Token-Secret fields.

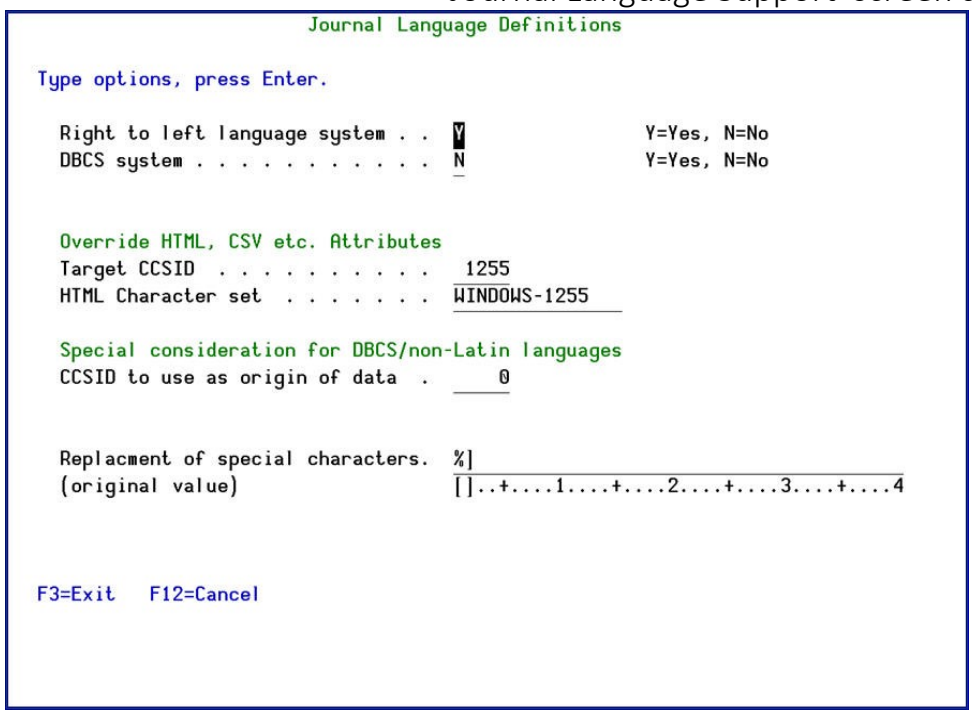
   For full instructions, see this guide: http://www.razlee.com/twitter/working-with-twitter.pdf.

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 iSecurity Language Support:

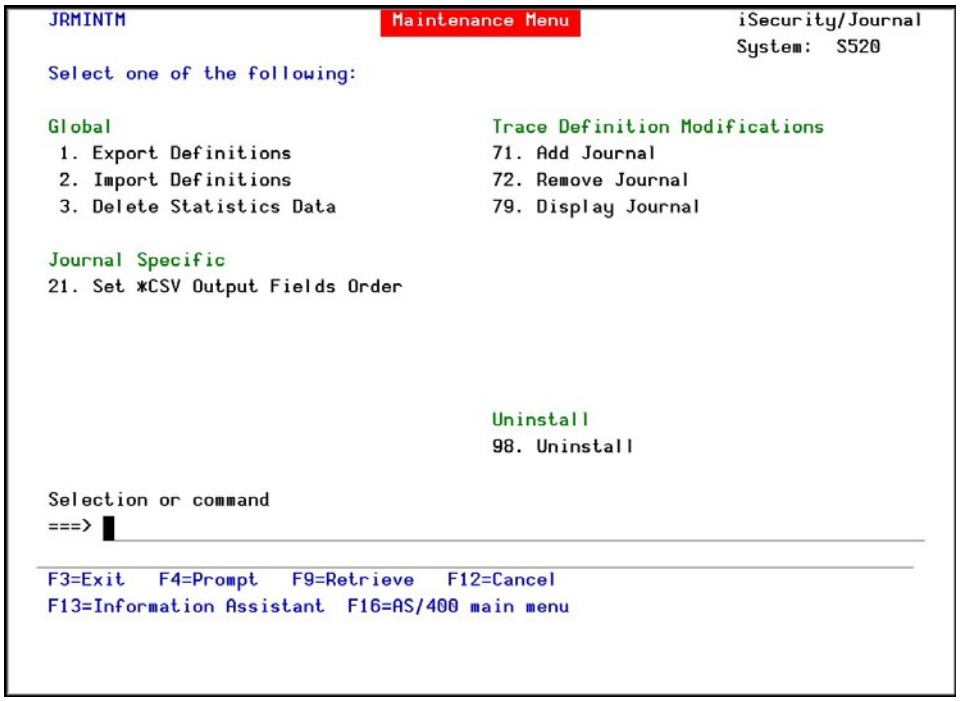
1. Select 91. Language Support from the System Configuration screen. The Journal Language Support screen appears.



Journal Language Definitions

2. Set your desired parameters and press Enter to confirm.

Maintenance 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. The Maintenance Menu appears.


JRMINTM
Maintenance Menu
iSecurity/Journal
System: S520
Select one of the following:
Global
1. Export Definitions
2. Import Definitions
3. Delete Statistics Data
Journal Specific
21. Set *CSV Output Fields Order
Trace Definition Modifications
71. Add Journal
72. Remove Journal
79. Display Journal
Uninstall
98. Uninstall
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12=Cancel
F13=Information Assistant F16=AS/400 main menu

Maintenance Menu

This option is useful in transferring configuration settings/definitions from one computer to another, or between LPARs.

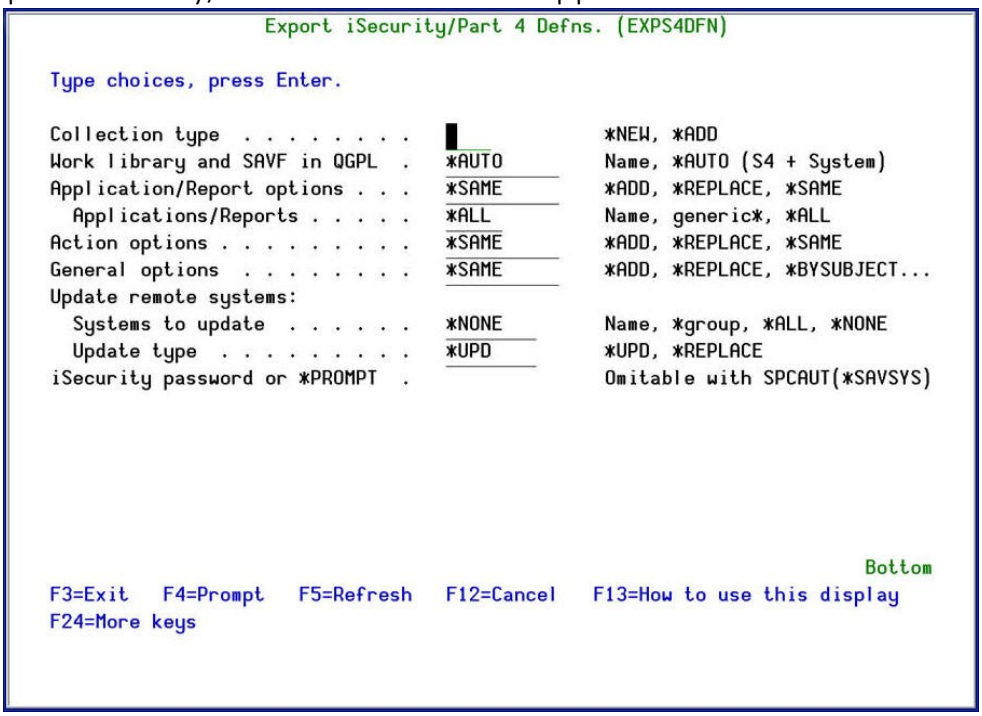
Among the settings and definitions that AP-Journal can export and import are the following:

- IP addresses
- System names (SNA)
- Users
- Groups
- Application
- Location
- Native & IFS
- Logon controls for FTP-TELNET-Passthrough
- Prechecks DDM-DRDA
- Time groups

Export Definitions

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

1. Select 1. Export Definitions from the Maintenance Menu screen. The Export iSecurity/Part 4 Defns. screen appears.



Export iSecurity/Part 4 Defns. (EXPS4DFN)

Option	Description
Collection type	*NEW = *ADD =

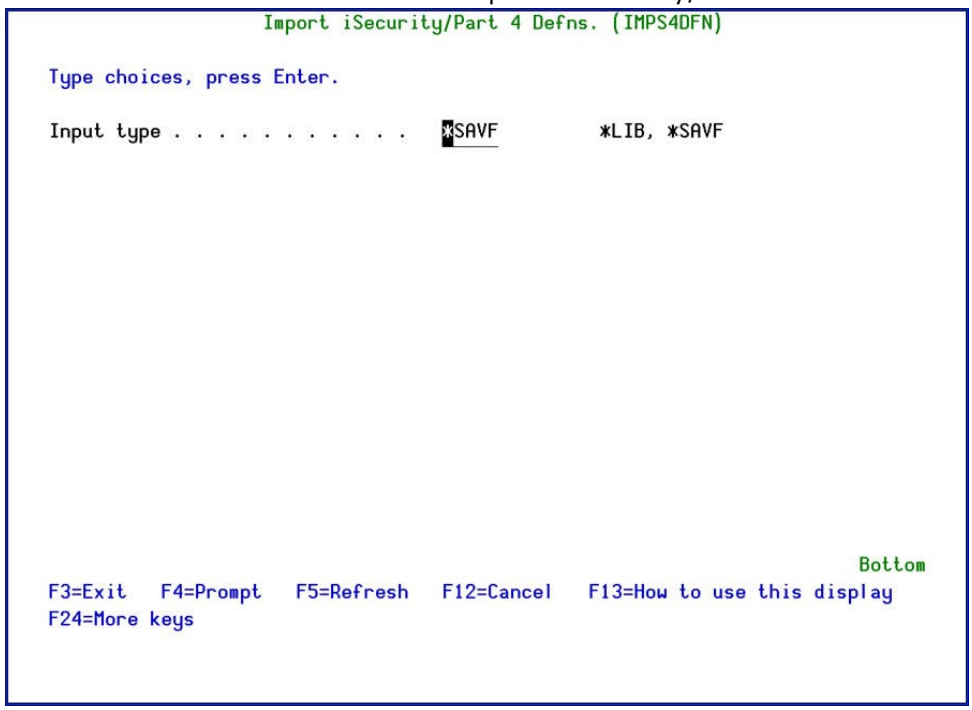
Option	Description
Work library and SAVF in QGPL	Destination of export library S4 is default setting
Application/Report options	*ADD = add to a previously imported/exported rule *REPLACE = replace a previously imported/exported rule *SAME = do not make any changes to Action options
Applications/Reports	Name = Name of the application/report to be exported *ALL = Export all applications/reports
Action options	*ADD = add to a previously imported/exported rule *REPLACE = replace a previously imported/exported rule *SAME = do not make any changes to Action options
General options	*ADD = add to a previously imported/exported rule *REPLACE = replace a previously imported/exported rule *BYSUBJECT = import/export rules by subject (IP address, etc.) *SAME = do not make any changes to General options
Update remote systems:	Systems to update = When exporting Firewall definitions, the user can choose to export and import at once by preparing the definitions in a

	SAVF and send it to a remote system or several remote systems, and automatically import them into it. Update type *UPD = add new records and replace existing records *REPLACE = clear the definition file and copy the new records.
iSecurity password or *PROMPT	This parameter can be omitted if SPCAUT (*SAVSYS) is defined.

2. Set your desired parameters and press Enter to confirm.

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

1. Select 2. Import Definitions from the Maintenance Menu screen. The Import iSecurity/Part 4 Defns. screen appears.



Import iSecurity/Part 4 Defns. (IMPS4DFN)

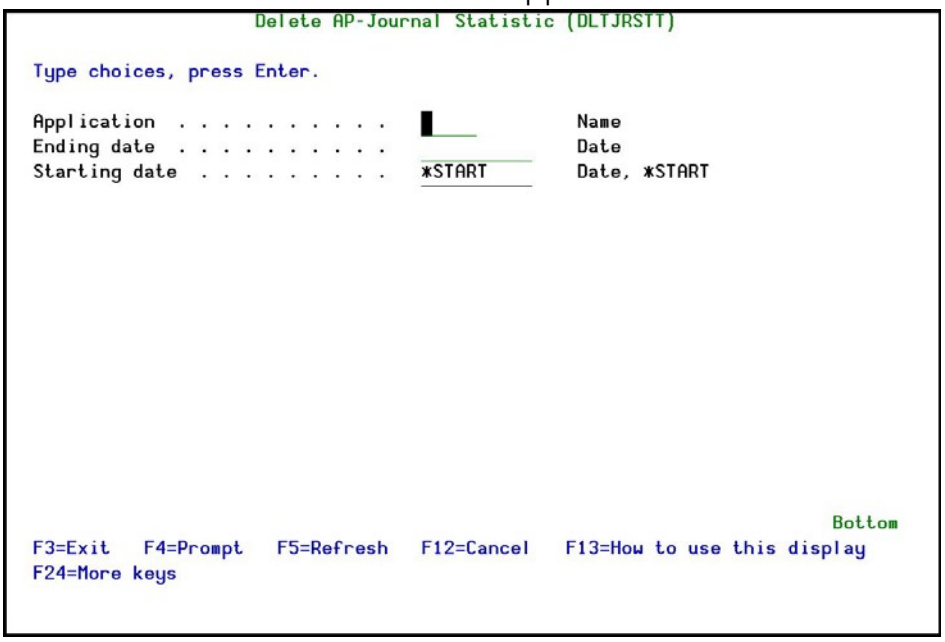
Option	Description
Import Type	*SAVF = Import from a Save File *LIB = Import from a Library

2. Set your desired parameters and press Enter to confirm.

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.

1. Select 3.DeleteStatisticsData from the Main-tenanceMenu . The Delete AP-Journal Statistic screen appears.



Option	Description
Application	The application for which you want to delete data.
Ending date	Enter the range of dates for which you want to delete data. The starting and ending dates are
Starting date	included in the range. Enter *START as a starting date to include all data from the beginning of the file.

2. Set your desired parameters and press Enter . The statistical data defined by the parameters is deleted.

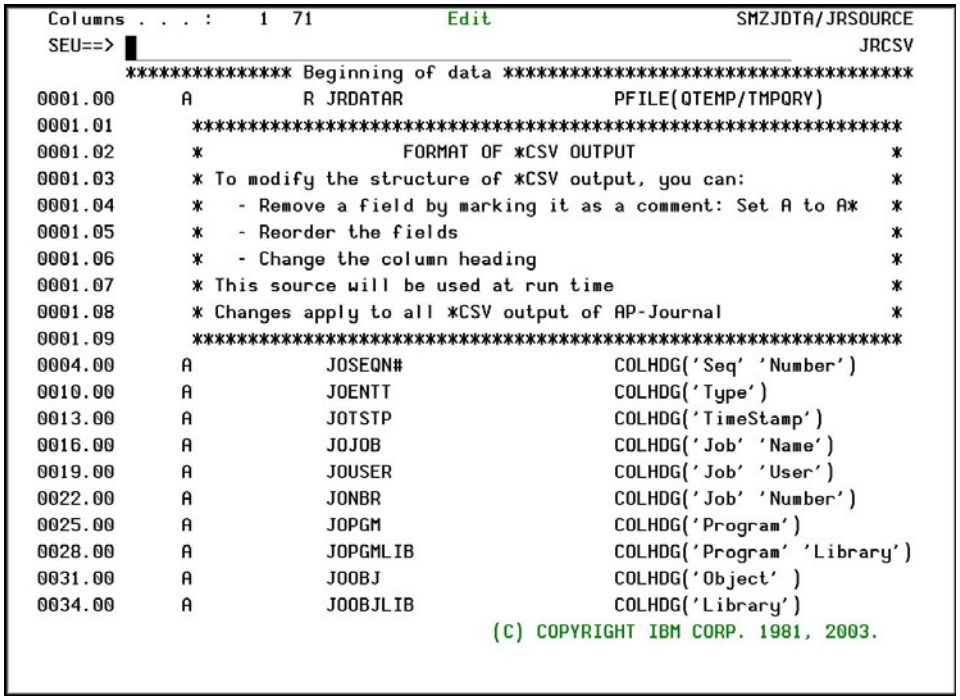
Journal Specific Maintenance

These options allow you to make changes that will only affect AP-Journal.

Customize *CSV Output Fields

You can customize your *CSV output by re-ordering fields, removing fields, and changing column headings.

1. Select 21.Set*CSVOutputFieldsOrder from the MaintenanceMenu . The **SEU Edit** screen appears showing the SMZJDTA/JRSOURCE JRCSV member.



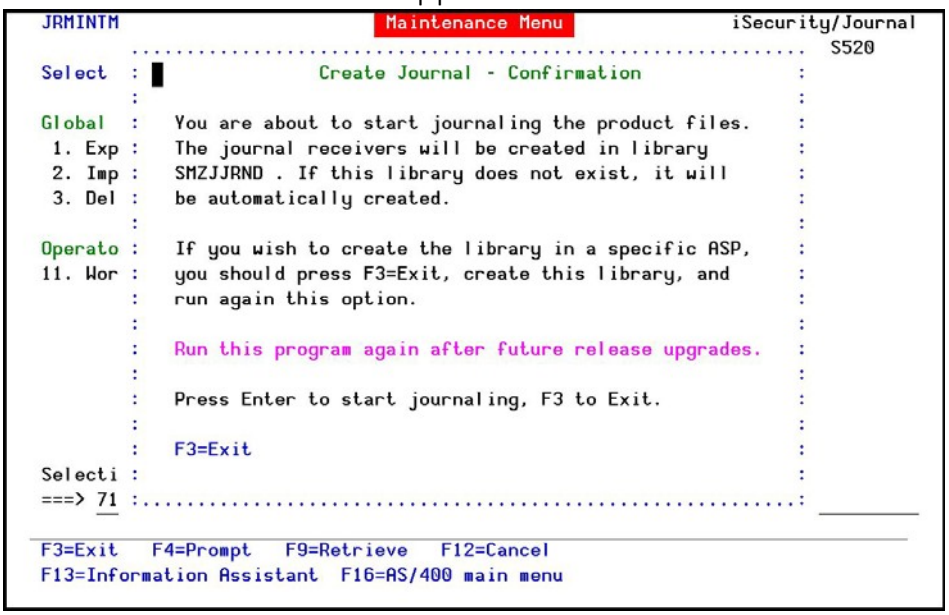
```
 Columns . . . :    1  71            Edit                        SMZJDTA/JRSOURCE
 SEU==> ____________________________________________________________________ JRCSV
        *************** Beginning of data ************************************
0001.00      A          R JRDATAR                    PFILE(QTEMP/TMPQRY)
0001.01       ***************************************************************
0001.02       *                  FORMAT OF *CSV OUTPUT                      *
0001.03       * To modify the structure of *CSV output, you can:            *
0001.04       *   - Remove a field by marking it as a comment: Set A to A*   *
0001.05       *   - Reorder the fields                                       *
0001.06       *   - Change the column heading                                *
0001.07       * This source will be used at run time                        *
0001.08       * Changes apply to all *CSV output of AP-Journal              *
0001.09       ***************************************************************
0004.00      A            JOSEQN#                    COLHDG('Seq' 'Number')
0010.00      A            JOENTT                     COLHDG('Type')
0013.00      A            JOTSTP                     COLHDG('TimeStamp')
0016.00      A            JOJOB                      COLHDG('Job' 'Name')
0019.00      A            JOUSER                     COLHDG('Job' 'User')
0022.00      A            JONBR                      COLHDG('Job' 'Number')
0025.00      A            JOPGM                      COLHDG('Program')
0028.00      A            JOPGMLIB                   COLHDG('Program' 'Library')
0031.00      A            JOOBJ                      COLHDG('Object' )
0034.00      A            JOOBJLIB                   COLHDG('Library')
                                        (C) COPYRIGHT IBM CORP. 1981, 2003.
```

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

NOTE: The changes you make will be valid for all AP-Journal *CSV output.

Add Journal

1. Select 71.AddJournal from the MaintenanceMenu . The CreateJournal- Confirmation screen appears.

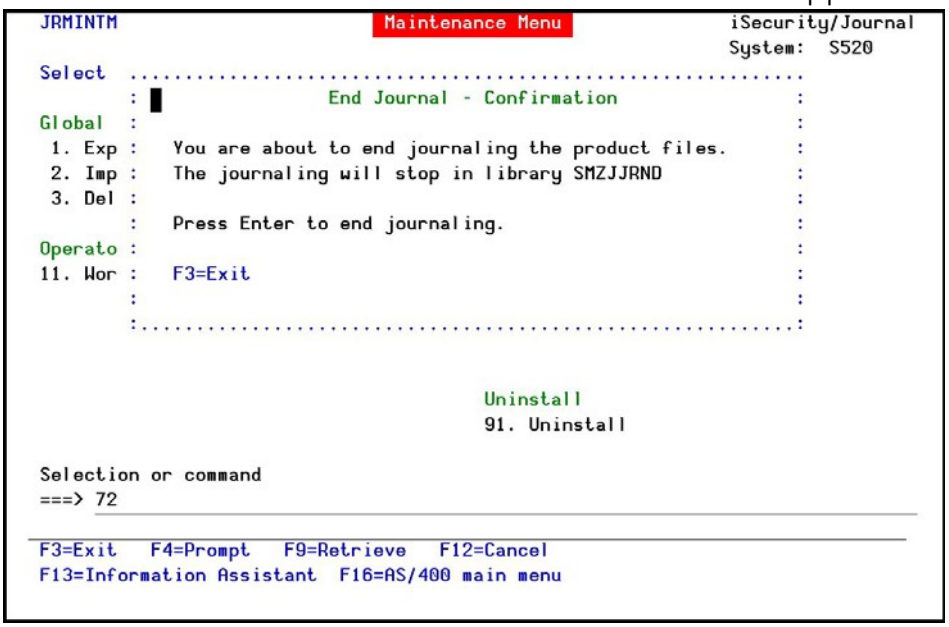


Create Journal - Confirmation

2. When you are ready to start journaling, press Enter .

Remove Journal

1. Select 72.RemoveJournal from the Main-tenanceMenu . The EndJournal - Confirmation screen appears.

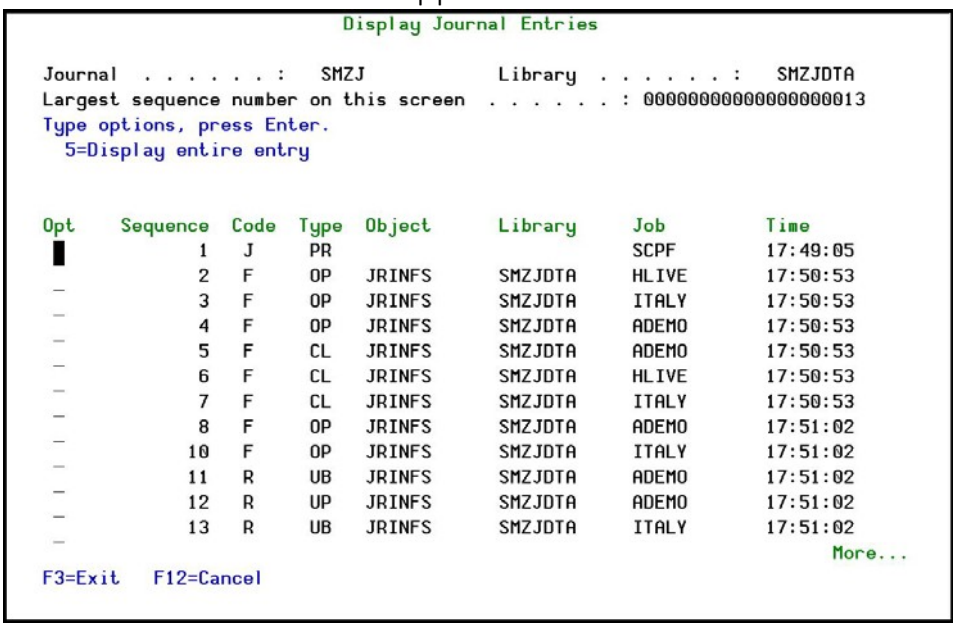


End Journal

2. When you are ready to end journaling, press Enter .

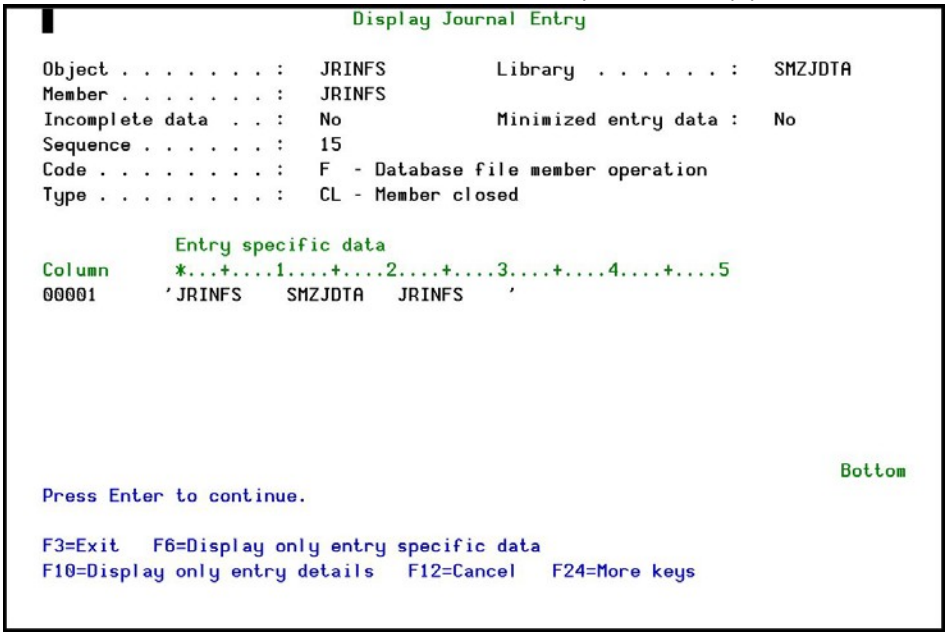
Display Journal

1. Select 79. Display Journal from the Maintenance Menu . The Display Journal Entries screen appears.



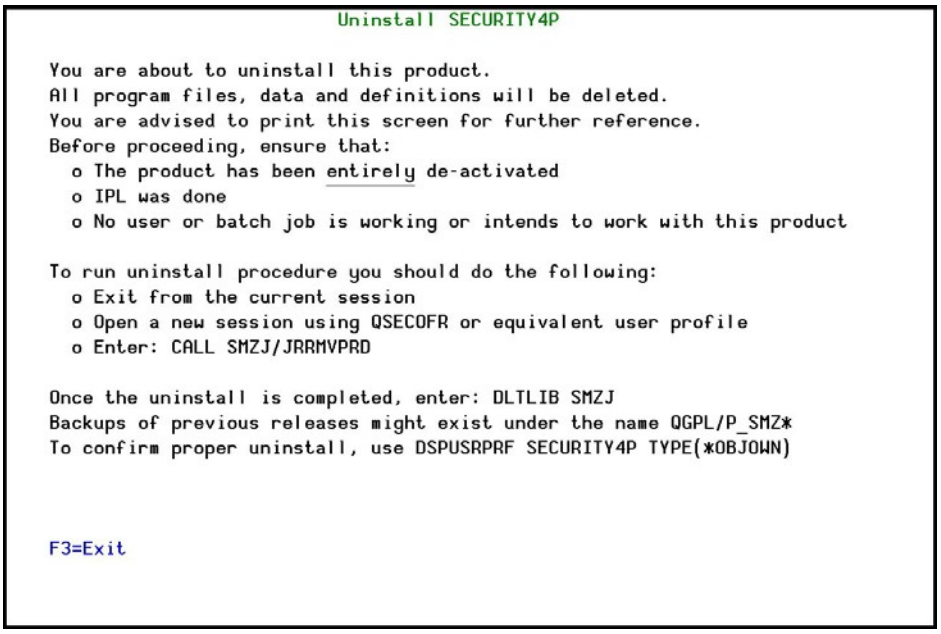
Display Journal Entries

2. Select the required entry and press 5 . The Display Journal Entry screen appears.



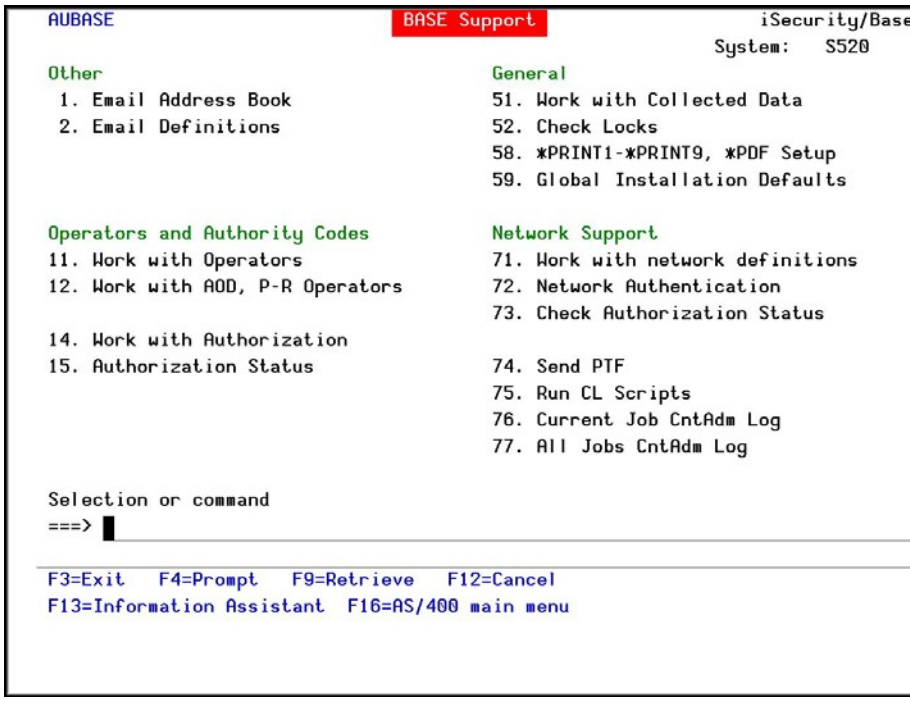
Display Journal Entry

- Choose 98. Uninstall Product from the Maintenance Menu , and follow the directions on the screen.



Uninstall

Base Support The BASE Support menu enables you to work with various settings that are common for 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 from the AP-Journal main menu.



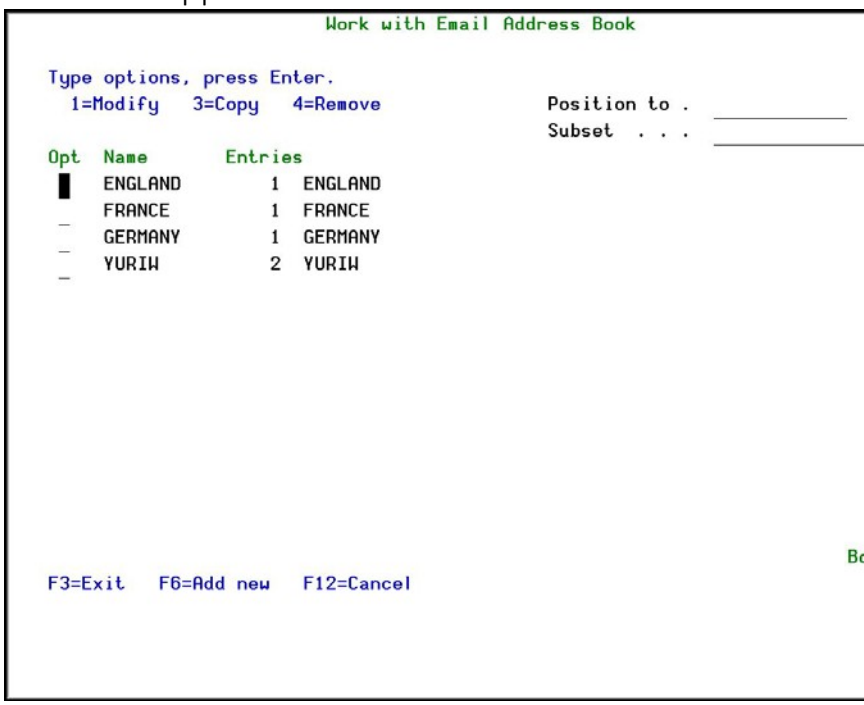
BASE Support menu

Other

Email Address Book

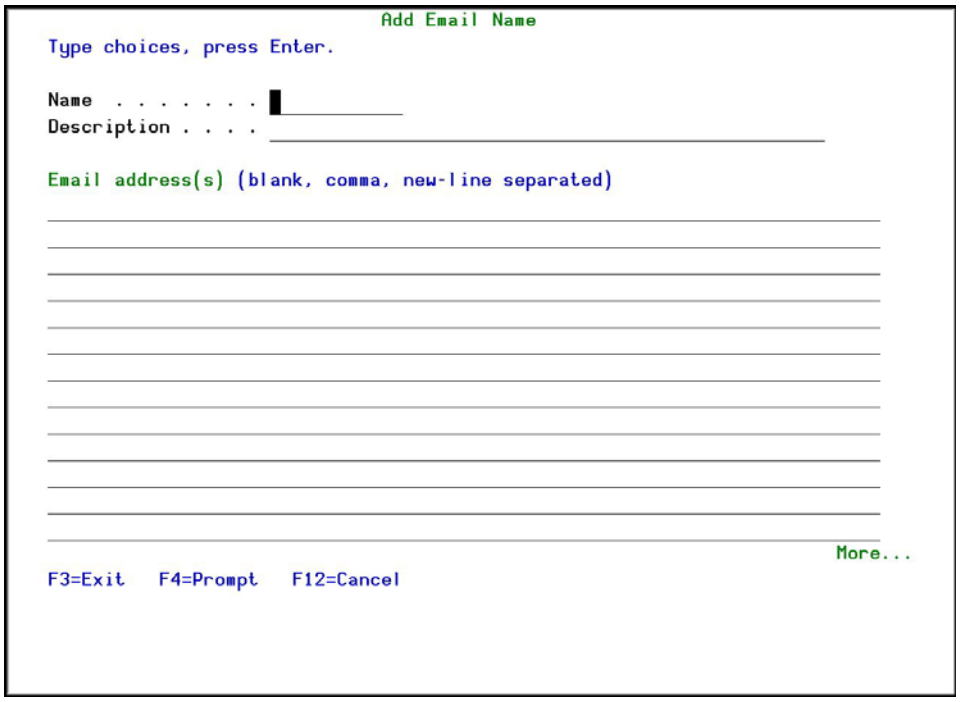
You can define the email address to be used for each user profile. You can also use this option to define an email group, with multiple addresses.

1. Select 1. Email Address Book from the BASE Support menu. The Work with Email Address Book screen appears.



Work with Email Address Book

2. Press F6 to add a new address entry (or type 1 next to a name to modify it). The Add Email Name screen appears.



Add Email Name

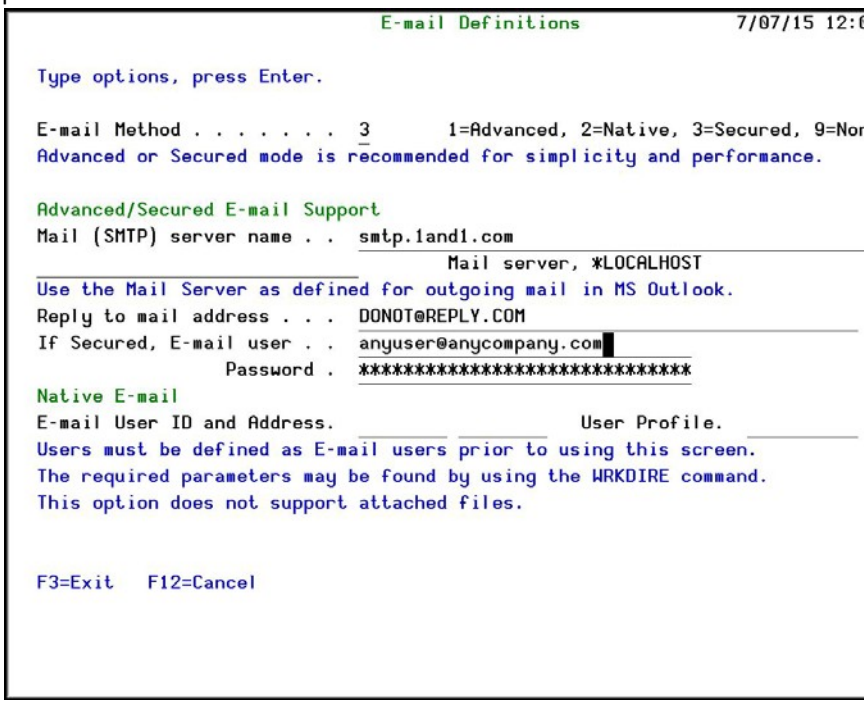
3. Enter a Name , Description , and all the associated email addresses and press

   Enter.

Email Definitions

AP-Journal can send out automatic emails for events that you define.

1. Select 2. Email Definitions from the BASE Support menu. The E-mail Definitions screen appears.



Email Definitions

Field	Description
E-mail Method	1=Advanced 2=Native 3=Secured 9=None Advanced or Secured mode is recommended for sim- plicity and performance. Note: If using 2=Native , Users must be defined as E- mail users prior to using this screen. The required parameters may be found by using the WRKDIRE com- mand. This option does not support attached files
Mail (SMTP) server name	The name of the STMP server or *LOCALHOST
Reply to mail address	The e-mail address to receive replies

Field	Description
If secured, email user and Password	If you chose 1=Advanced or 3=Secured for the E- mail method, enter the email user that will be used to send the emails and the password of that user
Email user ID and Address	If you chose 2=Native for the E-mail method, enter the user ID and address that will be used to send the emails
User Profile	If you chose 2=Native for the E-mail method, enter the user profile that will be used to send the emails

2. Enter the required fields and press Enter .

Work with Operators

The Operators' authority management is now maintained from one place for the entire

iSecurity on all its modules. There are three default groups:

- *AUD#SECAD - All users with both *AUDIT and *SECADM special authorities. By default, this group has full access (Read and Write) to all iSecurity components.
- *AUDIT - All users with *AUDIT special authority. By default, this group has only Read authority to Audit .
- *SECADM - All users with *SECADM special authority- By default, this group has only Read authority to Firewall .
  iSecurity related objects are secured automatically by product authorization lists (named **security1P**). This strengthens the internal security of the product. It is essential that you use Work with Operators to define all users who have ***SECADM**, ***AUDIT** or

  ***AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has Usr (user management) and Adm for all activities related to starting, stopping subsystems, jobs, import/export and so on. iSecurity automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

  Users may add more operators, delete them, and give them authorities and passwords according to their own judgment. Users can even make the new operators' definitions apply to all their systems; therefore, upon import, they will work on every system.

  Password = *BLANK for the default entries. Use **DSPPGM GSIPWDR** to verify. The default for other user can be controlled as well.

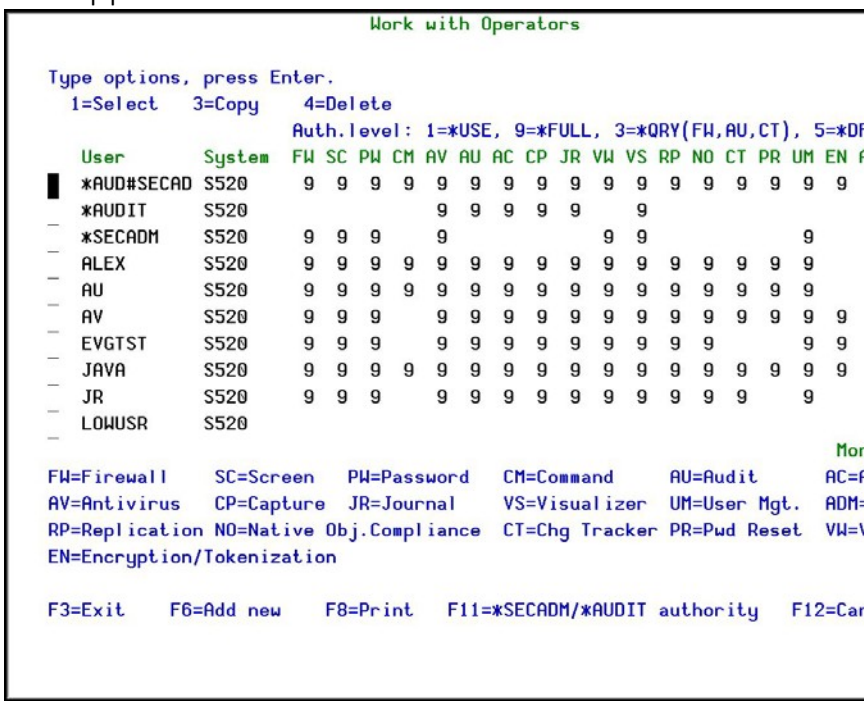
If your organization wants the default to be *BLANK, then the following command must be used:

CRTDTAARA SMZTMPC/DFTPWD *char 10

This command creates a data area called DFTPWD in library SMZTMPC. The data area is 10 bytes long and is blank.

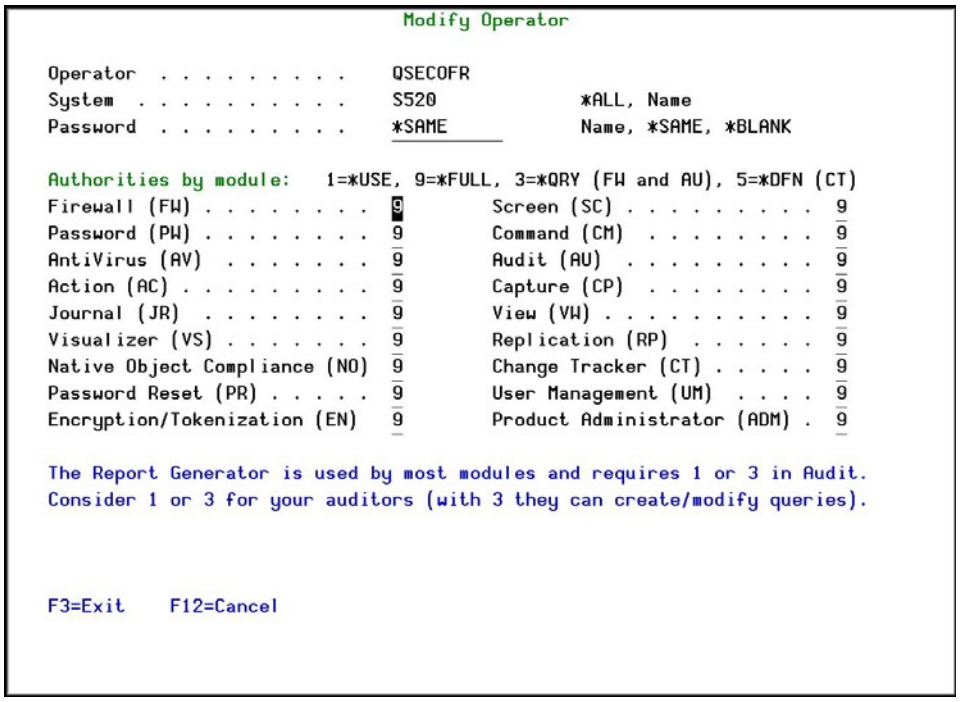
NOTE: When installing iSecurity for the first time, certain user(s) might not haveaccessaccordingtothenewauthoritymethod.Therefore,thefirst step you need to take after installing is to edit thoseauthorities.
To modify operators' authorities:

1. Select 11. Work with Operators from the BASE Support menu. The Work with Operators screen appears.



Work with Operators

2. Type 1 next to the user to modify his authorities (or press F6 to add a new user). The Modify Operator screen appears.



Modify Operator

Field	Description
Password	Name = Password *Same = Same as previous password when edited *Blank = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use
5 = *DFN	For Change Tracker use

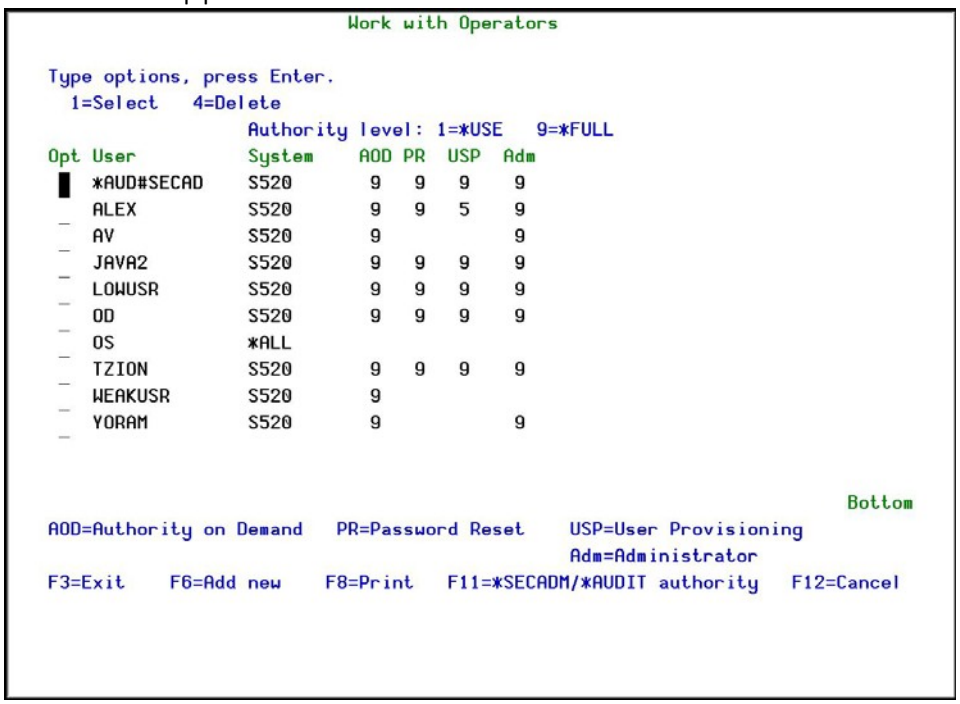
Most modules use the Report Generator, which requires access to the Audit module. For all users who will use the Report Generator, you should define their access to the Audit module as either **1** or **3**. Option **1** should be used for users who will only be running queries. Use option **3** for all users who will also be creating/modifying queries.

3. Set authorities and press Enter.
   A message appears to inform that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be granted Object operational authority. The Authority list is created in the installation/release upgrade process. The SECURITY_P user profile is granted Authority *ALL whilst the

   *PUBLIC is granted Authority *EXCLUDE. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

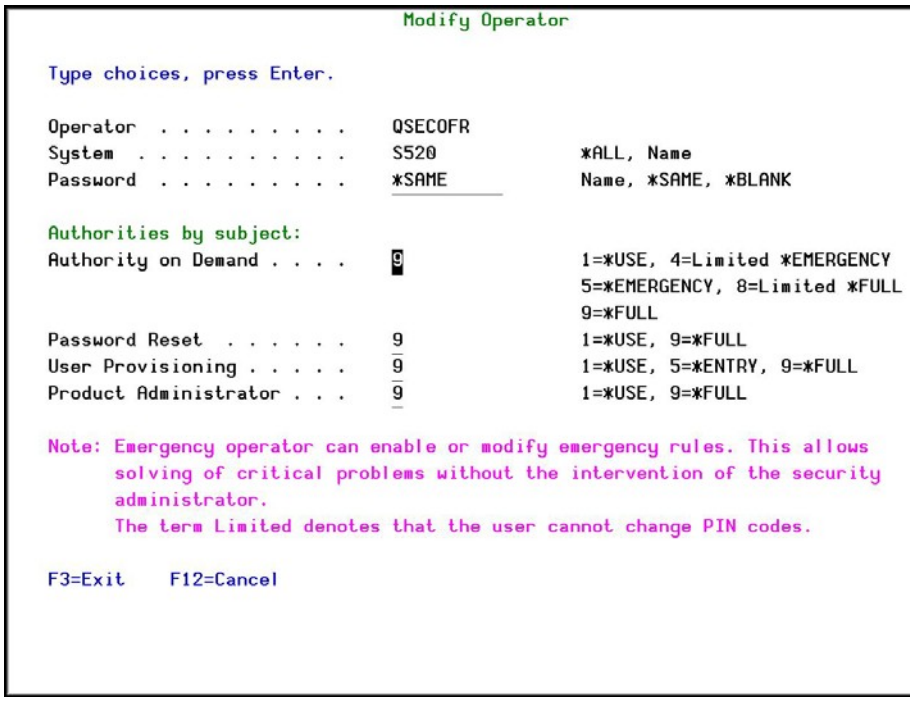
To modify operators' authorities:

1. Select 12. Work with AOD, P-R Operators from the BASE Support menu. The Work with Operators screen appears.



Work with Operators - AOD

2. Type 1 next to the user to modify his authorities (or press F6 to add a new user). The Modify Operator screen appears.



Modify Operator - AOD

Field	Description
Password	Name = Password Same = Same as previous password when edited Blank = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use
5 = *DFN	For Change Tracker use

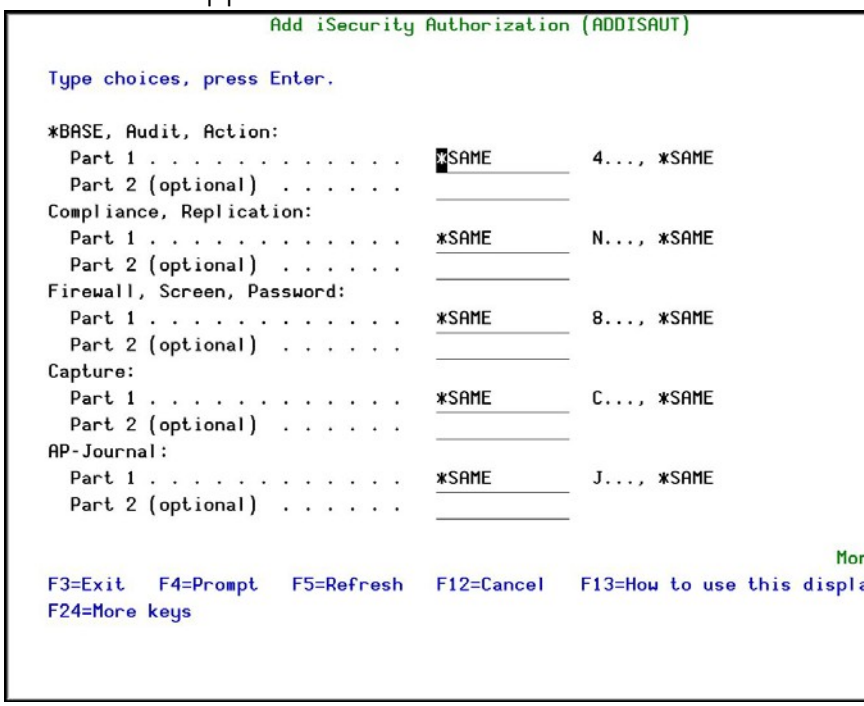
3. Set authorities and press Enter .
   A message appears to inform that the user being added/modified was added to the Authority list that secures the product's objects; the user carries Authority *CHANGE and will be

granted Object operational authority. The Authority list is created in the installation/release upgrade process. The SECURITY_P user profile is granted Authority *ALL whilst the

*PUBLIC is granted Authority *EXCLUDE. All objects in the libraries of the product (except some restricted special cases) are secured via the Authority list.

You can insert license keys for multiple products on the computer using one screen.

1. Select 14.WorkwithAuthorization from the BASESupport menu. The Add iSecurity Authorization screen appears.

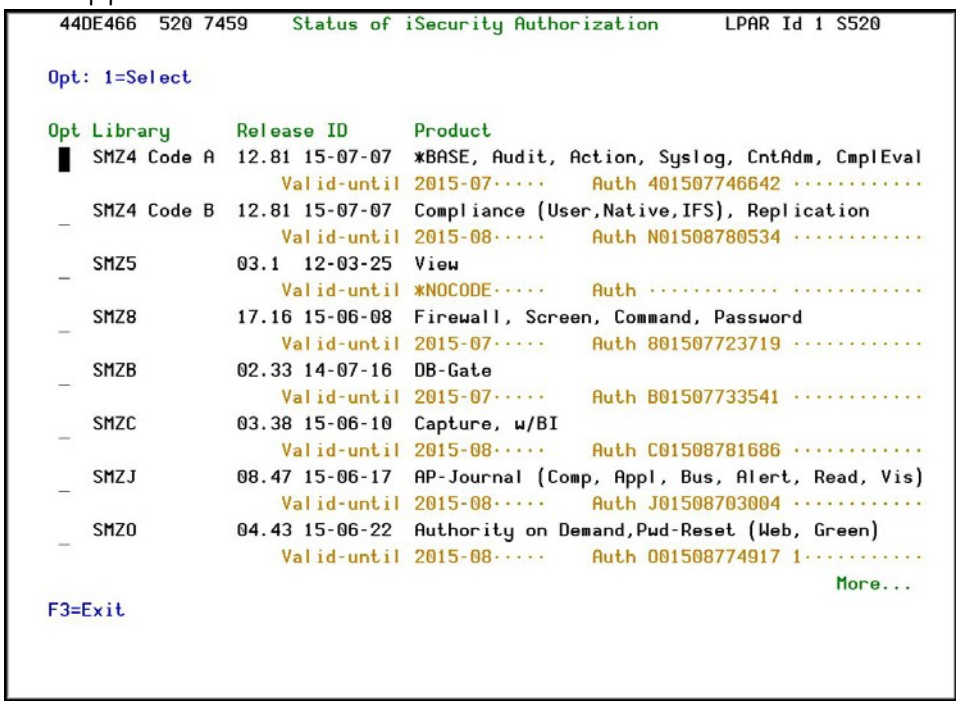


Add iSecurity Authorization (ADDISAUT)

2. Enter the required parameters and press Enter
.

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

1. Select 15.AuthorizationStatus from the BASESupport menu. The Status of iSecurity Authorization screen appears.



Status of iSecurity Authorization

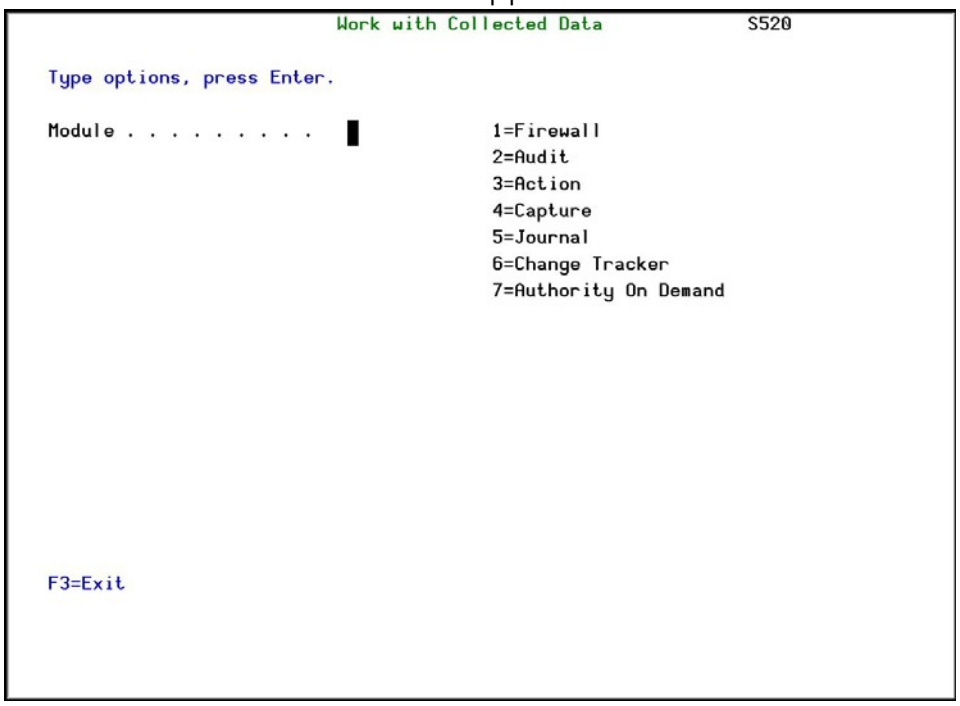
2. Select a specific line and type 1 in the Opt field to see the authority details of one specific product.

NOTE: Codes that will expire in less than 14 days appear in pink Permanent codes have deliberately been hidden in this screenshot.

Work with Collected Data

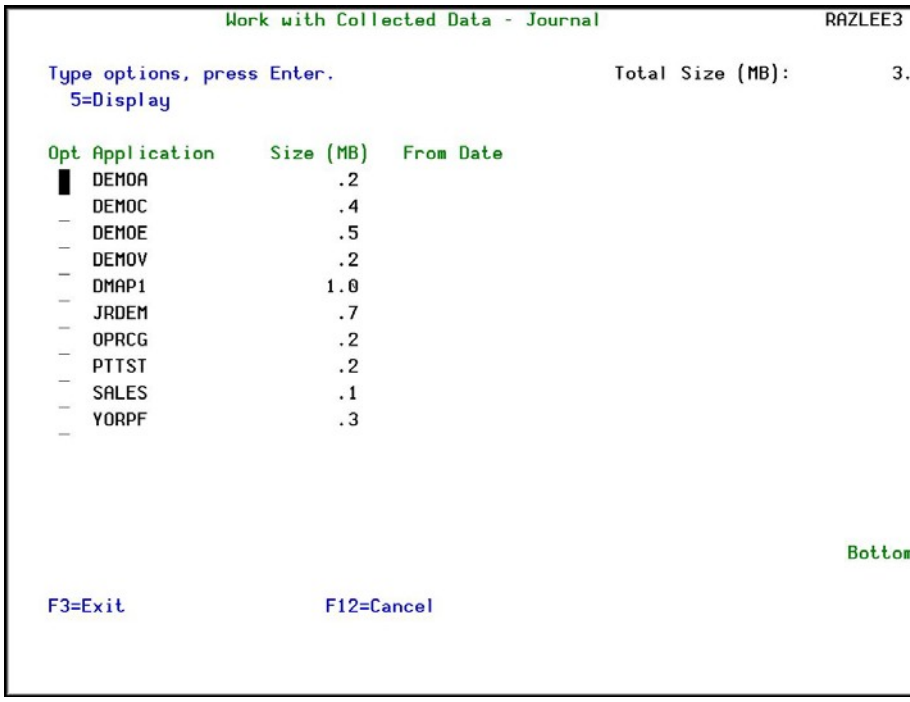
Administrators can view summaries of journal contents of various products by day, showing the number of entries for each day together with the amount of disk space occupied.

1. Select 51. Work with Collected Data from the BASE Support menu. The Work with Collected Data screen appears.



Work with Collected Data

2. Enter 5(Journal) and press Enter . The WorkwithCollectedData-Journal screen appears.



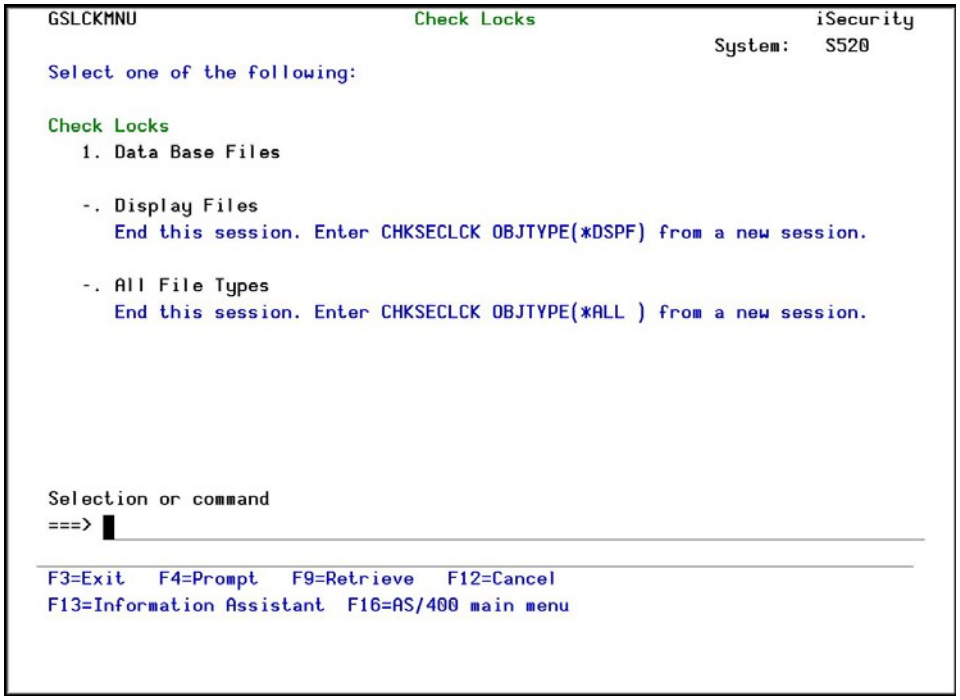
Work with Collected Data - Journal

3. Select 5 to see detailed information about a specific entry.

Check Locks

You need to run this option before you upgrade your system to check if any of the AP-Journal files are being used. If they are, you must ensure that they are not in use before you run the upgrade.

1. Select 52. Check Locks from the BASE Support menu. The CheckLocks screen appears.



2. Follow the instructions on the screen.
   *PRINT1 - *PRINT9 Setup

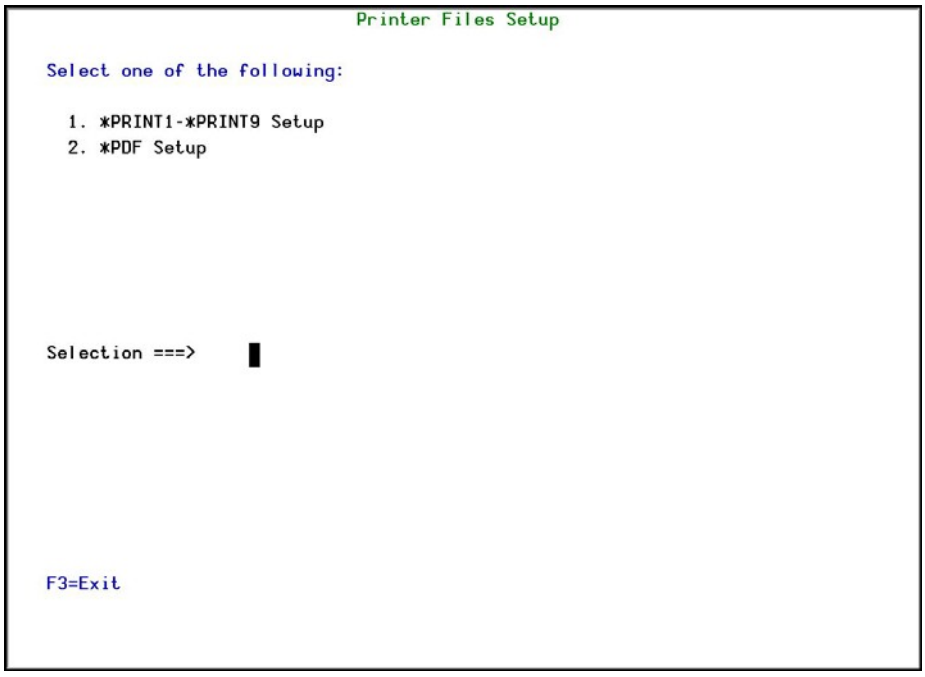
   AP-Journal allows you to define up to nine specific printers to which you can send printed output. These may be local or remote printers. ***PRINT1-*PRINT9** are special values which you can enter in the **OUTPUT** parameter of any commands or options that support printed output.

   Output to one of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the CHGOUTQ command to specify the IP address of the designated remote location and the name of the remote output queue.

   By default, two remote printers are predefined. ***PRINT1** is set to print at a remote location (such as the home office). ***PRINT2** is set to print at a remote location in addition to the local printer. In addition:

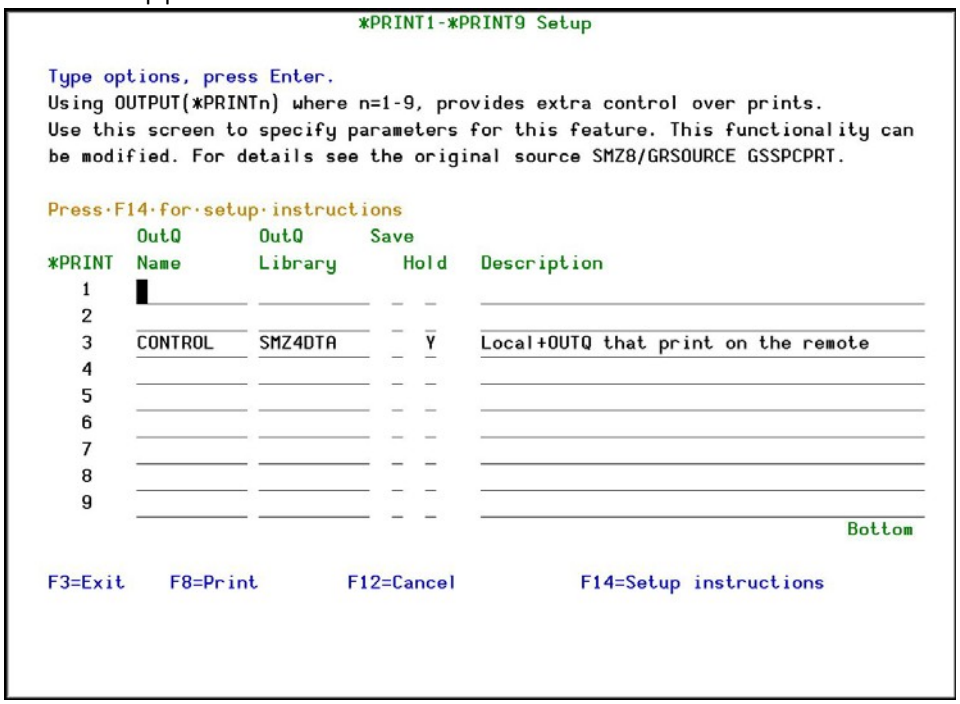
- *PRINT3 creates an excel file.
- *PRINT3-9 are user modifiable To define remote printers:

1. Select 58. *PRINT1 - *PRINT9, PDF Setup from the BASE Support menu. The Printer Files Setup screen appears.



Printer Files Setup

2. Enter 1 and press Enter . The *PRINT - *PRINT9 Setup screen appears.



3. Enter the name of the local output queue and library as shown in the above example. You can optionally enter a description.

Field	Description
OutQ name	The name of the local output queue
OutQ Library	The library of the local output queue
Save	Y = Yes N = No
Hold	Y = Yes N = No
Description	Enter a meaningful description (optional)

4. Enter the following command on any command line to direct output to the remote printer. This assumes that the designated output queue has already been defined.

CHGOUTQ OUTQ('local outq/library') RMTSYS(*INTNETADR)

+ RMTPRTQ('outq on remote') AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)

+ INTNETADR('IP of remote')

Parameter	Description
OUTQ()	Name of the local output queue
RMTPRTQ()	Name of the remote output queue
INTNETADR()	IP address of the remote system

If the desired output queue has not yet been defined, use the CRTOUTQ command to create it. The command parameters remain the same.

For example, *PRINT4 in the above screen, the following command would send output to the output queue 'MYOUTQ' on a remote system with the IP address '1.1.1.100' as follows:

CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS(*INTNETADR)

+ RMTPRTQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(*IP) TRANS- FORM (*NO)

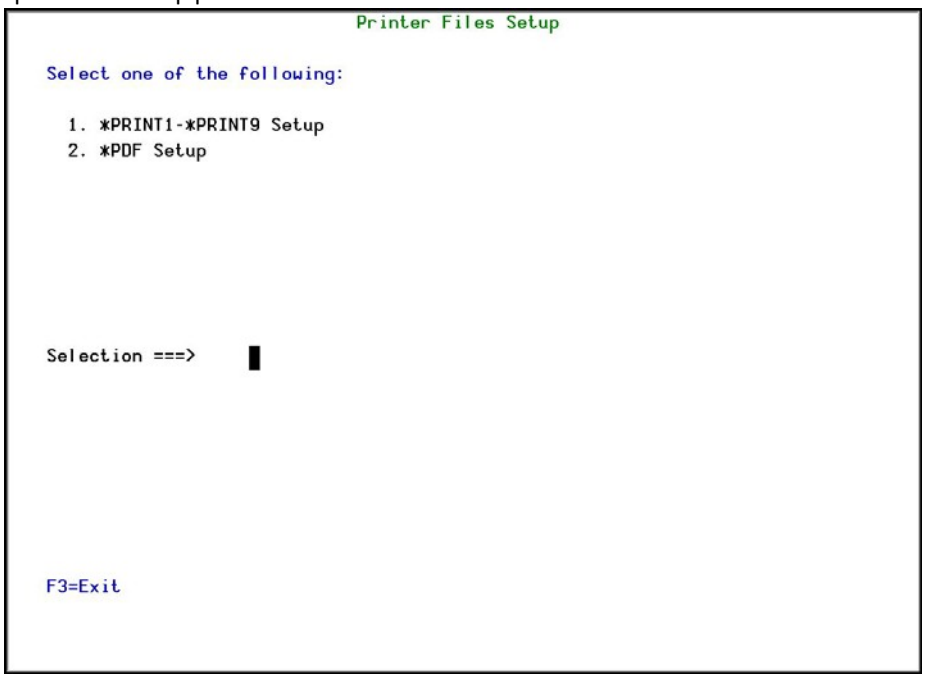
+ INTNETADR(1.1.1.100)

PDF Setup

The operating system, from release 6.1, directly produces *PDF prints. In the absence of such support a standard *PDF is printed by other means.

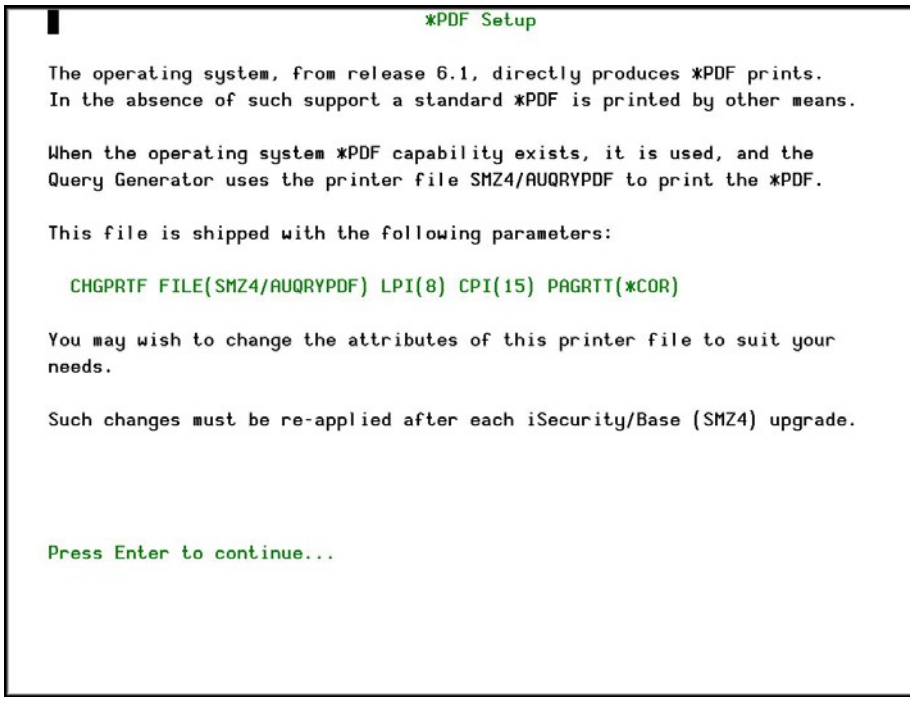
To define PDF printers:

1. Select 58. *PRINT1 - *PRINT9, PDF Setup from the BASE Support menu. The Printer Files Setup screen appears.



Printer Files Setup

2. Enter 1 and press Enter . The *PDF Setup screen appears.



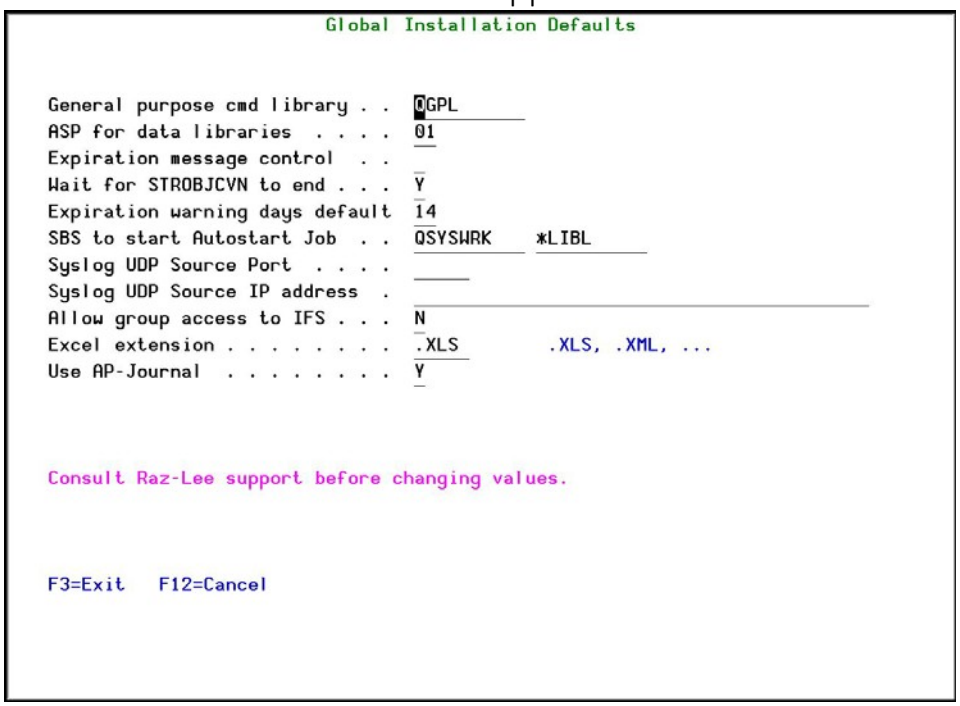
*PDF Setup

3. Follow the instructions on the screen.

NOTE: You must re-perform this task after every upgrade of AP-Journal.

You can set the parameters that iSecurity uses to control the Installation and upgrade processes.

1. Select 59. Global Installation Defaults from the BASE Support menu. The Global Installation Defaults screen appears.



Global Installation Defaults

Parameter	Description
General purpose cmd library	An alternative library to QGPL from which all STR* , RUN* , and *INIT commands will be run.

Parameter	Description
ASP for data libraries	Products being installed for the first time will be installed to this ASP. This refers to the product library and data library (for example, SMZ4, SMZ4DTA) In some products such as AP-Journal, other libraries are created. For example, in the AP-Journal a library is cre- ated per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number. Change the current ASP of the library. All future upgrades will use this ASP. All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.
Expiration message con- trol	Y =Yes N =No
Wait for STROBJCVN to end	Y =Yes N =No When installing the product on an OS400 version which is not the one that it was created for, objects require con- version and this is normally done in a batch job sent to work parallel to the installation. If you want the conver- sion to run inline, (wait until it ends), this field should be set to Y.
Expiration warning days default	All products whose authorization expires in less than this number of days are reported as an exception.

	Enter a number between 01 and 99. The default is 14 days.
SBS to start Autostart Job	The Subsystem name and library to use for the Autostart Job.
Syslog UDP Source Port	The source port for Syslog UDP
Syslog UDP Source IP Address	The source IP address for Syslog UDP
Allow group access to IFS	Y =Yes N =No Allow access to IFS from group profiles.
Excel extension	The extension to be used when creating Excel files .XLS .XML

Parameter	Description
Use AP-Journal	Y =Yes N =No If you want to use the self-journaling option that will allow you to trace all changes made to iSecurity prod- ucts, enter Y .

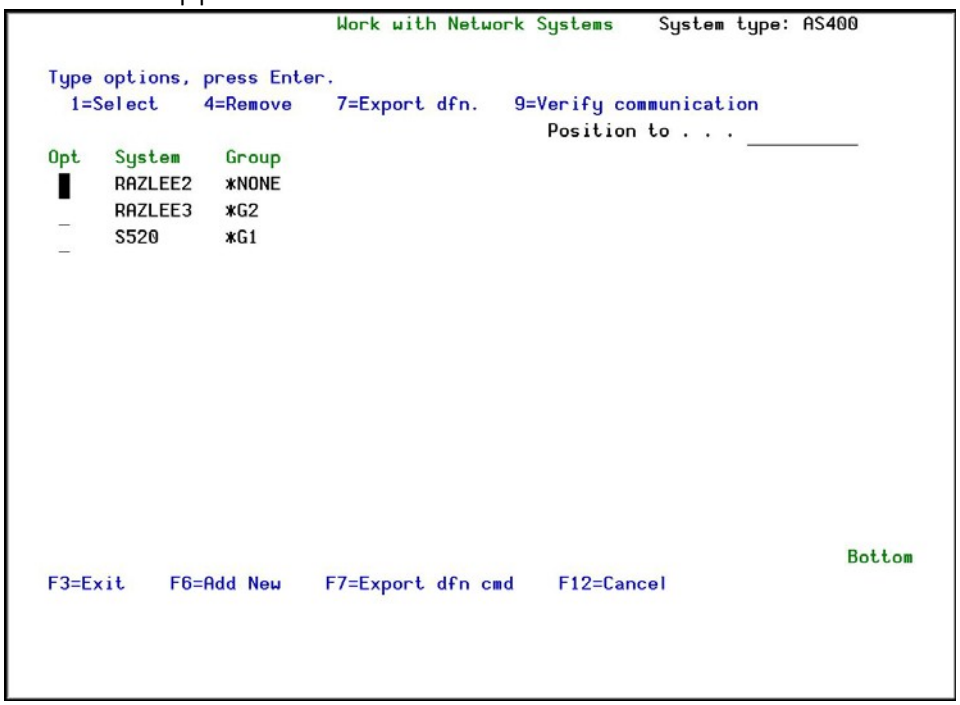
2. Enter your required parameters and press Enter .

NOTE: You should not change any of the values in this screen without first con- sulting with Raz-Lee support staff at support@razlee.com.

Work with Network Definitions

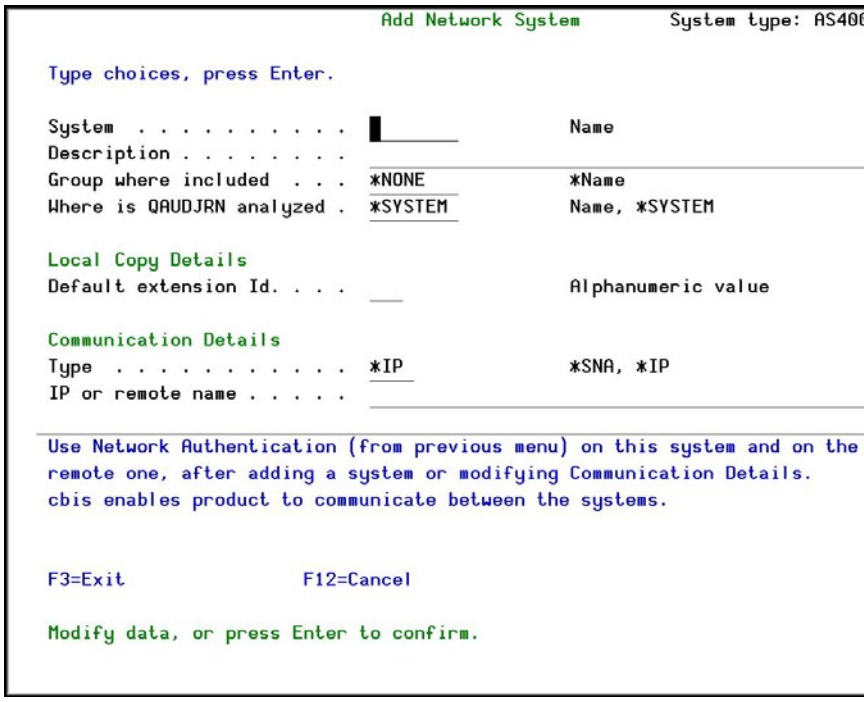
To get current information from existing report or query. Adjusting the system parameters only, to collect information from all the groups in the system to output files that can be sent via email.

1. Select 71.Workwithnetworkdefinitions from the BASESupport menu. The Work with Network Systems screen appears.



Work with Network Systems

2. Press F6 to define a new network system to work with. The AddNetwork System screen appears.



Add Network System

Parameter	Description
System	The name of the system
Description	A meaningful description of the system
Group where included	Enter the name of the group to which the system is assigned
Where is QAUDJRN ana- lyzed	Give the name of the System where QAUDJRN is ana- lyzed. Enter *SYSTEM if it is analyzed locally.
Default extension ID	Enter the extension ID for local copy details
Type	The type of communication this system uses *SNA *IP

Parameter	Description
IP or Remote Name	Enter the IP address or SNA Name, depending on the Type of communication you defined

3. Enter your required definitions and press Enter toconfirm .

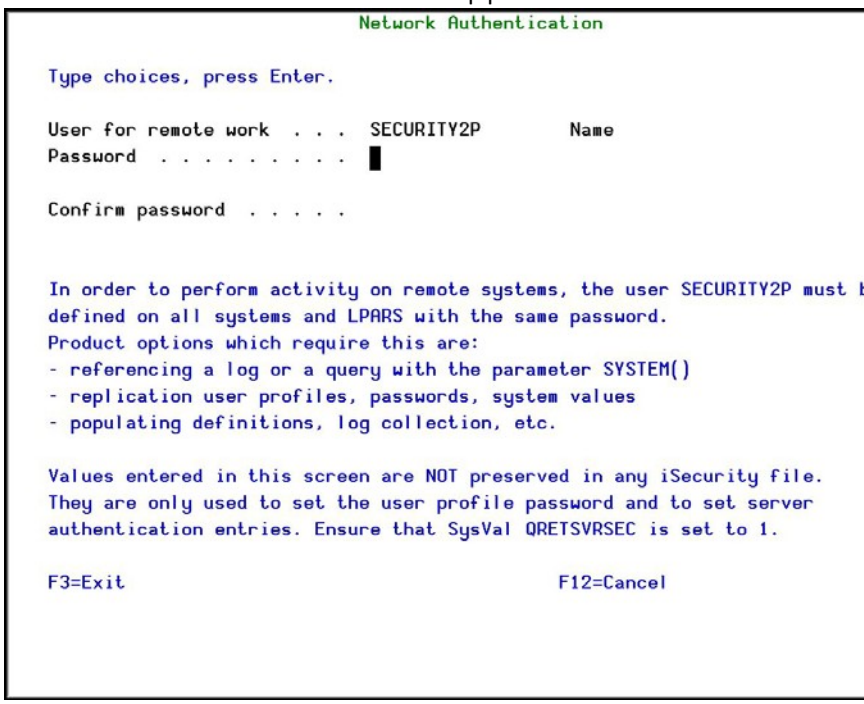
-

To perform activity on remote systems, you must define the user SECURITY2P with the same password on all systems and LPARS with the same password.

Product options which require this are:

- referencing a log or a query with the parameter SYSTEM()
- replication user profiles, passwords, system values
- populating definitions, log collection, and so on To authenticate the system:

1. Select 72. Network Authentication from the BASE Support menu. The Network Authentication screen appears.



Network Authentication

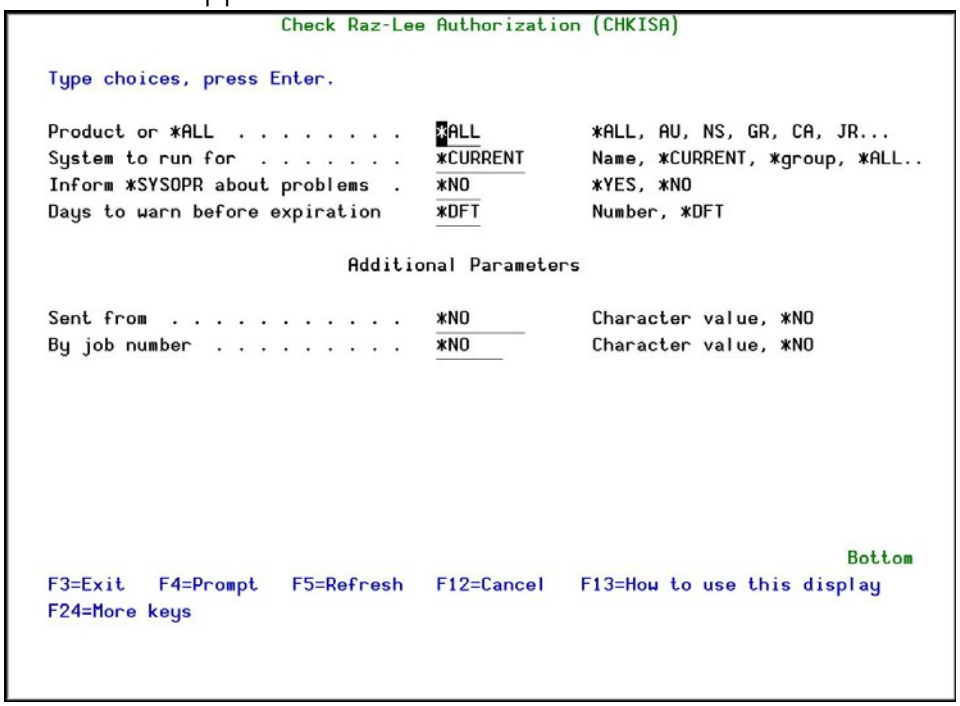
2. Enter the SECURITY2P user password twice and press Enter .

NOTE: The values entered in this screen are NOT preserved in any iSecurity file; they are only used to set the user profile password and to set server authentication entries. Ensure that the Return Server Security Data system value (QRETSVRSEC) is set to 1 (Retain Data).

You can set up the system so that the local *SYSOPR will get messages for all network wide authority problems.

Before you run this command, you must allow the system to run network commands and scripts. See Run CL Scripts on page 186 for more details.

1. Select 73.CheckNetworkAuthorityStatus from the BASESupport menu. The Check Razlee Authorization screen appears.



Check Raz-Lee Authorization

Parameter	Description
Product or *ALL	*ALL = report on all products AU = Audit NS = Native Object Security GR = Firewall CA = Capture JR = AP-Journal OD = Authority On Demand AV = Anti-Virus CT = Change Tracker DB = DB-Gate VW = View

Parameter	Description
System to run for	The system to run the authorization check for: Name = The name of a specific system in the network *CURRENT = The current system *group = The name of a group of systems *ALL = All systems in the network
Inform *SYSOPR about problems	*YES = *NO =
Days to warn before expi- ration	Number = Any system whose expiry date is less than this number of days will be reported. The default num- ber of days is 14. *DFT
Sent from	Value *NO
By job number	Value *NO

2. Enter your required options and press Enter .

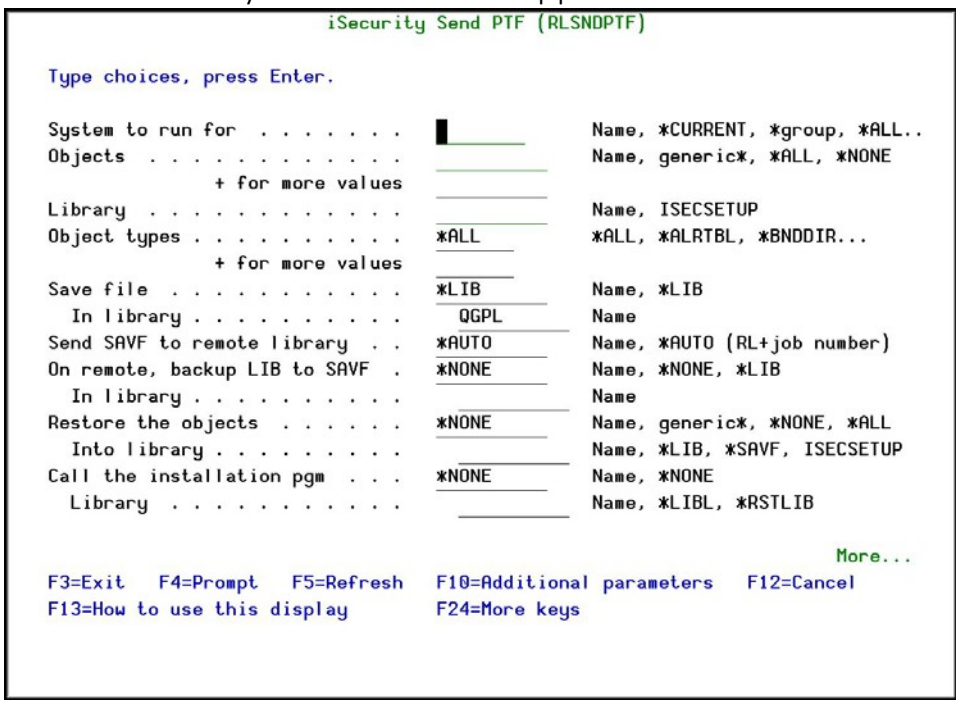
Send PTF

This option allows you to run of a set of commands that will send objects as a PTF. This option is restricted to iSecurity products only. If you need to send PTFs for other products, please contact RazLee Support.

Before you can use this option, ensure that you define the entire network, as described in Work with Network Definitions on page 177, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication on page 180.

To send PTFs

1. Select 74. Send PTF from the BASE Support menu. The iSecuritySend PTF screen appears.



iSecurity Send PTF

Parameter	Description
System to run for	The system to run the authorization check for: Name = The name of a specific system in the network *CURRENT = The current system *group = The name of a group of systems *ALL = All systems in the network

Parameter	Description
Objects	The objects you want to send. You can enter multiple values Name = A specific object generic* = A group of objects with the same prefix *ALL= All the objects *NONE= No objects need to be extracted, the SAVF has already been prepared
Library	The name of the library that contains the objects
Object types	The object types to be sent
Save file / Library	The name and library of the SAVF to contain the objects. If you enter *LIB for the file name, the name of the library containing the objects will be used. If you enter *AUTO as a name for the library, a library will be created with the name of RL< jobnumber >
Remote library for SAVF	The name of the remote library to receive the SAVF to contain the objects. If you enter *AUTO as a name for the library, a library will be created with the name of RL< jobnumber >
Restore objects	The objects to be restored Name = A specific object generic* = A group of objects with the same prefix *ALL = Restore all objects *NONE = Do not restore any objects
Restore to library	The name of the library to

	receive the restored objects Name = A specific library *LIB = the name of the original library containing the objects will be used. *SAVF = the same name as the SAVF
Program to run / Library	The name and library of a program to run after the objects have been restored.
Parameters	The parameters for the program that runs after the restore.

2. Enter your required options and press Enter .

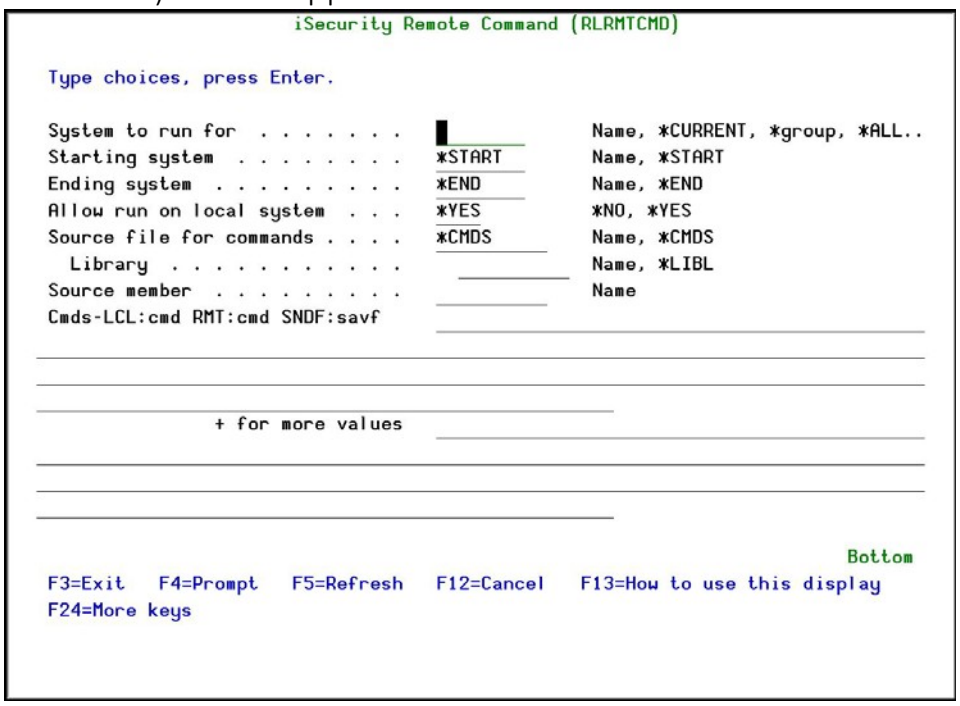
Run CL Scripts

This option allows you to run of a set of commands either from a file or by entering specific commands as parameters. Each command must be preceded by a label:

- LCL: Run the following command on the local system
- RMT: Run the following command on the remote system
- SNDF: Send the save file (format: library/file) to RLxxxxxxxx/file (xxxxxxxx is the local system name)
  You can use this option to define the commands to run to check system authorities, as described in Check Authorization Status on page 181.

  Before you can use this option, ensure that you define the entire network, as described in Work with Network Definitions on page 177, and that you define user SECURITY2P on all nodes, using the same password, as described in Network Authentication on page 180.

1. Select 75. Run CL Scripts from the BASE Support menu. The iSecurity Remote Command (RLRMTCMD) screen appears.



iSecurity Remote Command

Parameter	Description
System to run for	The system to run the authorization check for: Name = The name of a specific system in the network *CURRENT = The current system *group = The name of a group of systems *ALL = All systems in the network
Starting system	Use to define a the start of a subset within *group or *ALL This is useful if you want to rerun a command that previously failed

Parameter	Description
Ending system	Use to define a the end of a subset within *group or *ALL This is useful if you want to rerun a command that pre- viously failed
Allow run on local system	*YES = The remote command can run on the local sys- tem *NO = The remote command cannot run on the local system
Source file for commands	Name = The file where the commands to run are stored. *CMDS = Use the commands entered below
Library	Name = The library that contains the commands source file *LIBL =
Source member	Name = The member that contains the commands
Cmds -LCL:cmd RMT:cmd SNDF:savf	The commands that can be run (if the Source file for commands parameter is *CMDS): LCL:cmd = A command that will be run on the local computer RMT:cmd = A command that will be run on a remote computer SNDF:savf =

2. Enter your required options and press Enter .

Current Job CntAdm Log

Select 76. Current Job CntAdm Messages from the BASE Support menu to display the current job log.

Manage Resources

All Job CntAdm Log

Select 77.AllJobsCntAdmMessages from the BASESupport menu to display the job log for all jobs.

If it appears that AP-Journal is using too much resources after collecting statistics for two minutes, remember that the IBM i distributes CPU according to the job which requires CPU and has the highest Run Priority. AP-Journal runs in priority 60 which is LOWER than

regular batch jobs. It will accept CPU only when there is CPU available and no other job requires it. In such cases it may show high usage of CPU%

To improve the CPU usage do the following:

1. If AP-Journal is not alerting and its "today" data is not important – run journal at night.
2. Change run attribute to further improve per-formance.

AP-Journal backup system

Run the following command to ensure that the product releases the CPU at least once every second:

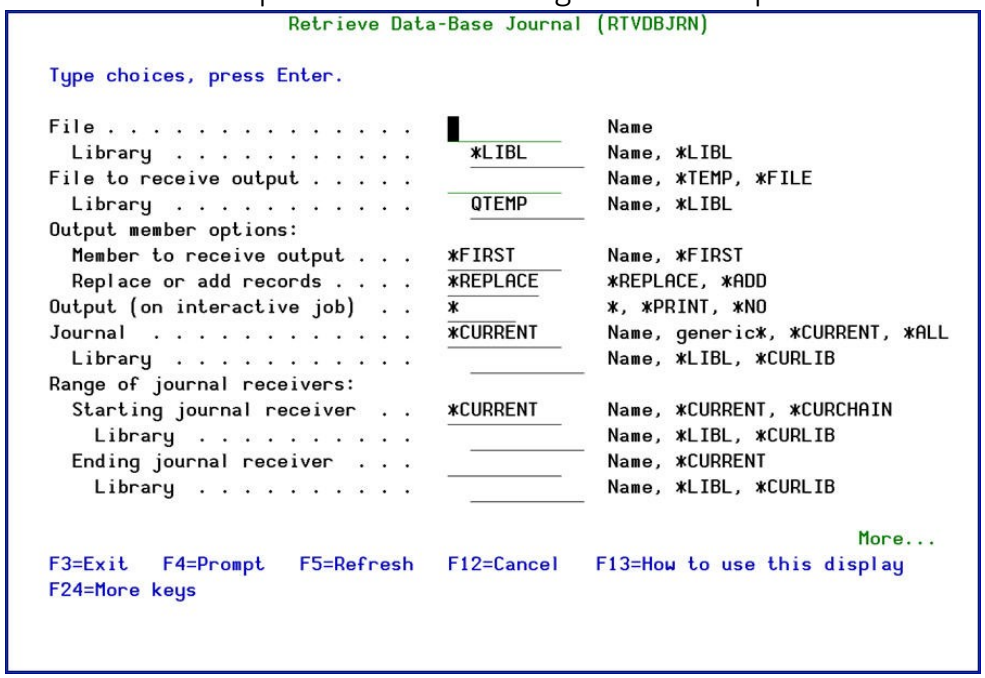
CHGCLS CLS(SMZJDTA/ZJOURNAL) TIMESLICE(1000)

Preferably use dedicated memory pools (performance know how is required) by doing one of the following:

- *CHGSBSD SBSD(SMZJDTA/ZJOURNAL) POOLS((1*SHRPOOLnn))*
- *CHGSBSD SBSD(SMZJDTA/ZJOURNAL) POOLS((1*BASE))*

To define how many days will the data remain in library SMZJ"Application" (SMZJCMBOL), select **1. Regulation Compliance** from the main menu and then select

9. Retrieve File Updates from the Regulation Compliance menu.



Retrieve Data-Base Journal (RTVDBJRN)

and what is the logic for the container change.

The daily maintenance program that runs during the night, will move the data files according to those parameters from the SMZJ"Application" (SMZJCMBOL) library, to the history libraries according to date parameter SMZJ'Date'=SMZJYYMMDD.

These files can be saved and removed.

When requesting a display of the history from the containers, the program will look in the SMZJ”Application” (SMZJCMBOL) library first. If the program does not find it, it will search the history libraries by date parameter SMZJ’Date’=SMZJYYMMDD. If the information is still not found, the program will act according to a missing data parameter MISDTA, while the possible values being *CANCEL/*IGNORE/*LOAD /*INQ …

If these files were saved and moved, the historical data can be reloaded and inquired.

If a file in SMZJ”Application” (SMZJCMBOL) was manually deleted, this procedure will not be available.