Capture™

The User Tracking Component of

iSecurity

User Manual
Version 4

RAZ-LEE™
The iSeries Security Experts

Updated: November 11, 2015

Copyright Notice

Visit our website at http://www.razlee.com .

Record your Product Authorization Code Here:

Computer Model:	
Serial Number:	
Authorization Code:	

About This Manual

Who Should Read This Book

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

Product Documentation Overview

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

Printed Materials

This user guide is the main printed documentation necessary for understanding **Capture**. It is available in user-friendly PDF format and 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/.

The **Capture** User Manual covers the following topics:

- Introduction
- Installation
- Start-up and Initial Configuration
- Using **Capture**

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

In addition, there is a quick-start, “Out-of-the Box” guide, which covers only installation and the basic steps needed to run the application. Contact your Raz-Lee distributor for more details.

Typography Conventions

- Menu options, field names, and function key names are written in **Sans-Serif Bold**.
- References to chapters or sections are written in *Italic*.
- OS/400 commands and system messages are written in ***Bold Italic***.
- Key combinations are separated by a dash, for example: **Shift-Tab**.
- Emphasis is written in **Times New Roman bold**.

Table of Contents

2

Chapter 1: Introducing Capture

Taking User Activity Tracking Seriously

In today's increasingly complex business environment, an effective audit trail is a key component of any organizational IT security program. In certain environments, such as banking and health care, regulations are now in effect that require organizations to maintain detailed transaction activity records and to retain these records for an extended period.

Simply creating a security policy and purchasing some security software tools is not enough. Management should ensure that security policies and procedures are properly implemented and enforced. In addition, managers must be able to evaluate and test the effectiveness of these policies on a continuing basis.

Outside auditing firms, as well as internal audit departments, routinely perform extensive reviews of data systems. Such audit programs typically involve:

- Transaction testing, including accuracy review
- Verification that transactions are initiated and approved only by authorized personnel
- Ensuring prompt detection and correction of errors with appropriate traceability
- Ensuring adequacy of the audit trail
- Implementing and testing the adequacy of IT security policy

Additionally, IT departments and technical support personnel need to monitor user activity in order to troubleshoot error conditions, track performance bottlenecks, and ensure compliance with organizational policies. This often requires detailed knowledge of not only what users are doing, but also, how they are doing it. Computer logs and audit reports, more often than not, do not provide enough forensic evidence for these purposes.

Auditors, managers and even many system administrators are less likely to be familiar with the complex, arcane nature of the IBM i (OS/400) operating system and its tools in today's IT environment. They need intuitive and user-friendly tools that provide solutions quickly and efficiently.

NOTE: This product works for Interactive jobs (INT)

Limitations of IBM i (OS/400) Auditing

The IBM i operating system, through its journaling facility, creates highly detailed logs of system activities. It is capable of tracking a wide variety of events and retains an extensive volume of data in its journal database. Unfortunately, IBM i provides only minimal, user hostile tools that allow operators to access and manage this data. Analysis and baseline tools are also sorely lacking.

The following is a list of several important limitations of IBM i auditing:

- IBM i journals alone do not provide a visual audit trail of activities that constitute a security breach or are contributing factors to errors. Likewise, the journals do not effectively track data entry errors or routine activities that violate organizational policies.
- The journals provide a primitive, unformatted data display of the journal log with minimal data filtering.
- IBM i lacks a query facility capable of easily extracting data buried in the journal database.
- IBM i provides no audit reports. You must manually export journal data to a file and then use Query, DFU or a third party query tool, such as **FileScope**, in order to create reports.
- Journal management is a difficult task. Unnecessary data in the security audit journal can adversely affect system performance and waste valuable disk space.

Limitations of IBM i (OS/400) Screen-Copy

As part of the native IBM i operating system which supports and runs the IBM AS/400 (also known as System i or System i) computers, IBM provides functionality for copying screen images of user sessions. This functionality includes capturing on-screen contents and saving the captured images as disk files.

The IBM i operating system includes a function called STRCPYSCN (Start Copy Screen) which enables copying Telnet session screen(s) onto a disk file. This function facilitates inspecting session activity at a later time.

The STRCPYSCN system function operates as follows:

- A monitor decides to start the STRCPYSCN function for a designated user session.
- The user session receives a message which “breaks into” its regular activity announcing that the screen is about to be copied and requesting confirmation from the user.
- When the user confirms this request, all session activity is recorded to a file.

The above described activities transpire without any further intervention to the session being monitored.

The Capture Solution

Capture is a unique solution that complements journals and reports with a visual audit trail of user activity. This powerful data security product shows exactly what users are doing and when they are doing it. **Capture** helps organizations comply with the strict security regulations that apply to many industries such as banking, insurance, health care, and defense. **Capture** also provides invaluable traceability capabilities to technical support departments by tracking user activities that result in application or system errors.

Principal Features

- Providing the possibility to display (that is, to replay) captured user session screens and to search contents or patterns in the captured screens. Such searching enables locating screen images in accordance with auditor's or regulator's requests.
- A monitor which decides to activate the STRCPYSCN system functionality for designated TELNET sessions. The decisions of this monitor are based on sets of rules which relate, for example, to the time of day, the user of the TELNET session, the IP address of the TELNET session, the device of the TELNET session, and so on.
- Nullifying the system requirement regarding confirmation by users whose screen images are to be recorded. The importance of this feature is in order to actually "capture" possibly illicit behavior without the user being aware that the incriminating session is being recorded.
- Before activating the system function, the user session attributes are modified so that the message will be issued will not "break" into the session but rather will be handled by an automatic feature of this method without the knowledge of the user.
- At the time the STRCPYSCN system function is activated, the message which is sent to the TELNET session as a result of this activation does not "break" into nor interfere with the on-going session activity. Rather the message is responded to automatically.
- A method which generates a warning when the user whose screen images are to be recorded actually initiates the session. It is at this point that Capture enables the possibility of copying screens.
- Managing all accumulated user session information to provide advanced capabilities for managing these saved session files.
- Facilitates retrieval of captured screens with an easy-to-use process and free text search capability.

- If, after inspection, the monitor realizes that the user session screens are not being copied to a disk file, the monitor will once again initiate the STRCPYSCN function.
- Preserves job logs and CL Command logs for subsequent review, changes the job attributes to ***LOGCLPGM(*YES)***.
- Uses a simple rule definition process suitable for both IT professionals and non-technical users
- Archives captured screens offline to meet data retention requirements without consuming excessive disk resources

How Capture Works

Capture works silently and invisibly in the background without adversely affecting system performance. User may not even be aware that it is working.

Screen Captures

Screen captures occur only when needed. It is not practical to track all users all the time, especially in a large organization, as this would affect system performance and it would be impossible to review such a large volume of data effectively.

Capture automatically triggers screen capturing according to predefined rules covering a variety of circumstances using variable criteria such as:

- Incoming IP address including subnet mask
- Day and time
- Job (Session or Terminal ID)
- User profile
- Subsystem

You can also manually initiate a screen capture session at any time, for example to track a suspicious user or error condition. **Action** can also trigger a manual capture session based on its rules.

Backup

Once a day, the previous day's recorded user screen sessions are transferred to a library named SMCPyymmdd. This library contains the log file and the data file for all the sessions which were "captured" during that day; these user screen sessions can be displayed using option **42. Display Restored Log** or printed/displayed using option **46. Display Restored Data**.

Information that is older than the specified retention definition (as defined using option **81. System Configuration** then option **2. Capture Retention**) can be backed up. If a backup program was defined on this screen, the backup program will run automatically before the captured data is deleted.

When the information is copied to a separate backup library, the library's name is updated in the online log; this online log is kept for an unlimited amount of time.

When an auditor or system administrator wishes to access a library, **Capture** first looks for the requested information in the product library, **SMZCDTA** (**SMZ4DTA** in previous releases). If the information is not found in this library, **Capture** will look for it in the backup library pointed to by the entry in the log.

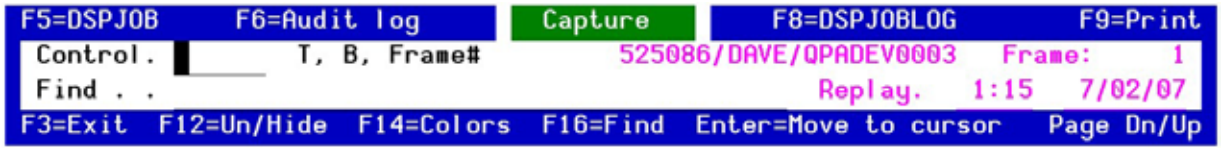
When historical (backed up) information is requested, a message will be sent to the system operator, requesting to load the backup library where the old information is stored.

Options **42. Display Restored Log** and **46. Display Restored Data** may be useful in this situation.

Retrieving Captured Screens

You can retrieve captured screens by means of an intuitive process and easy-to-use tools for locating the captured data screens and logs. Screens are arranged according to individual capture 'sessions'. Within each session, you can scroll through the screens sequentially or you can use the moveable **Capture Menu** to move directly to a particular screen or search for screens containing a specific text string.

The **Capture Menu** also provides commands for displaying the job log and the **Audit** log entries related to that particular screen and capture session. You can even access the ***DSPJOB*** command and print the screen directly from the **Capture Menu**.



Capture Menu

Integration with iSecurity

Capture is an integral part of the i**Security** suite and, as such, is designed to work together with other components in order to provide a comprehensive security auditing solution.

Effective security auditing requires several tools to provide a high level of traceability. The **Audit** tools add powerful query and reporting functionality to the IBM i operating system. These logs and reports, together with the visual audit trail provided by **Capture** together provide complete documentation of what is going on in your System i environment.

The visual audit trail also compliments the active security components, **Firewall** and **Screen** by showing specifically what a user did to trigger a given event. For example, if a particular user program repeatedly executes SQL commands that are rejected by **Firewall**, the captured screens can show when and how the user ran that program. This, in turn, helps to determine if indeed a security problem exists or perhaps that the **Firewall** rule needs to be modified.

Most importantly, **Action** rules can automatically trigger a capture session whenever a suspicious event occurs. This means that, even if a session is not being recorded, an event such as an attempt to access confidential data or an unusual error condition will turn on the **Capture** camera without the user's knowledge.

NOTE: *While* **Capture** *is active, transfer to a secondary job* (**System Request 1**) *is not available. You cannot start a copy to a job that has an active secondary job.*

New in Capture 4.0

- You can now set a Capture ALL rule.
- A new menu has been added – the **BASE Support** menu. This menu is option **89** in the main menu. This menu is available in all major iSecurity products and groups together all major common support activities. Some of the options for this menu have been taken from the **System Configuration** and **Maintenance** menus. To work with the new menu, you must install base library SMZ4.
- Double byte characters are now displayed correctly.
- You no longer receive missing member messages when displaying captured data.
- Data compression is now used on the log file to save disk space.

New in Capture 3.0

- Capture Business Items (CBI), Beta version. By focusing on application-specific business items such as customer number, loan number, patient number, and so on, CBI provides application managers and auditors alike with additional tools for ensuring application functionality.
- DSPCPT existing commands added as 45, 46. The output file can be sent as a compressed (ZIP) file. This reduces the size of the file by up to 90%.

New in Capture 2.0

- Improved Support of Group and Alternate Jobs, this version has improved support of Group jobs (same job name, same user, up to 16 on one screen). Alternate jobs (same job name, up to 2 on one screen – each can be a group job with up to 16 jobs), are handled better. The restriction of not being able to switch between alternate jobs while the screen is captured remains as this is an IBM restriction
- Improved Maintenance Process of Captured Log Files, the maintenance process of captured log files has been improved. In fact, a maintenance job which executes after a long period of time (not daily) will not cause data to disappear. The problem about entries with 0 frames, as well as user activity that has not been captured.
- Start Capture User Added, STRCPTUSR Start Capture User has been added to the known STRCPTSCN Start Capture Screen.

Other iSecurity Products

Action intercepts security breaches and other events in real-time and immediately takes appropriate corrective action. Actions may include sending alert messages to key personnel and/or running command scripts or programs that take corrective steps. No effective security policy is complete without **Action**.

Anti-Virus provides virus detection and prevention. Anti-Virus scans, validates, and checks IFS files as they are enrolled or modified, authenticates them, and erases/quarantines infected files. Includes updateable database and simple interface.

AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal.

Assessment checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.

Audit is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit triggers customized responses to threats via the integrated script processor contained in Action.

Authority on Demand (AOD) provides an advanced solution for emergency access to critical application data and processes, which is one of the most common security slips in System i (IBM i) audits. Current manual approaches to such situations are not only error-prone, but do not comply with regulations and often stringent auditor security requirements.

Change Tracker automatically tracks modifications in the software and file structure within production libraries. Changes are tracked at both the object and source levels. It does not require any special actions by programmers.

Command monitors and filters commands and their parameters before they are run, enabling you to control each parameter, qualifier or element, in conjunction with the context in which it is about to run. Options include Allow with Changes, and Reject. It includes a comprehensive log, proactive alerting and easily integrates with SIEM

DB-Gate empowers IBM i customers with exciting data access capabilities, based on Open database Connectivity (ODBC), employing standard IBM i facilities to enable full database-transparent access to remote systems.

Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via predefined entry points, and profiles activity by time. Its Best Fit Algorithm decreases system burden with no security compromise.

Password is a general-purpose password management product that ensures user passwords cannot be easily guessed or cracked. Password allows you to manage a variety of password security parameters and maintains a history log of attempts to create passwords. This log can easily be displayed or printed.

Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific time-out capabilities. Screen locking and signoff periods may be defined according to variable criteria such as date, time of day or user profile.

View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, and so on. Restricted users see asterisks or zeroes instead of real values. View requires no modification to existing applications.

Visualizer is an advanced data warehouse statistical tool with state-of-the-art technology. It provides security-related analysis in GUI and operates on summarized files; hence, it gives immediate answers regardless of the security data amount being accumulated.

2

Chapter 2: First Steps

Overview

This chapter guides you through the steps necessary to begin using **Capture** for the first time. Also covered in this chapter are the basic procedures for configuring the product for day-to-day use.

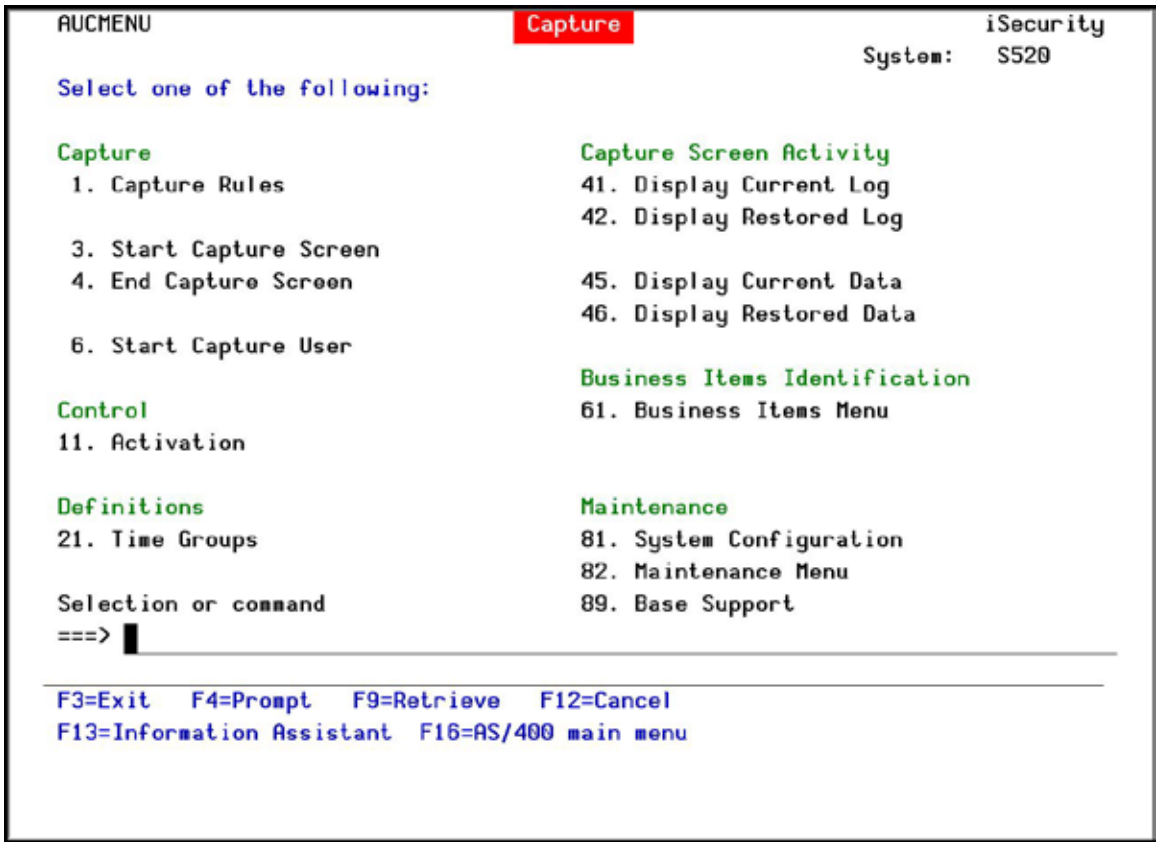
The following is an overview of the initial **Capture** process.

- Starting **Capture** for the First Time
- Configuring **Capture**
  - Defining General Definitions
  - Defining **Capture** Retention
  - Using **Capture** for the First Time
  - Practical Tutorials for Working with **Capture**

Starting Capture for the First Time

In order to use this product, the user must have ****SECOFR*** special authority. An additional product password may also be required to access certain functions. The default password is ***QSECOFR***. We recommend that you change this password as soon as possible, using the procedure described below.

1. To start **Capture**, type the ***STRCPT*** command at any command line. The main menu appears.



Capture Main Menu

2. Continue to the following procedures.

Configuring Capture

Capture is ready-to-run right out of the box. You should, however, review the default configuration parameters that control important features before using the product for the first time.

There is no "typical" or "optimal" configuration for a security product such as **Capture**. Each installation or application has different operational criteria and security needs. The auditing requirements for a large manufacturing environment are quite different from those for a bank, a software developer or a service organization.

To work with product configuration, select **81. System Configuration** from the main menu. The **System Configuration** menu appears.

```
CAPARMR              iSecurity/Capture System Configuration   27/04/14 14:24:43

Select one of the following:

Capture
 1. General Definitions
 2. Capture Retention
 3. Set Highlight Color

 7. Business Items Support


13. E-Mail Definitions

                                      General
                                        91. Language Support
Selection ===>                          99. Copyright Notice

Release ID . . . . . . . . . . . . . . . 03.24 13-10-14    44DE466  520 7459
Authorization code . . . . . . . . . . . C01404762713               1   S520


F3=Exit    F22=Enter Authorization Code
```

iSecurity/Capture System Configuration

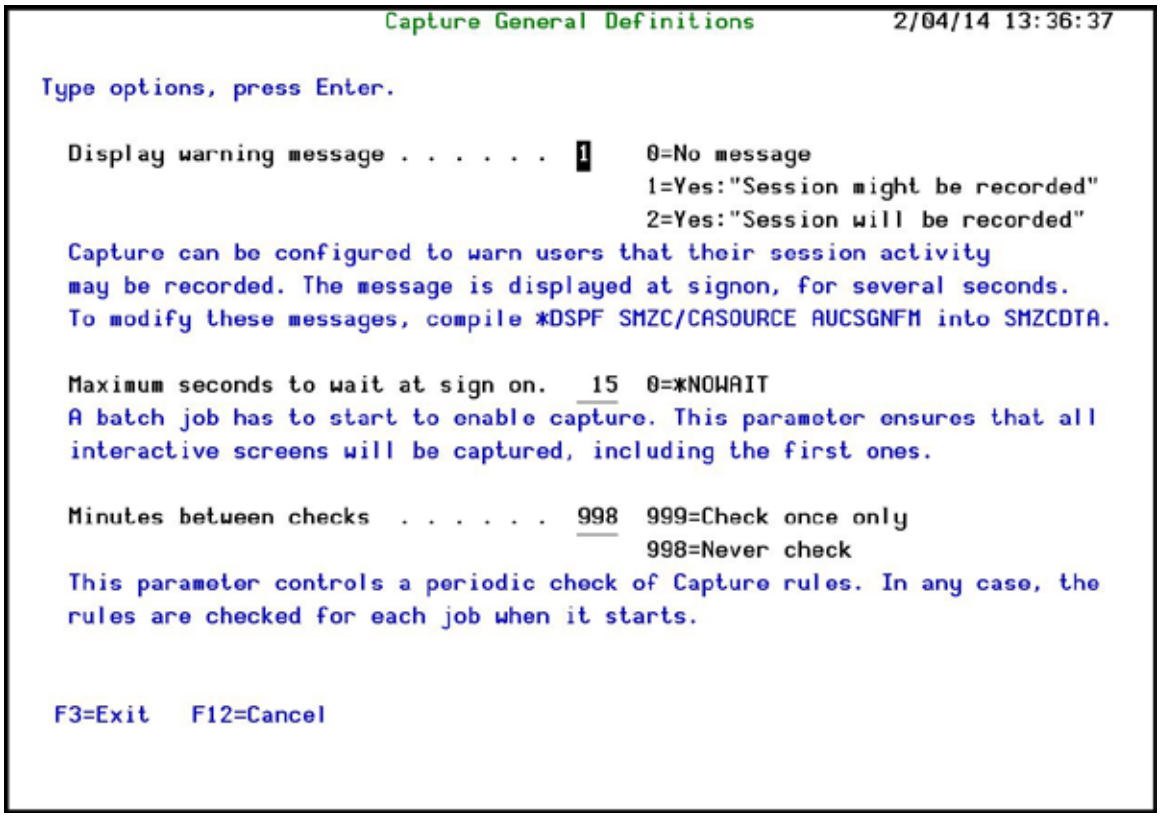
NOTE: *After you modify any of the parameters accessible from this menu, the message* "**Modify data, or press Enter**" *appears upon return to the menu.*

You must press **Enter** *again in order to save your changes and leave this menu. If you press* **F3**, *you will lose any changes that you have made.*

Defining General Definitions

You can choose to warn users that **Capture** is monitoring user activity on their workstation by selecting the **Display Warning Message** option. Warning messages appear each time a user signs on for a session. You can define the time to wait at sign on, so as to enable **Capture** to start before interactive jobs start and also how often to check **Capture** rules.

1. Select **1. General Definitions** from the **System Configuration** menu. The **Capture General Definitions** screen appears.



Capture General Definition

Parameter	Description
Display warning message	Capture can be configured to warn users that their session activity may be recorded. The message is displayed at signon, for several seconds. To modify these messages, compile *DSPF SMZC/CASOURCE AUCSGNFM into SMZCDTA. **0**=No message **1**=Yes: "Session might be recorded" **2**=Yes: "Session will be recorded"

Parameter	Description
Maximum seconds to wait at sign on	A batch job has to start to enable capture. This parameter ensures that all interactive screens will be captured, including the first ones. Time in seconds (1 – 999) **0**=*NOWAIT
Minutes between checks	This parameter controls a periodic check of Capture rules. The rules are always checked for each job when it starts. Time in minutes **999**=Check once only **998**=Never check

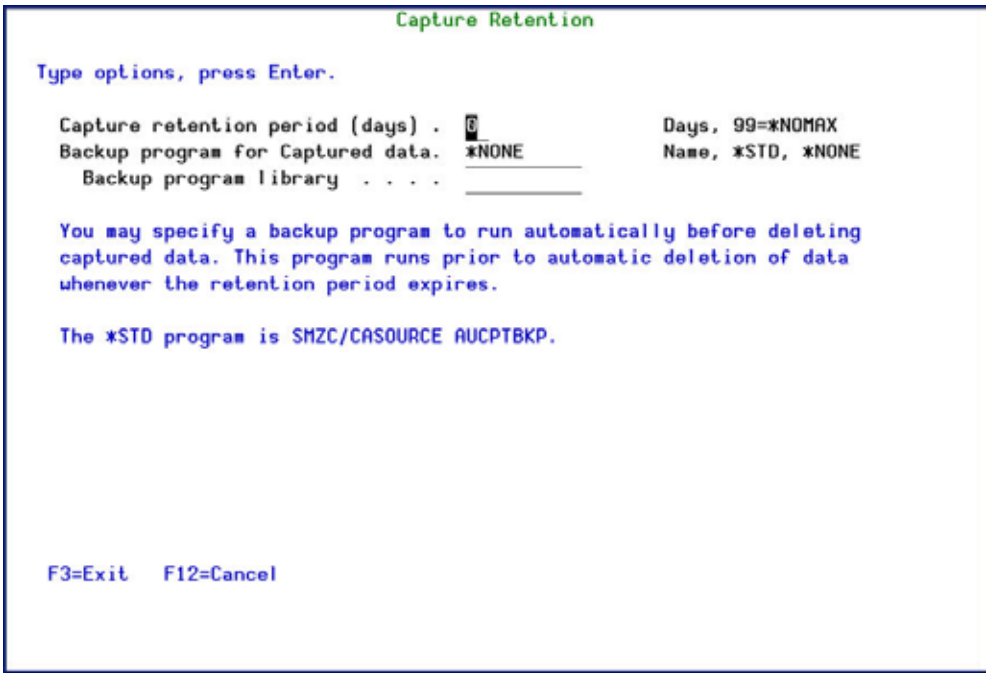
2. Enter your required parameters and press **Enter** to continue.

Defining Capture Retention

You can define the length of time that captured screens are retained on-line and also specify a backup routine to store archived captures off-line automatically after the designated retention period has expired. In order to ensure compliance with data retention requirements in certain industries, it is highly recommended that you store archived captures on external media, such as tape or optical media.

Captured Data Retention Period

1. Select **2. Capture Retention** from the **System Configuration** menu. The **Capture Retention** screen appears.



Capture Retention

Parameter	Description
Capture retention period (days)	Days **99**=*NOMAX
Backup program for Captured data	Name of a backup program that your organization provides ***STD**=the default backup program provided with **Capture**. The *STD program is SMZC/CASOURCE AUCPTBKP. ***NONE**
Backup program library	Name of the library where the backup program is stored.

2. Enter your required parameters and press **Enter** to continue.

Setting Highlight Color

You can specify a specific color to highlight key words specified in a free-text search of captured screens. All instances of the key words will appear in this color on the captured screen.

1. Select **3. Set Highlight Color** from the **System Configuration** menu. The **Capture Retention** screen appears.

Highlight Colors

2. Select the desired color and press **Enter** to continue.

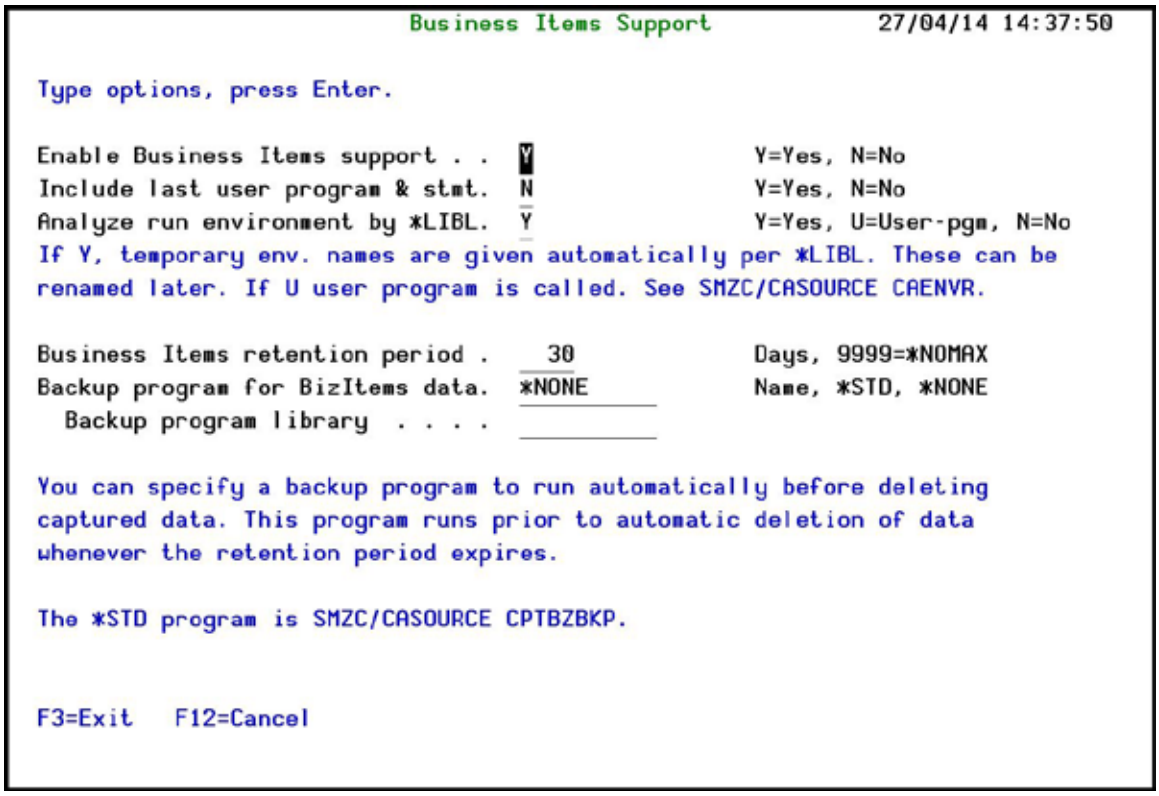
Auto-Save Definition

You can define a period of time in days after which all Capture files will automatically be saved.

Defining Business Items Support

You can define the Business Items Support parameters, such as if Business Items Support is enabled, for how long to retain Business Items, automatic backups of Business Items, and so on.

1. Select **7. Business Items Support** from the **System Configuration** menu. The **Business Items Support** screen appears.



Business Items Support Definitions

Parameter	Description
Enable Business Items support	**Y** = Yes **N** = No
Include last user program & stmt	**Y** = Yes **N** = No

Parameter	Description
Analyze run environment by *LIBL	**Y** = Yes **U** = User written program **N** = No If you select **Y**, temporary environment names are allocated automatically for the *LIBL and they can be renamed later. See *Environments* on page *78* for more information. If you select **U**, a user program is called. For an example, see SMZC/CASOURCE CPTBZBKP.
BizItems retention period (days)	The length of time in days that Business Items are retained online. Days **9999**=*NOMAX
Backup program for BizItems data	Name of the backup program that your organization uses ***STD**=the default backup program provided with **Capture**. The *STD program is SMZC/CASOURCE CPTBZBKP. ***NONE**
Backup program library	The name of the library where the backup program is stored.

2. Enter your required parameters and press **Enter** to continue.

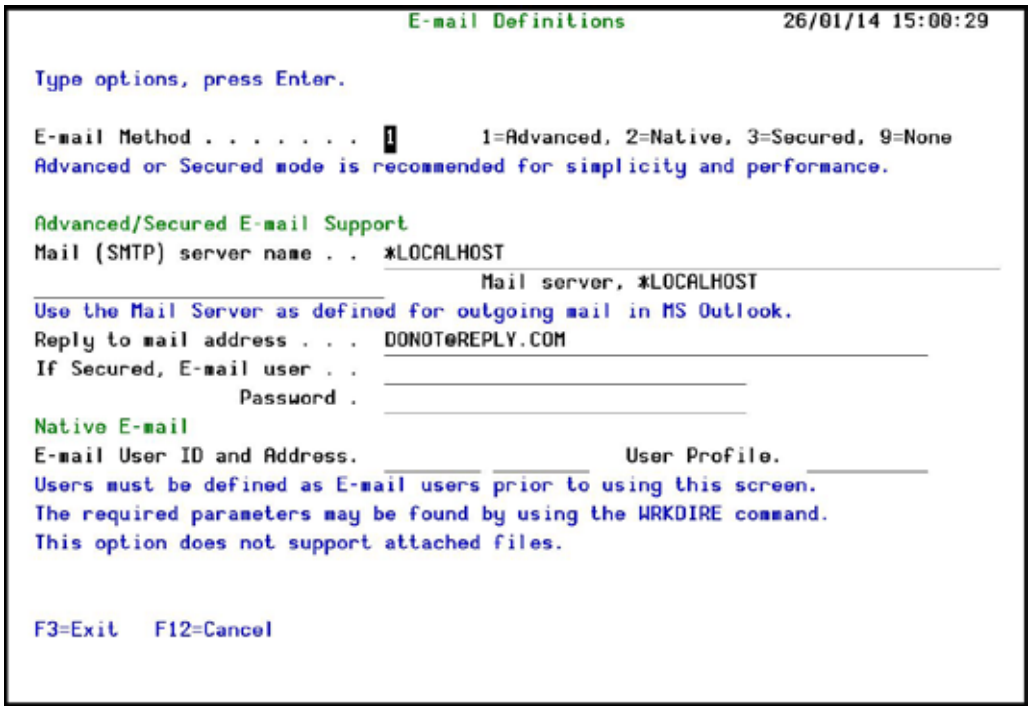
To work with Business Items, see *Chapter 5: Capture Business Items* on page *56*.

Email Definitions

Before **Capture** can send e-mail messages, your System i must be properly configured to send e-mail and at least one e-mail user must be defined in the Directory Entries table (***WRKDIRE***). This procedure can be quite complex and is beyond the scope of this manual. Refer to the appropriate IBM documentation for more details on these procedures.

To configure **Capture** to send e-mail messages, perform the following steps:

1. Select **13** from the **iSecurity/Base System Configuration** menu. The **E-Mail Definitions** screen appears.



Action E-mail Definitions

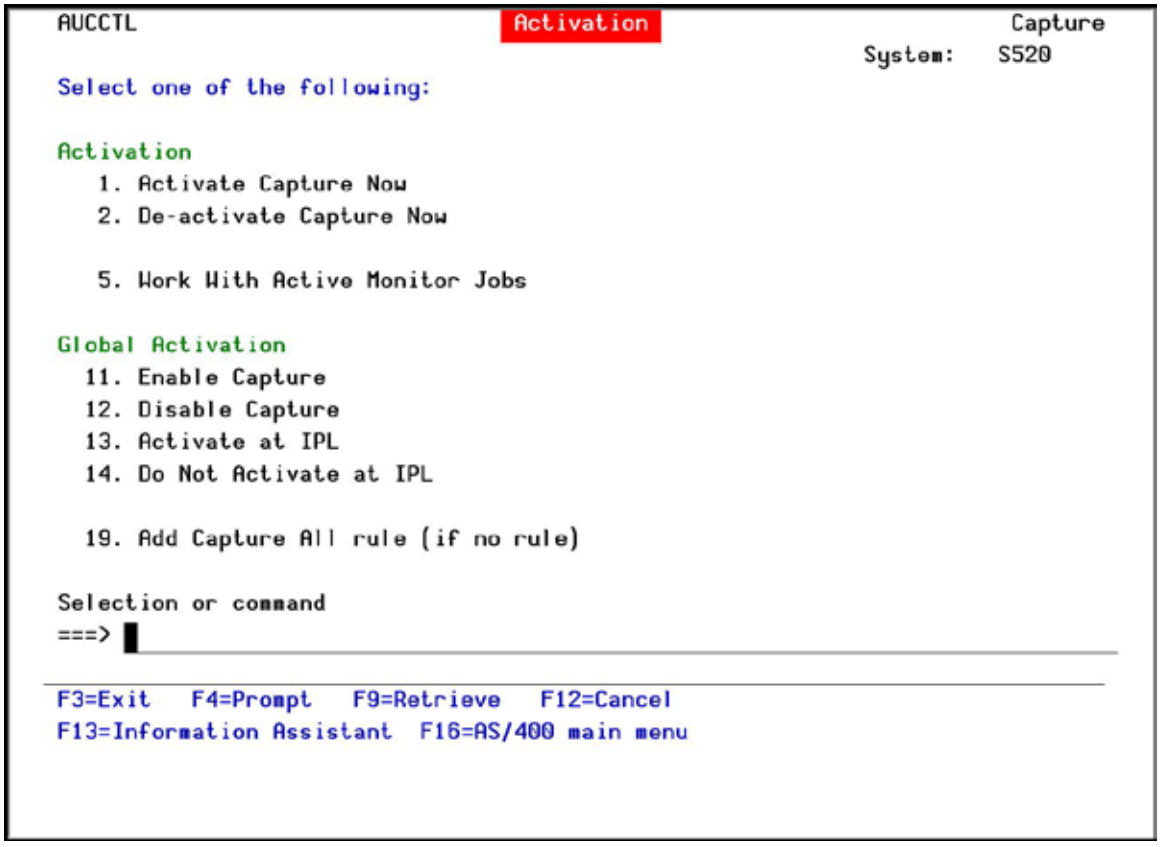
Parameter	Description
E-mail Method	**1**=Advanced **2**=Native **3**=Secured **9**=None Advanced or Secured mode is recommended for simplicity and performance. **Note**: If using **2**=native, Users must be defined as E-mail users prior to using this screen. The required parameters may be found by using the WRKDIRE 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.
If secured, 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 the required parameters and press **Enter**.

Activating Capture

You must activate the **Capture** monitor in order to enable the automatic capture features. It is strongly recommended that you configure **Capture** to activate automatically each time an IPL occurs on your System i.

To work with activation, select **11. Activation** from the main menu. You should perform each of the following activities prior to using **Capture** for the first time.



Activation

Local Activation

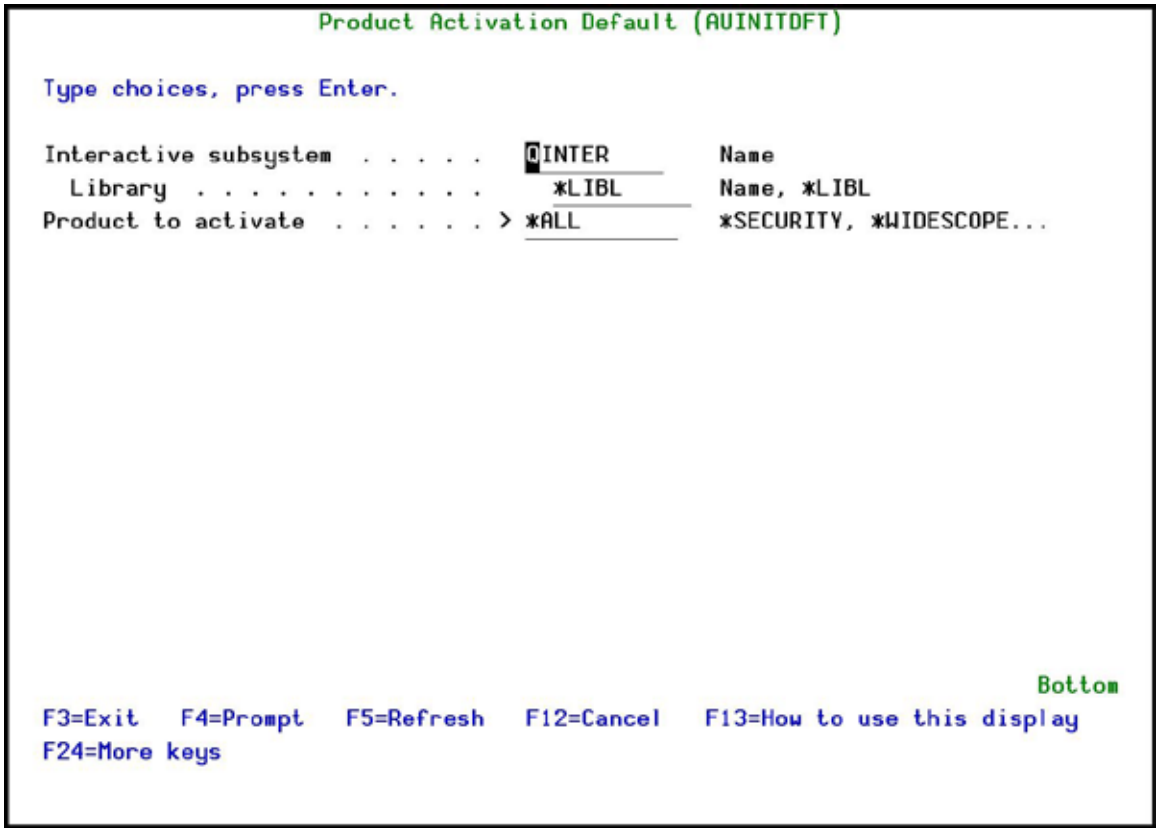
- To activate the **Capture** monitor, select **1. Activate Capture Now** from the **Activation** menu.
- To de-activate the **Capture** monitor, select **2. De-activate Capture Now** from the **Activation** menu.

Global Activation

Manual Activation

To enable **Capture**:

1. Select **11. Enable Capture** from the **Activation** menu. The **Product Activation Default** screen appears.



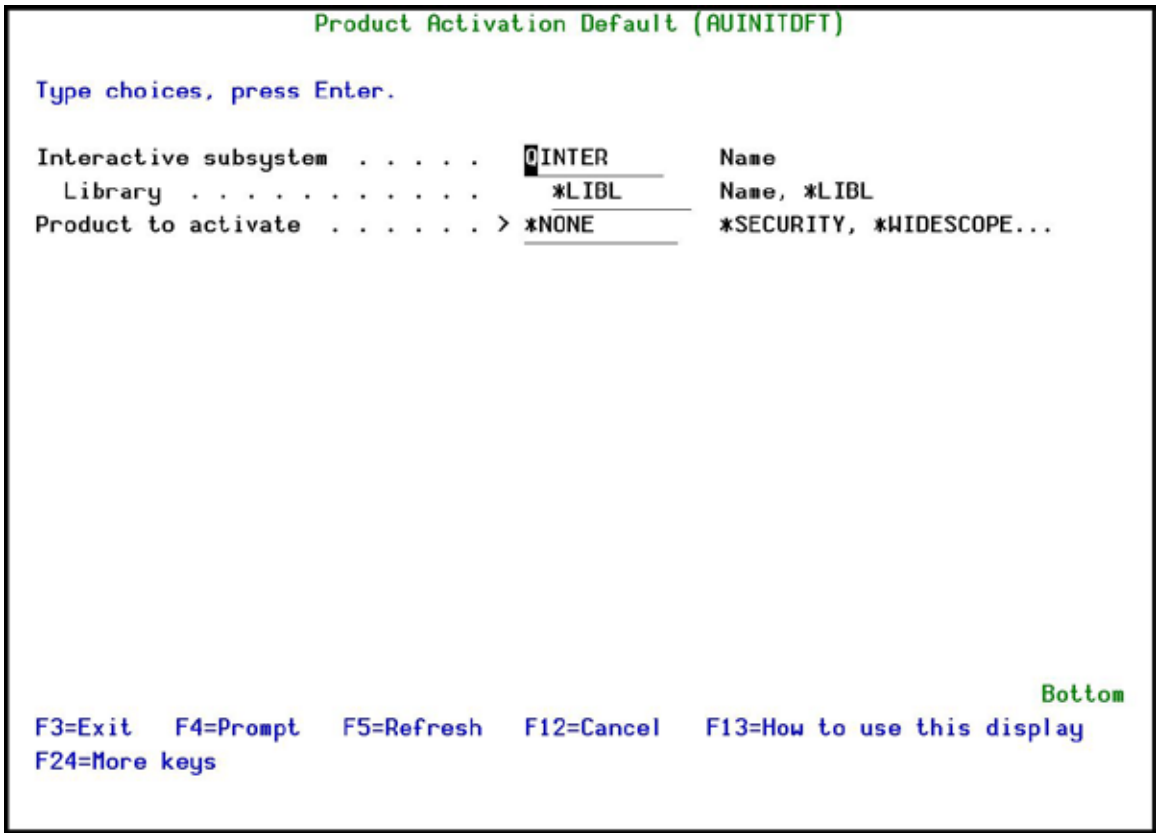
Product Activation Default

Parameter	Description
Interactive subsystem	**Name** = Type the name of the subsystem for which you want to enable **Capture**. The default value is QINTER.
Library	**Name** = Type the name of the library of the subsystem for which you want to enable **Capture**. ***LIBL**
Product to activate	***SECURITY** = Enable **Capture** for all Raz-Lee security products. ***WIDESCOPE** = Enable **Capture** for all Raz-Lee security products. ***ALL** = Enable **Capture** for the entire subsystem. ***NONE** = This parameter should only be *NONE when you are disabling **Capture**.

2. Enter the required parameters and press **Enter**. **Capture** is enabled.

To disable **Capture**:

1. Select **12. Disable Capture** from the **Activation** menu. The **Product Activation Default** screen appears.



Product Activation Default

Parameter	Description
Interactive subsystem	**Name** = Type the name of the subsystem for which you want to disable **Capture**.
Library	**Name** = Type the name of the library of the subsystem for which you want to disable **Capture**. ***LIBL**
Product to activate	***NONE** = This parameter should always be *NONE for disable.

2. Enter the required parameters and press **Enter**. **Capture** is disabled.

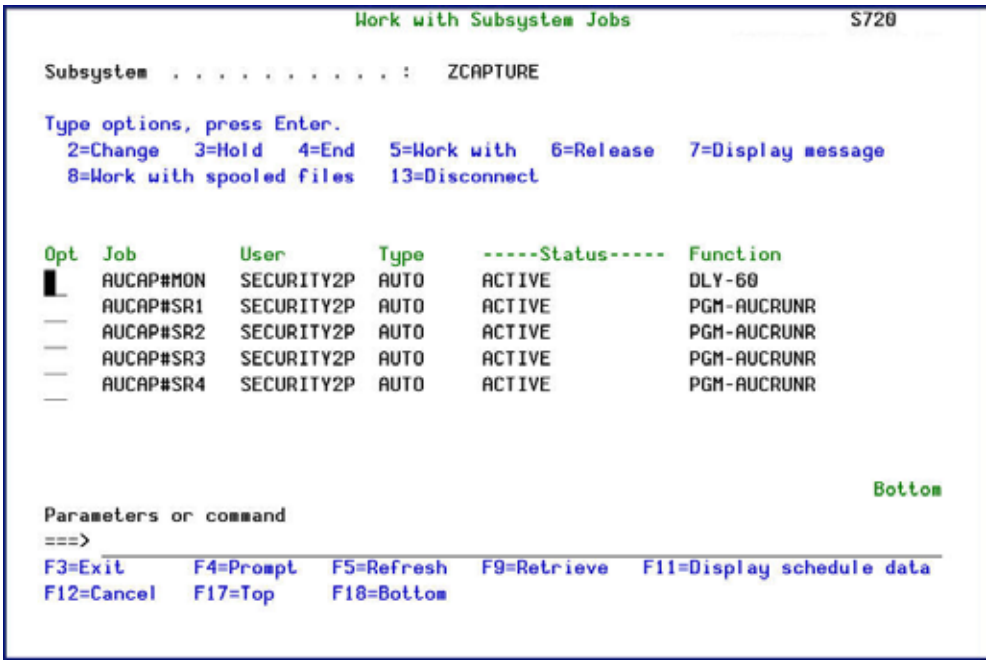
Automatic Activation

§ To activate **Capture** automatically each time an IPL occurs, select **13. Activate at IPL** from the **Activation** menu.

§ To cancel automatic activation, select **14. Do Not Activate at IPL** from the **Activation** menu.

Verifying that the Capture Monitor is Active

Select **5. Work With Active Monitor Jobs** from the **Activation** menu to view the **Capture** monitor subsystem. The **Work with Subsystem Jobs** screen appears. It should display several lines similar to those on the screenshot below.



Work with Subsystem Jobs

Capture All Rule

If you have not set any capture rules, you can set a general rule to capture all activity.

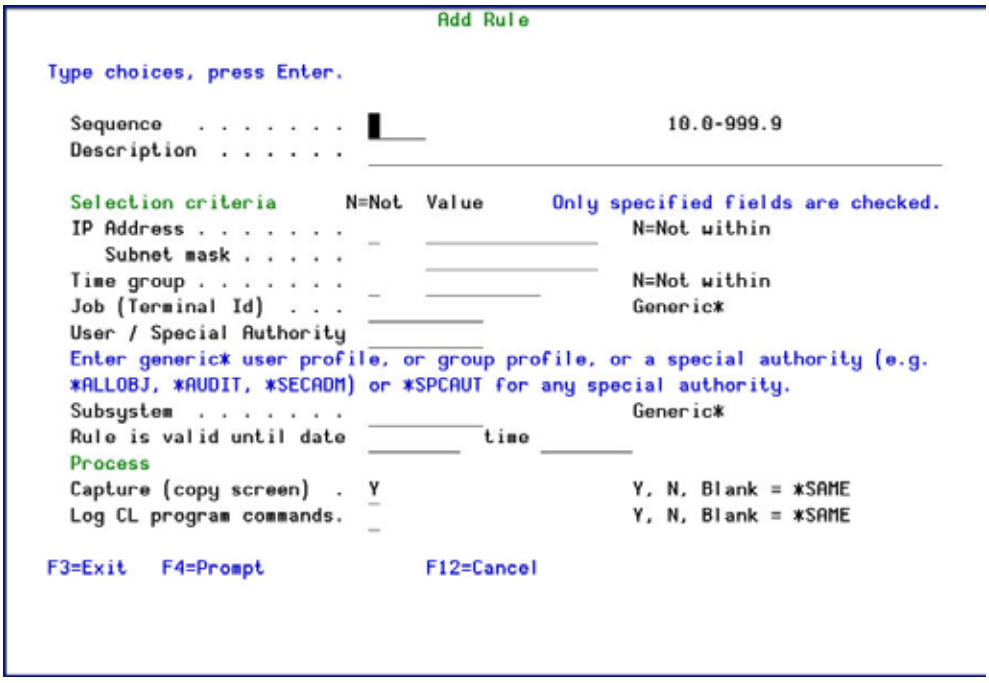
1. Select **19. Add Capture All rule (if no rule)** from the **Activation** menu. The rule is created.

Practical Tutorials for Working with Capture

Tutorial 1: Defining Your First Capture Rule

You must define **Capture** rules in order to begin capturing user screens automatically. In a new installation there are no default rules, therefore, screen captures will not occur until you define some rules. The following steps will guide you through the process of defining your first **Capture** rule. This example will capture all screen activity for the security officer (***QSECOFR***). The purpose of this exercise is simply to introduce you to the rule definition process. A detailed explanation of the various options can be found in *Chapter 3: Capture Rules*.

1. Select **1. Capture Rules** from the main menu. The **Work with Capture Rules** screen appears.
2. Press **F6** to add a new rule. The **Add Rule** screen appears.


Add Rule
Type choices, press Enter.
Sequence 10.0-999.9
Description . . . . . .
Selection criteria N=Not Value Only specified fields are checked.
IP Address . . . . . N=Not within
Subnet mask . . . . . .
Time group . . . . . N=Not within
Job (Terminal Id) . . . Generic*
User / Special Authority
Enter generic* user profile, or group profile, or a special authority (e.g.
*ALLOBJ, *AUDIT, *SECADM) or *SPCAUT for any special authority.
Subsystem . . . . . Generic*
Rule is valid until date time
Process
Capture (copy screen) . Y Y, N, Blank = *SAME
Log CL program commands. Y, N, Blank = *SAME
F3=Exit F4=Prompt F12=Cancel

Add Rule

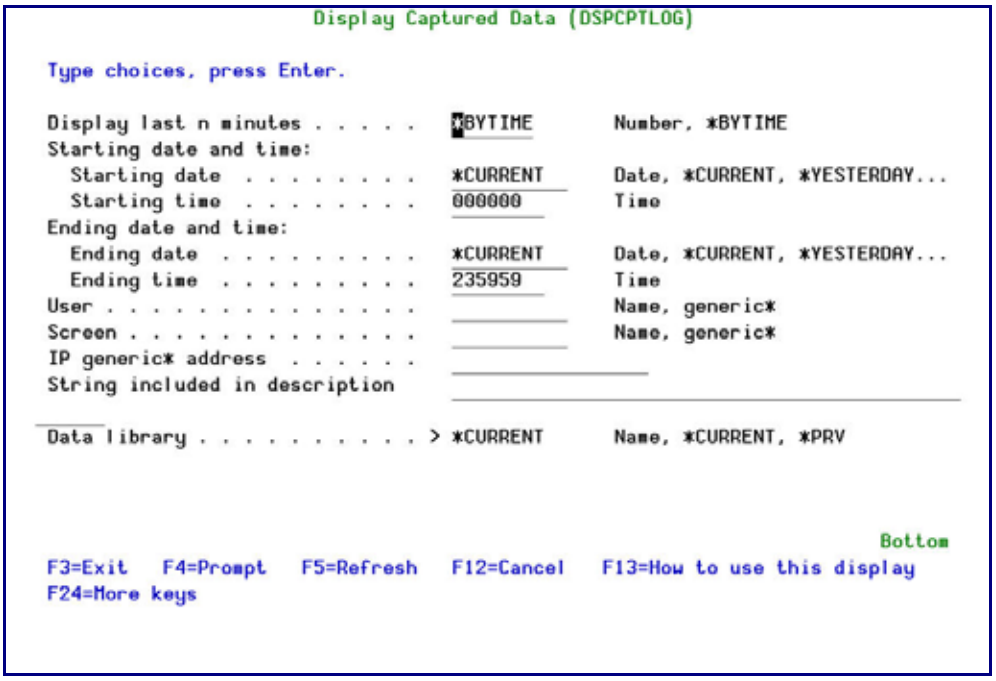
3. Type '***10***' in the **Sequence** field to cause this rule to be executed first.
4. Type a meaningful, descriptive text in the **Description** field.
5. Type '****ALL***' in the **IP Address** field. This indicates that the rule applies to all incoming addresses.
6. Type '***0.0.0.0***' in the **Subnet Mask** field. The subnet mask is required even though the rule applies to all IP addresses.
7. Type a user profile, a group or a special authority in the **User*, Special Auth, LMTCPB** field. This causes the rule to apply only to this user profile.
8. Type a '***Y***' in the **Copy screen** and **Log CL program commands** fields. This changes the job attributes to ***LOGCLPGM(*YES)*** and causes **Screen** to save screens, the job log and the CL command log for this user.
9. Press **Enter** to save the rule.
10. Press **F3** to exit the **Work with Capture Rules** screen.
11. Signon to your System i system as the ***QSECOFR*** and perform some routine tasks. **Capture** will record your activity for later review.

Tutorial 2: Viewing Your First Captured Screens

When **Capture** has been activated and rules created, the system begins saving screen captures and logs immediately according to the rule parameters. You can view captured screens at any time after a capture session begins.

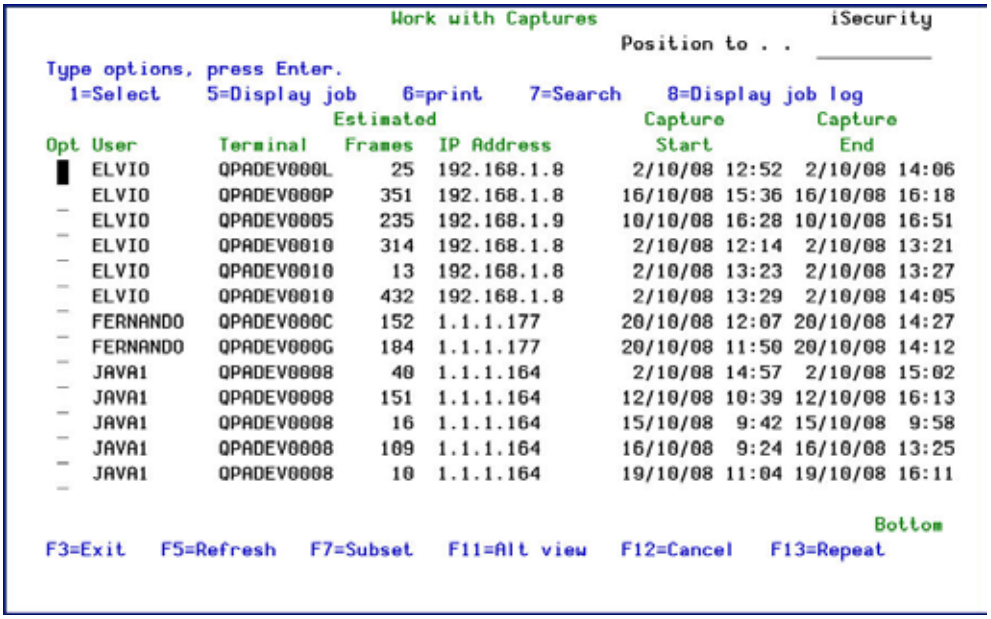
In this exercise, you will view several of the screens captured by the rule that you defined in the previous tutorial.

1. Select **41. Display Current Log** from the main menu. The **Display Captured Data** screen appears. This screen allows you to filter and display only those capture sessions that you wish to work with.



Display Capture Data

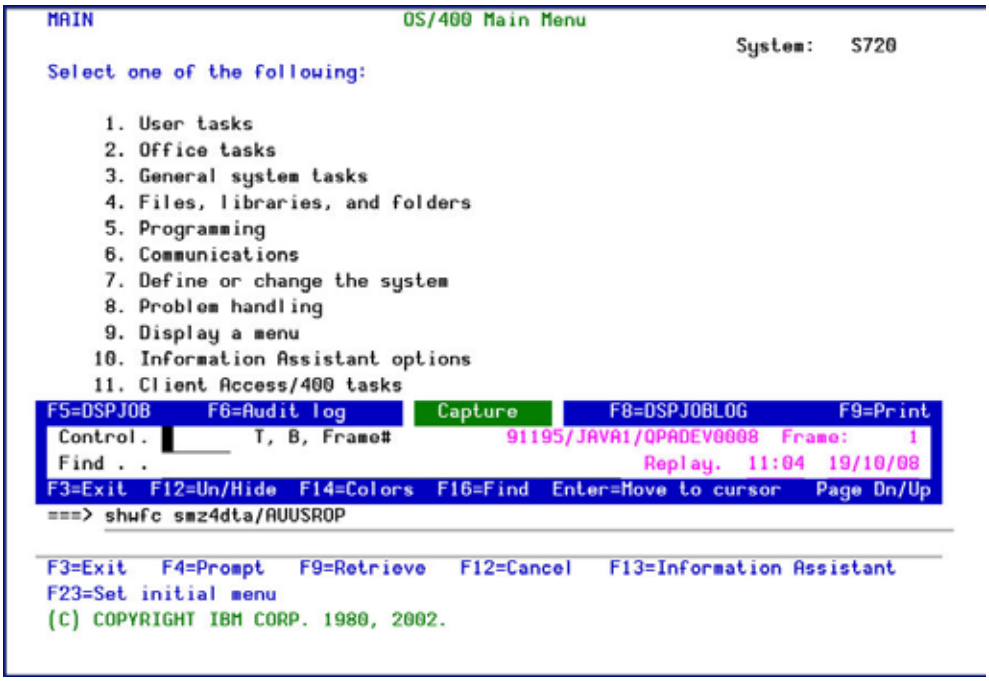
2. Press **Enter** to display the capture sessions for the current day. The **Work with Captures** screen appears allowing you to select a specific capture session to view.



Work with Captures

3. Type **1** to the left of the line showing the user.

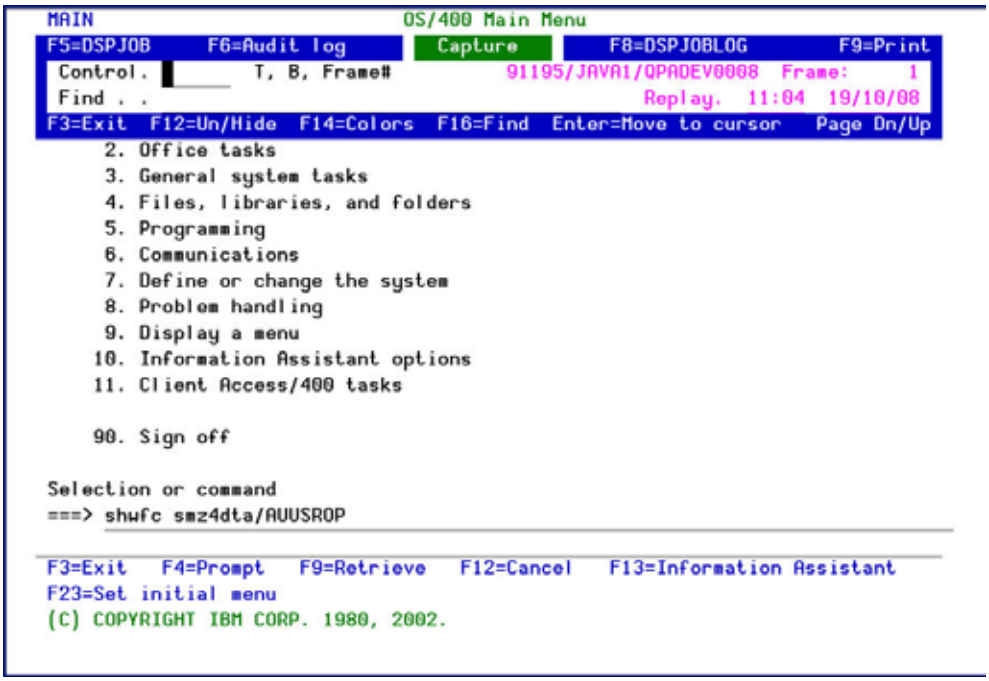
4. The **Replay** screen now appears showing the first screen captured in the session. A floating **Capture** menu appears by default on all **Replay** screens. Press **F12** to hide the **Capture** menu. Press **F12** again and the **Capture** menu re-appears.



IBM i (OS/400) Main Menu (with Capture menu)

5. Press **Page Down** and **Page Up** to scroll through the captured screens for this session. In this example, the user ***QSECOFR*** creates a new user profile.

6. Click at the top of the screen and press **Enter**. The **Capture** menu moves to the top, revealing the data hidden underneath.



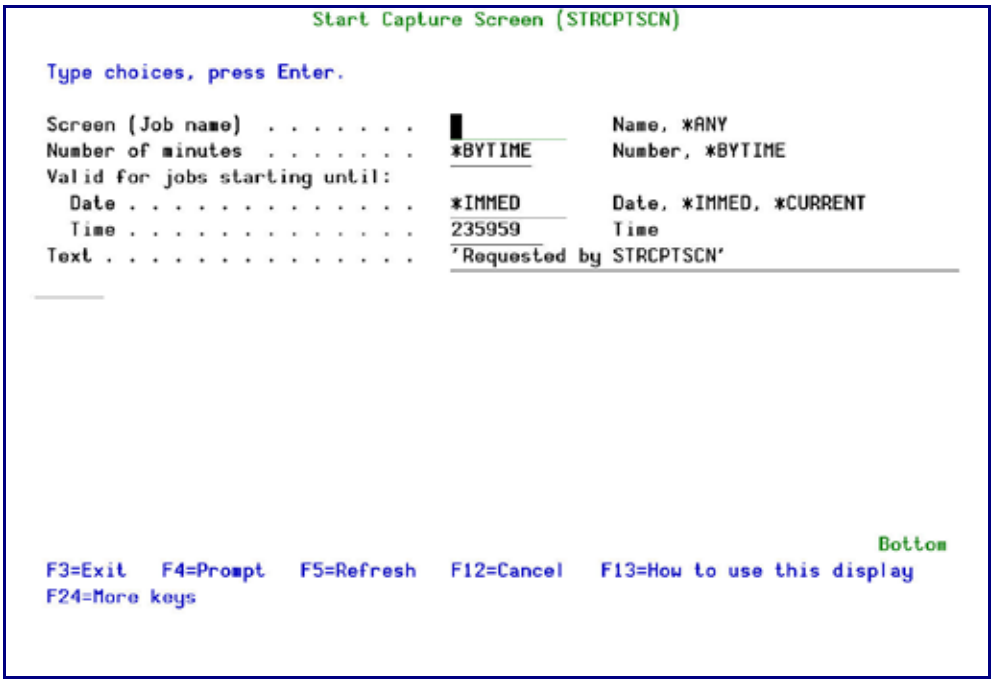
IBM i (OS/400) Main Menu (with Capture menu)

7. Type '***B***' in the **Control** field inside the **Capture** menu. The last screen captured in this session appears. Type '***2***' in the **Control** field. The second screen is displayed. You get the picture.

8. Press **F3** to exit the capture session. Press **F3** again to return to the main menu.

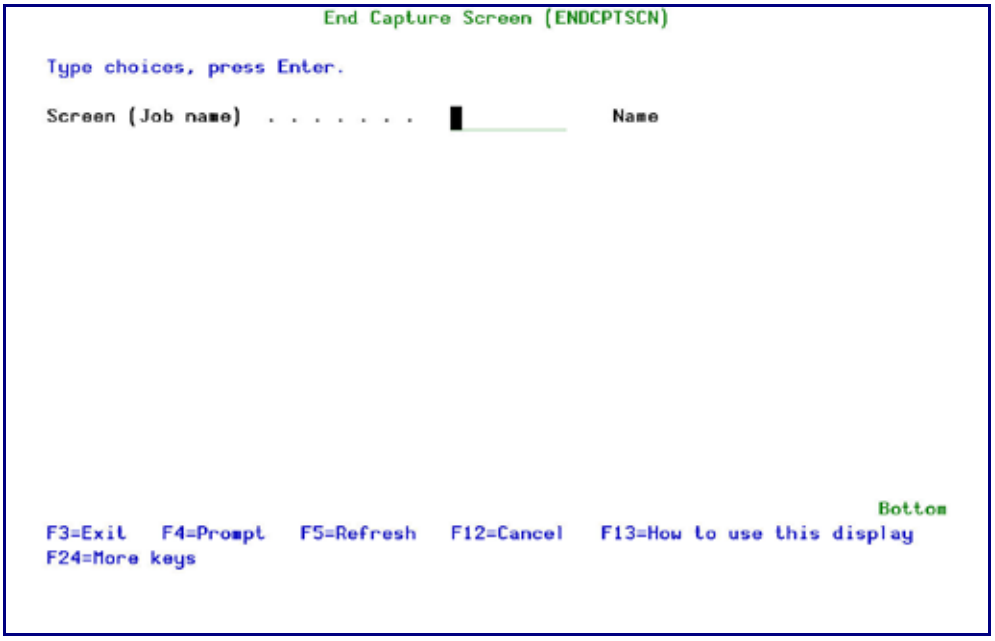
Tutorial 3: Start Capture Screen

1. Select **3. Start Capture Screen** off the main menu. The **Start Capture** screen appears. This screen allows you to immediately start capture sessions according to the screen (session/terminal) or the job name.



Start Capture Screen

2. In order to end this action, Select **4. End Capture Screen** off the main menu and insert the screen or job name that you wish to immediately stop capture.



End Capture Screen

3

Chapter 3: Capture Rules

Capture uses rules to initiate capture sessions automatically according to one or more **Trigger criteria** covering different situations. Additionally, you can also use **Action** rules to trigger capture sessions based on events detected by other **iSecurity** components, such as **Audit** and **Firewall**.

Overview of Capture Rules

Strategic Approach

An effective audit trail is comprised of data from several sources. **Capture** is most effective when used to supplement evidence collected from other security auditing tools (such as **Audit**) and network security tools (such as **Firewall**). Logs and reports generated by these tools provide an extensive written audit trail for virtually all security and system events. It is not necessary to have a visual audit trail for every event detected by these tools. However, a visual audit trail is highly appropriate for certain specific events and situations

Capture is provides you with tools that allow you to capture only those sessions where a visual audit trail is appropriate. You can define rules that trigger automatic captures according to a variety of conditions, such as time, user profile, IP address, and so on. Capturing all sessions at all times is **not recommended** because it may consume excessive system resources and contribute to performance degradation, especially in large organizations.

You should define capture rules to create a visual audit trail only when appropriate according to your security policies, regulatory environment, and operational requirements. The following paragraphs present a few examples of situational strategies.

Transaction Auditing in High Volume Environments

In environments with high transaction volumes, such as banking, retail, e-business, distribution, and so on, it is unrealistic to capture a lot of screen activity. In such cases, it would be more appropriate to capture a small sample of transactions for review. For example, you could define rules to capture input activity by various users for limited time periods on a rotating basis. Should subsequent review uncover a high error rate or suspicious activity, you should create rules to capture a larger sample for these users.

Alternatively, you may wish to capture all or most activity of a particularly sensitive nature such as users responsible for offshore bank transfers, workstations dedicated to classified data or activity occurring outside of normal working hours.

Security Breaches and Suspicious Activity

Suspicious activity may be uncovered by auditing captured screen samples or by other security tools. In such cases, it is appropriate to create a visual audit trail for the particular user, workstation or IP address involved. Captured screens and command logs can supply crucial forensic evidence for legal proceedings or disciplinary action.

You can also use **Action** rules to initiate a capture session automatically upon detection of a suspected security breach or other suspicious activity.

Error Tracking and Debugging

Technical support departments can use **Capture** to provide visual evidence of specific user activities occurring immediately prior to error conditions. When a user reports an error condition, technical support personnel can initiate a manual screen capture prior to asking the user to replicate the condition. Programmers can initiate capture sessions by defining rules for specific users or test workstations while debugging new programs or features. They can also use **Firewall** rules to trigger a capture session automatically whenever a specific program or command is executed.

Trigger Criteria

Capture rules consist of **Trigger criteria** that, when true, initiate capture sessions automatically. A rule may contain several criteria, all of which must be true in order to trigger a capture session. Trigger criteria allow you to initiate capture sessions only when specifically required. Below are brief explanations of the various trigger criteria.

IP Address

You can initiate a capture session for a connection originating from a specific IP addresses or for a range of IP addresses with the subnet mask. Additionally, you can use the Boolean **Not** field value to specify trigger criteria for all IP addresses **except** those specified in the rule. For example, if you wish to capture all sessions that originate outside your local area network, use the IP address and subnet mask to define the range of valid addresses in your LAN and then select the Boolean **Not** field value.

Day and Time (Time Groups)

You can initiate a capture session automatically at specific times and on specific days by using predefined sets of day and time combinations called **Time Groups**. After it is defined, a given Time Group may be used in any number of rules. If you change the definition of a Time Group, the change is incorporated automatically into all rules using that group. Additionally, you can use the **Boolean Not** field value to specify trigger criteria for activity occurring outside the times specified in the rule.

For example if you wish to capture activity for specific users working on the night shift, define a Time Group covering the days and working hours for the night shift and then specify this Time Group as a trigger criterion in your rules.

Terminal Session or Job

You can initiate a capture session for a specific terminal session by specifying the terminal name for that session. This is useful when tracking suspicious activity at a specific workstation.

You can also use the generic indicator '*****' at the end of a text string to apply a trigger criteria to all terminal sessions beginning with the specified text string. For example, type '***QPADEV****' to start a capture session for sessions beginning with '***QPADEV***'.

User Profile

You can initiate a capture session for a specific user. This is useful when tracking activity by specific users irrespective of the workstation or session name.

You can also use the generic indicator '*****' at the end of a text string to apply a trigger criteria to activity for all user profiles beginning with the specified text string. For example, type '***J****' to start a capture session for users beginning with the letter '***J***'.

Subsystem

You can initiate a capture session for jobs initiated under a particular subsystem. For example, if all of your payroll management applications run under a specific subsystem, you can capture all sessions using the payroll system with a single rule.

End Capture Session

You can specify a fixed time and date for the capture session to end. By default, a capture session ends only when the terminal session ends. This trigger criterion overrides the default.

Working with Time Groups

Time groups allow you to apply pre-defined sets of time-based criteria to capture rules without having to define complex criteria for each rule.

Time group filters can be:

- Inclusive **– Include all activities occurring during time group periods**
- Exclusive **– Include all activities** not **occurring during time group periods**

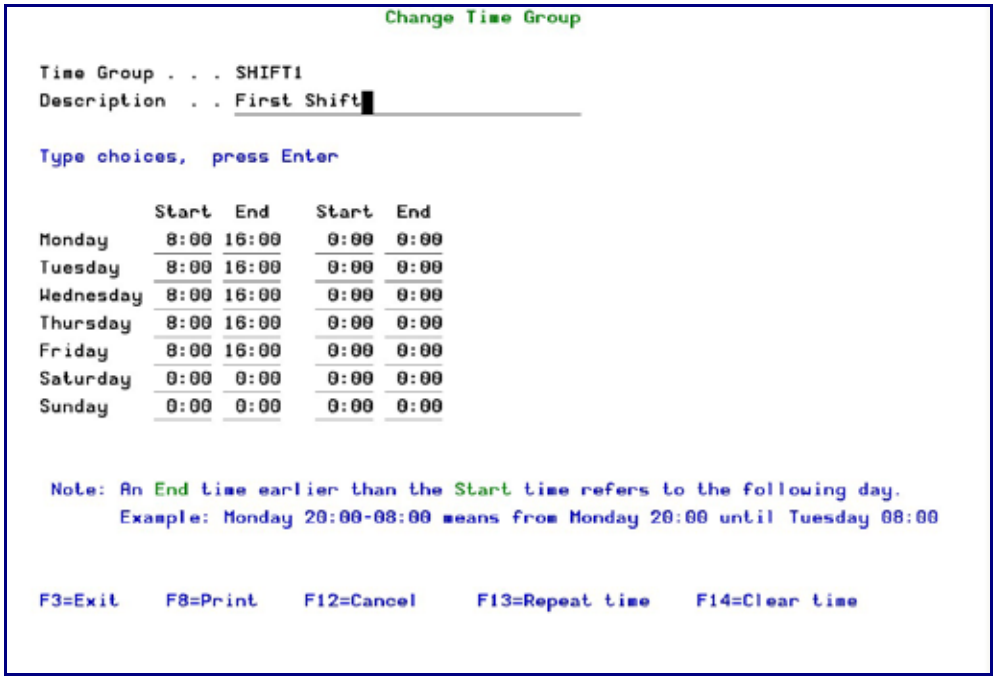
For example, you may define rules to track the activities of certain employees during normal working hours and others during nights and weekends. You can accomplish all of this with just one time group using the following guidelines.

1. Create a time group that defines normal working hours for each day of the week.
2. Use an inclusive time group filter (activities occurring during the time group periods) for each rule covering activity during normal working hours.
3. Use an exclusive time group filter (activities **not** occurring during the time group periods) for each rule covering activity outside of normal working hours.

Defining Time Groups

To define a Time Group, perform the following steps:

1. Select **21. Time Groups** from the Main menu. The **Define Time Groups** screen appears.
2. Select an existing time group to modify or press **F6** to create a new time group.
3. Enter the starting and ending times for each day of the week. Press **Enter** when finished.



Change Time Group

Parameter or Option	Description
Description	Description of the time group
Start and End	Starting and ending times for each period using 24 hour notation

Parameter or Option	Description
F13	Copy starting and ending times from the cursor line to all subsequent days
F14	Erase the starting and ending times for the cursor line and below

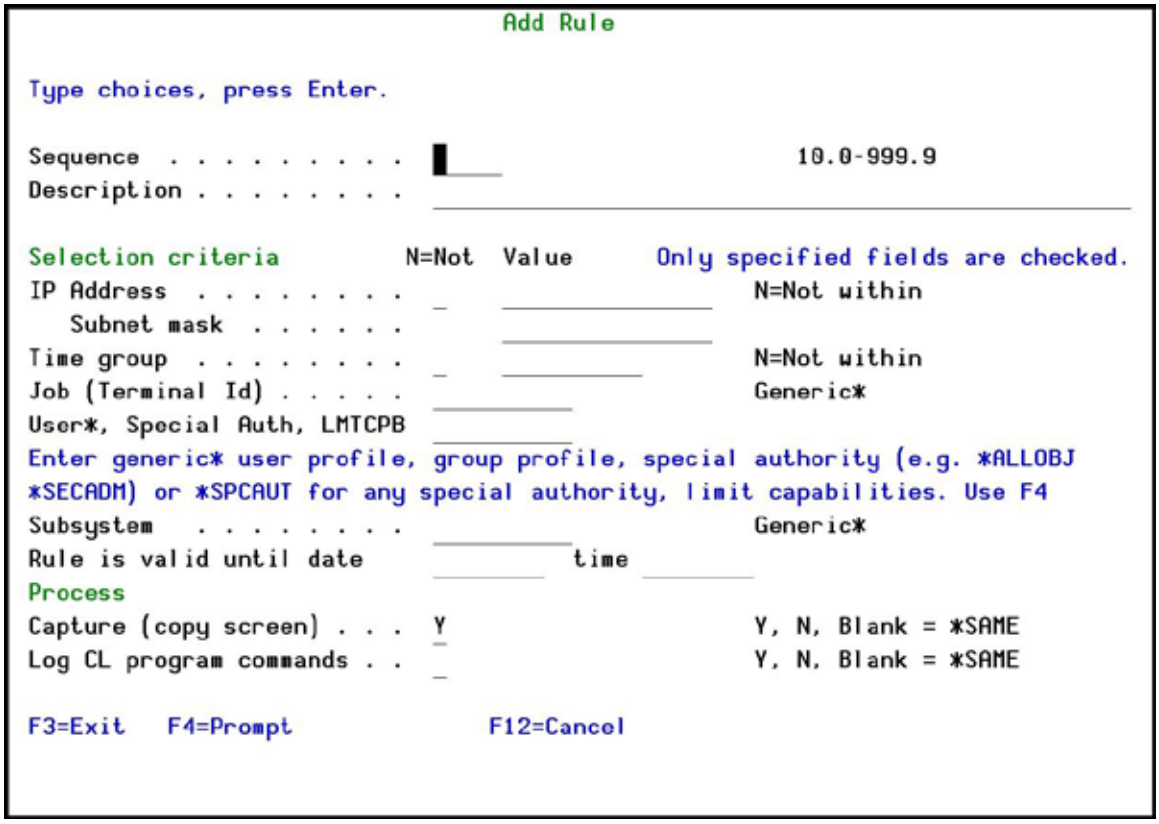
NOTE: If the ending time is less that the starting time, the period is considered to roll forward to the next day. For example, the period 20:00 – 08:00 extends from 20:00 until 08:00 the next morning.

Defining Rules for Automatic Capture Sessions

This section describes the procedures and data entry screens for defining rules that initiate capture sessions automatically.

To create or modify a rule:

1. Select **1. Capture Rules** from the **Main** menu. The Work with Capture Rules screen appears.
2. Press **F6**. The **Add Rule** screen appears. Leave a field blank if there are no trigger criteria for that item.



Add Rule

Parameter or Option	Description
Sequence	Sequence number for this rule. Rules are processed in sequential order according to this value.
Description	Type a meaningful description of this rule
IP Address	IP address in decimal notation. Type '***N***' in the **Not** field to apply this rule to all IP addresses other than that which is specified. ***ALL** = All IP addresses ***LCL** = All local 5250 (Twinax) terminal connections
Subnet mask	Subnet mask specifying IP address ranges. Press **F4** for help.
Time group	Time group that contains the times during which this rule will be applied. Press **F4** to select from list. Type '***N***' in the **Not** field to apply this rule to any time outside of that specified in the group.
Job (Terminal ID)	Terminal session name (This is also the job name.)
User*, Special Auth, LMTCPB	IBM i (OS/400) user profile or profile group
Subsystem	Subsystem in which the job is running
Rule is valid until…	Date and time when the capture session is to end **Blank** = Rule is valid until the end of the terminal session (default)
Copy screen	**Y** = Capture and retain user screens
Keep CL commands	**Y** = Changes the job attributes to ***LOGCLPGM(*YES)***.

3. Enter your trigger criteria and press **Enter**.

Manually Initiating Capture Sessions

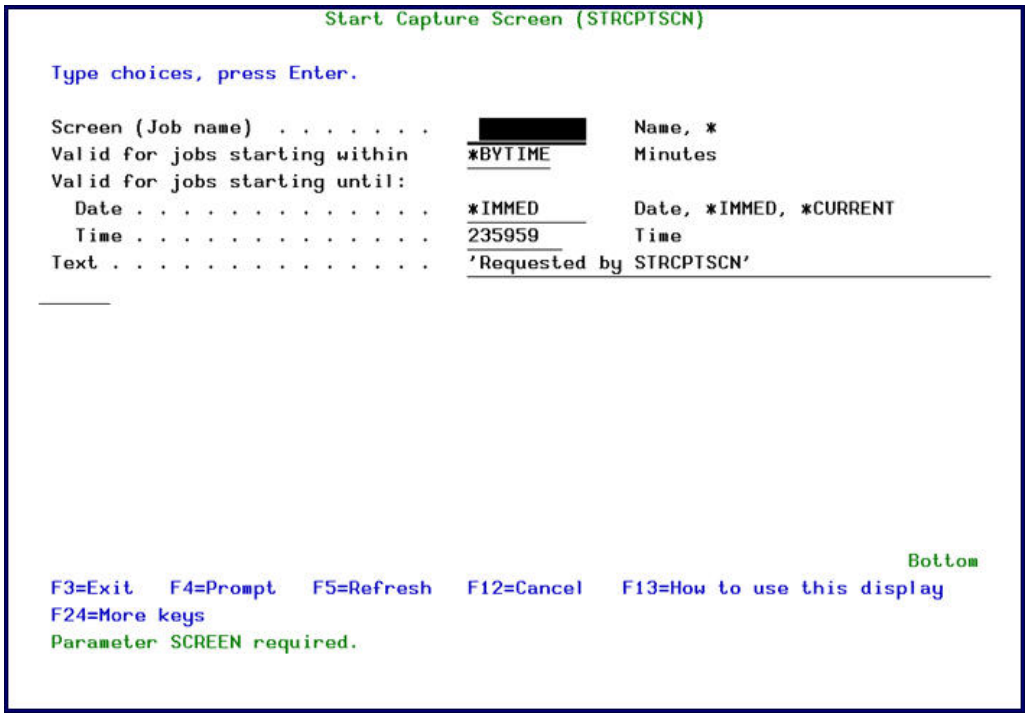
You can initiate a capture session either from the main menu or from any command line. This option is useful if you discover a security breach or suspicious activity. Technical support personnel may also wish to initiate a capture session manually while troubleshooting error conditions or debugging applications.

Manual capture sessions may be started for any active job. You must know the job name (terminal session name) in order to perform this action. Use the ***STRCPTSCN*** command to obtain the job name.

Starting a Capture Session from Capture

To manually start a capture session:

1. Select **3. Start Capture Screen** from the main menu. The **Capture Screen** command screen appears.



Start Capture Screen (STRCPTSCN)

Parameter or Option	Description
Screen (Job name)	Terminal session name (this is also the job name)
Valid for jobs starting within	Enter the number of minutes
Valid for jobs starting until	Enter the date and time after which this capture session will end. Press **F4** for options.
Text	Description of this capture session

2. Enter parameters as described in the following table. Enter your trigger criteria and press **Enter**.

Starting a Capture Session from the Command Line

To start a capture session from outside **Capture**:

1. Enter the ***STRCPTSCN*** command from any command line. The **Capture Screen** command screen appears.
2. Enter parameters as described in the *Starting a Capture Session from Capture* procedure on page *41*.

NOTE: In case the command ***STRCPTSCN*** is used for the same screen it is running in, no initial ***GRINIT*** is required.

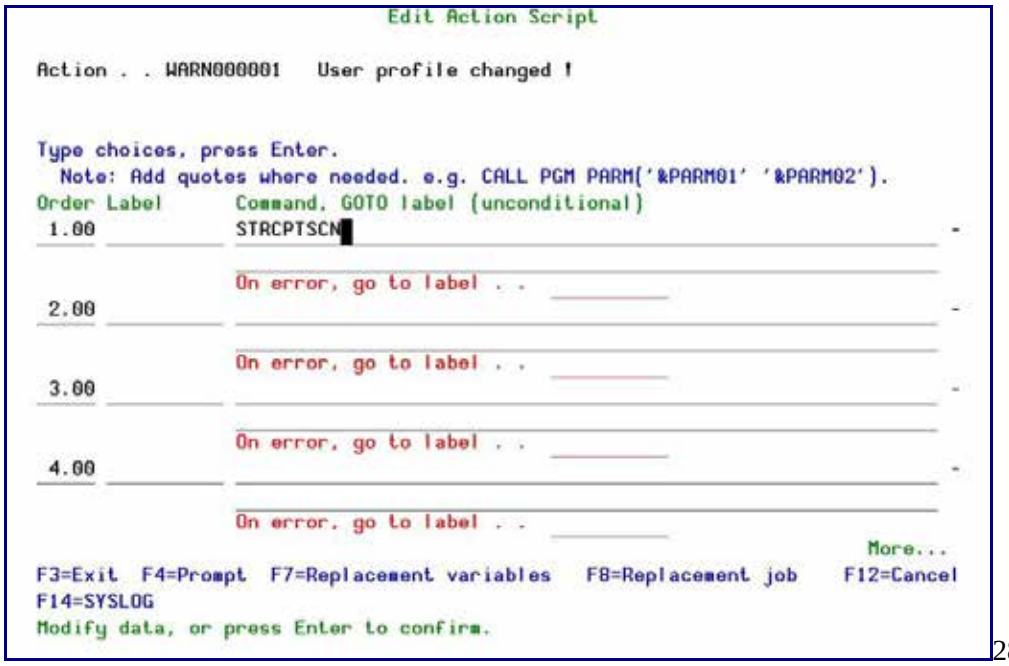
Using Action to Trigger a Capture Session

You can use an **Action** command script to initiate a capture session automatically upon detection of a particular event, such as suspicious activity or an error condition. This powerful feature allows you to capture user activity silently and invisibly whenever these conditions are detected by **Audit** real time auditing or if a violation of **Firewall** rules occurs.

Real time auditing must be active at in order to take advantage of this feature. Additionally, if you are using a **Firewall** rule, you must configure the IBM i (OS/400) server to allow **Action** to react. Refer to the documentation for these products for further details.

To use **Action** to trigger a Capture Session:

1. Define a real time auditing rule, as described in the **Audit** manual.
2. Define your rule until the **Edit Action Script** screen appears.



2803

Edit Action Script

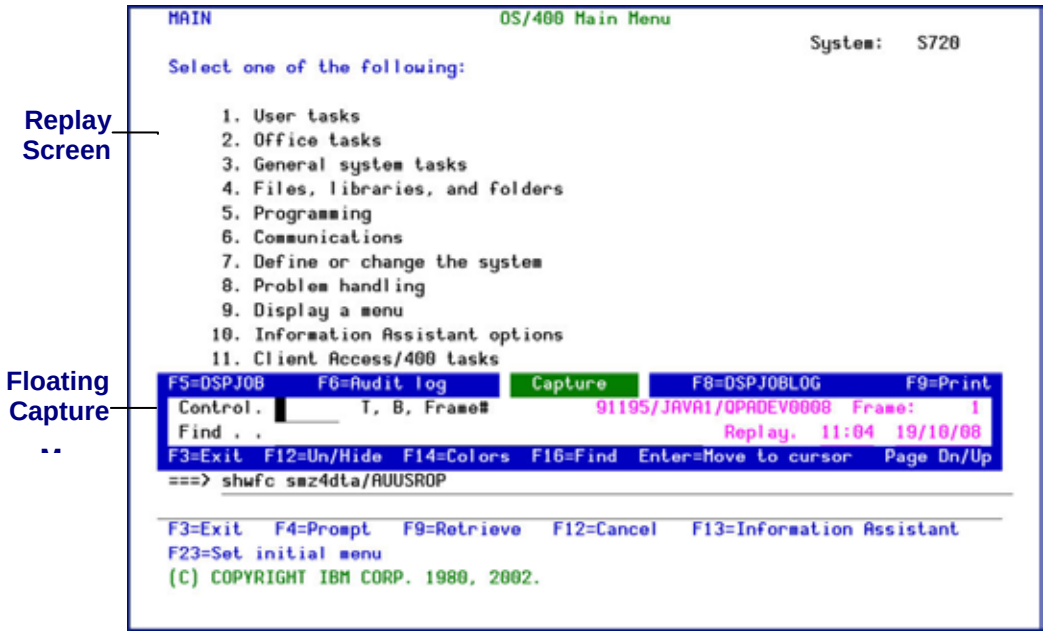
3. Enter the ***STRCPTSCN*** command to capture a device or the ***STRCPTUSR*** command to capture a user profile on the first line.
4. Press **F4** to add parameters. The Start Capture Screen appears.
5. Press **F10** to view all parameters.
6. Enter the required parameters and press **Enter**.
7. Press **F7** and select variables from the list. This inserts a **replacement variable** in the command script representing session (job) name.
8. Press **Enter** twice to complete the process.

Your capture session will begin automatically whenever the conditions defined in your rule are fulfilled.

Chapter 4: Auditing User Activity

Reviewing Captured Screens

You can replay captured screens by means of an intuitive process and easy-to-use tools for locating the captured data screens and logs. Captured screens are arranged as **frames** in individual capture sessions. Within each session, you can scroll through the frames sequentially or you can use the floating **Capture Menu** to move directly to a particular screen or search for screens containing a specific text string.



Replay of Captured Screen

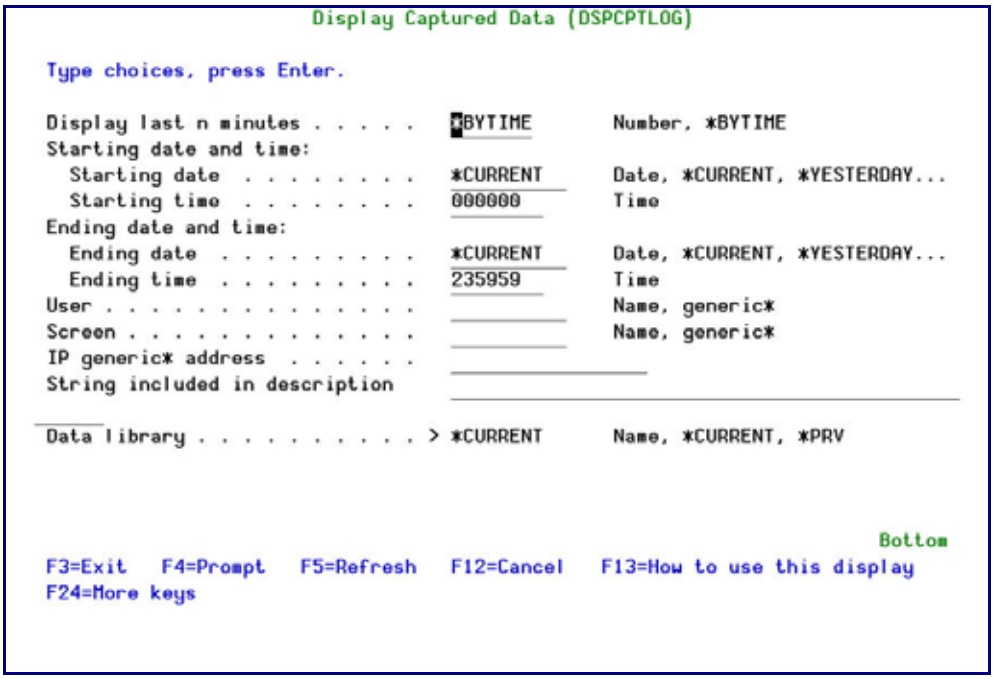
While reviewing the replay of captured screens, you can also use the Capture menu to display the job log, the Display Job menu and the **Audit** history log that relates to the current capture session.

The sections that follow describe the procedure and options for reviewing and auditing user activity as displayed on captured screens.

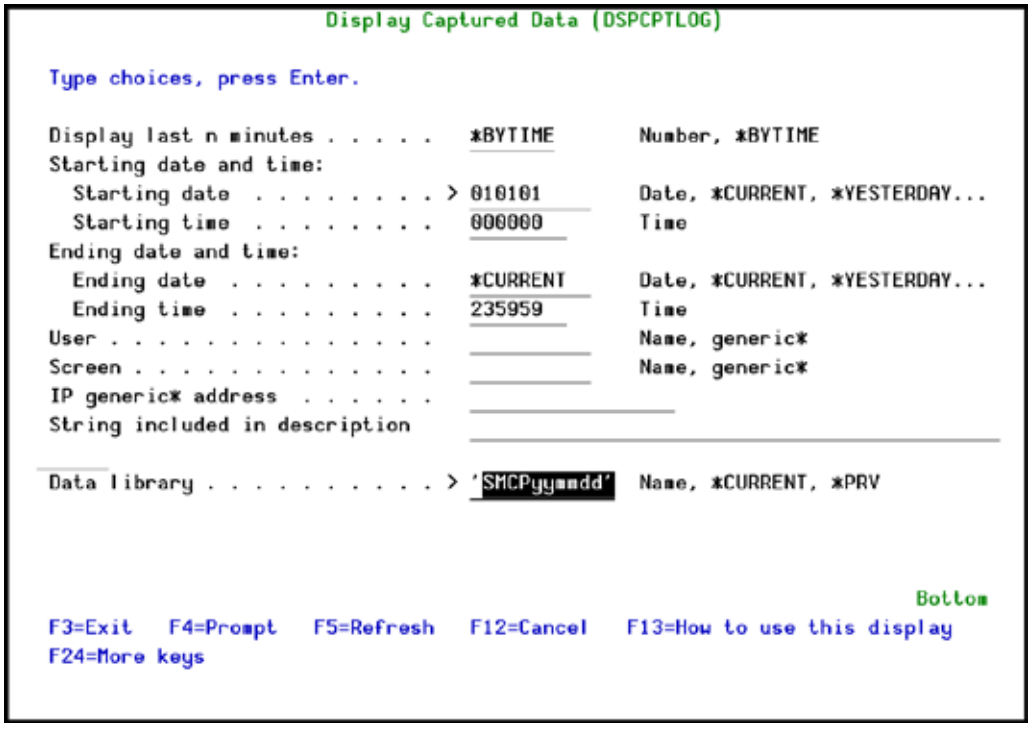
Selecting Screen Capture Sessions for Audit

You can work with screen capture sessions from either current data or restored data.

1. From the **Capture** main menu, select either **41. Display Current Log** or **42. Display Restored Log**. The **Display Captured Data** command screen appears. This screen allows you to select and display only those capture sessions that you wish to work with.



Display Captured Data – Current Data

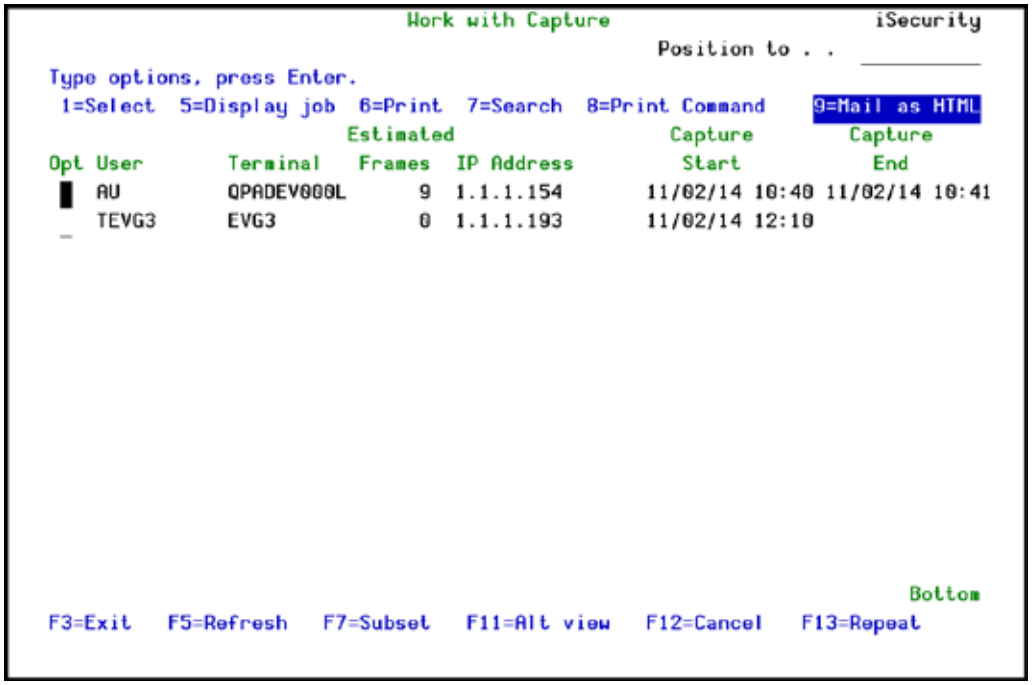


Display Captured Data – Restored Data

Parameter or Option	Description
Display Last n Minutes	Select only those records occurring within the previous number of minutes as specified by the user **Number** = Enter the number of minutes ***BYTIME** = Use starting and ending times specified below
Starting Date & Time **Ending Date & Time** **Starting Date & Time** **Ending Date & Time** **(Continued)**	Select only those records occurring within the range specified by the starting and ending date/time combination. **Date or Time** = Enter the appropriate date or time ***CURRENT** = Today (Current Date) ***YESTERDAY** = Previous date ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
User	IBM i (OS/400) user profile or profile group
Screen	Terminal session name (This is also the job name)
IP Generic Address	IP address in decimal notation **BLANK**= All IP addresses
String included in description	Enter text contained capture session description. Only sessions containing this text string in the description field will be displayed.

Parameter or Option	Description
Data library	For Restored Data only Enter the name of the library to which the data was backed up. The name of the library is ***SMCPyymmdd***, where ***SMCP*** is a constant and ***yymmdd*** is the date of the backup

2. Press **Enter** to display the capture sessions for the selected date and time. The **Work with Captures** screen appears which allows you to select a specific capture session to view. Each line represents a single capture session.



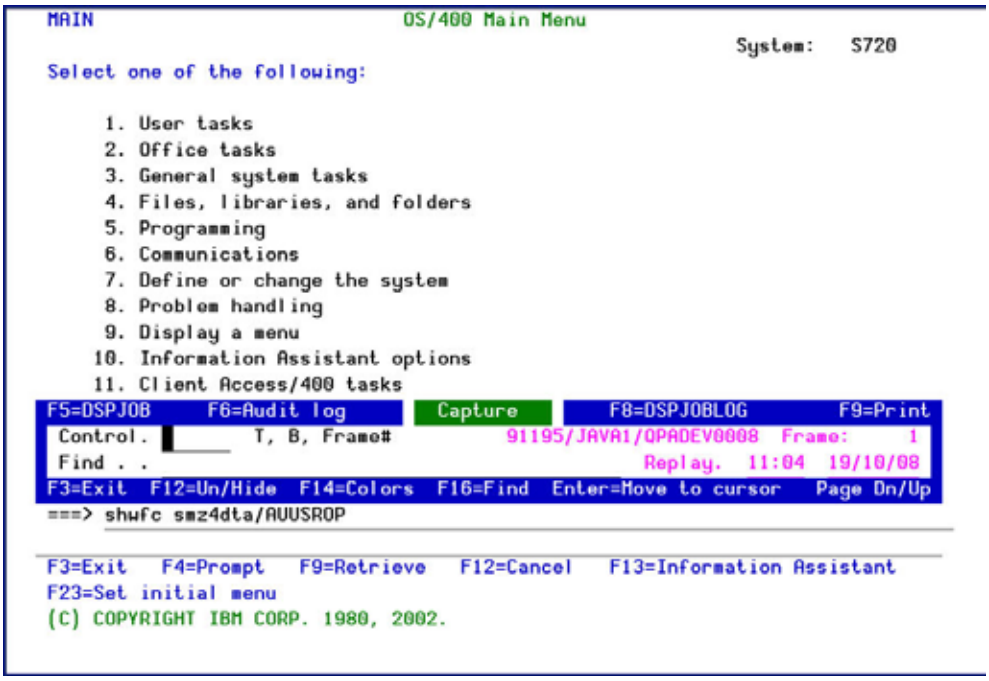
Work With Captures

Option or Command	Description
1	Replay screens in the selected capture session
5	Displays the IBM i (OS/400) Display Job (***DSPJOB***) menu for the selected capture session (Active jobs only)
6	Print selected frames in the selected capture session
7	Perform a **free text search** on the selected capture session. Type the search string in the pop-up window that appears and then press **Enter** to jump to the first screen containing the search string.
8	Print the selected capture session
9	Mails the selected capture session as an HTML email
F7	Refine selection parameters to display a smaller subset of the capture sessions
F11	Toggle the screen display to show different capture session parameters

Option or Command	Description
F13	Repeat the option entered on the current line for all subsequent lines. For example, if you type '***1***' to select the fifth line, you can press **F13** to select all lines that follow.

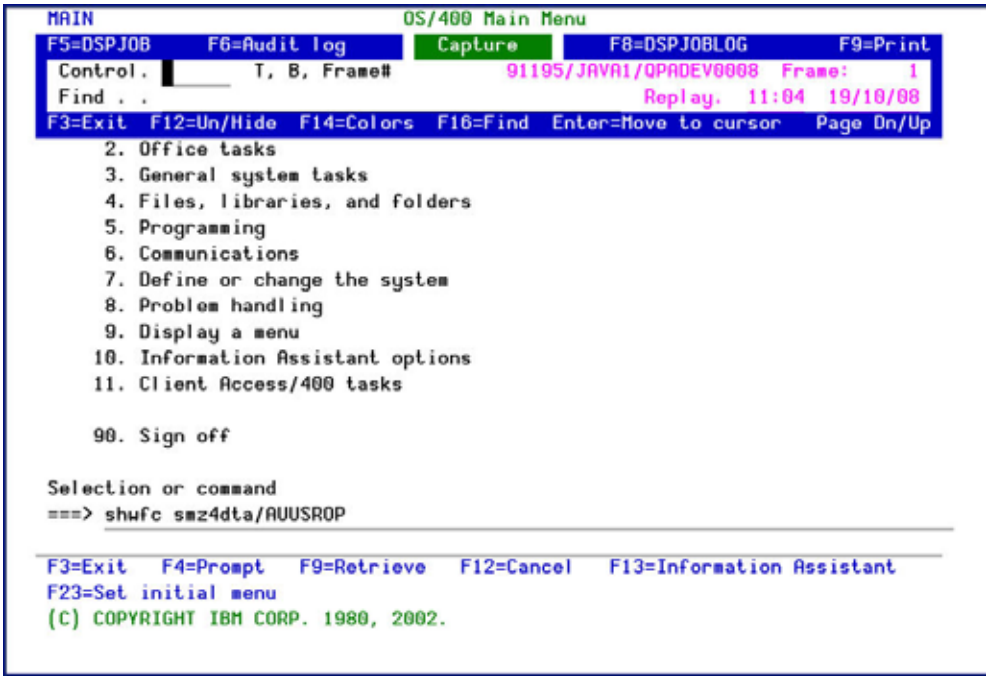
Navigating Through a Capture Session

When you select a capture session, the **Replay** screen appears showing the first frame (captured screen). The floating **Capture** menu appears by default on all **Replay** screens. Press **F12** to hide the **Capture** menu. Press **F12** again and the **Capture** menu re-appears.



IBM i (OS/400) Main Menu

- To scroll through the captured screens one screen at a time, use the **Page Down** and **Page Up** keys.
- To move the **Capture** menu and show the text below, simply move the cursor to another line on the screen and press **Enter**. The **Capture** menu moves to the cursor location.

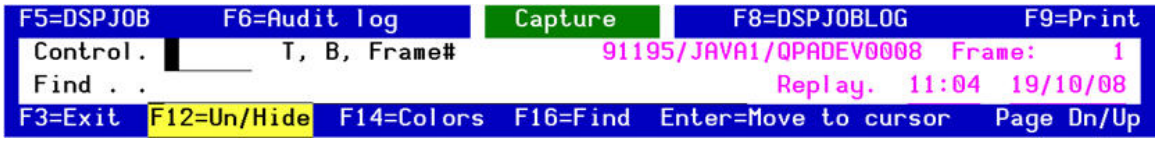


IBM i (OS/400) Main Menu

- To hide or re-display the **Capture** menu, Press **F12**.
- To move to the last frame in the capture session, type '***B***' (Bottom) in the **Control** field inside the **Capture** menu. To move to the first frame, type '***T***'. To move to a specific frame, type the frame number.

Using the Capture Menu

The floating Capture menu serves as a convenient control panel for navigating through frames and for displaying job and audit history logs associated with the current capture session. The following table describes the features available from this menu.



Floating Capture Menu

Parameter or Option	Description
Control	Move to a specific frame in the capture session **T** = First frame (Top) **B** = Last frame (Bottom) **Frame Number** = Move to the designated frame
Replay	Shows the capture time, date and frame number for the current

Parameter or Option	Description
	frame
Find	Type a text string here to search for frames containing that string
F3	Exit the current capture session
F5	Show the **Display Job** screen associated with the current capture session
F6	Display the audit history log associated with the current capture session
F8	Display the job log associated with the current capture session
F9	Print one or more frames from the current capture session
F12	Hide or un-hide the **Capture** menu
F14	Change the color used to highlight the search text string in frames
F16	Find the next frame containing the search text
Enter	Move the **Capture** menu to the cursor position
PgUp/PgDn	Scroll forward or backward through frames

Free Text Search

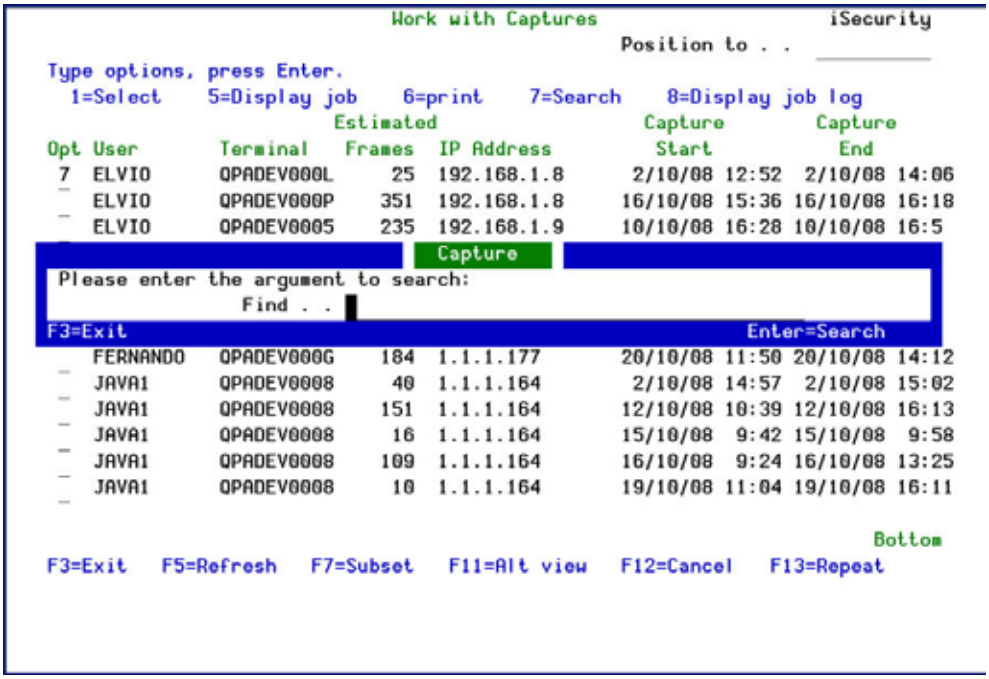
Capture lets you search for screens within a capture session that contain a specific text string. This powerful feature allows you to locate specific screens quickly and easily within a capture session containing hundreds of screens. For example, you can use the free text search to locate screens containing:

- Specific data items, such as customer numbers or transaction codes
- Occurrences of error messages
- Use of certain commands, applications or parameters
- Programming keywords
- User profiles names

The free text search feature is available from both the **Work with Captures** list screen and from the **Capture** menu on replay screens. The basic procedure is the same with both methods.

Searching from the Work with Captures List Screen

1. Type '*7*' in the option field on any capture session line in the list and press **Enter**.
2. Type the search string in the pop-up window and press **Enter** again.

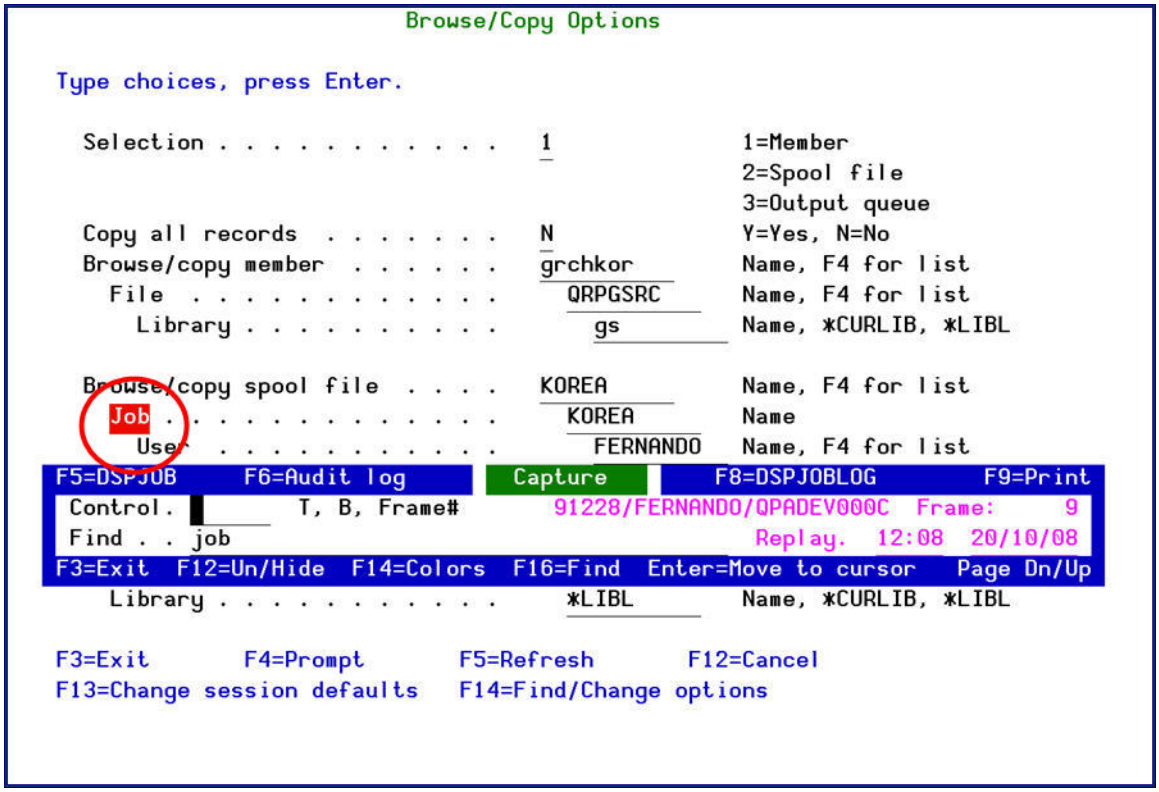


Work with Captures

4. The first replay screen containing the desired text string appears. The text string appears highlighted in the color specified in system configuration (Default = **Red**). You can change this color by pressing **F14**.
5. To search for additional occurrences of the text string, press **F16**.

Searching Using the Capture Menu

1. Type the search string in the **Find** field in the **Capture** menu and press **Enter**.



Modify User Restriction – Part 1

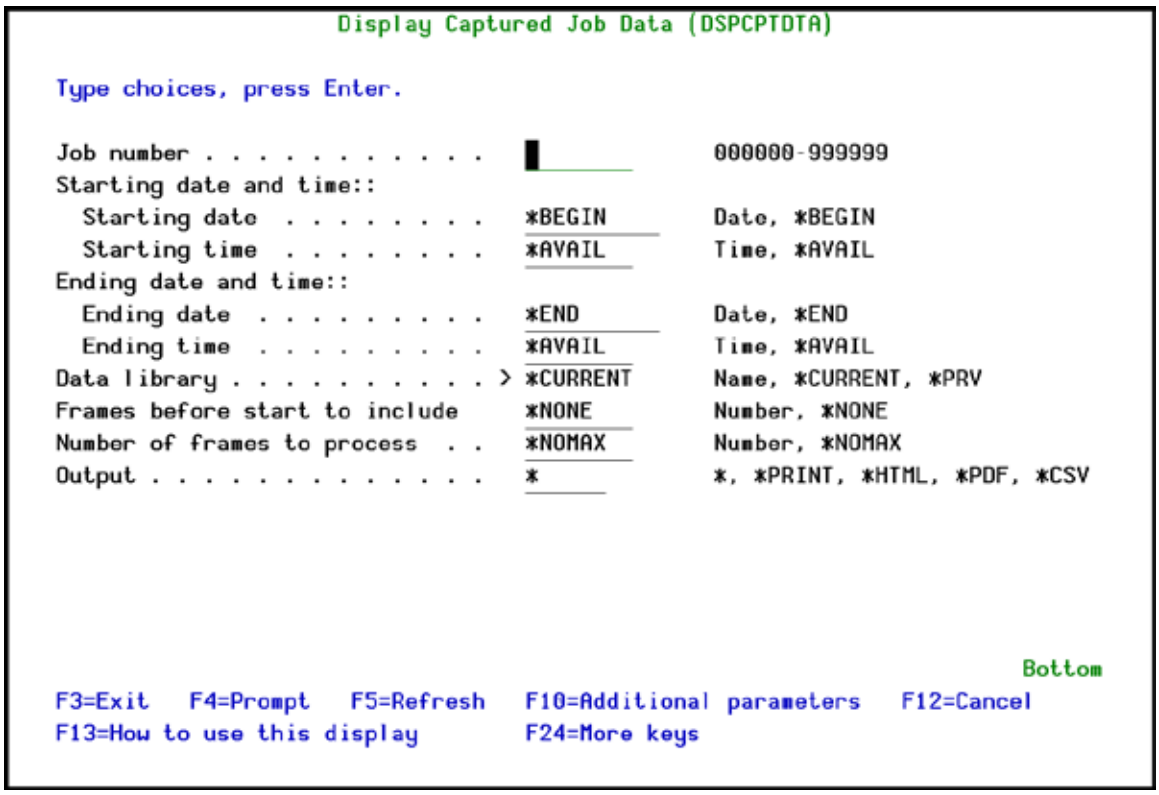
2. The first replay screen containing the desired text string appears. The text string appears highlighted in the color specified in system configuration (Default = **Red**). You can change this color by pressing **F14**.
3. To search for additional occurrences of the text string, press **F16**.

Printing and Mailing Captured Screens

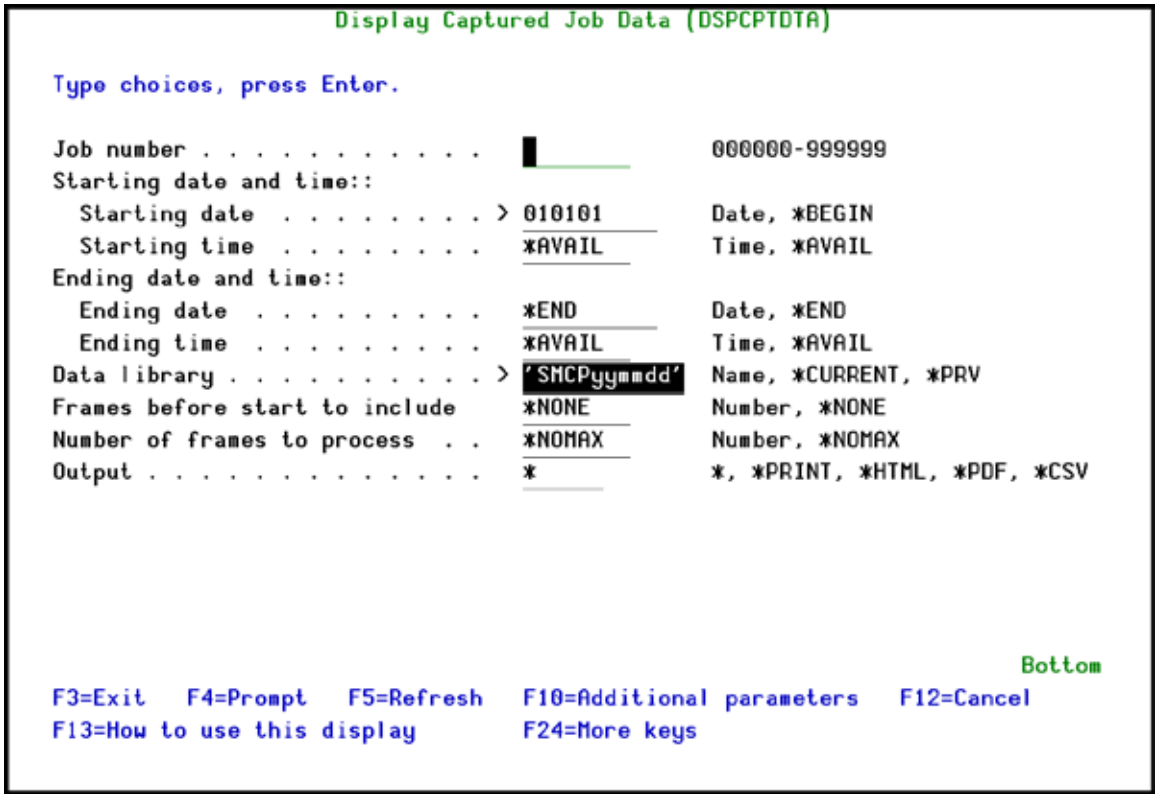
While reviewing the replay of captured screens, you can also use the Capture menu to print/mail the job log, the Display Job menu and the **Audit** history log that relates to a specific job within a capture session.

Printing/Mailing Jobs from a Captured Session

1. From the **Capture** main menu, select either **45. Display Current Data** or **46. Display Restored Data**. The **Display Captured Job Data** command screen appears. This screen allows you to select the job that you wish to work with.



Display Captured Job Data – Current Data



Display Captured Job Data – Restored Data

Parameter or Option	Description
Job Number	000000 - 999999
Starting Date & Time **Ending Date & Time** **Starting Date & Time** **Ending Date & Time** **(Continued)**	Select only those records occurring within the range specified by the starting and ending date/time combination. **Date or Time** = Enter the appropriate date or time ***CURRENT** = Today (Current Date) ***YESTERDAY** = Previous date ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
Data library	For Restored Data only Enter the name of the library to which the data was backed up. The name of the library is ***SMCPyymmdd***, where ***SMCP*** is a constant and ***yymmdd*** is the date of the backup
Frames before start to include	**Number** = The number of frames before the job started to include ***NONE** = Do not include any frames before the start
Number of frames to process	**Number** = The number of frames to process. ***NOMAX** = Process all the frame

Parameter or Option	Description
Output	* *PRINT *HTML *PDF *CSV
Keep as IFS file	*NO *YES
Directory	
Mail to	
Mail text	
Delete if attached	NO *YES
Compress and send together	NO *YES

5

Chapter 5: Capture Business Items

Business Items are the unique keys that access your data, such as a social security number, an insurance policy number, a bank account number. Use the Business Items menu to capture information relating to these important pieces of data.

Business Items provides all screen-related activities for specific business items and allows you to do the following:

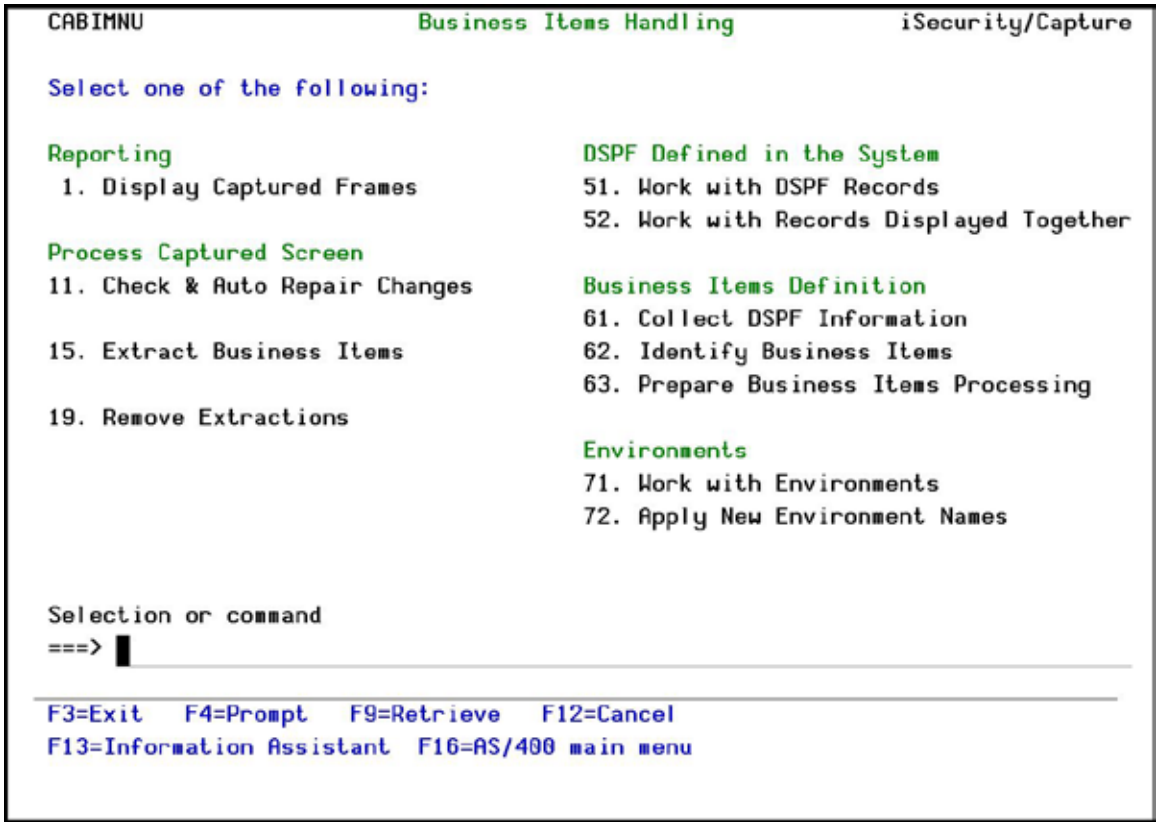
- Extract business-items
- Isolate business items, even if programmers change their placement, as business item position is obtained directly from display file objects
- Detect related “environment” aspects such as the bank whose screen data is being viewed, whether the screen is from a test or production environment, and so on.
- Log all screens and pertinent information such as the job name, current user, name of display file and record format, name of the program which sent the screen and the line number within the program, library list, and so on.
- Send captured screens via HTML email to relevant people, aids in documenting the application, admissible in court, enables search and playback of captured screens

Capture Business Items uses files CAFF and CABI, both of which are located in library SMZCDTA. The files are connected by the common fields of Job Name and Job Number. It is the responsibility of your organization to manage these files and to ensure that they do not fill up.

To use Capture Business Items, use the following workflow:

- Enable Business Items, as described in *Defining Business Items Support* on page *22*.
- Define Business Items, as described in *Business Items Definition* on page *69*.
- If you set **Analyze run environment by *LIBL** to **Y** when you enabled Business Items, define the Business Items environments, as described in *Environments* on page *78*.
- Define where Business Items appear in Display Files, as described in *Extract Business Items* on page *63*.
- On a regular basis, check if any changes have been made in the Display Files, as described in *Check and Auto Repair Changes* on page *62*.

To access the Business Items Handling menu, select **61. Business Items Menu** from the main menu. The **Business Items Handling** menu appears.



Business Items Handling

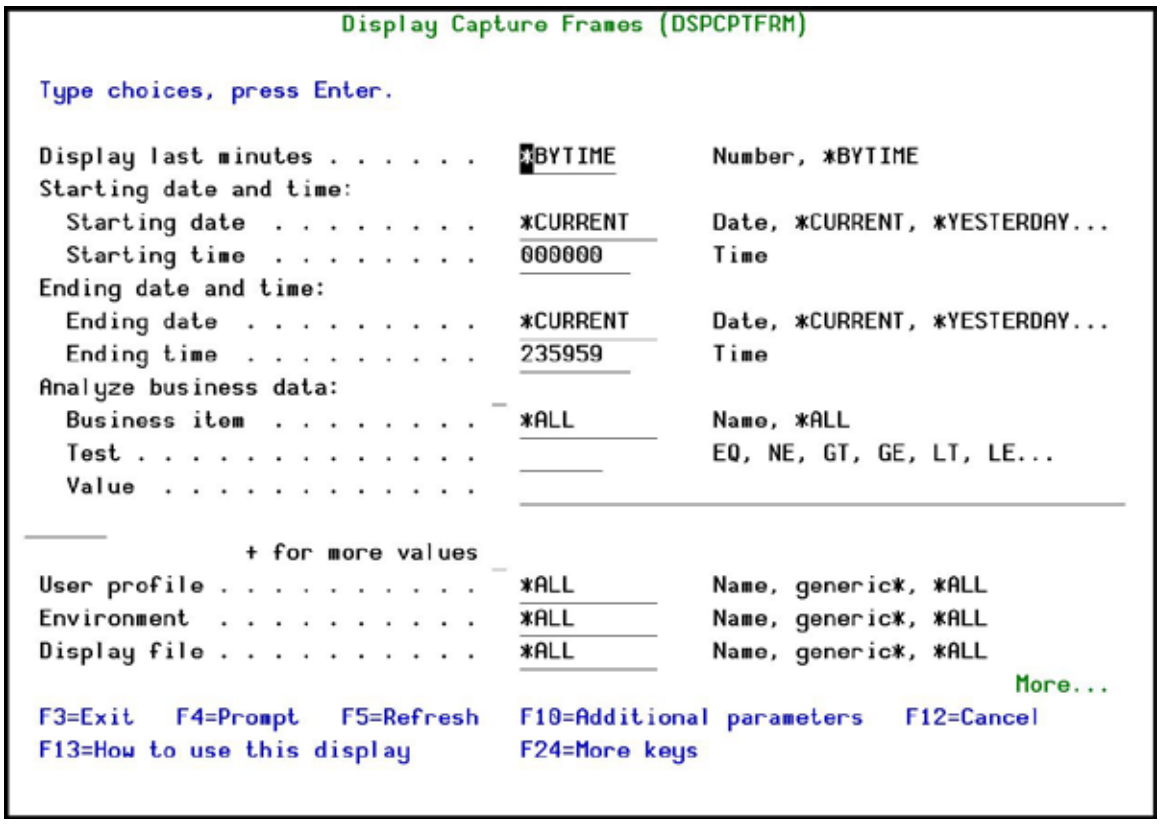
Reporting

Display Captured Frames

Displaying the captured frames allows you to see a step by step replay of the actions that were performed on the selected Business Items.

To display captured frames:

1. Select **1. Display Captured Frames** from the **Business Items Handling** menu. The **Display Capture Frames** screen appears.



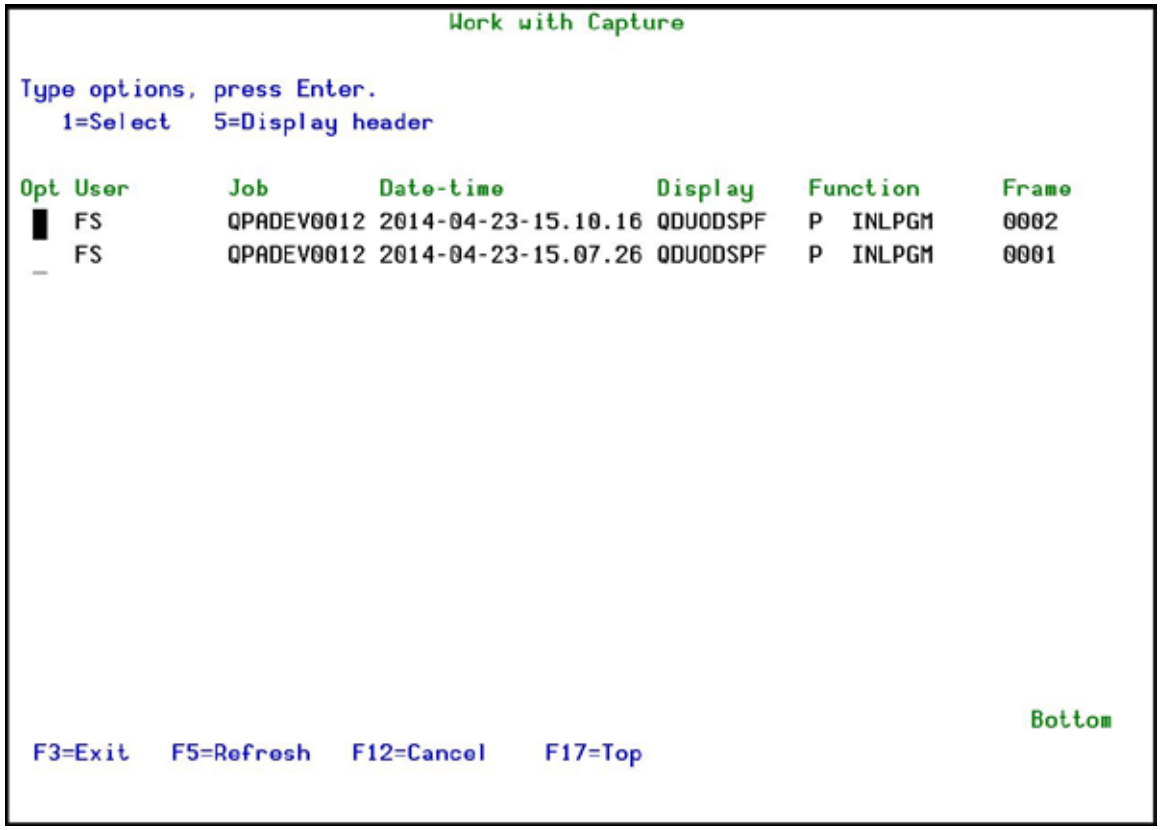
Display Capture Frames

Parameter or Option	Description
Display last minutes	Select only those records occurring within the previous number of minutes as specified by the user **Number** = Enter the number of minutes ***BYTIME** = Use starting and ending times specified below

Parameter or Option	Description
Starting Date & Time **Ending Date & Time**	Select only those records occurring within the range specified by the starting and ending date/time combination. **Date or Time** = Enter the appropriate date or time ***CURRENT** = Today (Current Date) ***YESTERDAY** = Previous date ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
Analyze business data: **Business Item** **Test** **Value**	Select a subset of records by Business Item and its value, for example all Account Numbers that start with the number 9. **Business Item**: Either enter the name of one of your defined Business Items or enter *ALL. **Test** and **Value**: If you enter a Business Item, you can filter further by testing it for specific values. You can use the following for testing: **EQ** = Equals the value in the Value field **NE** = Not Equal to the value in the Value field **GT** = Greater Than the value in the Value field **GE** = Greater Than or Equal to the value in the Value field **LT** = Less Than the value in the Value field **LE** = Less Than or Equal to the value in the Value field **LIKE** = Contains the value in the Value field **NLIKE** = Does not contain the value in the Value field **LIST** = Is in the List in the Value field **NLIST** = Is not in the List in the Value field
User Profile	Selects a subset of records by user profile **Name** **Generic*** ***ALL**
Environment	Selects a subset of records by environment **Name** **Generic*** ***ALL**
Display file	Selects a subset of records by display file **Name** **Generic*** ***ALL**
Program name **Library**	Filter records by the name and library of the program that created the record.
Job name **User** **Number**	Filter records by IBM i (OS/400) job name user. Filter records by IBM i (OS/400) job number.

Parameter or Option	Description
Filter by time group - Relationship	***IN** = Include all records in time group ***OUT** = Include all records not in time group ***NONE** = Do not use time group, even if included in query definition ***QRY** = Use time group as specified in query definition
Filter by time group - Time group	**Name** = Name of time group ***SELECT** = Select time group from list at run time
Filter using query rules	**Name** = Name of the query ***NONE** = Do not use query rules to filter
Number of records to process	**Number** = The number of records to process. ***NOMAX** = Process all the records
Output	*** ***PRINT** ***PRINT1 – PRINT9** ***OUTFILE**
Outfile format	*BYLINE ***FRAME**
File to receive output - name	**Name**
File to receive output - library	**Name** ***LIBL**
Output member options: - Member to receive output	**Name** ***FIRST**
Output member options: - Replace or add records	***REPLACE** ***ADD**
User defined data	

2. Enter your required parameters and press **Enter**. The **Work with Capture** screen appears with the appropriate entries.



Work With Capture

3. Select option **1** to open the captured frames of a session or option **5** to see header information.

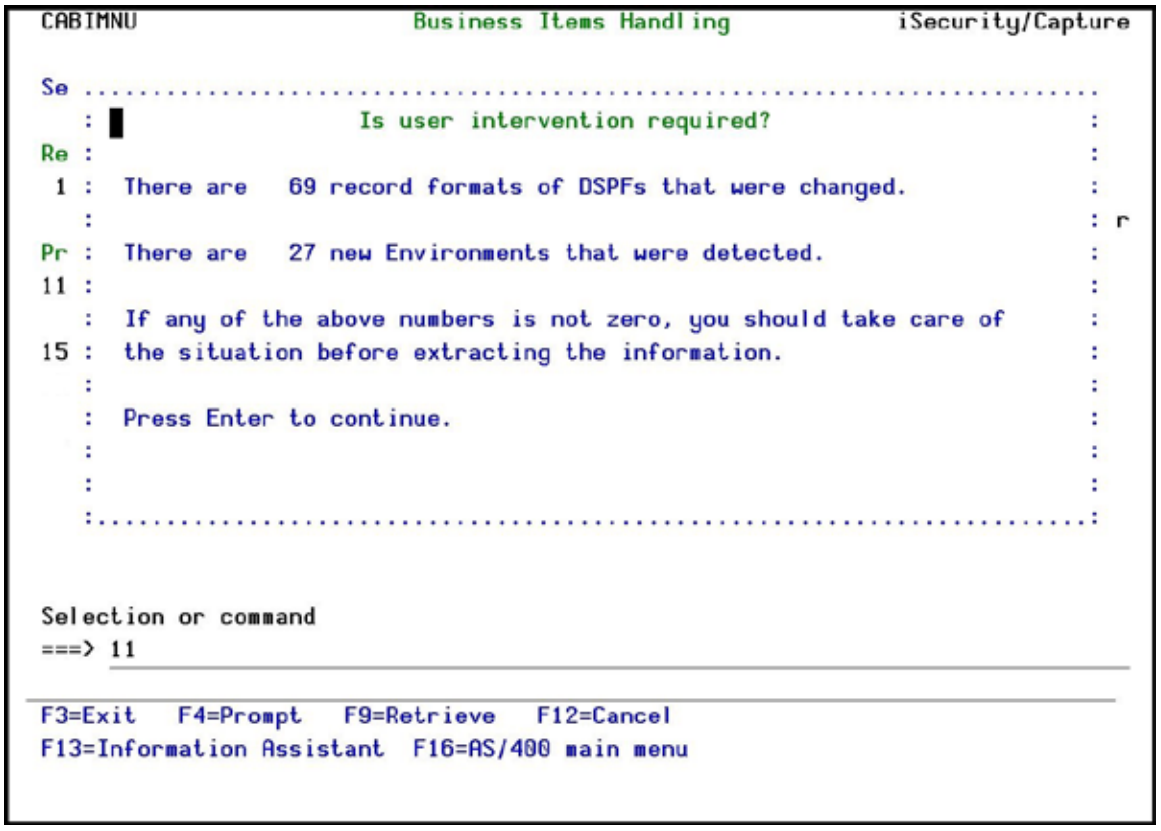
Process Captured Screen

Check and Auto Repair Changes

Once a day you should check that your Business Items are up to date.

To perform the daily check:

1. Select **11. Check & Auto Repair Changes** from the **Business Items Handling** menu. The **Is user intervention required?** screen appears.



Is User Intervention Required?

2. If the screen reports that either DSPFs or environments were changed, run the processes described in *Business Items Definition* on page *69*.

Extract Business Items

Run an automatic procedure to extract all Business Items appearances in display files.

To extract the Business Items:

1. Select **15. Extract Business Items** from the **Business Items Handling** menu. If found, the Business Items are extracted. A message shows the result of the process.

Remove Extractions

You can remove some of the extracted Business Items from the repository.

To remove the extracted Business Items:

1. Select **19. Remove Extractions** from the **Business Items Handling** menu. The **Remove BI Extractions** screen is displayed.

```
                    Remove BI Extractions (RMVBIEXT)

Type choices, press Enter.

Starting date and time:
  Starting date  . . . . . .            Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . .  000000    Time
Ending date and time:
  Ending date  . . . . . .    *CURRENT  Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . .    235959    Time
Display file . . . . . .      *ALL      Name, generic*, *ALL
  Library  . . . . . .          *ALL      Name, generic*, *ALL
  Record . . . . . .            *ALL      Name, generic*, *ALL

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

Remove BI Extractions

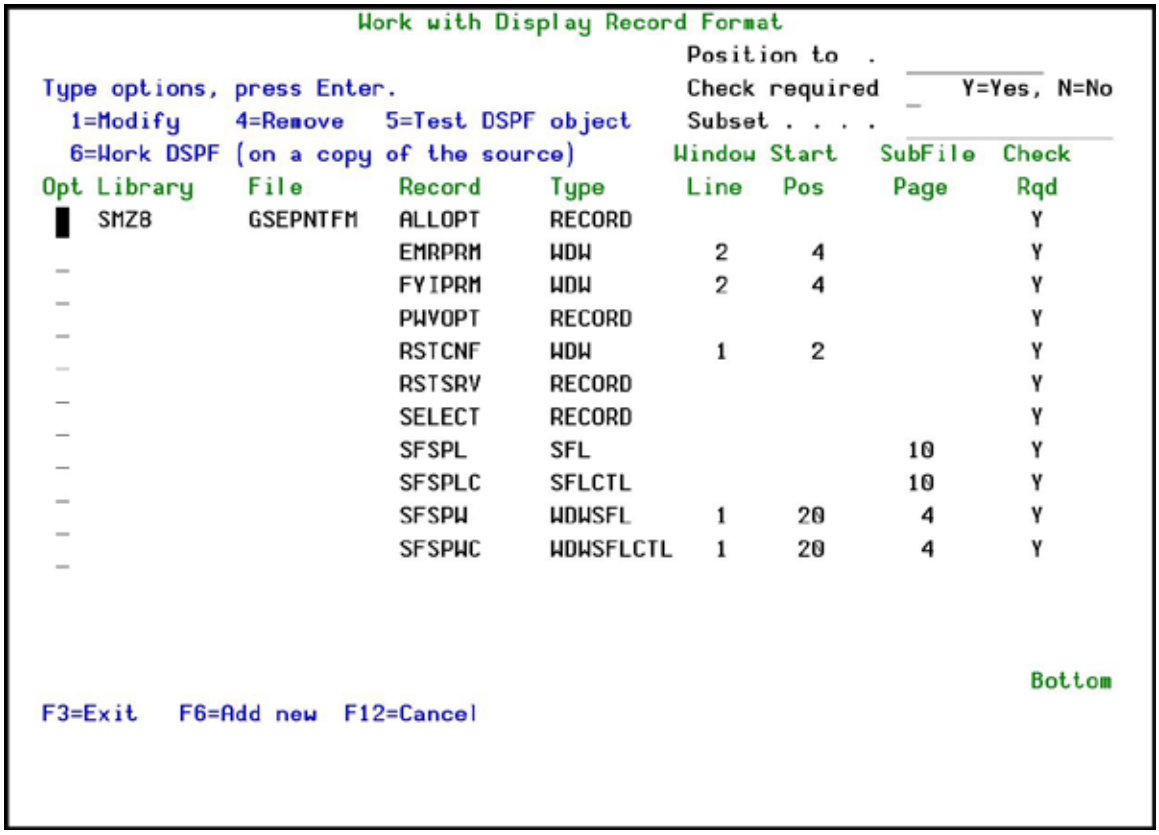
Parameter or Option	Description
Starting Date & Time **Ending Date & Time**	Remove only those Business Items records for which the event occurred within the range specified by the starting and ending date/time combination. **Date or Time** = Enter the appropriate date or time ***CURRENT** = Today (Current Date) ***YESTERDAY** = Previous date ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
Display file	Selects a subset of records by display file **Name** **Generic*** ***ALL**
Library	Selects a subset of records by library **Name** **Generic*** ***ALL**
Record	Selects a subset of records by record **Name** **Generic*** ***ALL**

2. Enter your required parameters and press **Enter**. The appropriate extracted Business Items are removed from the system.

DSPF Defined in the System

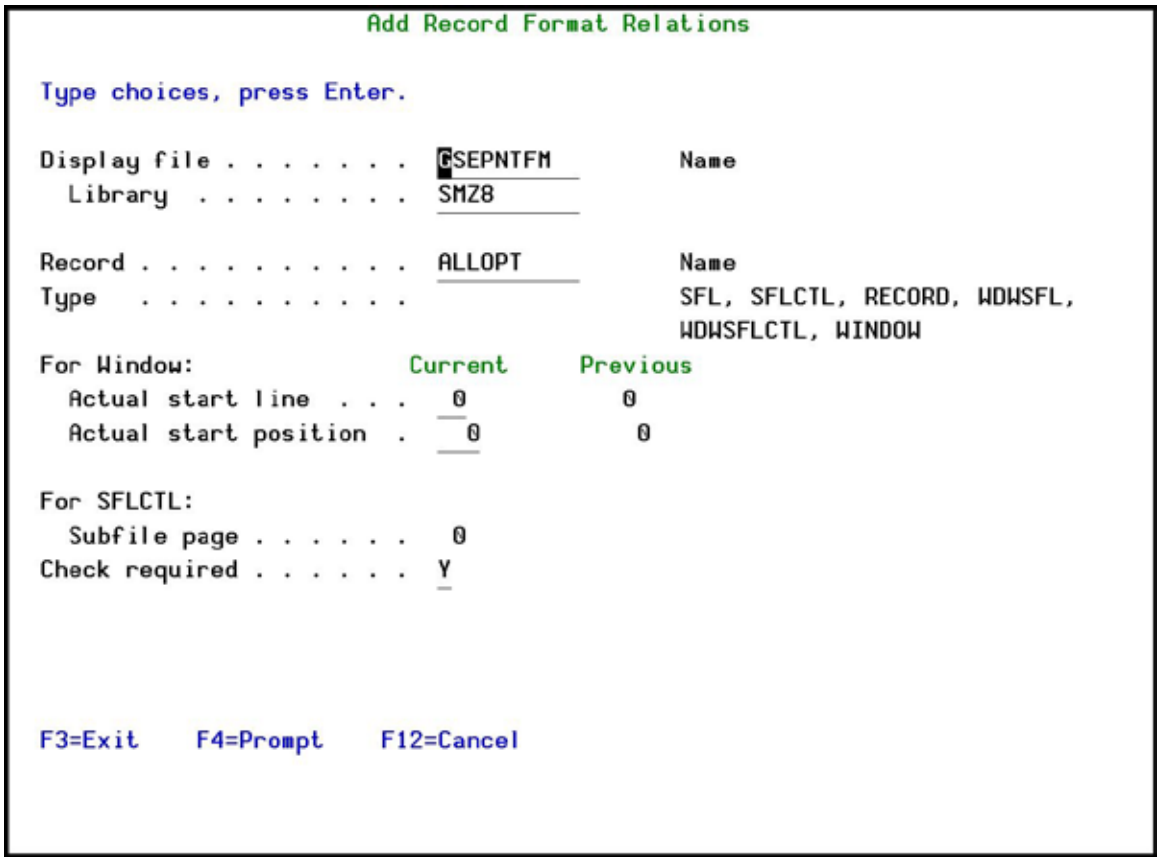
Work with DSPF Records

1. Select **51. Work with DSPF Records** from the **Business Items Handling** menu. The **Work with Display Record Format** screen appears.



Work with Display Record Format

2. Type **1** next to a format to modify it or press **F6** to add a new format. The **Add Record Format Relations** screen appears. Values are pre-populated according to the position of the cursor in the **Work with Display Record Format** screen.



Add Record Format Relations

Parameter or Option	Description
Display file	The display file to be changed
Library	The library where the display file is stored
Record	The record within the display file to be changed
Type	**SFL** **SFLCTL** **RECORD** **WDWSFL** **WDWSFLCTL** **WINDOW**
For Window: Actual start line	The start line of the Window
For Window: Actual start position	The starting position of the Window

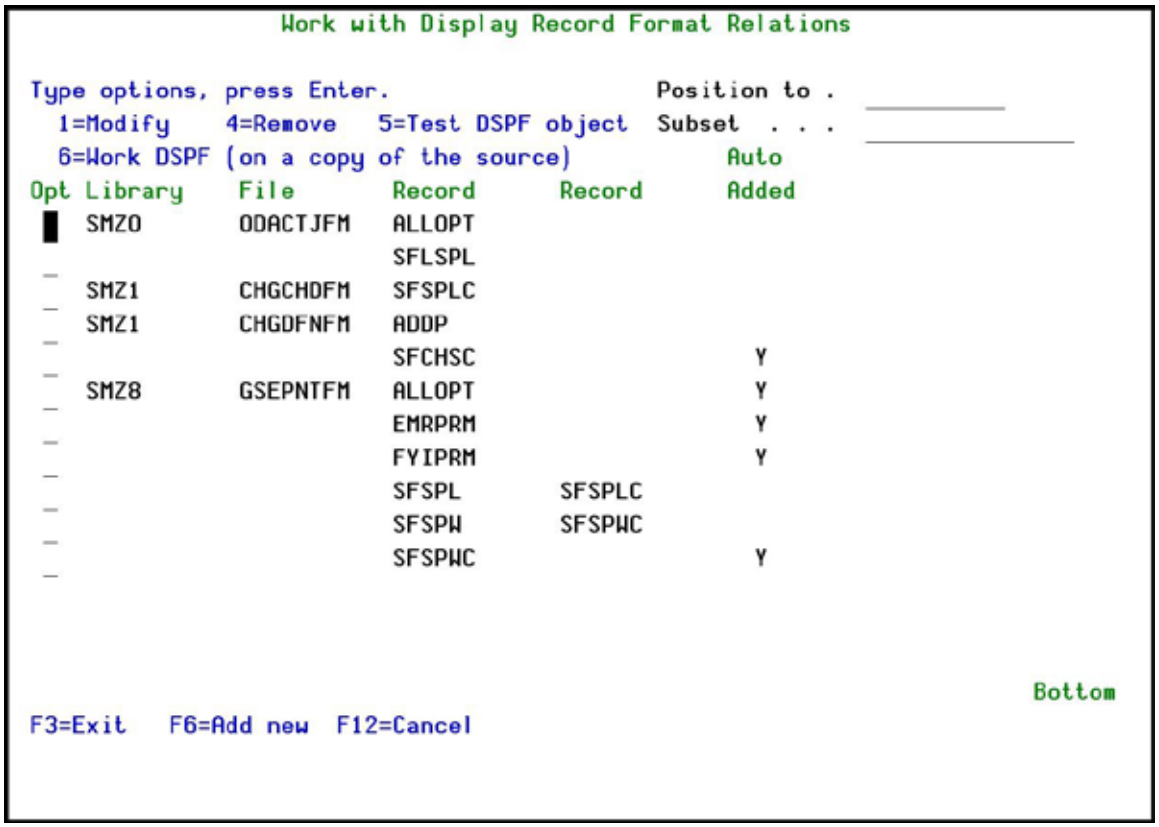
Parameter or Option	Description
For SFLCTL: Subfile page	The subfile page number of the SFLCTL
Check required	**Y** = This record will be shown as requiring intervention in the **Is user intervention required?** screen. For more information, see *Check and Auto Repair Changes* on page *62*.

3. Enter your selection parameters and press **Enter**. The **Work with Display Record Format** screen re-appears.
4. Press **Enter**. The **Auto Update DSPF Record and Fields** screen appears.
5. Press **Enter**. Changes to DSPFs are automatically corrected in the Repository.

   For DSPFs that have been modified, changes such as the position of fields on the screen or changes to the SFLPAG (Subfile page) are automatically corrected. Other changes, such as the renaming of Records or Fields, require user intervention.

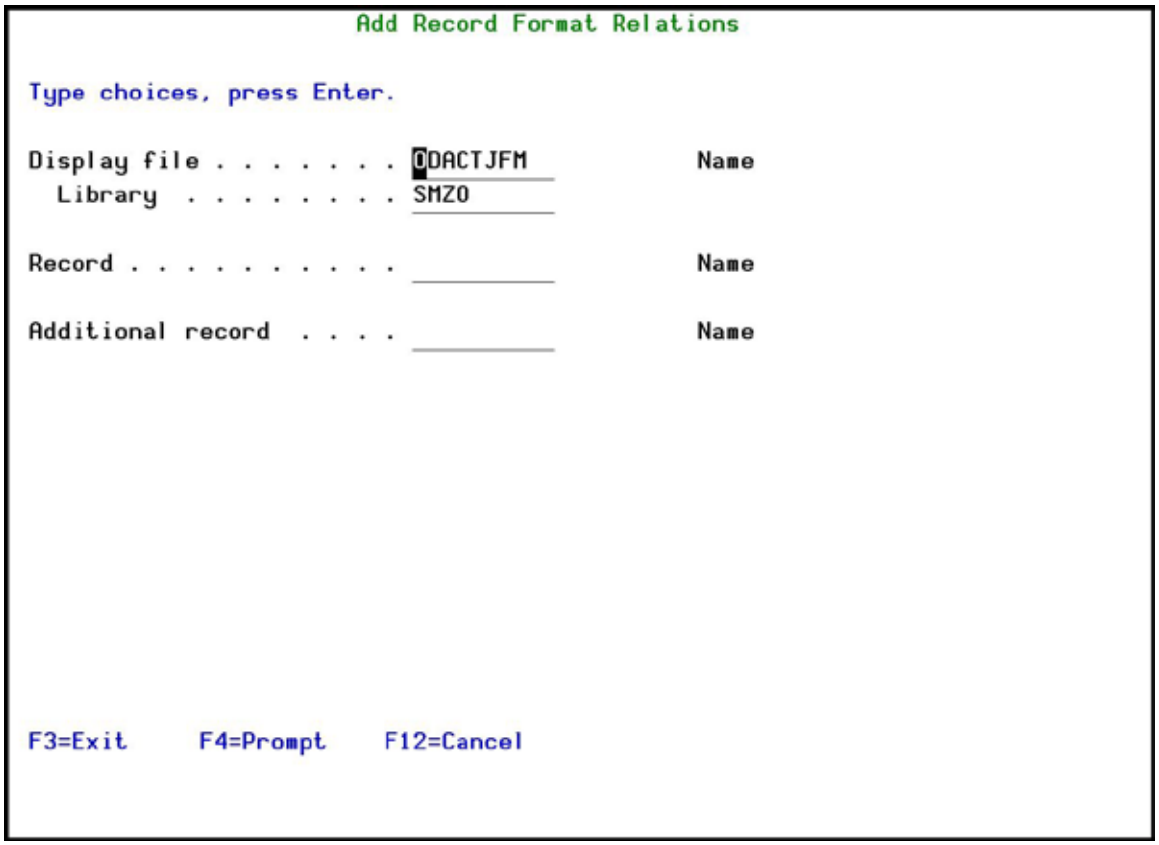
Work with Records Displayed Together

1. Select **52. Work with Records Displayed Together** from the **Business Items Handling** menu. The **Work with Display Record Format Relations** screen appears.



Work with Display Record Format Relations

2. Type **1** next to a format to modify it or press **F6** to add a new format. The **Add Record Format Relations** screen appears. Values are pre-populated according to the position of the cursor in the **Work with Display Record Format** screen.



Add Record Format Relations

Parameter or Option	Description
Display file	The display file from which you want to define Business Items.
Library	The library where the display file is stored.
Record	The record in the display file from which you want to define Business Items.
Additional record	An additional record in the display file from which you want to define Business Items. If you specify an additional record, it must be different from the first record specified.

3. Enter your selection parameters and press **Enter**.

Business Items Definition

To work with Business Items in **Capture**, you must first define them to **Capture**. You do this by first collecting fields from all display files in the systems that you want to capture and then within that collection of fields, you identify the relevant Business Items.

Collect DSPF Fields

You must run this option once for every library for which you want to collect display fields. After you have run the option for every library, run the process described in *Identify Business Items* on page *71*.

To collect display file fields from a library:

1. Select **61. Collect DSPF Fields** from the **Business Items Handling** menu. The **Collect Capture DSPF Fields** screen appears.

```
                  Collect Capture DSPF Fields (CLTCAFLD)

Type choices, press Enter.

Library . . . . . .              Name
DSPF Name . . . . . .  *ALL      Name, generic*, *ALL
Replace or add records . . . . .  *REPLACE  *ADD, *REPLACE

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

Collect Capture DSPF Fields

Parameter or Option	Description
Library	The name of the library for which you want to collect display fields
DSPF Name	Name = The name of a specific Display File Generic* = A group of Display Files *ALL = All the Display files in the library

Parameter or Option	Description
Replace or add records	*ADD = Add the records to the file. *REPLACE = Replace the records in the file. For the first library for which you collect fields, use either *ADD or *REPLACE. For all consequent libraries, use *ADD.
Work Library	The name of the library to receive the results. The default is QTEMP. Note that if you work with QTEMP, you must finish the process by running Identify Business Items before signing off from the session. If you sign off, then all information is lost and you must repeat the collection process again. Also, if you work with QTEMP, you must run the Identify Business Items option from the same workstation.

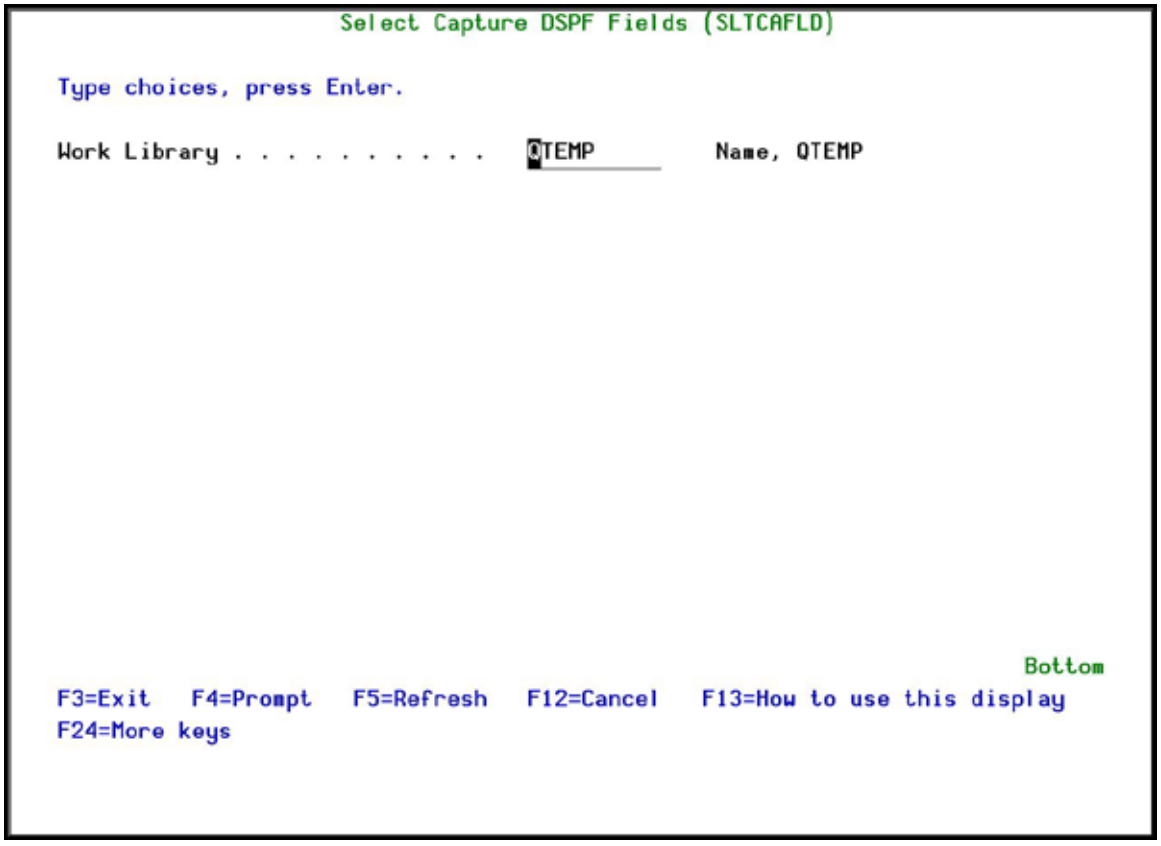
2. Enter your required parameters and press **Enter**. The fields that match the parameter requirements are collected.

Identify Business Items

Before you identify the Business Items in the display files, you must first prepare the information by running the process described in *Collect DSPF Fields* on page *69*.

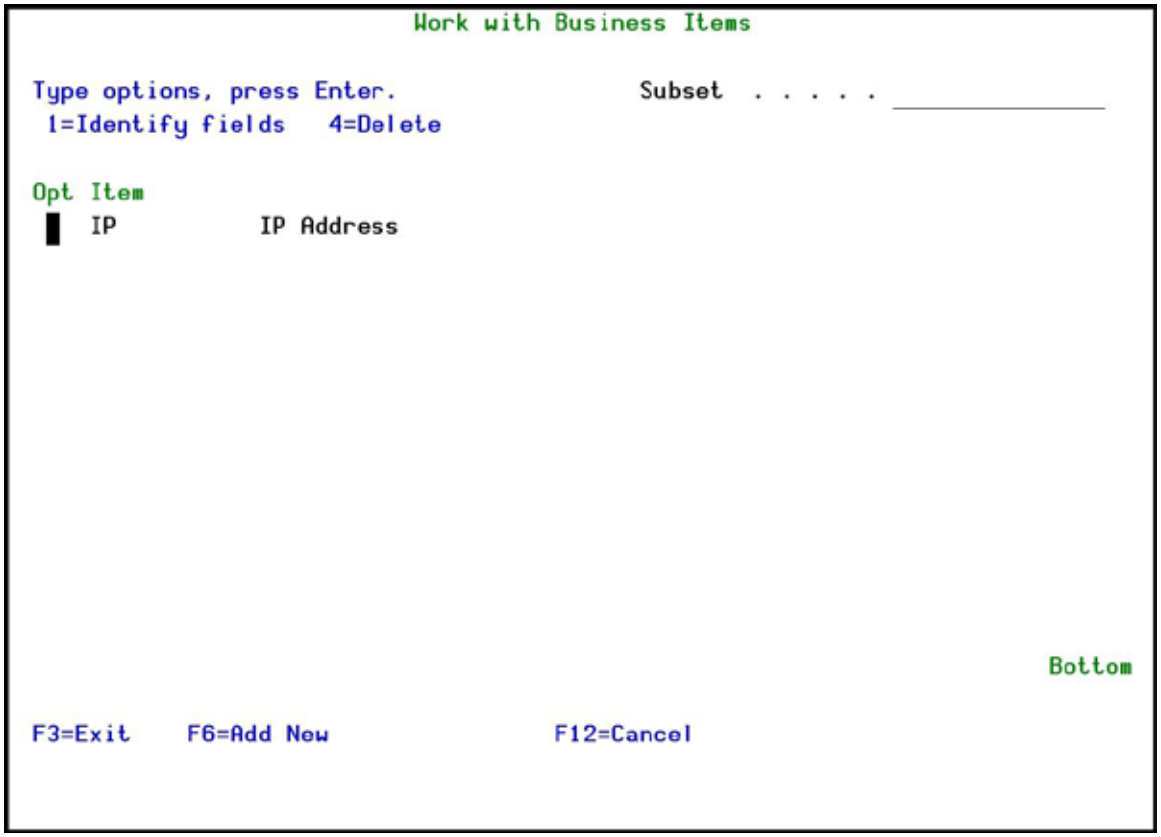
To collect display file fields from a library:

1. Select **62. Identify Business Items** from the **Business Items Handling** menu. The **Select Capture DSPF Fields** screen appears.



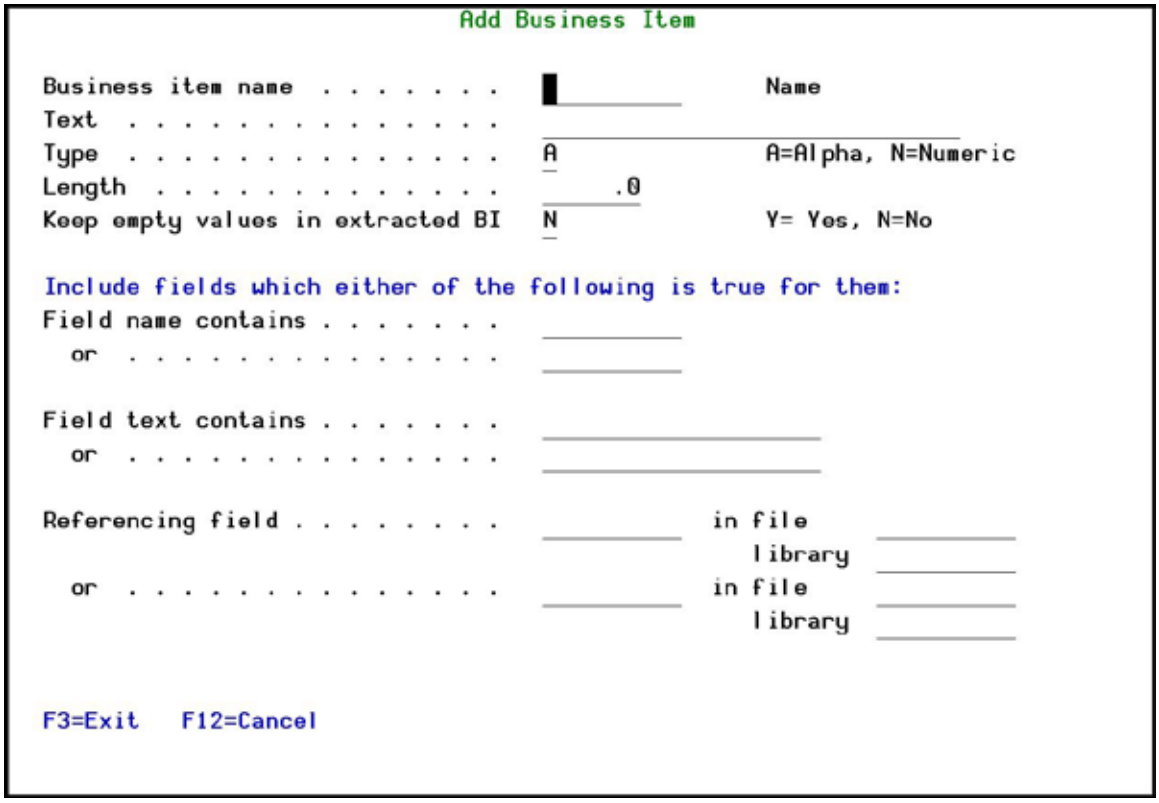
Select Capture DSPF Fields

2. Enter the **Work Library** you used in the Collect DSPF Fields process and press **Enter**. The **Work with Business Items** screen appears.



Work with Business Items

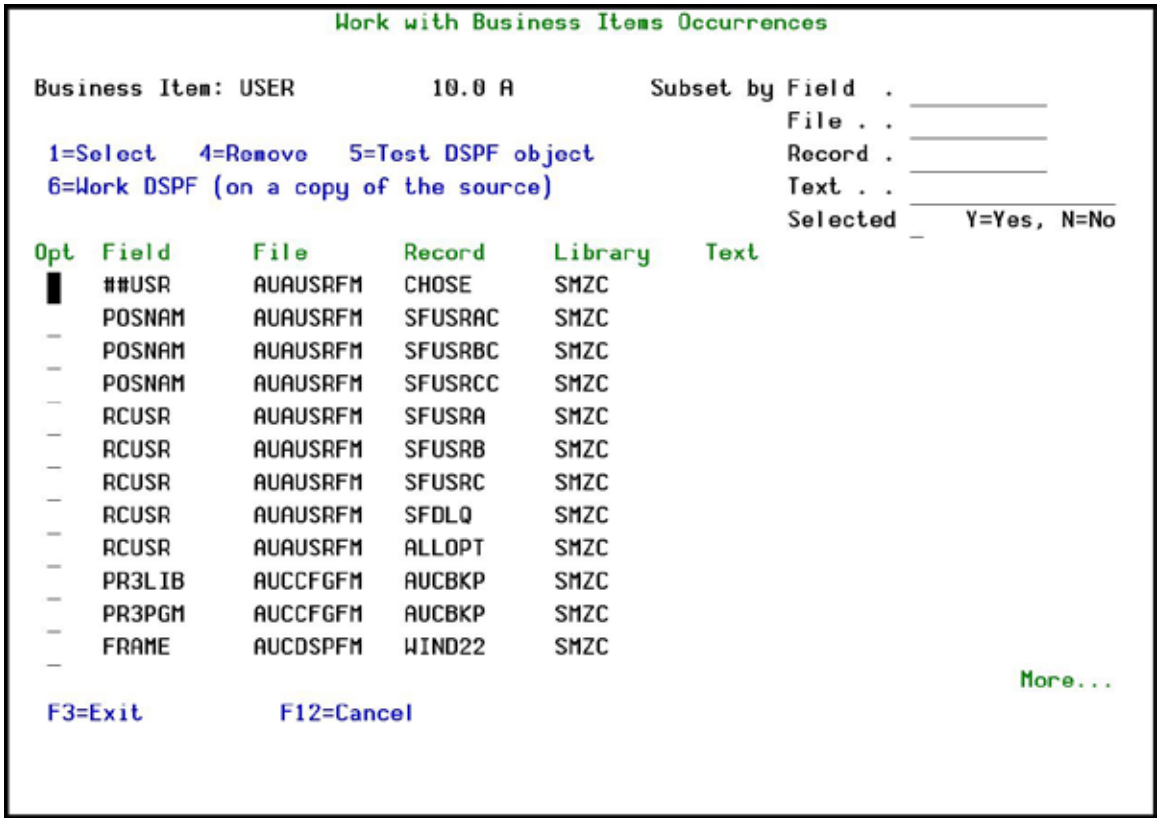
3. Press **F6** to add new Business Items. The **Add Business Item** screen appears. Use this screen to filter for Business Items you want to track.



Add Business Item

Parameter or Option	Description
Business item name	Type a name for the Business Item
Text	Type a meaningful description for the Business Item
Type	The type of field to search for: **A** = Alphameric **N** = Numeric
Length	Enter the field length to search for. For a numeric field, include the number of decimal places.
Keep empty values in extracted BI	You can choose whether you want to extract a Business Item whose value is empty. **Y** = Yes **N** = No
Field name contains	Filters for field name.
Field text contains	Filters for field text
Referencing field	Filters for referencing fields. Enter the field name, the file name and the library.

4. Enter your selection parameters and press **Enter**. The **Work with Business Items Occurrences** screen appears, showing all fields that meet the selection parameters.



Work with Business Items Occurrences

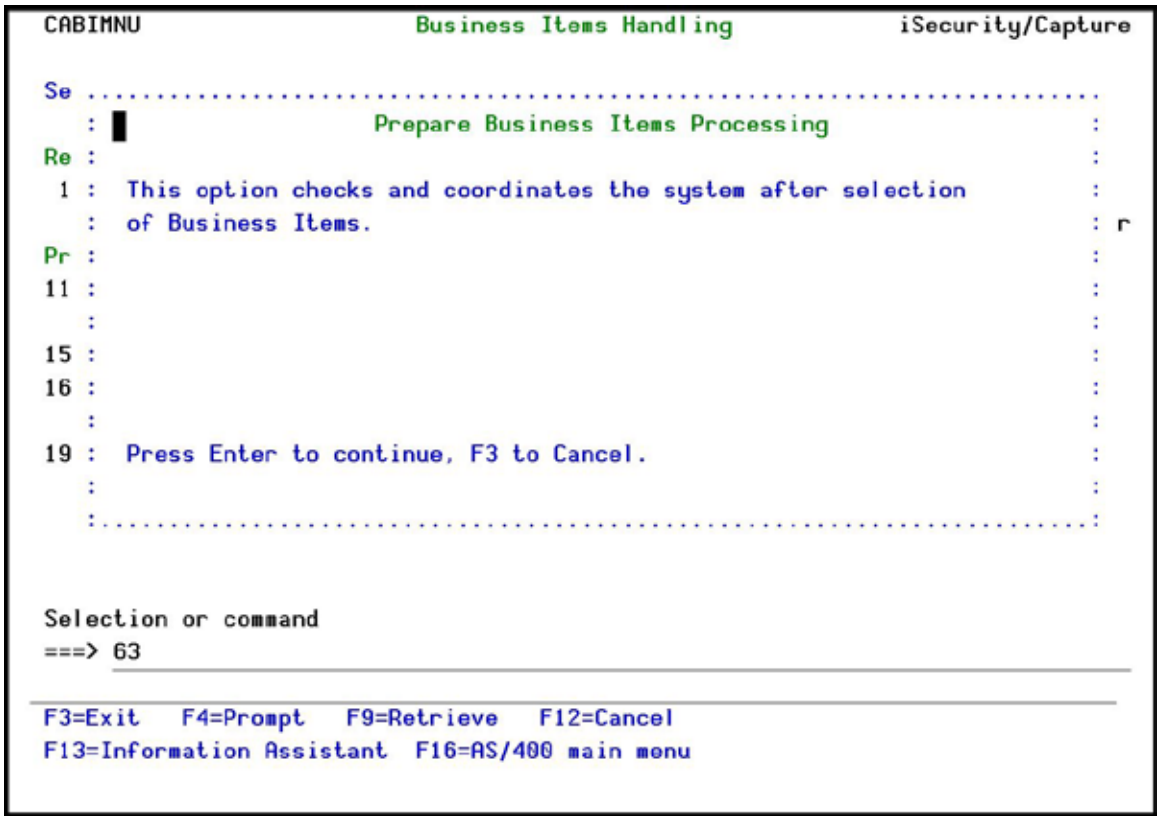
5. Use option **1** to select all the fields you want to include and press **Enter**. The fields you want to track for this Business Item are chosen.

Prepare Business Items Processing

You should finally run a process to check if any changes have been made to the Display Files that contain the Business Items.

To prepare Business Items processing:

1. Select **63. Prepare Business Items Processing** from the **Business Items Handling** menu. The **Prepare Business Items Processing** screen appears.



Prepare Business Items Processing

2. Press **Enter**. The display files are checked and a message showing the result of the checks appears.
3. If the message indicates that changes were detected, you must re-run the processes described in *Extract Business Items*
4. *Run an* automatic procedure to extract all Business Items appearances in display files.

To extract the Business Items:

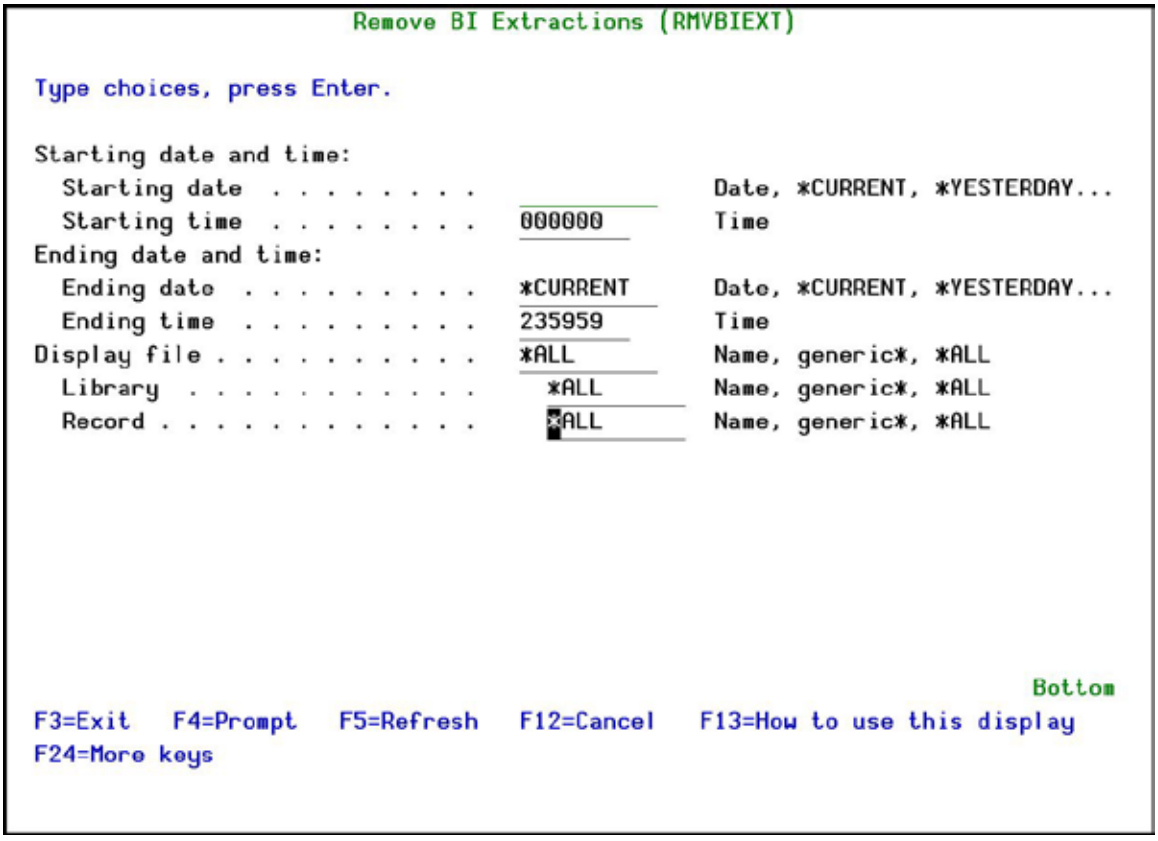
5. Select **15. Extract Business Items** from the **Business Items Handling** menu. If found, the Business Items are extracted. A message shows the result of the process.

Remove Extractions

You can remove some of the extracted Business Items from the repository.

To remove the extracted Business Items:

6. Select **19. Remove Extractions** from the **Business Items Handling** menu. The **Remove BI Extractions** screen is displayed.



Remove BI Extractions

Parameter or Option	Description
Starting Date & Time **Ending Date & Time**	Remove only those Business Items records for which the event occurred within the range specified by the starting and ending date/time combination. **Date or Time** = Enter the appropriate date or time ***CURRENT** = Today (Current Date) ***YESTERDAY** = Previous date ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
Display file	Selects a subset of records by display file **Name** **Generic*** ***ALL**
Library	Selects a subset of records by library **Name** **Generic*** ***ALL**
Record	Selects a subset of records by record **Name** **Generic*** ***ALL**

7. Enter your required parameters and press **Enter**. The appropriate extracted Business Items are removed from the system.

8. DSPF Defined in the System on page *63*.

Environments

If, when you configured Business Items Support, you answered **Y** for the **Analyze run environment by *LIBL**, then temporary environment names are allocated automatically by Library List (See *Defining Business Items Support* on page *22* for more details). You should change these names to a meaningful name.

Work with Environments

1. Select **71. Work with Environments** from the **Business Items Handling** menu. The **Work with Provide Environment** screen appears.

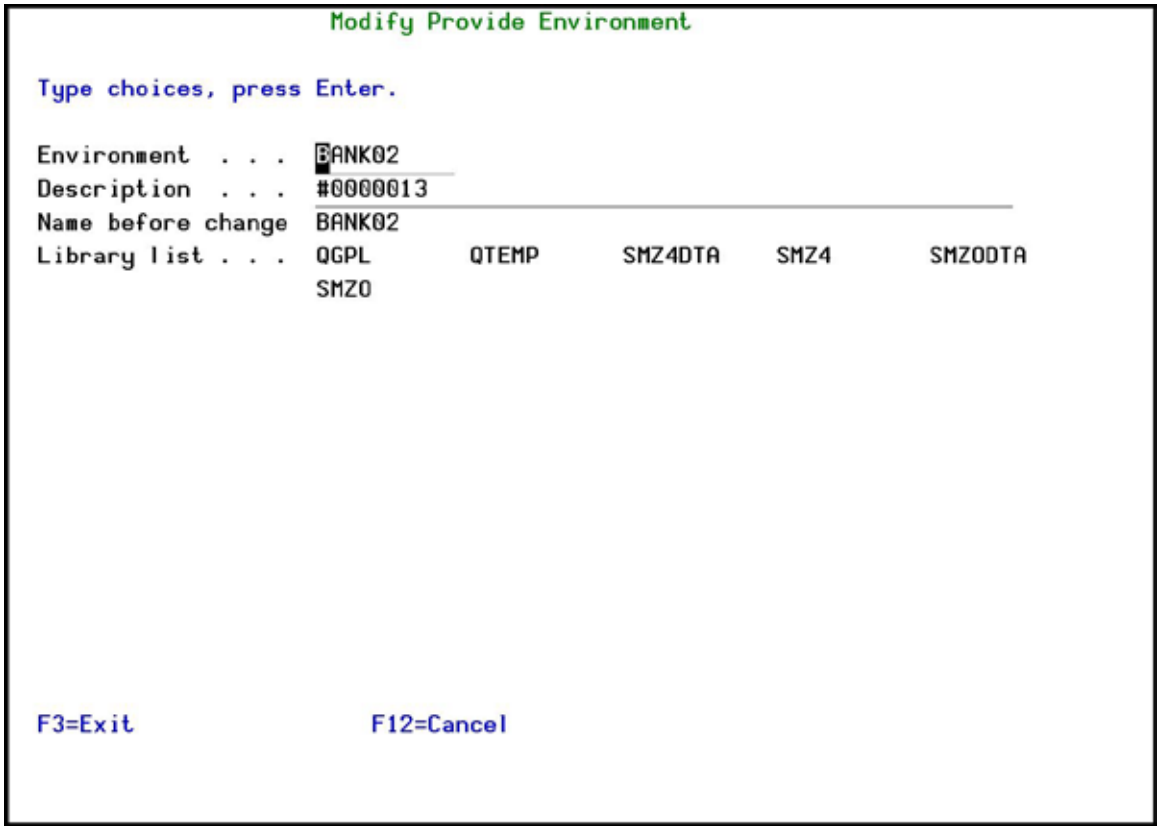
```
                    Work with Provide Environment

Type options, press Enter.
  1=Modify                                  Subset  . . .  _____________

                Name before
Opt Environment   change
 _  #0000003                #0000003
 _  #0000008                #0000008
 _  #0000009                #0000009
 _  #0000010                #0000010
 _  #0000012                #0000012
 _  #0000014                #0000014
 _  #0000022                SMZ8 SMZJ SMZ1 FS QTEMP QGPL QRPG          ...
 _  #0000023                SMZ6DTA SMZ6 CS QRPG QGPL QTEMP            ...
 _  AGENT007                #0000007
 _  BANK02                  #0000013
 _  BANK03                  #0000005
 _  BANK04                  #0000019
 _  BANK17                  #0000011
 _  BANK54                  #0000015
                                                                  More...
F3=Exit              F12=Cancel
```

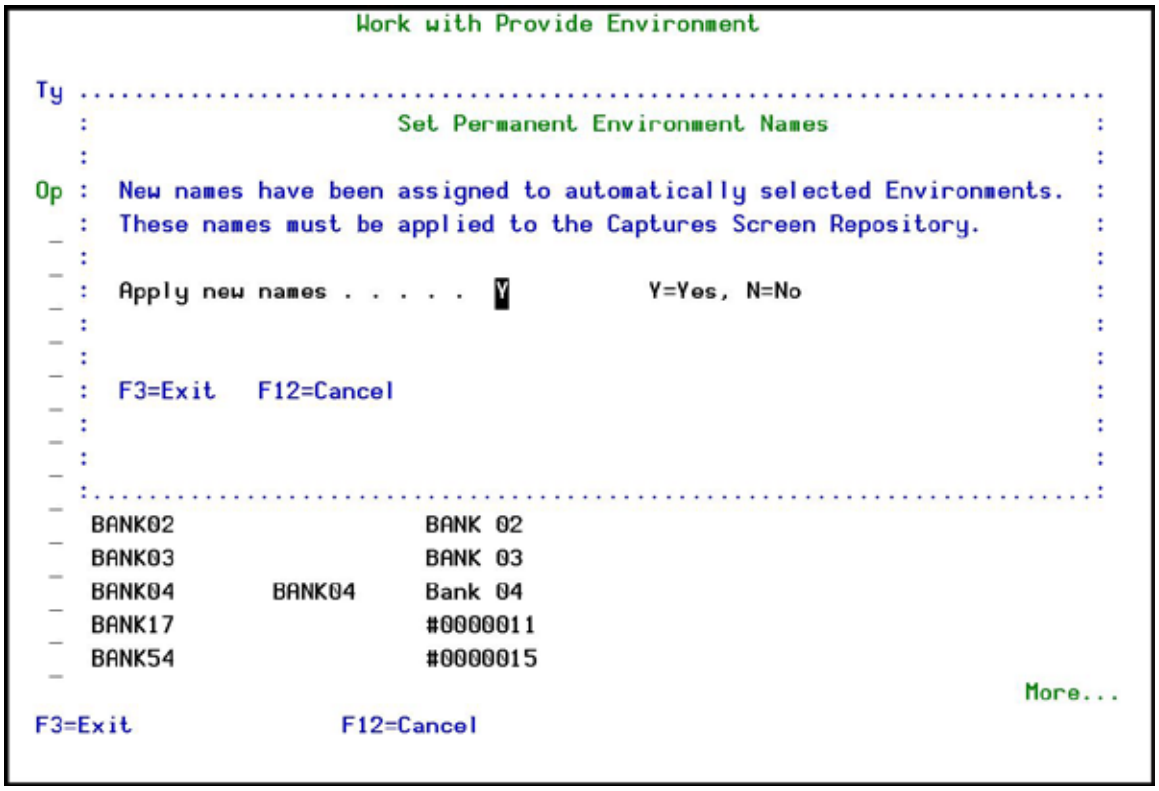
Work with Provide Environment

2. Type **1** by the Environment you want to change. The **Modify Provide Environment** screen appears.



Modify Provide Environment

3. Update either the Environment field, or the Description field, or both fields, and press **Enter** twice. The **Work with Provide Environment** screen appears.
4. Press **F3** to exit the **Work with Provide Environment** screen. The **Set Permanent Environment Names** screen appears. This screen allows you to apply your changes to the Captures Screen Repository.



Set Permanent Environment Names

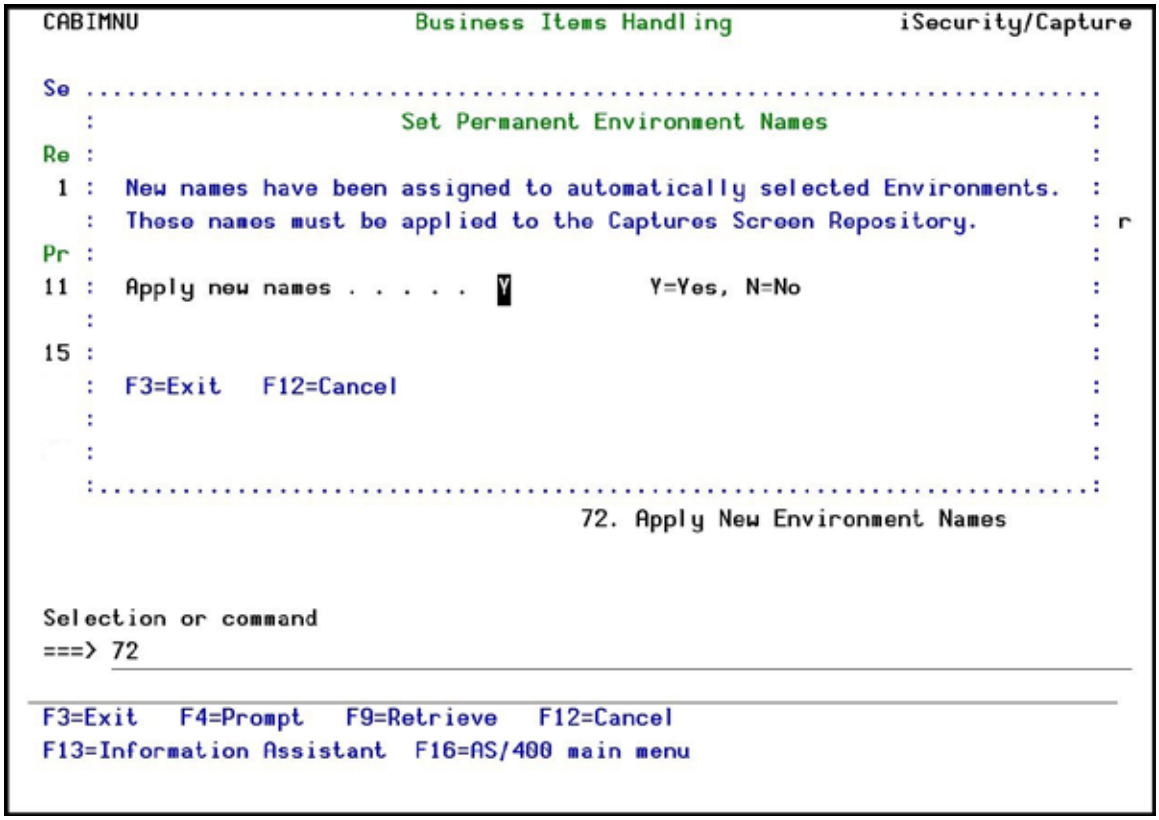
5. Enter **Y** and press **Enter** to apply the new names.

If you enter **N** or exit this screen using **F3** or **F12**, you can apply the changes later using option **72. Apply New Environment Names**. If you have many changes to do, you might want to update all the changes together. For more details, see *Apply New Environment Names* on page *80*.

Apply New Environment Names

If you have multiple changes to Environment Names, you can apply all the changes at the same time.

1. Select **72. Apply New Environment Names** from the **Business Items Handling** menu. The **Set Permanent Environment Names** screen appears.

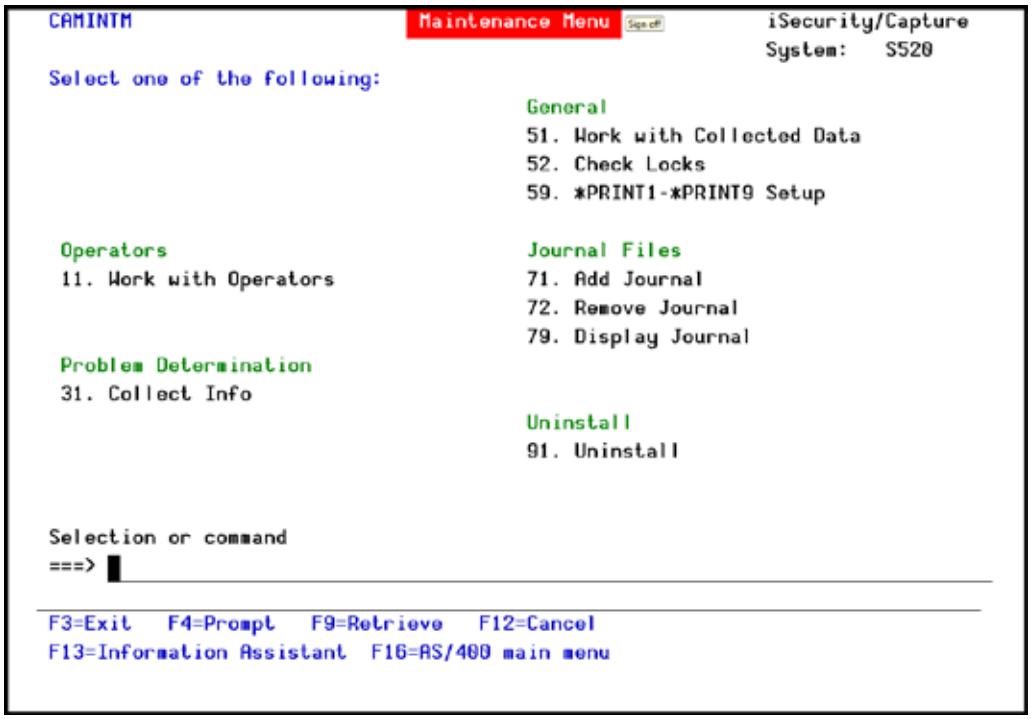


Set Permanent Environment Names

2. Press **Enter** to apply your changes.

Chapter 6: Maintenance Menu

The **Maintenance Menu** enables you set and display global definitions for **Capture**. To access the **Maintenance Menu**, select **82. Maintenance Menu** from the main menu. The **Maintenance Menu** appears.

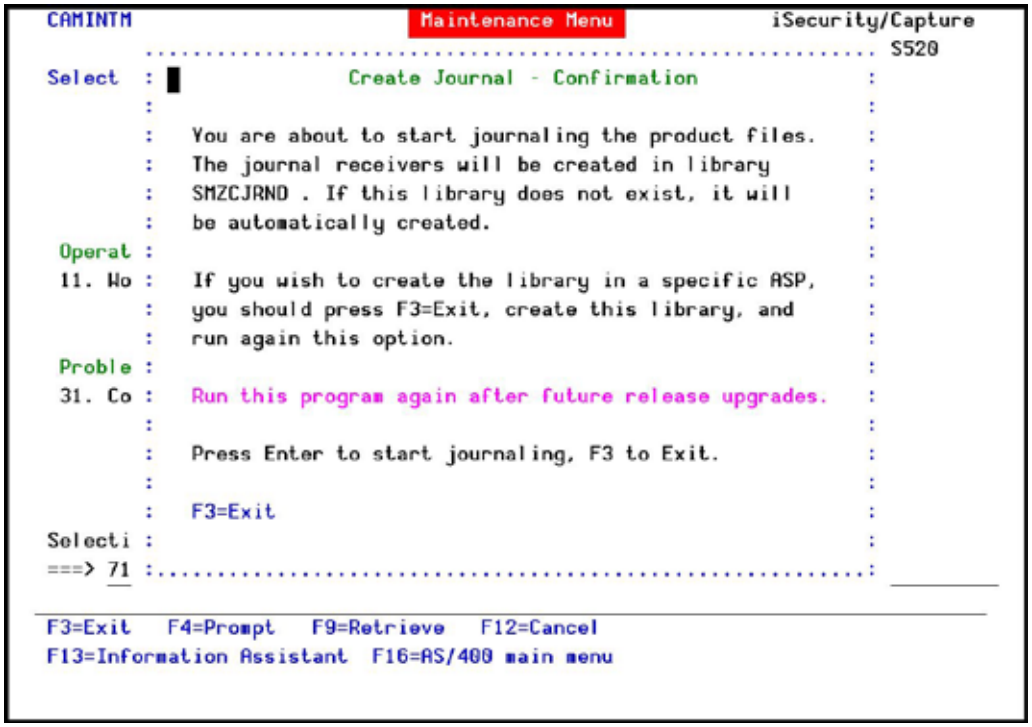


Maintenance Menu

Journal Files

Add Journal

1. Select **71. Add Journal** from the **System Maintenance** menu. The **Create Journal – Confirmation** screen appears.



Create Journal - Confirmation

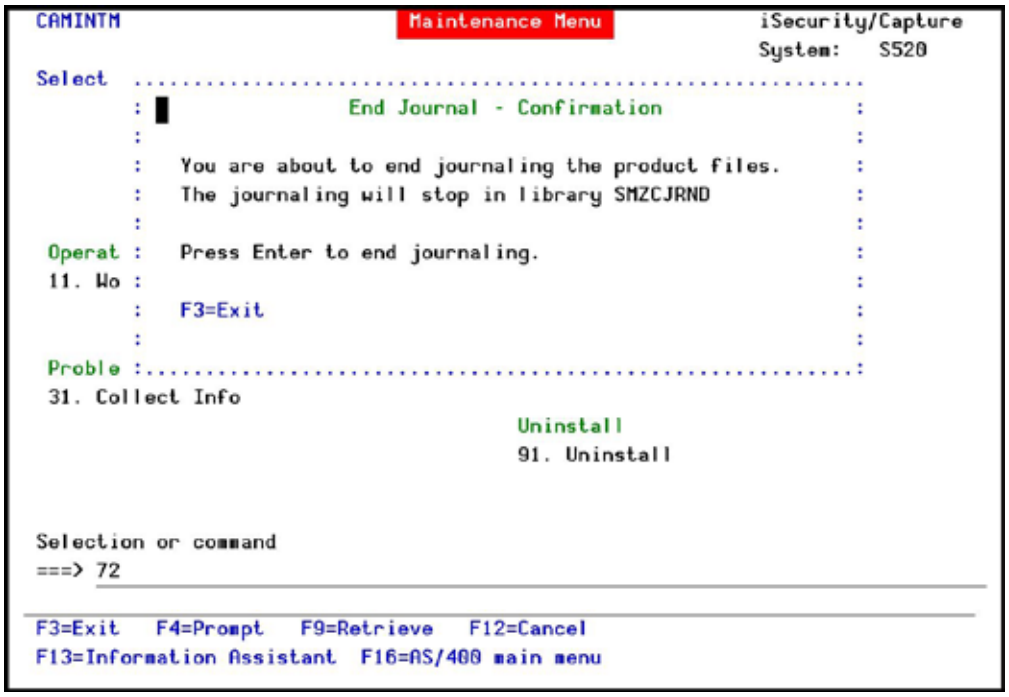
2. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZCJRND**. If this library does not exist, it will be automatically created.

Note: If you wish to create the library in a different ASP, press F3=Exit, create the library and run this option again.

Note: You must re-run this option after every release upgrade.

Remove Journal

1. Select **72. Remove Journal** from the **System Maintenance** menu. The **End Journal – Confirmation** screen appears.

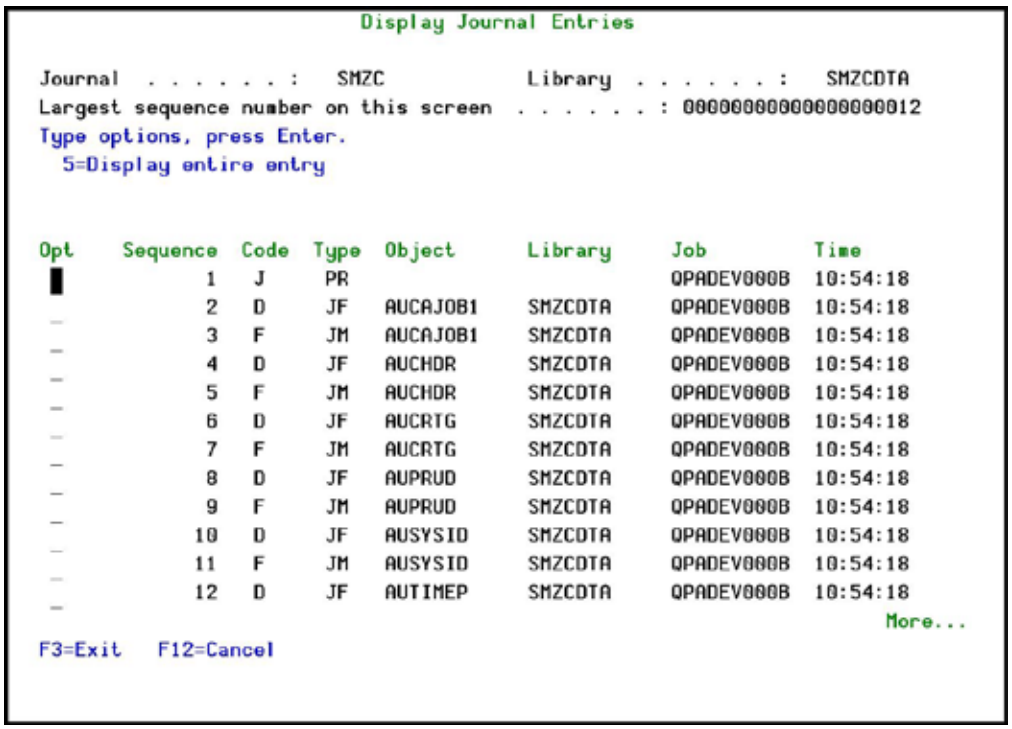


End Journal - Confirmation

2. Press **Enter** to confirm.

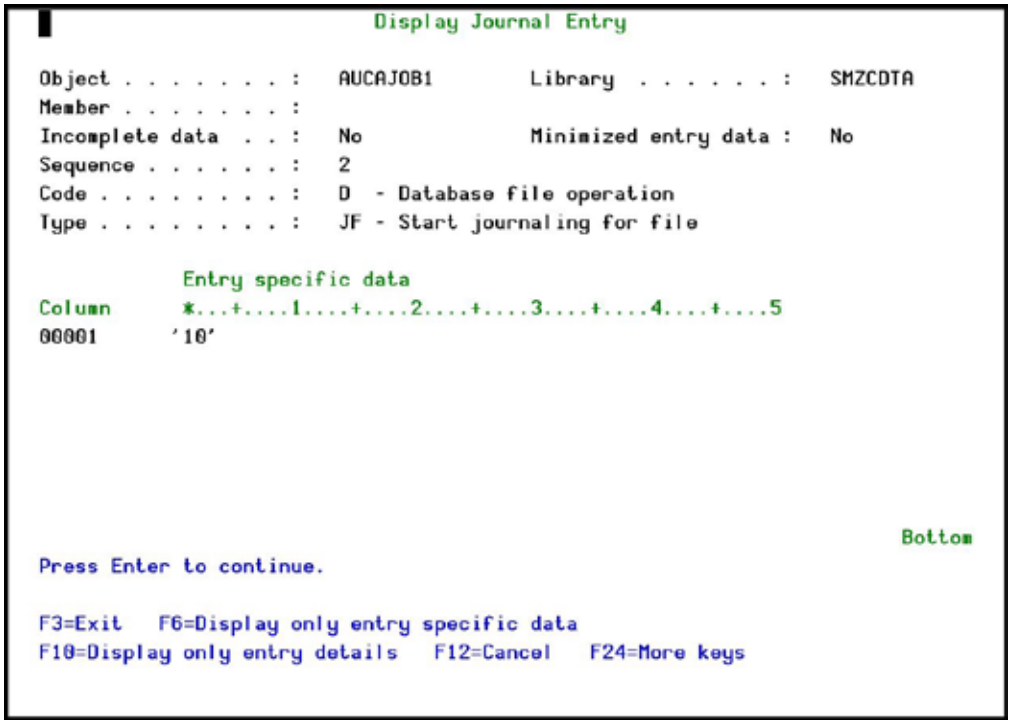
Display Journal

3. Select **79. Display Journal** from the **System Maintenance** menu. The **Display Journal Entries** screen appears.



Display Journal Entries screen

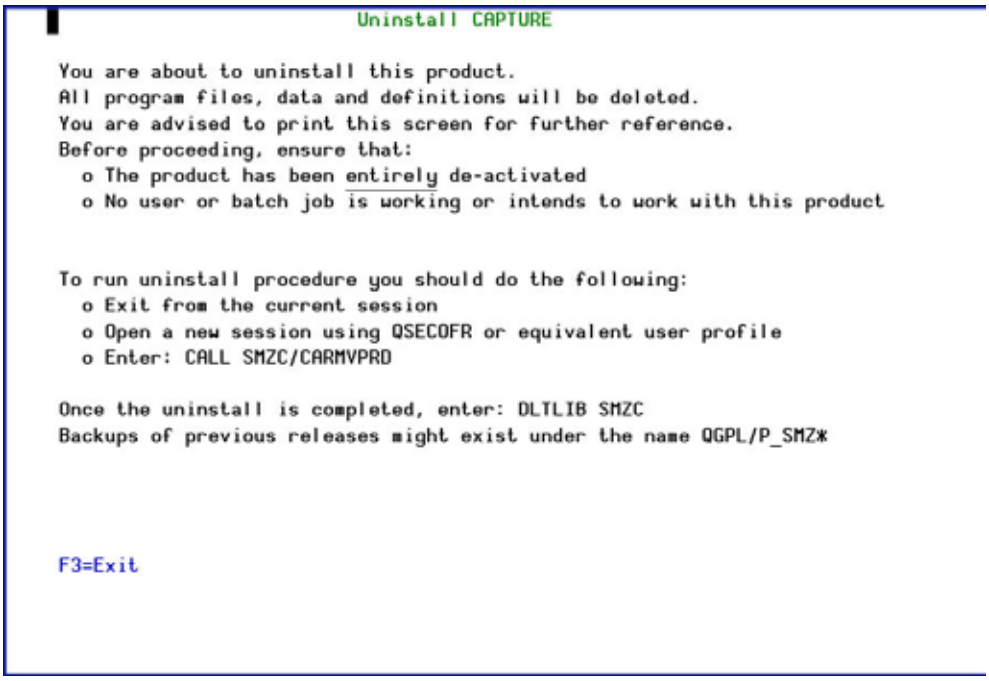
4. To display a specific entry, type **5** by that entry and press **Enter**. The **Display Journal Entry** screen appears.



Display Journal Entry screen

Uninstall

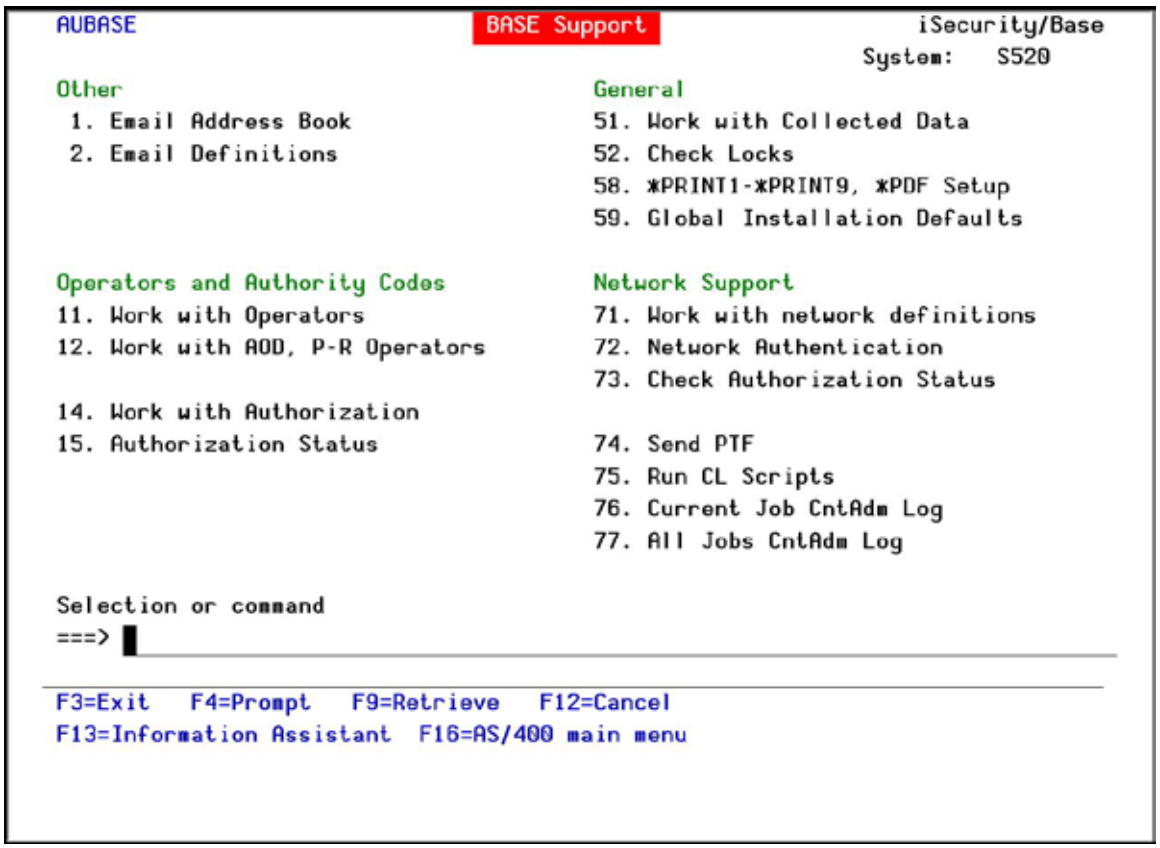
Choose **98. Uninstall Product** from the **Maintenance** Menu, and follow the directions on the screen.



Uninstall CAPTURE

Chapter 7: BASE Support Menu

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 **Capture** main menu.



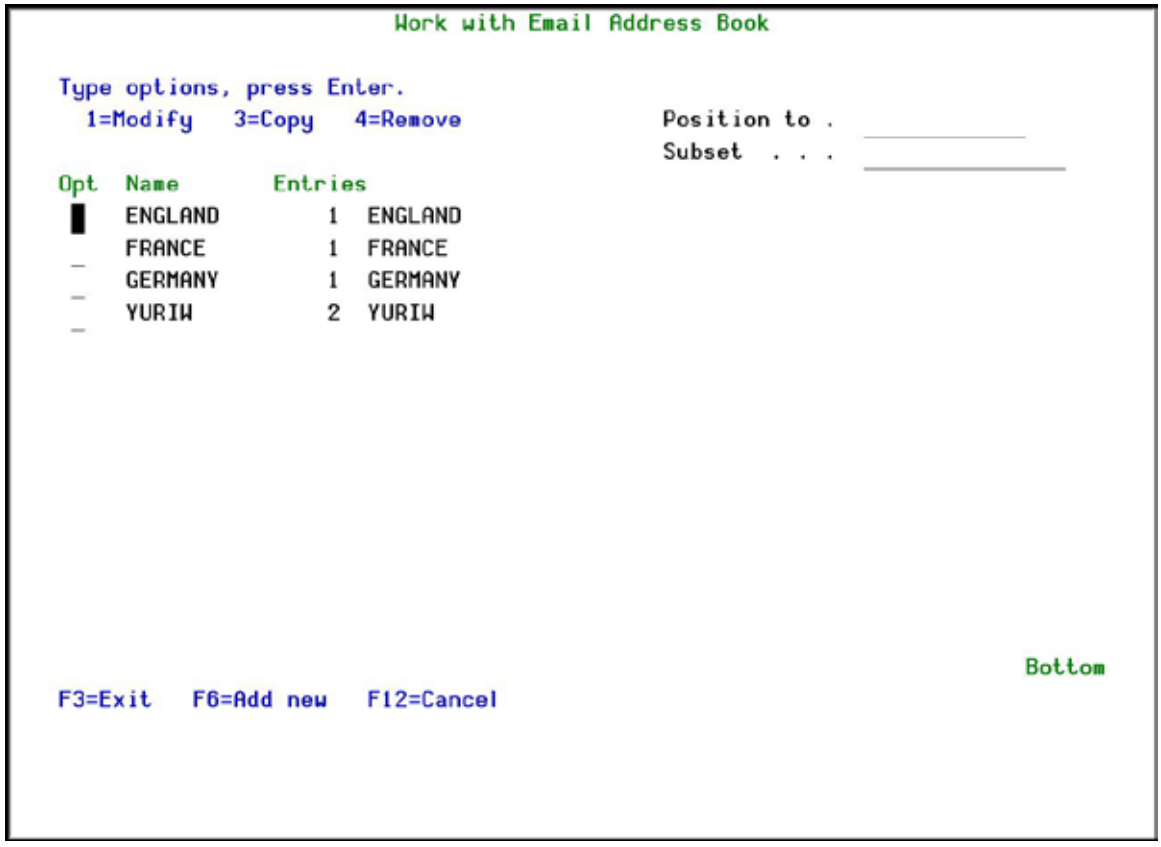
BASE Support

Other

Email Address Book

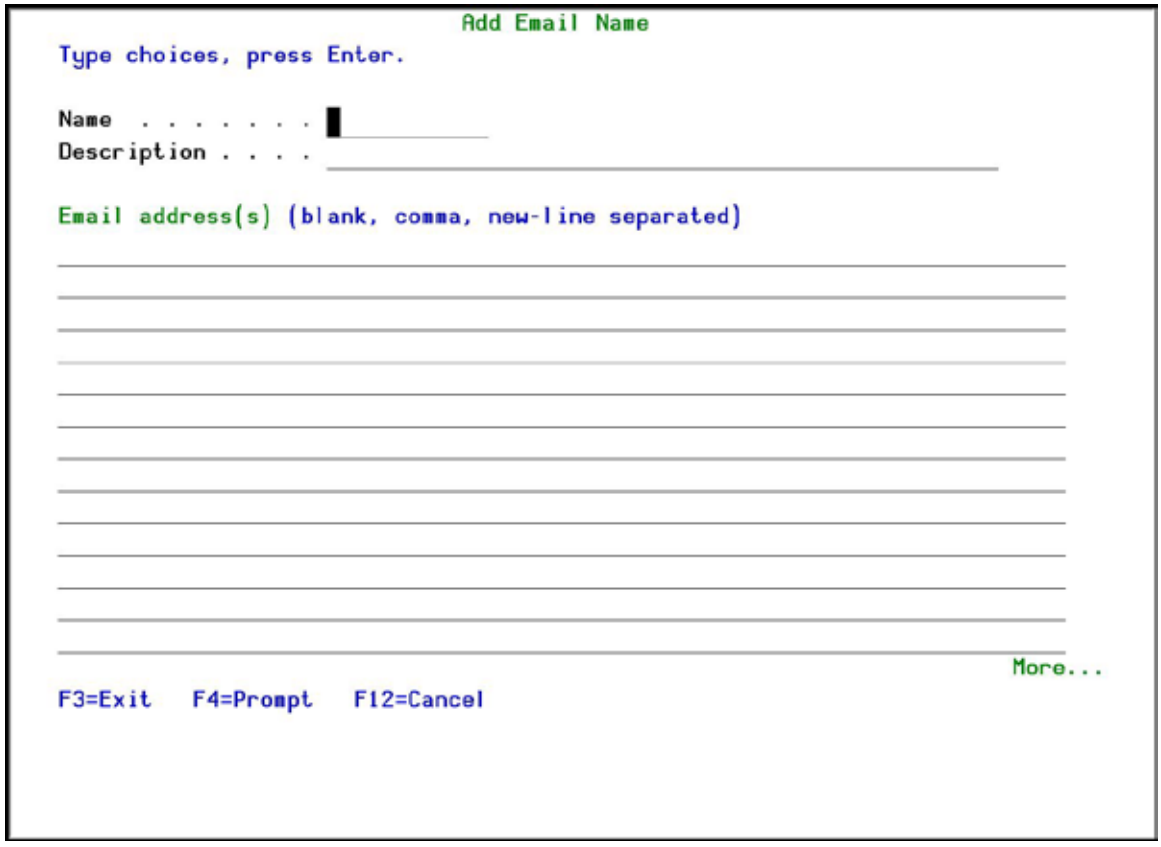
You can define the email address to be used for each user profile. You can also use this option to define an email group, with multiple addresses.

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.



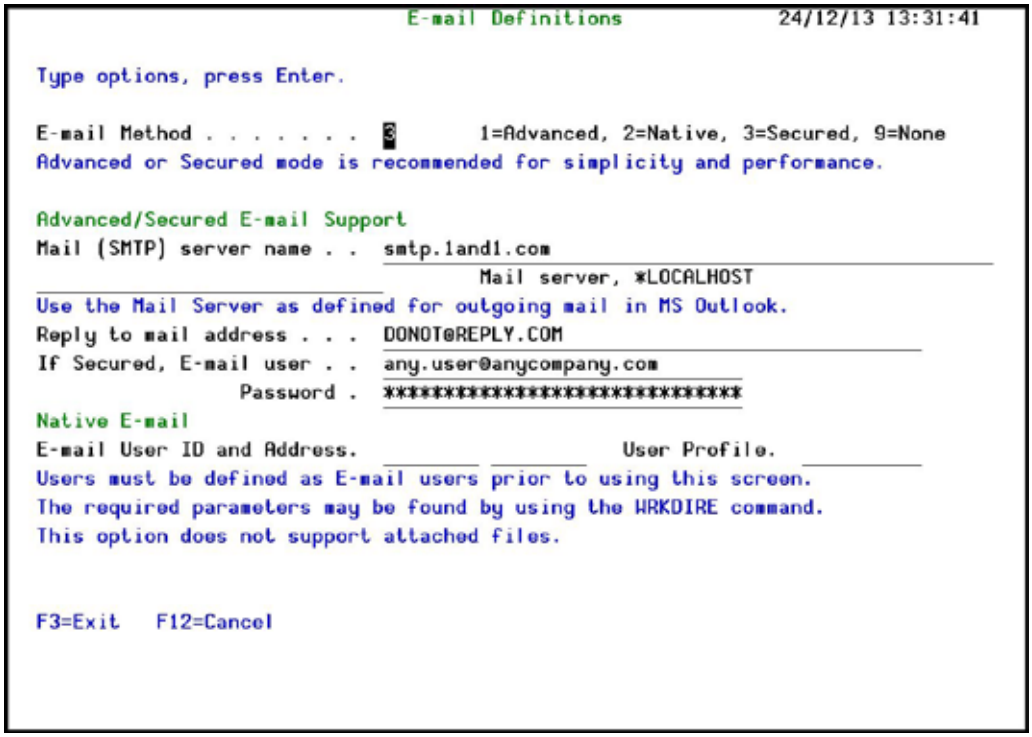
Add Email Name

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

Email Definitions

Authority on Demand can send out automatic emails every time a temporary authority is used.

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



E-mail Definitions

Parameter	Description
E-mail Method	**1**=Advanced **2**=Native **3**=Secured **9**=None Advanced or Secured mode is recommended for simplicity 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 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.
If secured, 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 the required fields and press **Enter**.

Operators and Authority Codes

Work with Operators

For a detailed explanation of this feature, see *Chapter 2: First Steps*.

Work with AOD, P-R Operators

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.

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

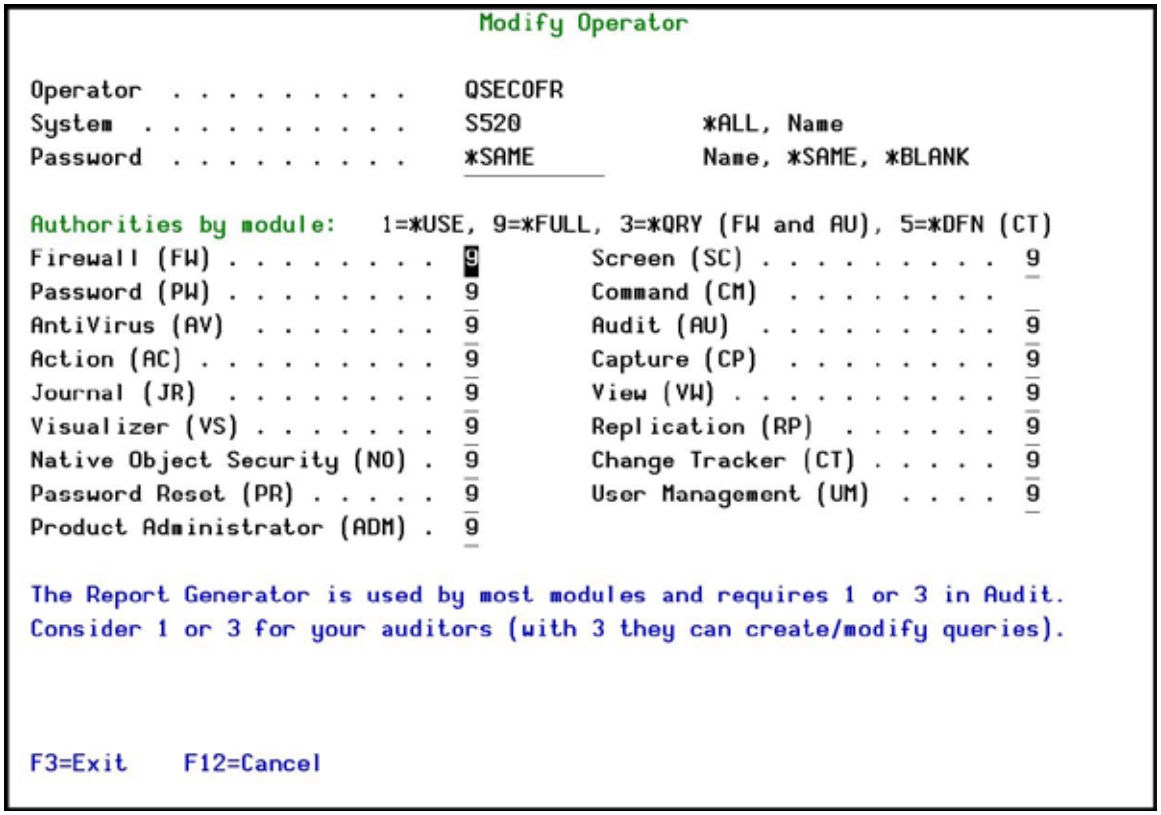
```
                          Work with Operators

Type options, press Enter.
  1=Select   4=Delete
                   Authority level: 1=*USE   9=*FULL
Opt User           System     AOD PR  USP  Adm
  *AUD#SECAD       S520         9  9    9    9
  ALEX             S520         9  9    5    9
  AV               S520         9            9
  JAVA2            S520         9  9    9    9
  LOWUSR           S520         9  9    9    9
  OD               S520         9  9    9    9
  OS               *ALL
  TZION            S520         9  9    9    9
  WEAKUSR          S520         9
  YORAM            S520         9            9


                                                                      Bottom
AOD=Authority on Demand   PR=Password Reset    USP=User Provisioning
                                               Adm=Administrator
F3=Exit    F6=Add new    F8=Print   F11=*SECADM/*AUDIT authority   F12=Cancel
```

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

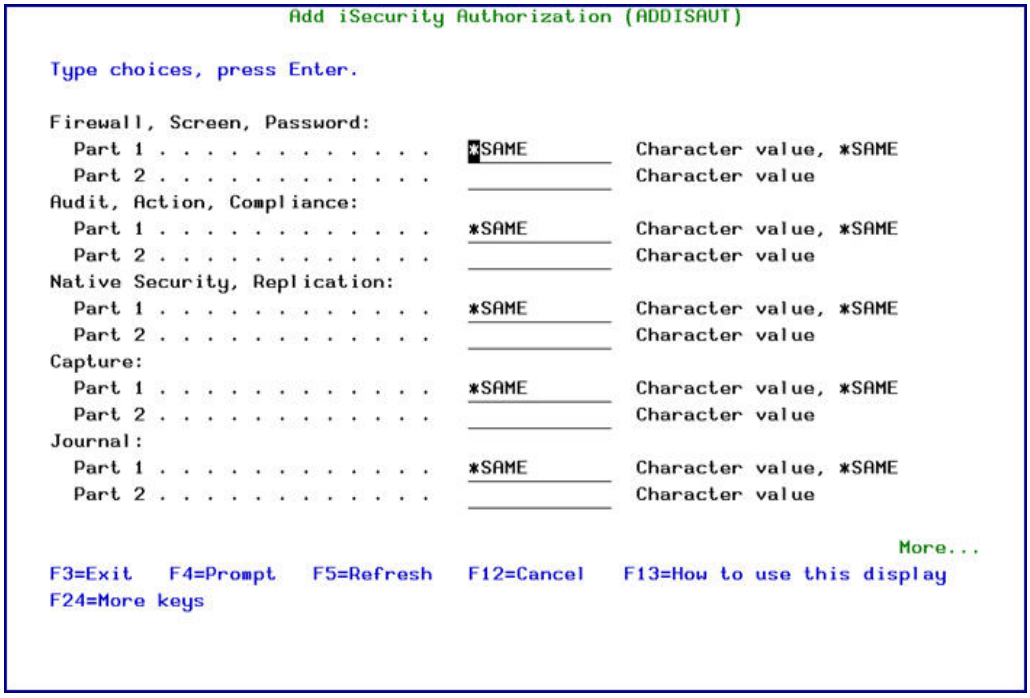
Option	Description
Password	**Name** = Password **Same** = Same as previous password when edited **Blank** = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use.
5 = *DFN	For Change Tracker use.

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.

Work with Authorization

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

1. Select **14. Work with Authorization** from the **BASE Support** menu. The **Add iSecurity Authorization** screen appears.



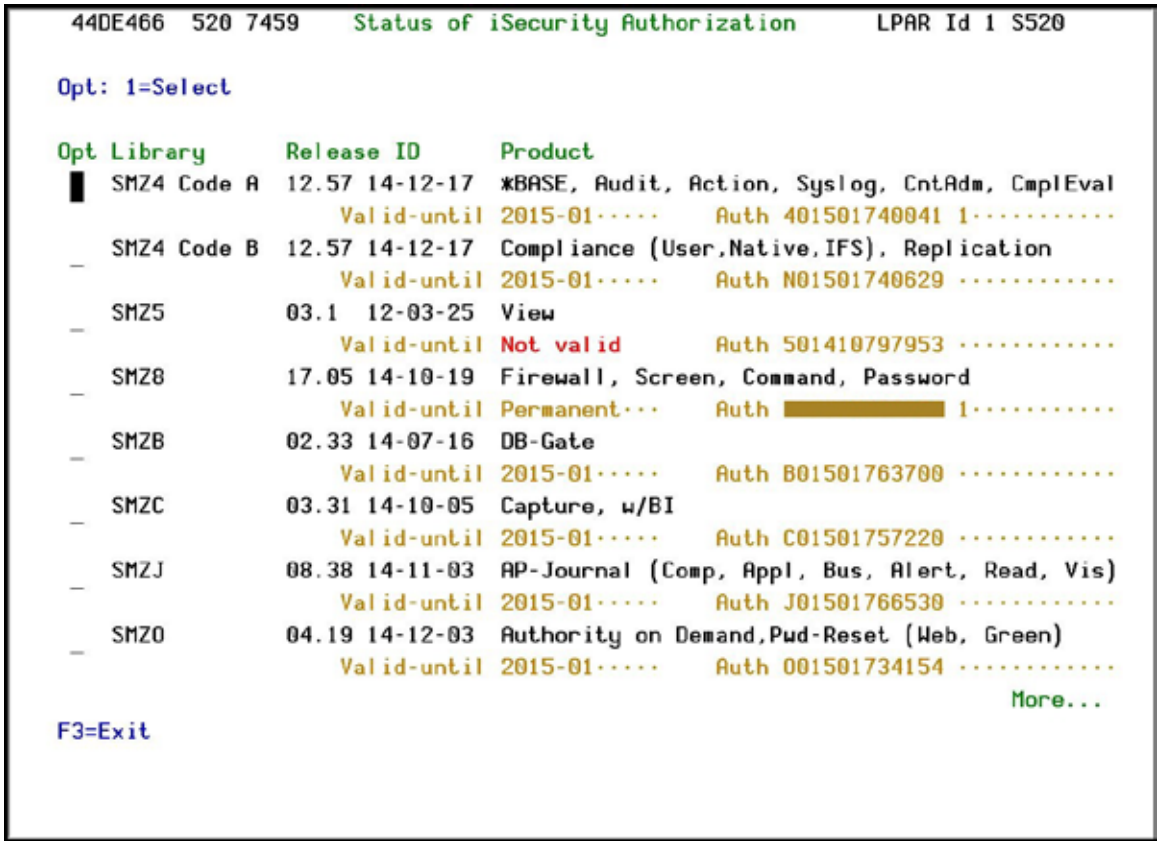
Add iSecurity Authorization (ADDISAUT)

2. Enter the required parameters and press **Enter**.

Display Authorization Status

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

1. Select **15. Authorization Status** from the **BASE Support** menu. The **Status of iSecurity Authorization** screen appears.



Status of iSecurity Authority Codes

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

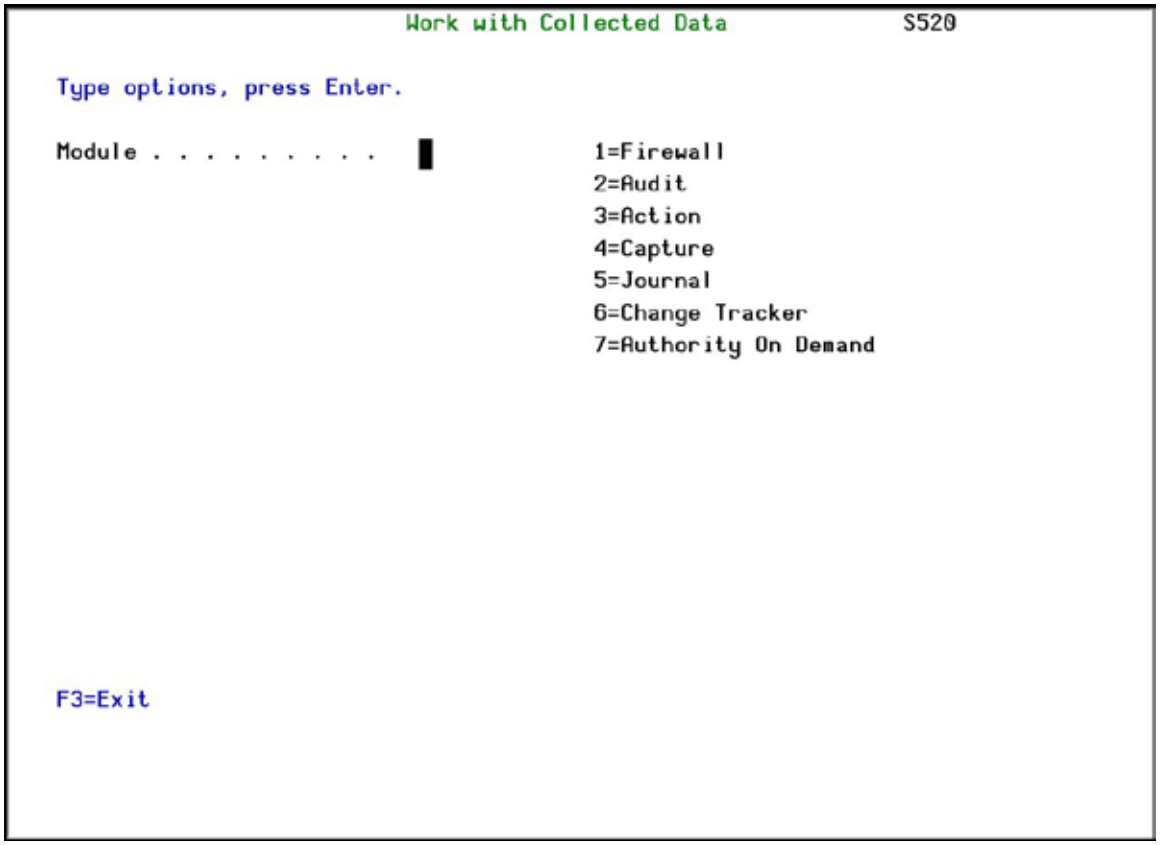
NOTE: Codes that will expire in less than 14 days appear in pink Permanent codes have deliberately been hidden in this screenshot.

General

Work with Collected Data

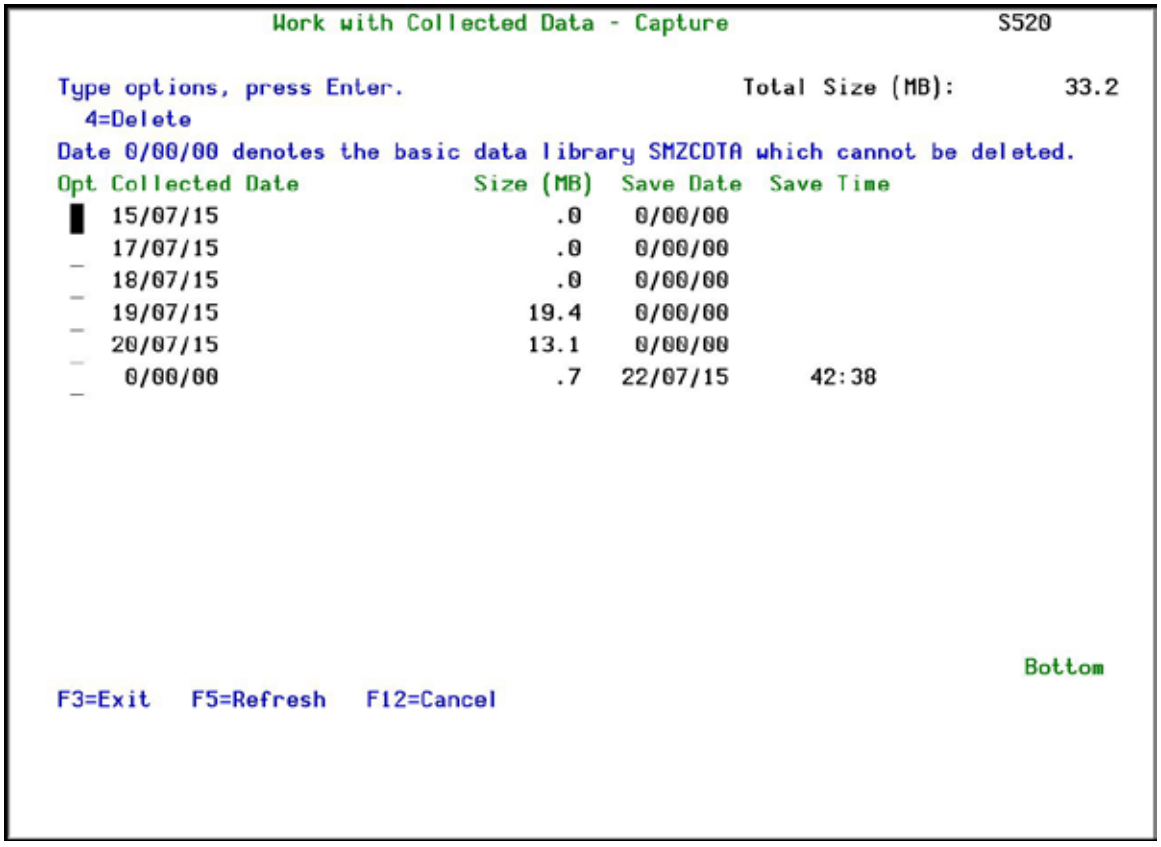
Administrators can view summaries of **Audit, Firewall,** and **Action** journal contents by day, showing the number of entries for each day together with the amount of disk space occupied. Administrators can optionally delete individual days to conserve disk space.

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 **4** (Capture) and press **Enter**. The **Work with Collected Data – Capture** screen appears.



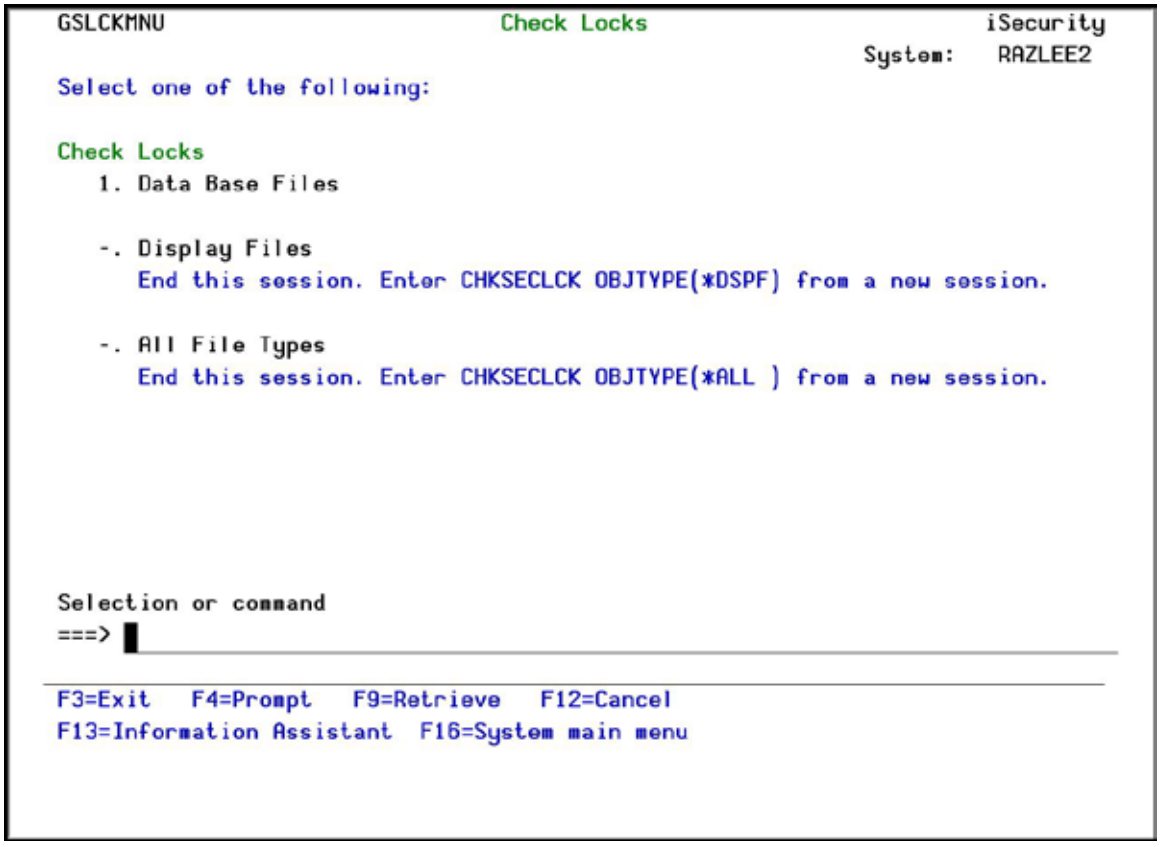
Work with Collected Data - Capture

3. Select **4** to delete data from specific date(s) and press **Enter**.

Check Locks

You need to run this option before you upgrade your system to check if any of the **Capture** 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 **Check Locks** screen appears.



Check Locks

2. Select one of the commands that appear on the screen.

*PRINT1-*PRINT9 Setup

Capture 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.

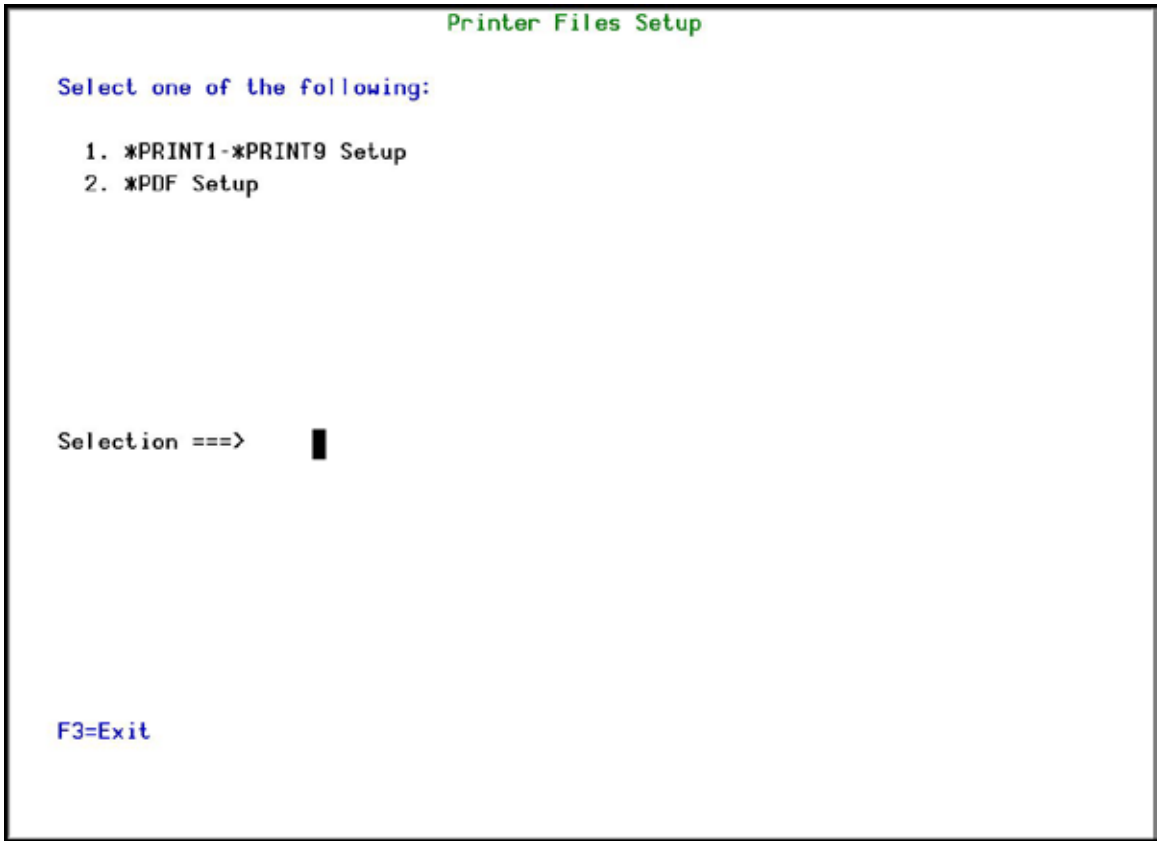
Output to one of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the ***CHGOUTQ*** command to specify the IP address of the designated remote location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

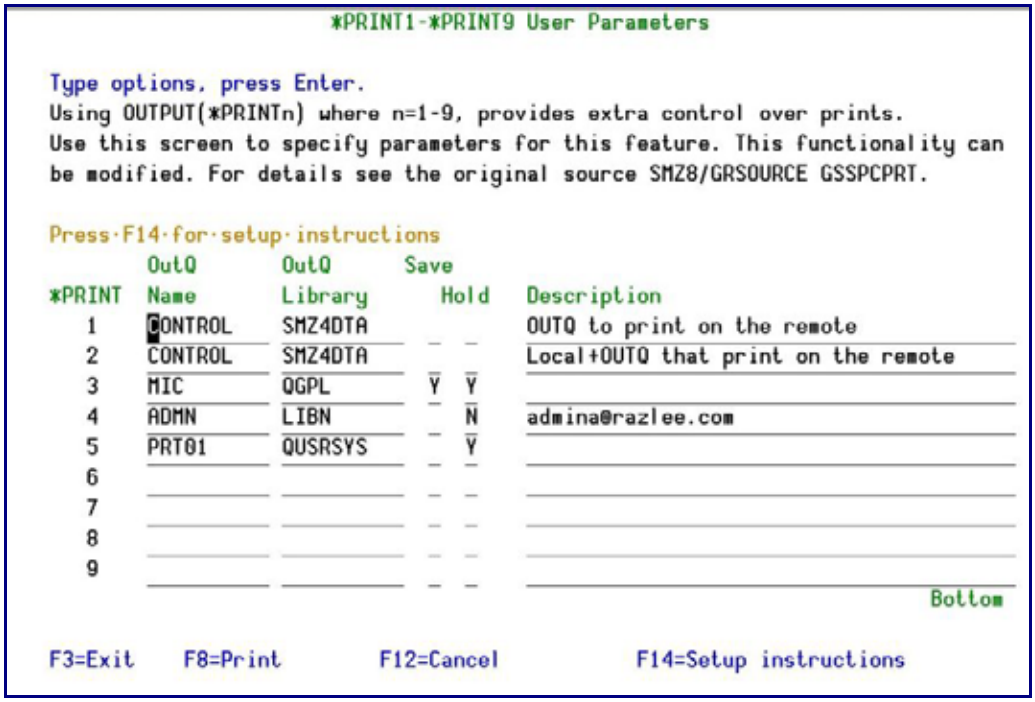
To define remote printers, perform the following steps:

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 ***PRINT1 - *PRINT9 Setup** screen appears.



PRINT1-*PRINT9 User Parameters

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

Parameter	Description
User Parameter	Name of the local output queue and its library
Description	Optional text description

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
QUTQ()	Name of the local output queue
RMTPRTQ()	Name of the remote print 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, ****PRINT1*** 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) TRANSFORM(*NO)
+ INTNETADR(1.1.1.100)

*PDF Setup

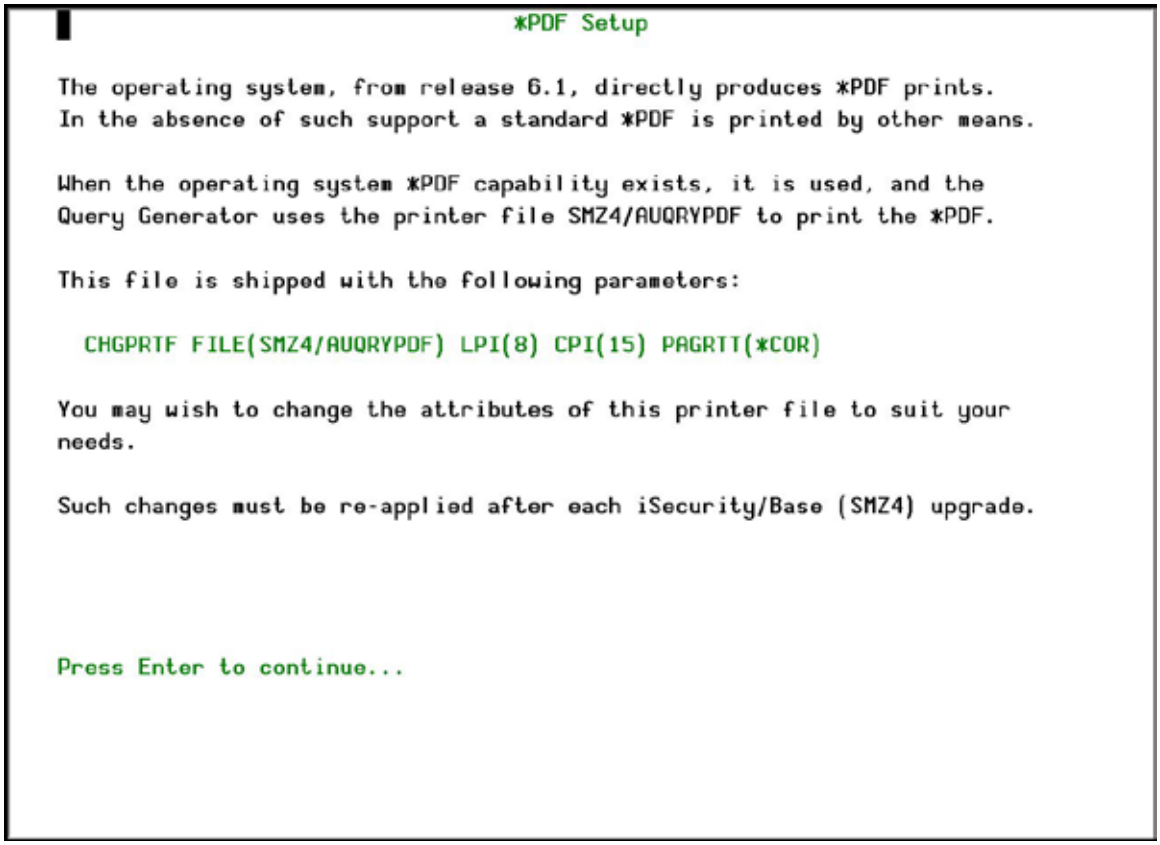
The operating system, from release 6.1, directly produces *PDF prints. In the absence of such support a standard *PDF is printed by other means.

To define PDF printers, perform the following steps:

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

Printer Files Setup

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



***PDF Setup**

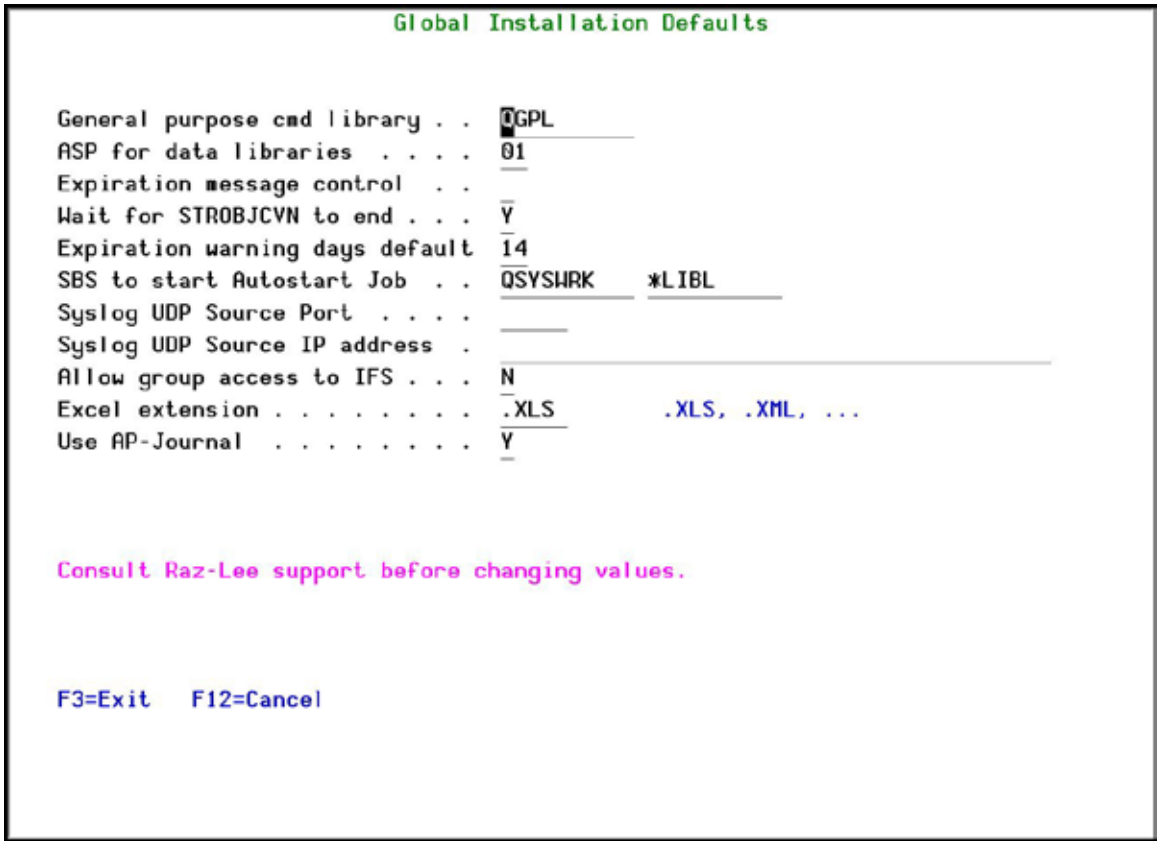
3. Follow the instructions on the screen.

Note: You must re-perform this task after every upgrade of **Capture**.

Global Installation Defaults

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.
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 APJournal, other libraries are created. For example, in the AP-Journal a library is created per application. When created you are prompted with the CRTLIB (Create Library) so that you can set the ASP number. · Change the current ASP of the library. All future upgrades will use this ASP. · •All products will try to preserve the current ASP at upgrade time. Due to its sensitivity, you should check it.
Expiration message control	**Y**=Yes **N**=No

Parameter	Description
Wait for STROBJCVN to end	**Y**=Yes **N**=No When installing the product on an OS400 version which is not the one that it was created for, objects require conversion and this is normally done in a batch job sent to work parallel to the installation. If you want the conversion 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	
Allow group access to IFS	**Y**=Yes **N**=No Allow access to IFS from group profiles.
Excel extension	
Use AP-Journal	

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

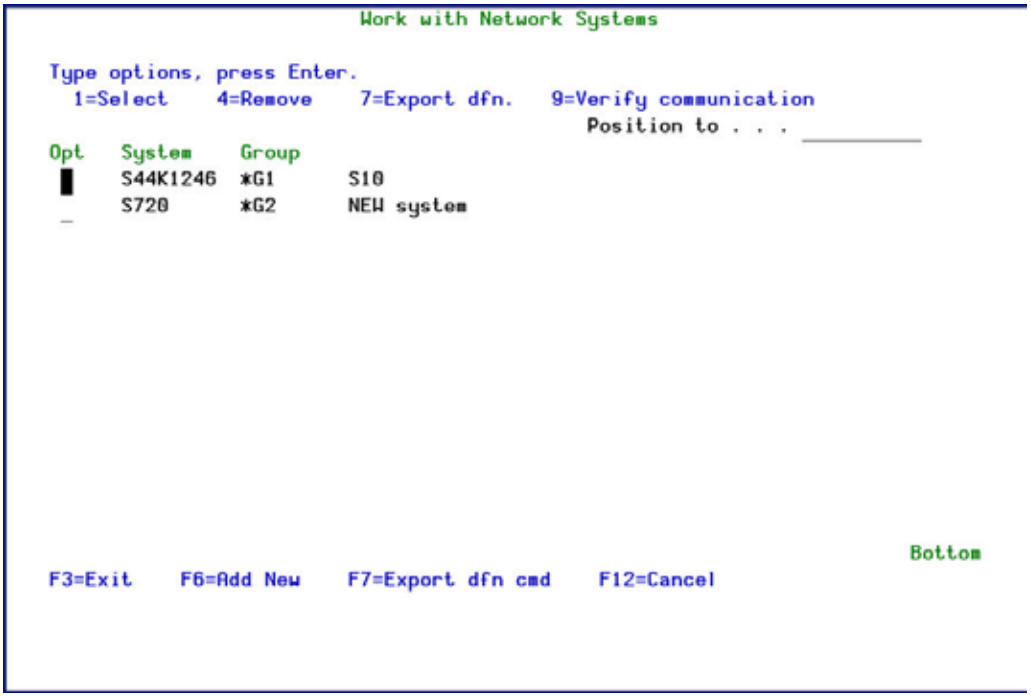
NOTE: You should not change any of the values in this screen without first consulting with Raz-Lee support staff at support@razlee.com.

Network Support

Work with network definitions

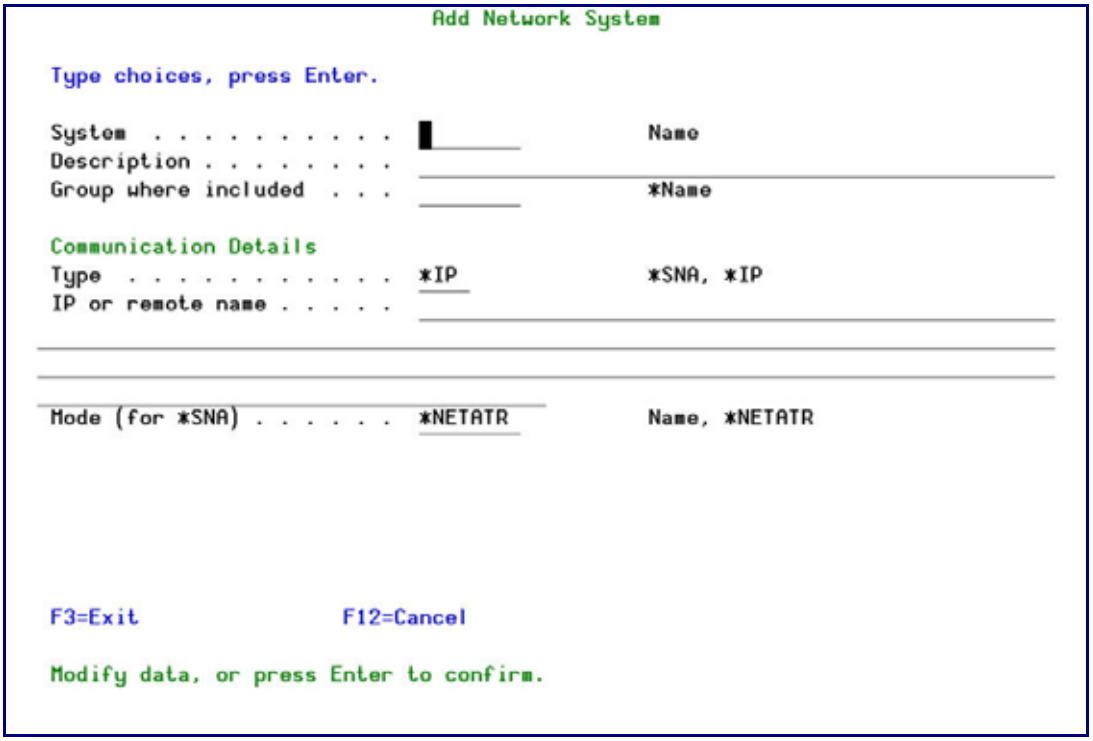
To get current information from existing report or query. Adjusting the system parameters only, to collect information from all the groups in the system to output files that can be sent via email.

1. Select **71. Work with network definitions** from the **BASE Support** menu. The **Work with Network Systems** screen appears.



Work with Network Systems

2. Press **F6** to define a new network system to work with and press **Enter** to confirm.



Add Network System

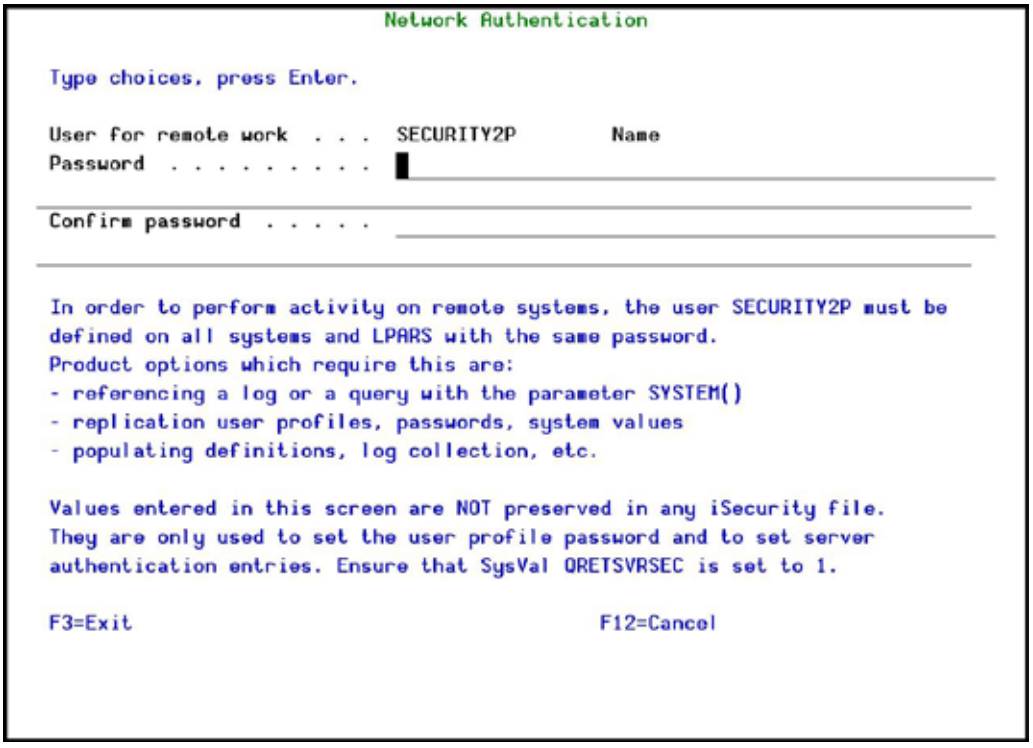
Parameter	Description
System	The name of the system
Description	A meaningful description of the system
Group where included	Enter the name of the group to which the system is assigned
Where is QAUDJRN analyzed	Give the name of the System where QAUDJRN is analyzed. Enter ***SYSTEM** if it is analyzed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

Network Authentication

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.

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



Work with Network Systems

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

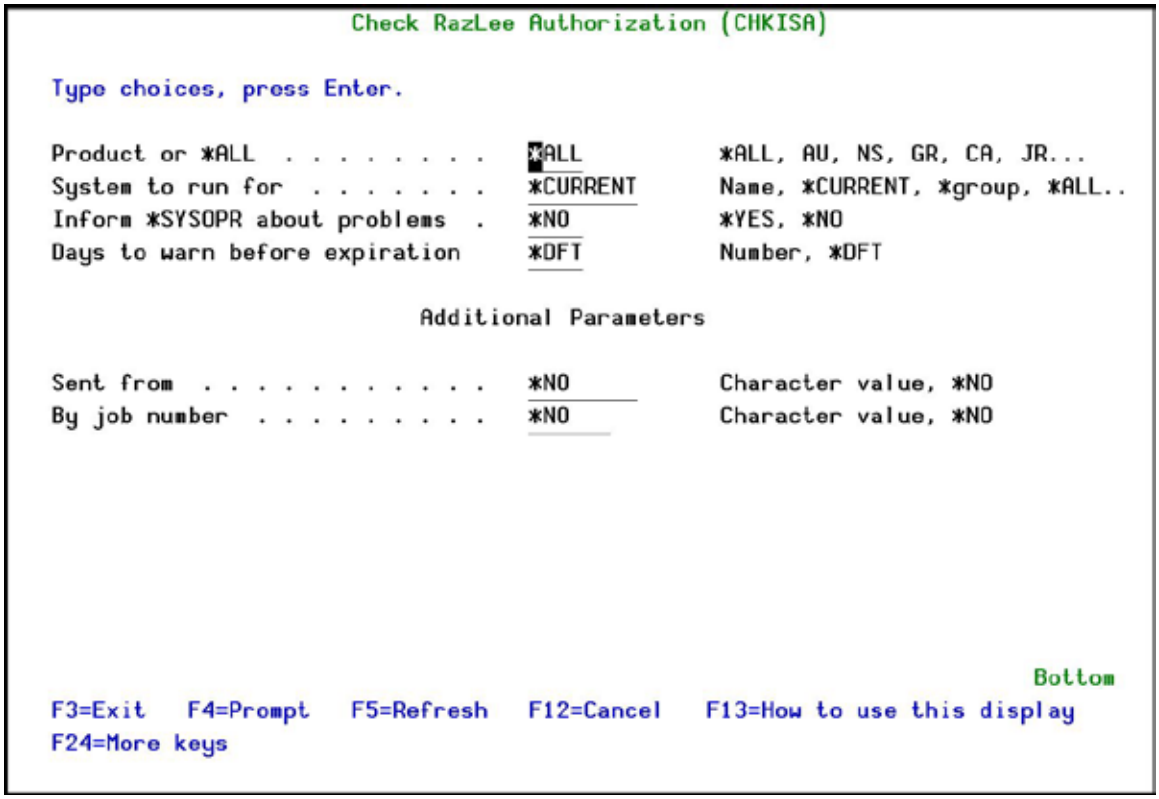
Check Authorization Status

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 Network Scripts* on page ***Error! Bookmark not defined.*** for more details.

1. Select **73. Check Network Authority Status** from the **BASE Support** menu.

   The **Check Razlee Authorization** screen appears.



Check Razlee Authorization

Parameters or Options	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
System to run for	**Name** = The name of the library where you want to transfer the Journal receiver ***Same** = The library where the current Journal Receiver is found
Inform *SYSOPR about problem	***YES** = ***NO** =
Days to warn before expiration	**Number** = Any system whose expiry date is less than this number of days will be reported. The default number of days is 14. ***DFT**
Sent from	Value ***NO**
By job number	Value ***NO**

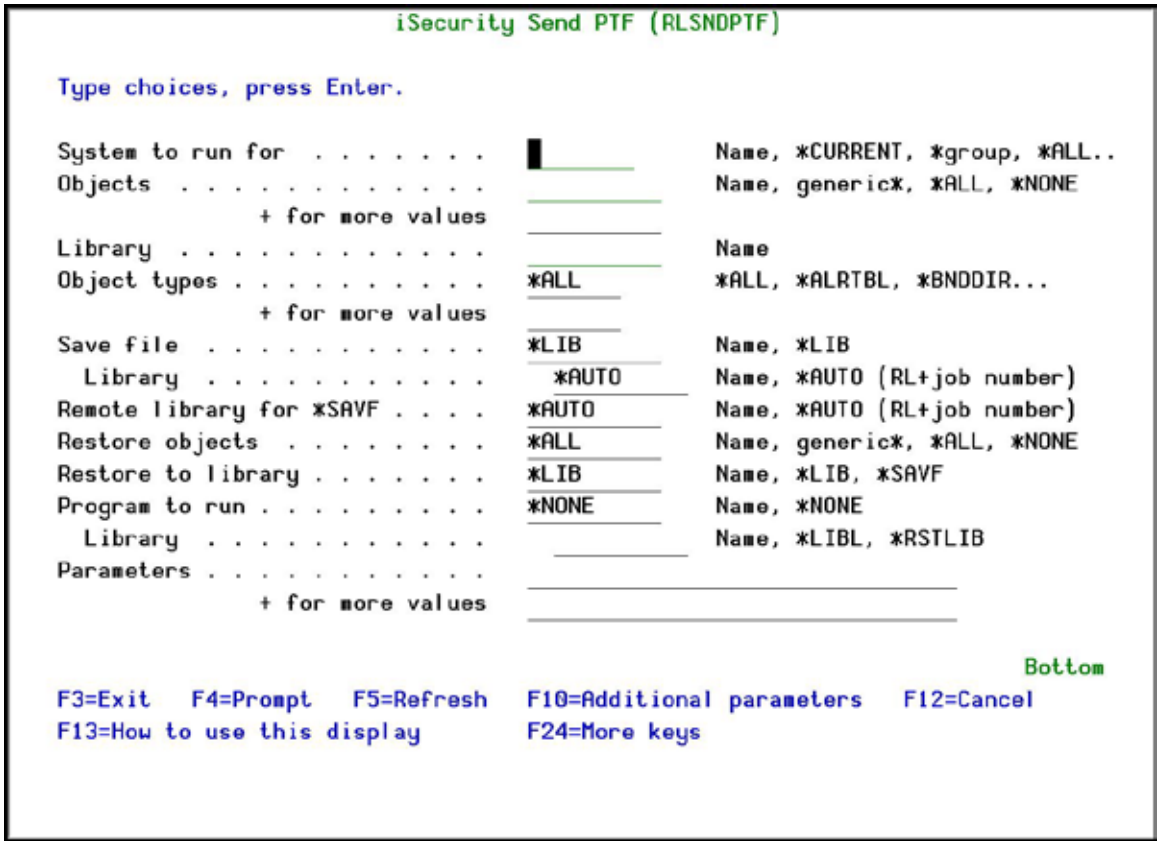
2. Select the correct options and press **Enter**.

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 *Network Definitions* on page ***Error! Bookmark not defined.***, and that you define user SECURITY2P on all nodes, using the same password, as described in *Network Authentication* on page ***Error! Bookmark not defined.***.

1. Select **74. Send PTF** from the **BASE Support** menu. The **iSecurity Send PTF (RLSNDPTF)** screen appears.



iSecurity Send PTF

Parameter	Description
System to run for	**Name** = The specific name of the system ***CURRENT** = The current system ***group** = All systems in the group ***ALL** = All systems on the network
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>

Parameter	Description
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. Select the correct 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 Network Authority Status* on page ***Error! Bookmark not defined.***.

Before you can use this option, ensure that you define the entire network, as described in *Network Definitions* on page ***Error! Bookmark not defined.***, and that you define user SECURITY2P on all nodes, using the same password, as described in *Network Authentication* on page ***Error! Bookmark not defined.***.

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

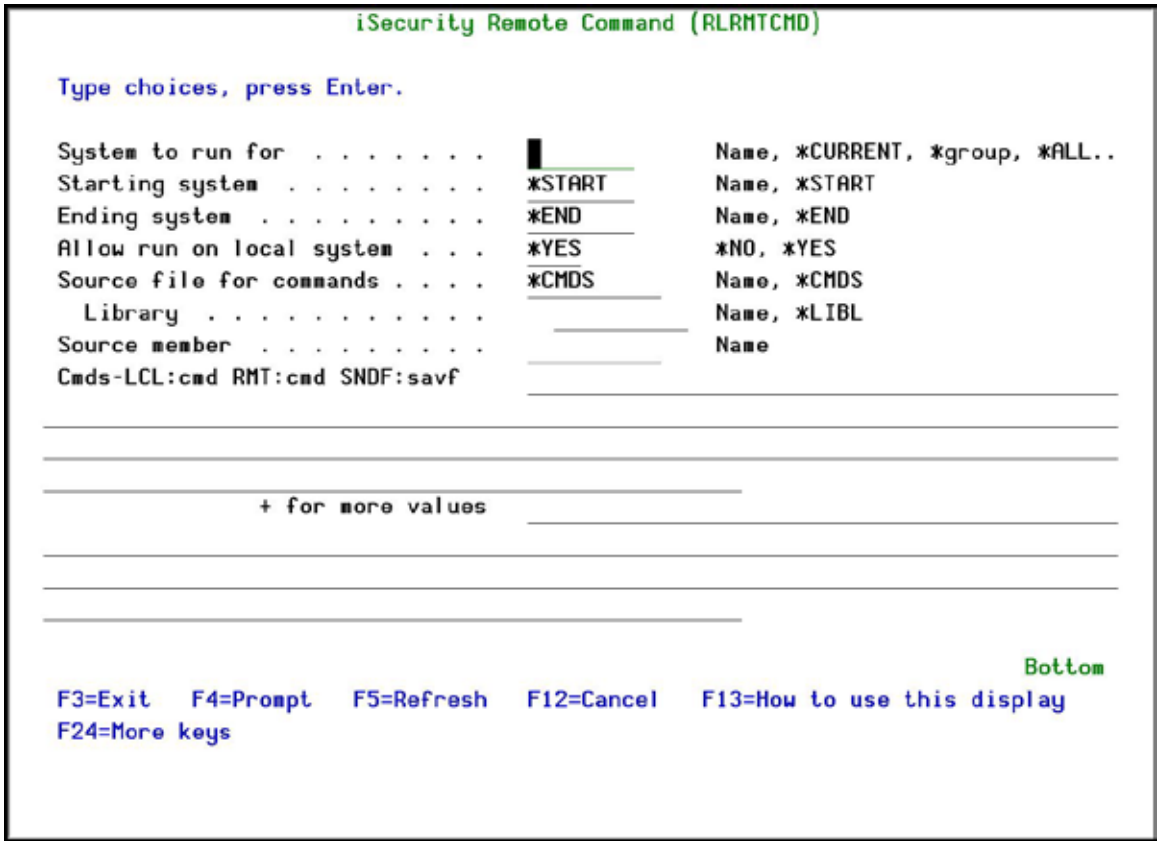


Figure 1: iSecurity Remote Command

Parameter	Description
System to run for	**Name** = The specific name of the system ***CURRENT** = The current system ***group** = All systems in the group ***ALL** = All systems on 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
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 previously failed
Allow run on local system	***YES** = The remote command can run on the local system ***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

Parameter	Description
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. Select the correct options and press **Enter**.

Current Job Central Administration Messages

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

All Jobs Central Administration Messages

Select **77. All Jobs CntAdm Messages** from the **BASE Support** menu to display the job log for all jobs.