iSecurity Action

User Guide
Version 13

www.razlee.com

Contents

-

-

About this Manual

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

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

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

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

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

Intended Audience

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

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

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

Conventions Used in the Document

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

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on page 7.

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRACT **> 81 > 32**

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

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

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

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

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

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

Contacts

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

Chapter 1: Introducing Action

Overview

In today's business environment, it is no longer sufficient to discover a security problem after it occurs. **Action's** purpose is to neutralize security events or cross-purpose events which appear to the system to be suspicious. This includes blocking or suspending users, application suspension and re-activation, termination of user sessions, warnings and notifications and Real-time alerts.

Action enables your business processes to tune in to every-day activities and take corrective action before security breaches occur. **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**.

This Chapter includes the following sub-sections:

- Real-Time Detection
- Rules
- Actions
- History Log
- User Absence Security
- Inactive User Security
- Control Adopted Authority
- Working with Active Users

NOTE: **Action** has a cross purpose mission in and amongst other Razlee known products.

Real-Time Detection

Real-time detection is governed by a series of user-defined rules and actions. Rules identify which specific events will trigger actions and under what conditions a response should occur. Actions define the specific responsive actions that take place whenever rule conditions are met.

Action real-time detection constantly monitors and also takes action, for a wide variety of security and system related events, including:

- Real-time auditing rules: Events detected by **Audit**
- Network security rules: Transactions rejected by **Firewall**
- Terminal screens locked/released: Jobs terminated by **Screen**
- Monitoring Statuses: System Active jobs, Current System and Memory pool

Rules

Rules determine which conditions trigger actions. For example, you can create a rule that triggers a message whenever the user *JOHN* modifies a ***FILE** object, located in the *ACCOUNTING* folder, on or after **`05-January-2021`**.

Rules, such as the above example, are based on one or more filter conditions. Conditions are based on a variety of criteria such as, “equal to/not equal to”, “greater/less than”, “included/not included in list”, “like” and “starts with”. In addition, multiple conditions may be combined using Boolean “and/or” conditions.

Action incorporates a user-friendly Rule Wizard to assist you in defining complex conditions.

Actions

An action may consist of alert messages sent to designated personnel and/or command scripts that run automatically. You can send alert messages via e-mail, IBM i (OS/400) system messaging, network, SMS, or pagers.

Action command scripts may include multiple statements that execute IBM i commands or run programs. Conditional branching on error conditions is fully supported.

History Log

Action maintains a history log of all actions performed. This log provides a complete audit trail for later review and follow-up. You may display or print the contents of this log using a variety of powerful filter criteria.

User Absence Security

Action includes security features that limit user signon to specific days and times. This tool is useful for restricting signon to established working hours and for ensuring that users cannot signon during scheduled absences, such as holidays, vacations, sick leave, and so on.

Inactive User Security

One of the most common tricks that hackers use is to discover user names and passwords for users who use the system infrequently or have left the organization. **Action** enables you to disable such users automatically.

Control Adopted Authority

Allowing users to run programs that adopt authority is an intentional loss of control. Programs using adopted authority grant users permission to perform actions, access objects and use special authorities, such as ***ALLOBJ***, which the original user would not ordinarily have.

Action enables you to control which users can create programs that grant adopted authority. Also included are tools that provide an effective audit trail over the creation and use of such programs.

Working with Active Users

Action includes a convenient tool that enables you to view and modify various security-related user profile parameters, such as:

- Enable/Disable users
- Resetting the counter for invalid signon attempts to prevent automatic disabling
- Set user passwords to ‘expire’

Native IBM i (OS/400) User Interface

Action is designed from the ground up to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard System i CUA conventions. All product features are available via the menus, so **no** command memorization required. Some features are also accessible via the command line, for the convenience of experienced users.

Menus

Product menus enable easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products.

To select a menu option, simply type the option number and press **Enter**.

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

Commands

Many **Action** features are accessible from any command line simply by typing the appropriate commands. Some of the most commonly used commands appear below.

- Display action log (***DSPACLOG***)
- Print user profile information report (***PRTAUUSRP***)
- Print adopted authority reports (***AUPRTADP***)

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following table describes the various data entry screen options:

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

Function Keys

The following function keys may appear on data entry screens:

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

Chapter 2: Getting Started

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

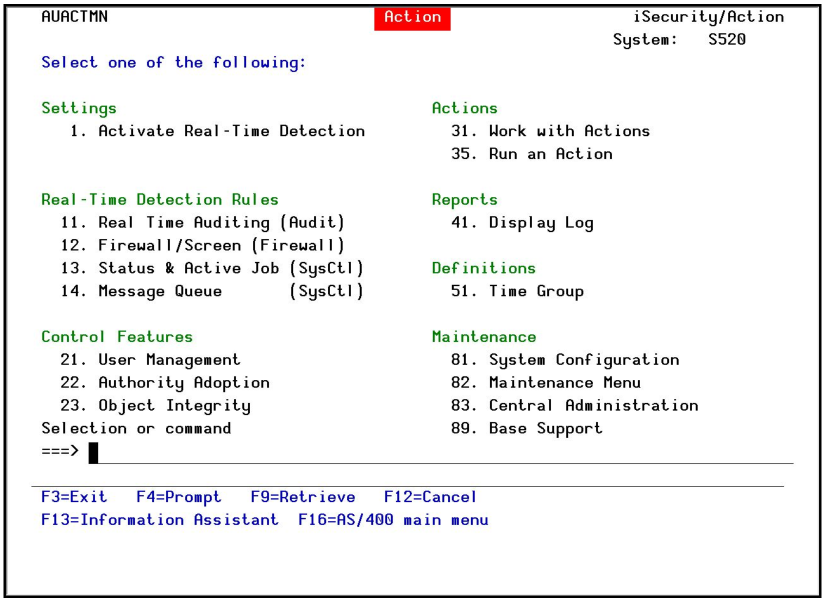
Obtaining Your Authorization Code

A valid product authorization code is required to run this product. Please contact your authorized Raz-Lee distributor or reseller to receive the proper code. If you are evaluating the product, you will receive a temporary authorization code valid for 30 days. If you have purchased a license, you will receive a permanent authorization code that is specific to the serial number and model of the computer on which it is installed. If you upgrade your System i hardware, or purchase a more recent version of the product, you must request a new authorization code.

Starting Action for the First Time

Users must have ****AUDIT*** special authority to use this product. An additional product password may also be required to access certain functions. The default product password is ***QSECOFR***. We recommend changing this password as soon as possible.

To start **Action**, type the ***STRACT*** command in the command line, and then ***ENTER.*** The **Action** Main menu appears.



```
AUACTMN                               Action                 iSecurity/Action
                                                             System:    S520
Select one of the following:

Settings                                    Actions
   1. Activate Real-Time Detection            31. Work with Actions
                                              35. Run an Action

Real-Time Detection Rules                   Reports
  11. Real Time Auditing (Audit)              41. Display Log
  12. Firewall/Screen (Firewall)
  13. Status & Active Job (SysCtl)          Definitions
  14. Message Queue       (SysCtl)            51. Time Group

Control Features                            Maintenance
  21. User Management                         81. System Configuration
  22. Authority Adoption                      82. Maintenance Menu
  23. Object Integrity                        83. Central Administration
Selection or command                          89. Base Support
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 1: Action Main Menu

System Configuration

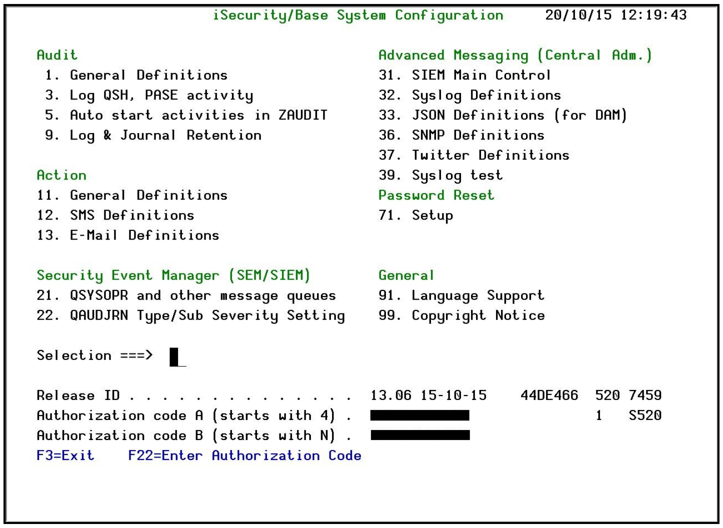
Action is ready-to-run right out of the box. You should review and modify certain system configuration parameters that control important features prior to using the product for the first time.

It should be pointed out that there is no “typical” or “optimal” configuration for a security product such as **Action**. Each installation or application has different operational criteria and security needs. The security requirements for a large manufacturing environment are quite different from those for a bank, a software developer or a service organization.

This section discusses the following configuration settings:

- Entering authorization code
- Enabling real-time detection (**Audit**, **Firewall**, **Screen**, Active jobs and system status)
- iSecurity password
- SMS messaging
- E-Mail definitions
- Pager (Beeper) interface

1. To work with **Action**, type **`STRACT`**,
   -Or-
   `STRAUD > 69 > 2`
   -Or-
   `STRFW > 49 > 2`. The **`Action`** Main menu appears.
2. Select **`81. System Configuration`**. The iSecurity/Base System Configuration screen appears.



```
                      iSecurity/Base System Configuration     20/10/15 12:19:43

 Audit                                     Advanced Messaging (Central Adm.)
  1. General Definitions                   31. SIEM Main Control
  3. Log QSH, PASE activity                32. Syslog Definitions
  5. Auto start activities in ZAUDIT       33. JSON Definitions (for DAM)
  9. Log & Journal Retention               36. SNMP Definitions
                                           37. Twitter Definitions
 Action                                    39. Syslog test
 11. General Definitions                   Password Reset
 12. SMS Definitions                       71. Setup
 13. E-Mail Definitions

 Security Event Manager (SEM/SIEM)         General
 21. QSYSOPR and other message queues      91. Language Support
 22. QAUDJRN Type/Sub Severity Setting     99. Copyright Notice

 Selection ===>

 Release ID . . . . . . . . . . . . . .  13.06 15-10-15    44DE466  520 7459
 Authorization code A (starts with 4) .  [redacted]                  1   S520
 Authorization code B (starts with N) .  [redacted]
 F3=Exit    F22=Enter Authorization Code
```

Figure 2: iSecurity/Base System Configuration

3. Continue to the following options. After you modify any of the parameters accessible from this menu, the message “Modify data, or press Enter” appears upon return to the menu.
4. You must press **Enter** again to save your changes and leave this menu. If you press **F3**, you will lose any changes that you have made.

Entering your Authorization Code

If you did not enter your authorization code during the installation process, do so now. Perform the following steps.

1. Select **`81 >F22=Enter Authorization Code`**.
2. Enter your computer serial number and authorization code in the spaces provided. Press **`Enter`** to continue.

NOTE: If you enter an incorrect code, you will receive an error message when you attempt to access product features. If this occurs, simply repeat the above procedure to enter the correct code.

Modifying Operators' Authorities

The Operators' authority management is now maintained from one place for the entire **iSecurity** on all its modules.

There are three default groups:

- ***AUD#SECAD**- All users with both ***AUDIT** and ***SECADM** special authorities. By default, this group has full access (Read and Write) to all **iSecurity** components.
- ***AUDIT** - All users with ***AUDIT** special authority. By default, this group has only Read authority to **Audit**.
- ***SECADM**- All users with ***SECADM** special authority- By default, this group has only Read authority to **Firewall**.

iSecurity related objects are secured automatically by product authorization lists (named **security1P**). This strengthens the internal security of the product. It is essential that you use **Work with Operators** to define all users who have ***SECADM**, ***AUDIT** or ***AUD#SECAD** privileges, but do not have all object authority. The **Work with Operators** screen has Usr (user management) and Adm for all activities related to starting, stopping subsystems, jobs, import/export and so on. **iSecurity** automatically adds all users listed in **Work with Operators** to the appropriate product authorization list.

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

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

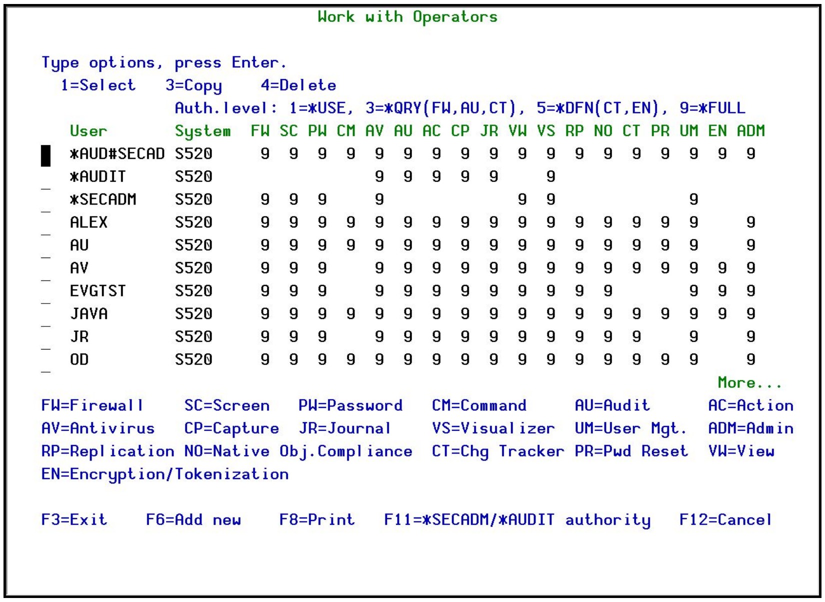
If your organization wants the default to be *BLANK, then the following command must be used:
CRTDTAARA SMZTMPC/DFTPWD *char 10

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

NOTE: When installing **iSecurity** for the first time, certain user(s) might not have access according to the new authority method. Therefore, the first step you need to take after installing is to edit those authorities.

To modify operators' authorities:

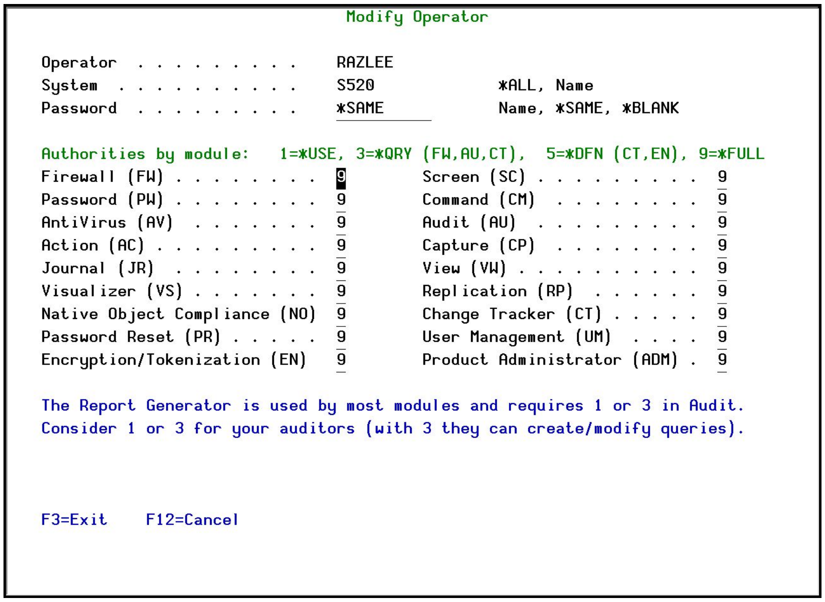
1. Select **89 > 11. Work with Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



```
                           Work with Operators

 Type options, press Enter.
   1=Select   3=Copy    4=Delete
              Auth.level: 1=*USE, 3=*QRY(FW,AU,CT), 5=*DFN(CT,EN), 9=*FULL
  User       System   FW SC PW CM AV AU AC CP JR VW VS RP NO CT PR UM EN ADM
_ *AUD#SECAD S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_ *AUDIT     S520                 9  9  9  9  9     9
_ *SECADM    S520     9  9  9     9              9  9              9
_ ALEX       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_ AU         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
_ AV         S520     9  9  9     9  9  9  9  9  9  9  9  9  9  9  9  9  9
_ EVGTST     S520     9  9  9     9  9  9  9  9  9  9  9  9        9  9  9
_ JAVA       S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_ JR         S520     9  9  9     9  9  9  9  9  9  9  9  9  9     9     9
_ OD         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9     9
                                                                      More...
 FW=Firewall    SC=Screen    PW=Password   CM=Command     AU=Audit      AC=Action
 AV=Antivirus   CP=Capture   JR=Journal    VS=Visualizer  UM=User Mgt.  ADM=Admin
 RP=Replication NO=Native Obj.Compliance   CT=Chg Tracker PR=Pwd Reset  VW=View
 EN=Encryption/Tokenization

 F3=Exit    F6=Add new    F8=Print    F11=*SECADM/*AUDIT authority    F12=Cancel
```

Figure 3: Work with Operators

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



```
                             Modify Operator

 Operator  . . . . . . . . .  RAZLEE
 System  . . . . . . . . . .  S520              *ALL, Name
 Password  . . . . . . . . .  *SAME             Name, *SAME, *BLANK

 Authorities by module:   1=*USE, 3=*QRY (FW,AU,CT),  5=*DFN (CT,EN), 9=*FULL
 Firewall (FW) . . . . . . .  9         Screen (SC) . . . . . . . . .  9
 Password (PW) . . . . . . .  9         Command (CM)  . . . . . . . .  9
 AntiVirus (AV)  . . . . . .  9         Audit (AU)  . . . . . . . . .  9
 Action (AC) . . . . . . . .  9         Capture (CP)  . . . . . . . .  9
 Journal (JR)  . . . . . . .  9         View (VW) . . . . . . . . . .  9
 Visualizer (VS) . . . . . .  9         Replication (RP)  . . . . . .  9
 Native Object Compliance (NO)  9       Change Tracker (CT) . . . . .  9
 Password Reset (PR) . . . . .  9       User Management (UM)  . . . .  9
 Encryption/Tokenization (EN)  9        Product Administrator (ADM) .  9

 The Report Generator is used by most modules and requires 1 or 3 in Audit.
 Consider 1 or 3 for your auditors (with 3 they can create/modify queries).



 F3=Exit    F12=Cancel
```

Figure 4: Modify Operator

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

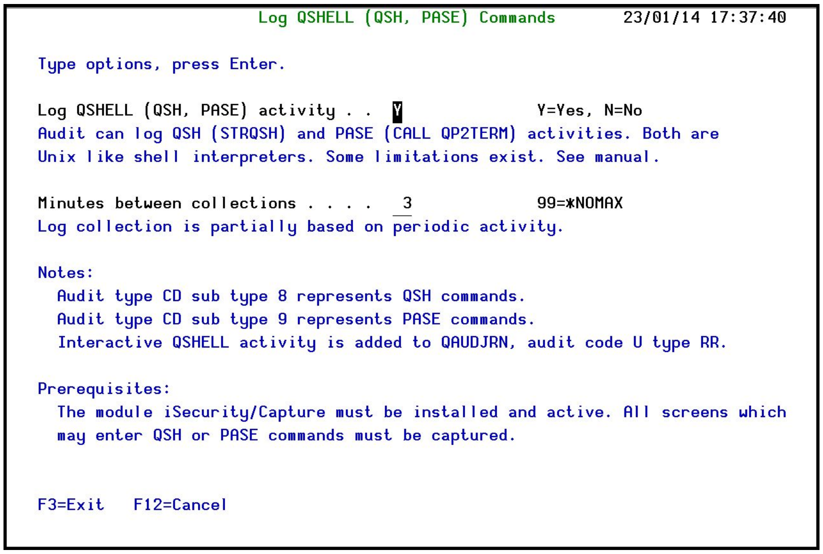
Most modules use the Report Generator which requires access to the Audit module. For all users who will use the Report Generator, you should define their access to the Audit module as either 1 or 3. Option 1 should be used for users who will only be running queries. Use option 3 for all users who will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

3. Set authorities and press **Enter**. A message is prompted informing 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.

Log QSH, PASE activity

To be able to log QSH and PASE activity, the iSecurity **Capture** module must be installed and active. Capture all screens that can enter QSH or PASE commands.

1. Select `81 > 3`. `Log QSH, PASE activity` in the iSecurity/Base System Configuration menu. The Log QSHELL (QSH, PASE) Commands screen appears.



```
                          Log QSHELL (QSH, PASE) Commands       23/01/14 17:37:40

   Type options, press Enter.

   Log QSHELL (QSH, PASE) activity . .  Y               Y=Yes, N=No
   Audit can log QSH (STRQSH) and PASE (CALL QP2TERM) activities. Both are
   Unix like shell interpreters. Some limitations exist. See manual.

   Minutes between collections . . . .   3              99=*NOMAX
   Log collection is partially based on periodic activity.

   Notes:
     Audit type CD sub type 8 represents QSH commands.
     Audit type CD sub type 9 represents PASE commands.
     Interactive QSHELL activity is added to QAUDJRN, audit code U type RR.

   Prerequisites:
     The module iSecurity/Capture must be installed and active. All screens which
     may enter QSH or PASE commands must be captured.


   F3=Exit   F12=Cancel
```

Figure 5: Log QSHELL (QSH, PASE) Commands

Parameter	Description
Log QSHELL (QSH, PASE) activity	**Y** = Yes **N** = No Audit can log QSH (STRQSH) and PASE (CALL QP2TERM) activities. Both are UNIX like shell interpreters.
Minutes between collections	01 – 99. 99 = *NOMAX Log collection is partially based on periodic activity.

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

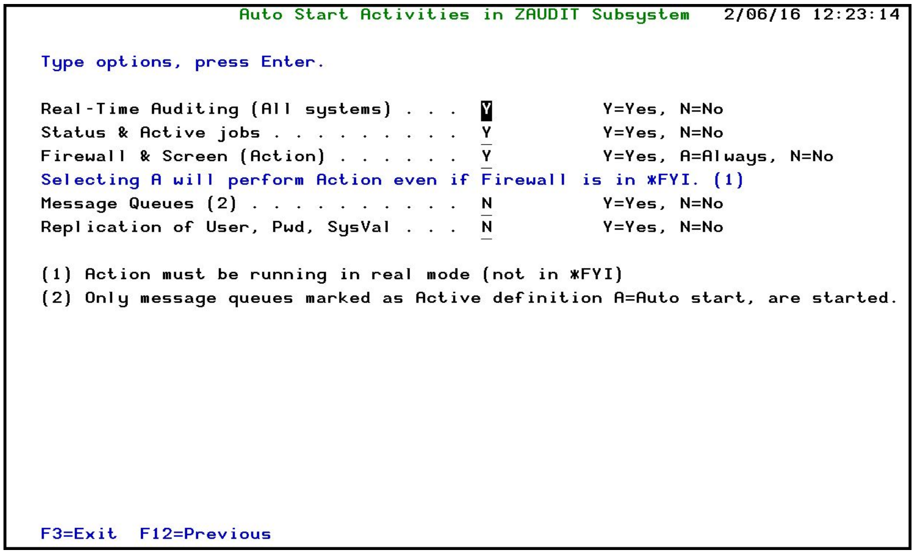
NOTE Audit type CD sub type 8 represents QSH commands. Audit type CD sub type 9 represents PASE commands. Interactive QSHELL activity is added to QAUDJRN, audit code U type RR.

Enabling Real-Time Detection

In order for **Action** to send alert messages and run command scripts, you must enable real-time detection and to specify several parameters. In addition, you must also enable real-time detection in the **Audit**, **Firewall** and **Screen** applications.

To work with these parameters:

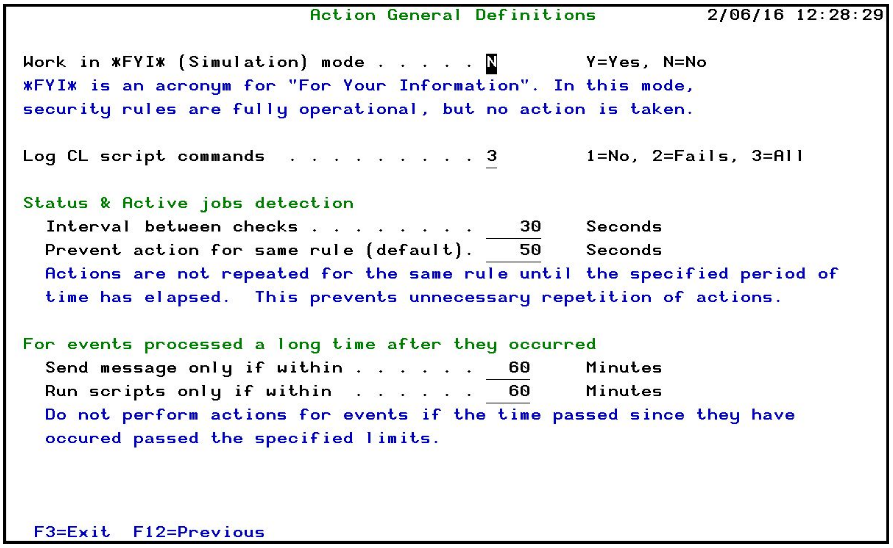
1. Select `81 > 5. Auto start activities in ZAUDIT` from the **`iSecurity/Base System Configuration`** screen. The **`Auto Start Activities in ZAUDIT Subsystem`** screen appears.



```
                    Auto Start Activities in ZAUDIT Subsystem   2/06/16 12:23:14

 Type options, press Enter.

 Real-Time Auditing (All systems) . . .  Y          Y=Yes, N=No
 Status & Active jobs . . . . . . . . .  Y          Y=Yes, N=No
 Firewall & Screen (Action) . . . . . .  Y          Y=Yes, A=Always, N=No
 Selecting A will perform Action even if Firewall is in *FYI. (1)
 Message Queues (2) . . . . . . . . . .  N          Y=Yes, N=No
 Replication of User, Pwd, SysVal . . .  N          Y=Yes, N=No

 (1) Action must be running in real mode (not in *FYI)
 (2) Only message queues marked as Active definition A=Auto start, are started.








 F3=Exit  F12=Previous
```

Figure 6: Auto start activities in ZAUDIT subsystem

2. Type '**`Y`**' to automatically start system activities after the activation of subsystem ZAUDIT (as shown above) and press **`Enter`**. You are returned to the **`iSecurity/Base System Configuration`** menu.
3. Select **`11. General Definitions`** from the **`iSecurity/Base System Configuration`** menu. The **`Action General Definitions`** screen appears.



```
                          Action General Definitions          2/06/16 12:28:29

 Work in *FYI* (Simulation) mode . . . . . N        Y=Yes, N=No
 *FYI* is an acronym for "For Your Information". In this mode,
 security rules are fully operational, but no action is taken.

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

 Status & Active jobs detection
   Interval between checks . . . . . . . .   30     Seconds
   Prevent action for same rule (default).   50     Seconds
   Actions are not repeated for the same rule until the specified period of
   time has elapsed.  This prevents unnecessary repetition of actions.

 For events processed a long time after they occurred
   Send message only if within . . . . . .  60      Minutes
   Run scripts only if within  . . . . . .  60      Minutes
   Do not perform actions for events if the time passed since they have
   occured passed the specified limits.



  F3=Exit  F12=Previous
```

Figure 7: Action General Definitions

Parameter or Option	Description
Work in *FYI* (Simulation) mode	**Y**=Yes **N**=No
Log CL script commands	1=No - Do not log any CL commands 2=Fails – Only log CL commands that fail 3=All – Log all CL commands
Status & Active jobs detection:	
Interval Between Checks	Delay interval in seconds between consecutive checks of system status and active job status (Default=60) (similar to pressing F5=refresh for WRKSYSSTS, WRKACTJOB, WRKSHRPOOL)
Prevent Action for Same Rule (default)	Delay interval prior to an action for the same rule
For events processed a long time after they occurred:	
Send message only if within	**Minutes** = Send messages if Maximum delay (in minutes) between the occurrence of an event and performance of the action is equal to this amount of minutes. Action examines the journals for events that have occurred in the past, but were not detected in real-time. This situation can occur if real- time detection was temporarily disabled. Actions are normally triggered retroactively in such cases. This parameter prevents retroactive triggering of events older than the specified number of minutes.
Run Scripts Only if Within	**Minutes** = Run scripts if the maximum delay between the event and the action is equal to this amount of minutes.

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

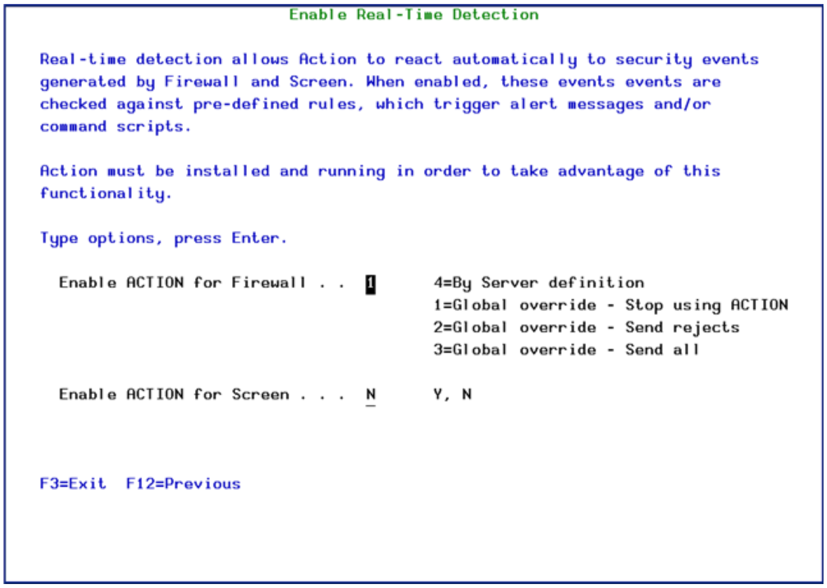
Enabling Real-Time Detection in Audit

1. To enable real-time detection in Audit, that module must be installed. If not, see your Raz-Lee distributor.
2. Select **`2. Activation`** from the Audit main menu. The **`Activation`** menu appears.
3. Select **`1. Activate ZAUDIT subsystem`** from the **`Activation`** menu. Audit starts to work.

Enabling Real-Time Detection in Firewall & Screen

To enable real-time detection in **Firewall** and **Screen**, these modules must be installed. See your Raz-Lee distributor for more information.

1. Select **81** from the **Firewall** or **Screen** Main menu. The **iSecurity (part I) Global Parameters** screen appears.
2. Select **7. Enable ACTION (CL Script + more)** from the **iSecurity (part I) Global Parameters** menu. The **Enable Real-Time Detection Screen** appears.



```
                          Enable Real-Time Detection

 Real-time detection allows Action to react automatically to security events
 generated by Firewall and Screen. When enabled, these events events are
 checked against pre-defined rules, which trigger alert messages and/or
 command scripts.

 Action must be installed and running in order to take advantage of this
 functionality.

 Type options, press Enter.

   Enable ACTION for Firewall . .  1      4=By Server definition
                                          1=Global override - Stop using ACTION
                                          2=Global override - Send rejects
                                          3=Global override - Send all

   Enable ACTION for Screen . . .  N      Y, N



 F3=Exit  F12=Previous
```

Figure 8: Enable Real-Time Detection

3. Enter **4** to enable real-time detection for **Firewall** by the server definitions.

Message Queue

This new unique solution enables real-time auditing on message queues. Users have the option to:

- Modify rules according to all the message queue parameters
- Respond to the message by alerting the user (emails, SMS) and by reacting to it directly (send auto response).

Each message queue is classified to a group ID. This helps distinguish between ***QSECOFR*** and other standard users.

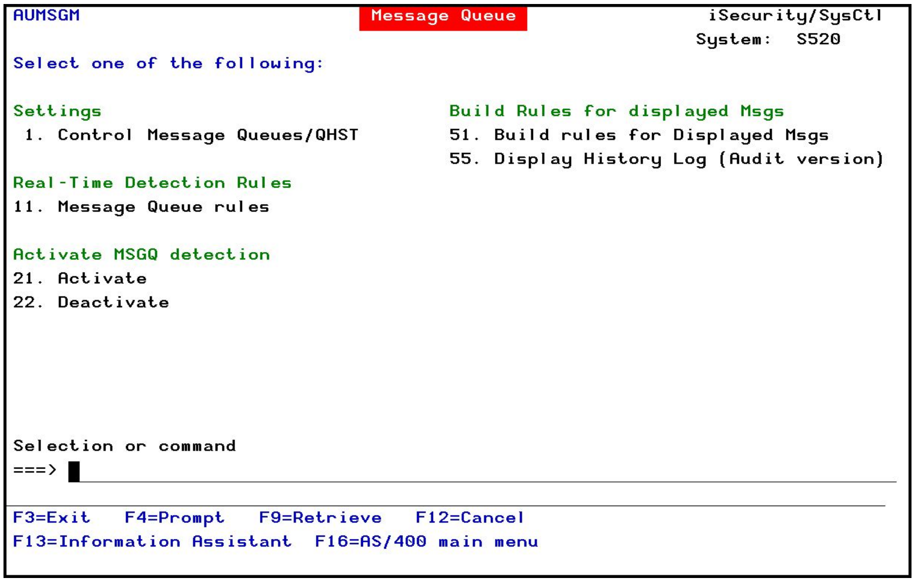
Working with Message Queues

This unique solution enables real-time auditing on message queues. Users have the option to:

- Modify rules according to all the message queue parameters
- Respond to the message by alerting the user (emails, SMS) and by reacting to it directly (send auto response).

To work with message queues:

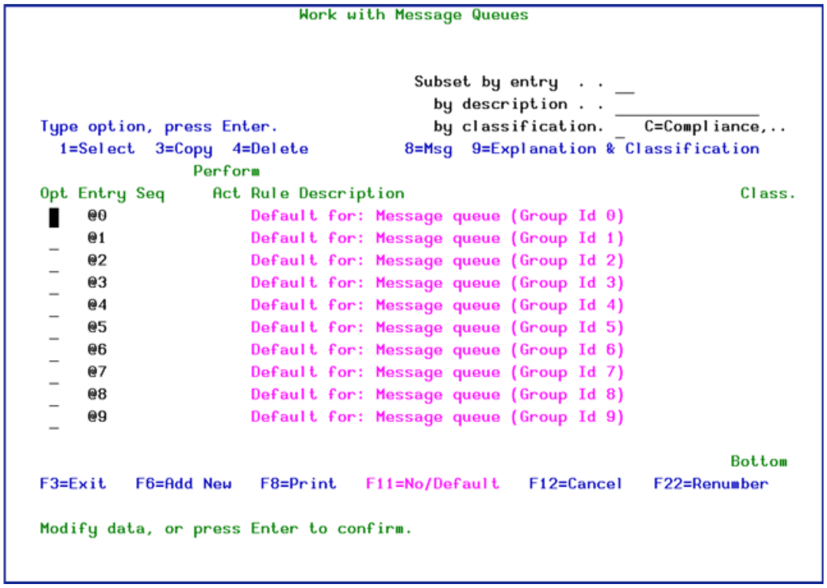
1. Select **14. Message Queue (SysCtl)** from the Action Main menu. The **Message Queues** menu appears.



```
AUMSGM                         Message Queue                iSecurity/SysCtl
                                                              System:   S520
Select one of the following:

Settings                                Build Rules for displayed Msgs
 1. Control Message Queues/QHST         51. Build rules for Displayed Msgs
                                        55. Display History Log (Audit version)
Real-Time Detection Rules
11. Message Queue rules

Activate MSGQ detection
21. Activate
22. Deactivate




Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

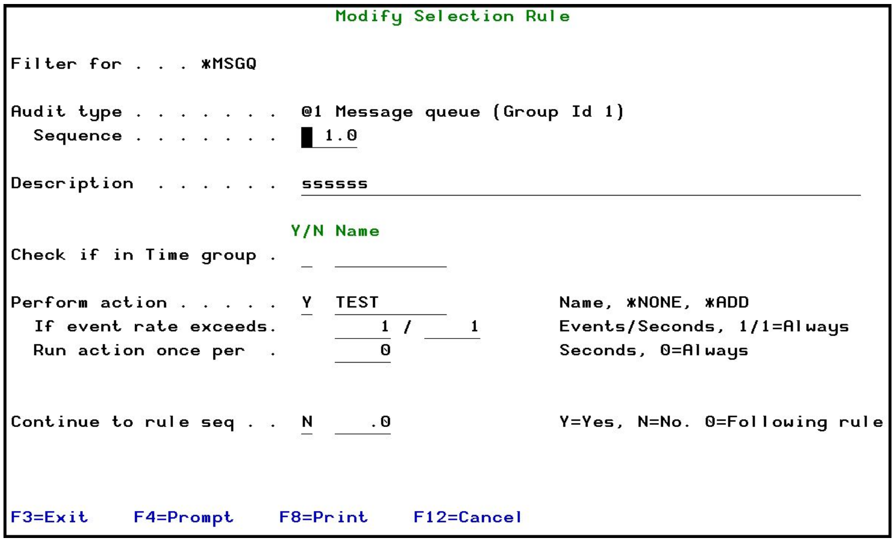
Figure 9: Message Queues

2. Select options **11. Message Queue rules**. The **Work with Message Queues** screen appears.
3. Type **1**=select to modify rules. A table of explanations follows the **Work with Message Queues** wizard, which comprises **Work with Message Queues** and **Modify Selection Rule**.



```
                          Work with Message Queues


                                            Subset by entry  . .  __
                                              by description . .  ____________
Type option, press Enter.                     by classification.  _  C=Compliance,..
  1=Select  3=Copy  4=Delete               8=Msg  9=Explanation & Classification
                Perform
Opt Entry Seq     Act Rule Description                                     Class.
 _    @0              Default for: Message queue (Group Id 0)
 _    @1              Default for: Message queue (Group Id 1)
 _    @2              Default for: Message queue (Group Id 2)
 _    @3              Default for: Message queue (Group Id 3)
 _    @4              Default for: Message queue (Group Id 4)
 _    @5              Default for: Message queue (Group Id 5)
 _    @6              Default for: Message queue (Group Id 6)
 _    @7              Default for: Message queue (Group Id 7)
 _    @8              Default for: Message queue (Group Id 8)
 _    @9              Default for: Message queue (Group Id 9)

                                                                        Bottom
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber

Modify data, or press Enter to confirm.
```

Figure 10: Work with Message Queues



```
                         Modify Selection Rule

Filter for . . . *MSGQ

Audit type . . . . . . .  @1 Message queue (Group Id 1)
  Sequence . . . . . . .   1.0

Description  . . . . . .  ssssss

                        Y/N Name
Check if in Time group .  _   __________

Perform action . . . . .  Y   TEST             Name, *NONE, *ADD
  If event rate exceeds.         1 /    1      Events/Seconds, 1/1=Always
  Run action once per  .         0             Seconds, 0=Always


Continue to rule seq . .  N      .0            Y=Yes, N=No. 0=Following rule



F3=Exit    F4=Prompt    F8=Print    F12=Cancel
```

Figure 11: Modify Selection Rule

Option	Description
Audit Type	Audit types are **@1-@9**. All choices have the same parameters. The ID numbers are only for organizational purposes.
Seq (Sequence)	The order in which the rule will be checked in this audit type (**1** = first rule checked, and so on).
Time Group	Find time group
Perform Action	**Y** = Perform this action according to rule **N** = Do not perform this action
Action	Optionally trigger this action **Name** = name of action to trigger by this rule **F4** = Select an action from the list **ADD** = Define a new action for this rule ***NONE** = No actions are triggered by this rule

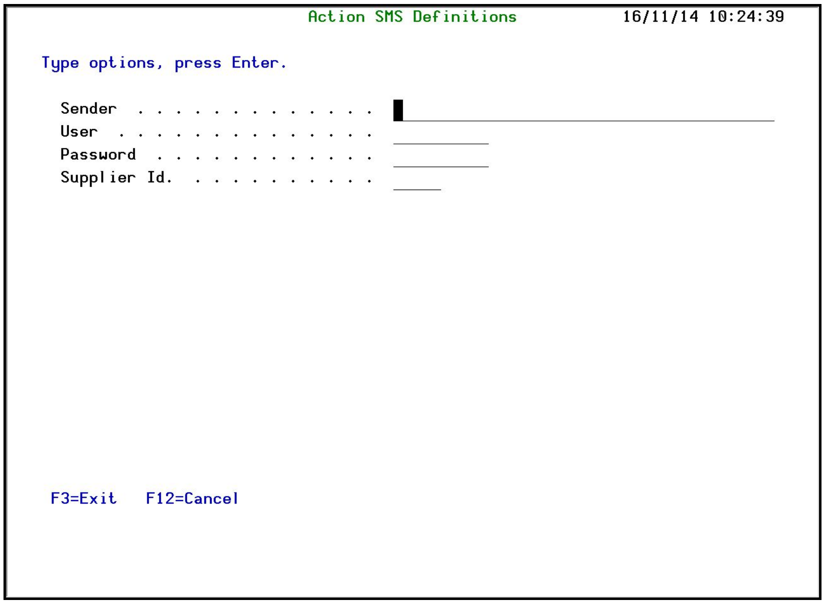
SMS Definitions

To send alert messages via SMS messaging, you must subscribe to a commercial SMS service. SMS service may be supplied by your cellular telephone provider or an independent service provider. Typically, SMS messages are sent to your supplier via the Internet, and the supplier then forwards the message to the recipient.

SMS messaging through **Action**, in addition to the following message types (pager and e-mail), does not require any special hardware. However, you may implement hardware if your system is not linked to the internet.

To work with SMS definitions:

1. Select **`81 > 12. SMS Definitions`** from the **`iSecurity/Base System Configuration`** menu. The **`Action SMS Definitions`** screen appears.



```
                         Action SMS Definitions          16/11/14 10:24:39

 Type options, press Enter.

   Sender  . . . . . . . . . . . . .  
   User  . . . . . . . . . . . . . .  
   Password  . . . . . . . . . . . .  
   Supplier Id. . . . . . . . . . .  

 F3=Exit   F12=Cancel
```

Figure 12: Action SMS Definitions

Parameter or Option	Description
`Sender`	
`User`	User ID provided by your SMS supplier
`Password`	Password provided by your SMS supplier
`Supplier ID`	Internet URL of your SMS supplier (for example, sms.supplier.com)

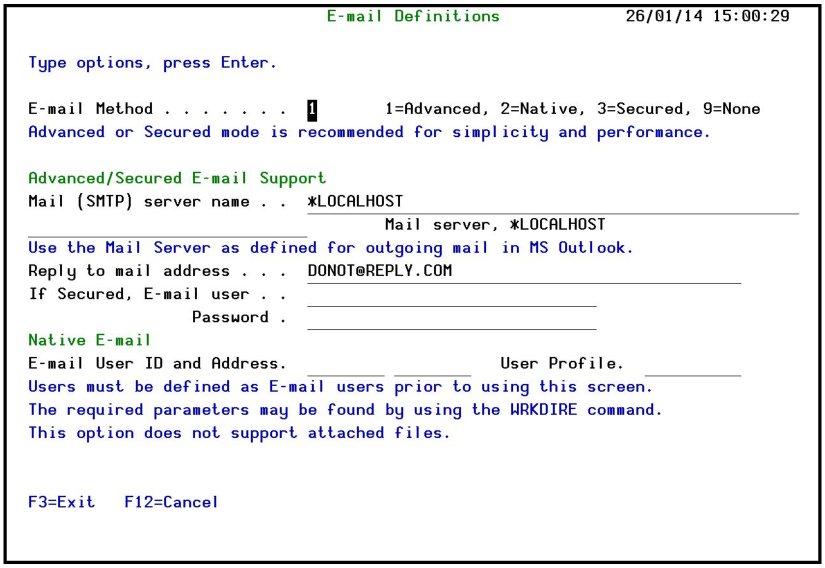
2. Set parameters according to the options described and click **`Enter`**.

Please contact your local distributor for additional assistance with SMS definitions. E-Mail Definitions

Before **Action** 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. Please refer to the appropriate IBM documentation for more details on these procedures.

To configure **Action** to send e-mail messages, perform the following steps in order:

1. Select **81 > 13** from the **iSecurity/Base System Configuration** menu. The **E-Mail Definitions** screen appears.



```
                              E-mail Definitions           26/01/14 15:00:29

 Type options, press Enter.

 E-mail Method . . . . . . .  1       1=Advanced, 2=Native, 3=Secured, 9=None
 Advanced or Secured mode is recommended for simplicity and performance.

 Advanced/Secured E-mail Support
 Mail (SMTP) server name . .  *LOCALHOST
                                      Mail server, *LOCALHOST
 Use the Mail Server as defined for outgoing mail in MS Outlook.
 Reply to mail address . . .  DONOT@REPLY.COM
 If Secured, E-mail user . .
                   Password .
 Native E-mail
 E-mail User ID and Address.                      User Profile.
 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.


 F3=Exit   F12=Cancel
```

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 which 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**.

Pager (Beeper) Definitions

Many different types of pager services are available throughout the world, and not all of them subscribe to a single international standard. For this reason, **Action** provides an interface module that communicates with an external program supplied by the customer (or the customer's pager service provider). This external program should accept the recipient address and the message text from **Action**, as well as define the communication protocols and other parameters specific to your service provider and installation. **Action** does not provide any specific definition parameters.

To use the pager feature, you must connect an asynchronous modem to a V24 communications adapter on your IBM System i. This modem should be capable of sending data at a relatively slow speed (300 - 2,400 bps). It is also highly recommended that you use a dedicated communication resource and modem for this purpose.

NOTE: The exact interface to the Email, SMS and Pager options can be adjusted by the user as needed. The exact interface can be found in file ***SMZ4DTA/AUSOURCE***, programs ***AUALR1R*** (Email), ***AUALR6R*** (SMS), ***AUALR7R*** (Pager)

To activate the user changes to the interface, you should modify the relevant program and compile into the library ***SMZ4DTA***.

Advanced Messaging (Central Adm.)

SIEM Support

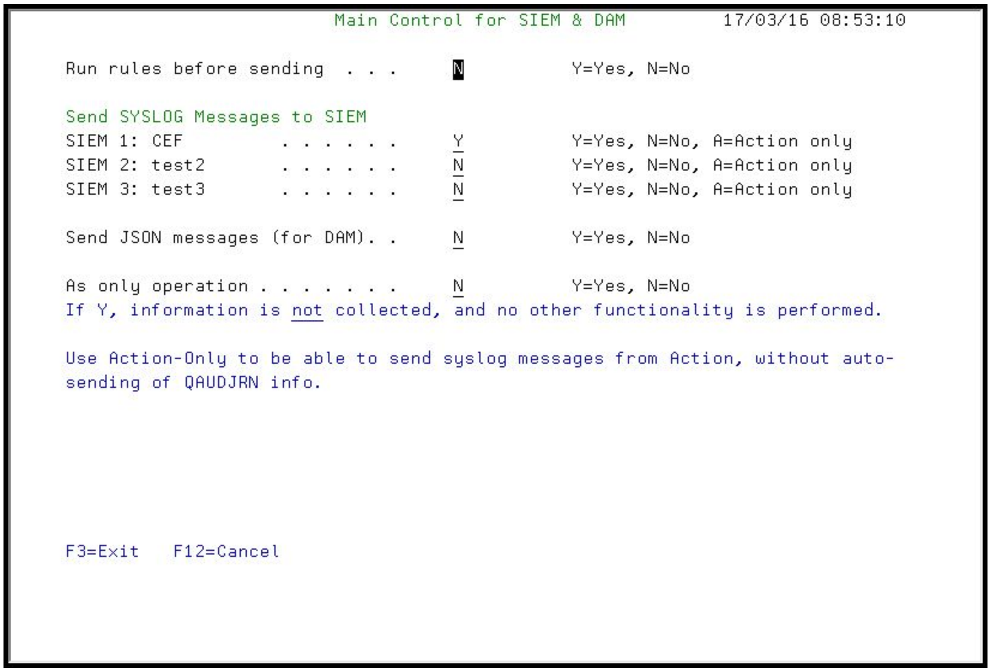
Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems; web-based alerts are supported using Twitter www.twitter.com (can transmit up to 1000 lines per second). Message alerts contain detailed event information about application data changes,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

Syslog Parameters

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

To send syslog messages for SIEM:

1. Select **81 > 31. Main Control**. The **Main Control for SIEM & DAM** screen is displayed.



```
                         Main Control for SIEM & DAM        17/03/16 08:53:10

 Run rules before sending  . . .     N          Y=Yes, N=No

 Send SYSLOG Messages to SIEM
 SIEM 1: CEF         . . . . . .     Y          Y=Yes, N=No, A=Action only
 SIEM 2: test2       . . . . . .     N          Y=Yes, N=No, A=Action only
 SIEM 3: test3       . . . . . .     N          Y=Yes, N=No, A=Action only

 Send JSON messages (for DAM). .     N          Y=Yes, N=No

 As only operation . . . . . . .     N          Y=Yes, N=No
 If Y, information is not collected, and no other functionality is performed.

 Use Action-Only to be able to send syslog messages from Action, without auto-
 sending of QAUDJRN info.




 F3=Exit   F12=Cancel
```

Figure 13: Main Control for SIEM & DAM

Parameter	Description
Run rules before sending	**Y** = Yes **N** = No
Send SYSLOG messages to SIEM	**Y** = Yes **N** = No **A** = Action only
Send JSON messages (for DAM)	**Y** = Yes **N** = No
As only operation	**Y** = Yes **N** = No

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

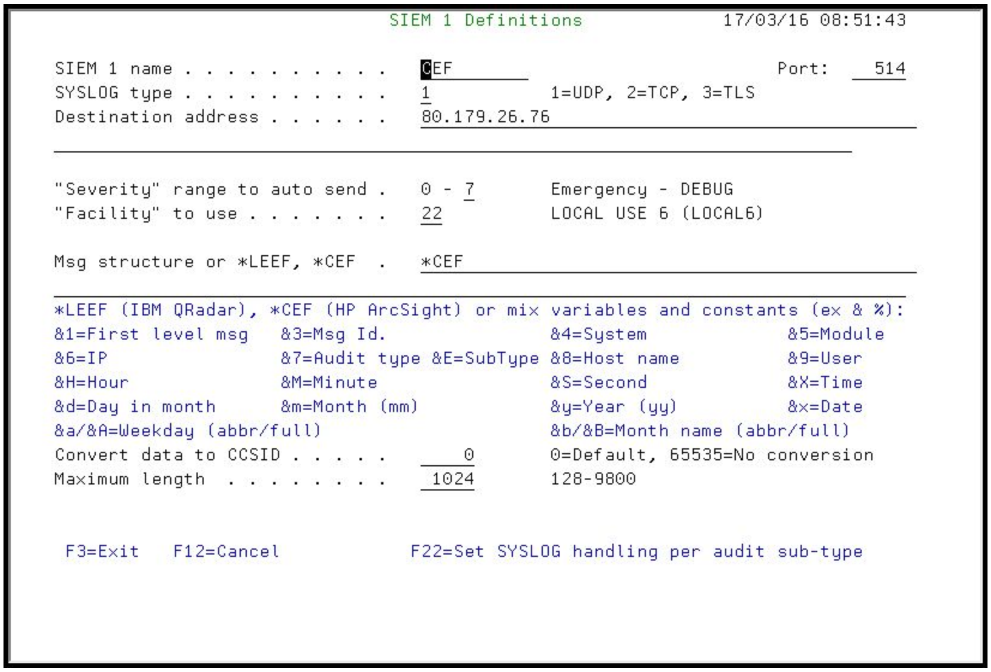
Triple Syslog Definitions (#1-#3)

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

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

To configure SIEM message structure:

3. Select **81 > 32/33/34. SIEM 1, SIEM 2, SIEM 3** in the **iSecurity/Base System Configuration** menu. The selected **SIEM Definitions** screen is displayed.



```
                                SIEM 1 Definitions             17/03/16 08:51:43

  SIEM 1 name . . . . . . . . . .   CEF                          Port:    514
  SYSLOG type . . . . . . . . . .   1           1=UDP, 2=TCP, 3=TLS
  Destination address . . . . . .   80.179.26.76


  "Severity" range to auto send .   0 - 7       Emergency - DEBUG
  "Facility" to use . . . . . . .   22          LOCAL USE 6 (LOCAL6)

  Msg structure or *LEEF, *CEF  .   *CEF

  *LEEF (IBM QRadar), *CEF (HP ArcSight) or mix variables and constants (ex & %):
  &1=First level msg   &3=Msg Id.               &4=System             &5=Module
  &6=IP                &7=Audit type &E=SubType &8=Host name          &9=User
  &H=Hour              &M=Minute                &S=Second             &X=Time
  &d=Day in month      &m=Month (mm)            &y=Year (yy)          &x=Date
  &a/&A=Weekday (abbr/full)                     &b/&B=Month name (abbr/full)
  Convert data to CCSID . . . . .       0       0=Default, 65535=No conversion
  Maximum length  . . . . . . . .    1024       128-9800


   F3=Exit   F12=Cancel            F22=Set SYSLOG handling per audit sub-type
```

Figure 14: SIEM definitions

Parameter	Description
SIEM # name	The name of the Syslog
Port	The port the Syslog is listening to according to the SYSLOG type
SYSLOG type	**1=UDP** **2=TCP** **3=TLS (**SYSLOG **over TLS uses port number 6514)**
Destination address	Enter the destination IP address (without quotes)
Severity range to auto send	Enter the severity range from which the SYSLOG message will be sent: 0-7 Emergency – DEBUG Where: 0 = EMERGENCY - EMERGENCY 1 = EMERGENCY - ALERT 2 = EMERGENCY - CRITICAL 3 = EMERGENCY - ERROR 4 = EMERGENCY - WARNING 5 = EMERGENCY - NOTICE (SIGNIFICANT) 6 = EMERGENCY - INFORMATIONAL 7 = EMERGENCY - DEBUG
Facility to use	Enter the facility from which the SYSLOG message will be sent Where: 1. USER-LEVEL MESSAGES 2. MAIL SYSTEM 3. SYSTEM DAEMONS 4. SECURITY/AUTHORIZATION MESSAGES 5. SYSLOGD INTERNAL 6. LINE PRINTER SUBSYSTEM 7. NETWORK NEWS SUBSYSTEM 8. UUCP SUBSYSTEM 9. CLOCK DAEMON 10. SECURITY/AUTHORIZATION MESSAGES 11. FTP DAEMON 12. NTP SUBSYSTEM 13. LOG AUDIT 14. LOG ALERT 15. CLOCK DAEMON 16. LOCAL USE 0 (LOCAL0)

Parameter	Description
17.	LOCAL USE 1 (LOCAL1)
18.	LOCAL USE 2 (LOCAL2)
19.	LOCAL USE 3 (LOCAL3)
20.	LOCAL USE 4 (LOCAL4)
21.	LOCAL USE 5 (LOCAL5)
22.	LOCAL USE 6 (LOCAL6)
23.	LOCAL USE 7 (LOCAL7)
Message Structure	Two built-in message structures are available which send data in Field Mode by pairs of Field name and Field value: ***LEEF** = Log Event Extended Format ***CEF** = Common Event Format -Or- Use mixed variables and constants (ex & %). A full description of the available variables is in the table below. (For more information on LEEF/CEF, see (*Advanced Messaging (Central Adm.)*).
Convert data to CCSID	**0** = Default **65535** = No conversion
Maximum length	128 - 9800

Variable	Description
&a	Abbreviated name of the day of the week (Sun, Mon, and so on).
&A	Full name of the day of the week (Sunday, Monday, and so on).
&b	Abbreviated month name (Jan, Feb, and so on).
&B	Full month name (January, February, and so on).
&c	Date/Time in the format of the locale.
&C	Century number [00-99], the year divided by 100 and truncated to an integer.
&d	Day of the month [01-31].
&D	Date Format, same as &m/&d/&y.
&e	Same as &d, except single digit is preceded by a space [1-31].
&g	2 digit year portion of ISO week date [00,99].
&G	4 digit year portion of ISO week date. Can be negative.
&h	Same as &b.
&H	Hour in 24-hour format [00-23].
&I	Hour in 12-hour format [01-12].
&j	Day of the year [001-366].
&L	Three digit milliseconds part of event time
&m	Month [01-12].
&M	Minute [00-59].
&n	Newline character.
&O	UTC offset. Output is a string with format +HH:MM or –HH:MM, where + indicates east of GMT, - indicates west of GMT, HH indicates the number of hours from GMT, and MM indicates the number of minutes from GMT.
&p	AM or PM string.
&r	Time in AM/PM format of the locale. If not available in the locale time format, defaults to the POSIX time AM/PM format: &I:&M:&S &p.
&R	24-hour time format without seconds, same as &H:&M.
&S	Second [00-61]. The range for seconds allows for a leap second and a double leap second.

Variable	Description
&t	Tab character.
&T	24-hour time format with seconds, same as &H:&M:&S.
&u	Weekday [1,7]. Monday is 1 and Sunday is 7.
&U	Week number of the year [00-53]. Sunday is the first day of the week.
&V	ISO week number of the year [01-53]. Monday is the first day of the week. If the week containing January 1st has four or more days in the new year then it is considered week 1. Otherwise, it is the last week of the previous year, and the next year is week 1 of the new year.
&w	Weekday [0,6], Sunday is 0.
&W	Week number of the year [00-53]. Monday is the first day of the week.
&x	Date in the format of the locale.
&X	Time in the format of the locale.
&y	2 digit year [00,99].
&Y	4-digit year. Can be negative.
&z	UTC offset. Output is a string with format +HHMM or -HHMM, where + indicates east of GMT, - indicates west of GMT, HH indicates the number of hours from GMT, and MM indicates the number of minutes from GMT.
&Z	Time zone name.
&1	The first level message
&3	The ID of the first level message
&4	The name of the system where the event took place
&5	The full name of the RazLee product
&6	The IP address of the system where the event took place
&7	The two character Audit type of the transaction
&8	The Host name of the system where the event took place
&9	The user ID for the event

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

&0 or &2 can now be used as last parameter in SYSLOG format.

&0 = bytes 1-9800 in USRDTA (9800 bytes)

&2 = bytes   1101-9800 in USRDTA (8700 bytes)

Notes:

1. These fields are not converted to ASCII.

2. SYSLOG manager must set maximum message length from default (1024) to expected size (10000).

3. SYSLOG manager must take care of non-printable characters option.

** SYSLFC - SYSLOG FACILITY:

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

**SYSLSV - SYSLOG SEVERITY :

0 = EMERGENCY - EMERGENCY
1 = EMERGENCY - ALERT
2 = EMERGENCY - CRITICAL
3 = EMERGENCY - ERROR

4 = EMERGENCY - WARNING
5 = EMERGENCY - NOTICE (SIGNIFICANT)
6 = EMERGENCY - INFORMATIONAL
7 = EMERGENCY - DEBUG

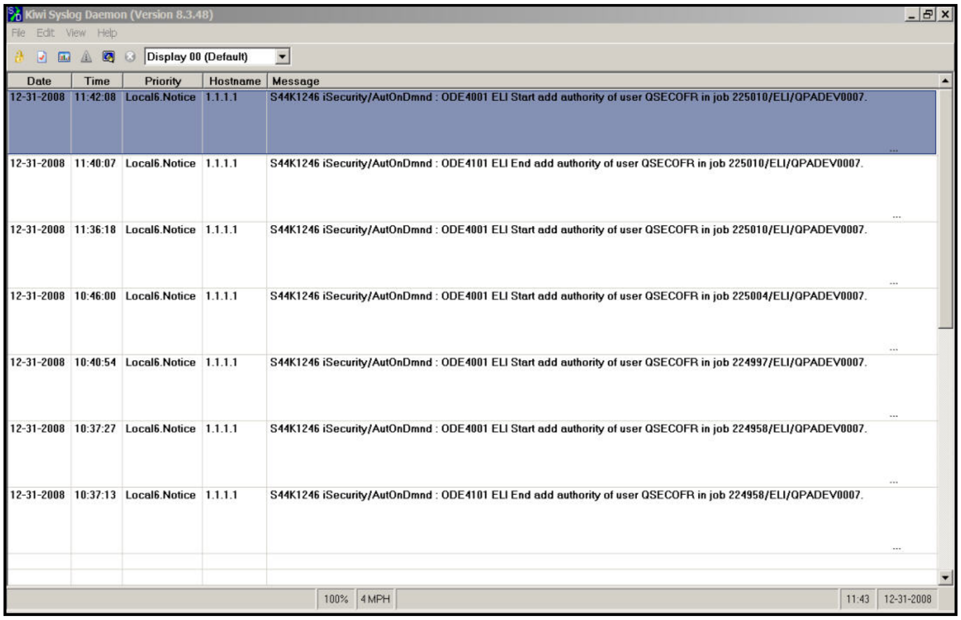
By using Firewall **> 81. System Configuration > 8. SYSLOG**, a user can decide whether he wants the SYSLOG to contain all of Firewall events (2=All), rejects only (1) or none (0).

To prompt and receive alerts, define an **Alert Message** in Action (Use **31.Work with** Actions in the Action Main menu).

Syslog simulation

To see how the Syslog definitions work without actually setting up the software on an IP address and to receive the Syslog messages:

5. Download Kiwi Syslog Server from http://www.kiwisyslog.com
6. Enter the PC IP address in the field on the Syslog definition screen. The command entry of **Get Authority on Demand** (*GETAOD*) writes a Syslog message and can be seen immediately in the Kiwi Syslog Server.

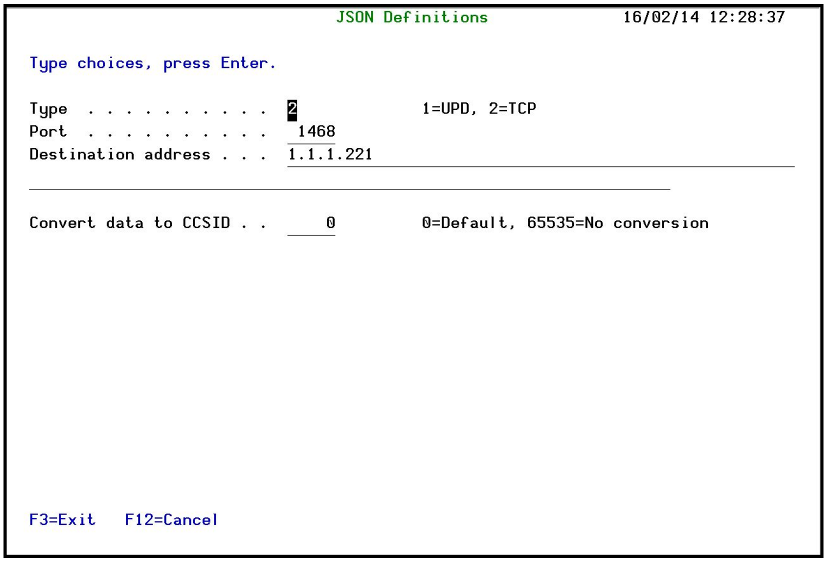


Date	Time	Priority	Hostname	Message
12-31-2008	11:42:08	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4001 ELI Start add authority of user QSECOFR in job 225010/ELI/QPADEV0007.
12-31-2008	11:40:07	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4101 ELI End add authority of user QSECOFR in job 225010/ELI/QPADEV0007.
12-31-2008	11:36:18	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4001 ELI Start add authority of user QSECOFR in job 225010/ELI/QPADEV0007.
12-31-2008	10:46:00	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4001 ELI Start add authority of user QSECOFR in job 225004/ELI/QPADEV0007.
12-31-2008	10:40:54	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4001 ELI Start add authority of user QSECOFR in job 224997/ELI/QPADEV0007.
12-31-2008	10:37:27	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4001 ELI Start add authority of user QSECOFR in job 224958/ELI/QPADEV0007.
12-31-2008	10:37:13	Local6.Notice	1.1.1.1	S44K1246 iSecurity/AutOnDmnd : ODE4101 ELI End add authority of user QSECOFR in job 224958/ELI/QPADEV0007.

Figure 15: Kiwi Syslog Server

JSON Definitions

1. Select **33. JSON Definitions (for DAM)** from the **iSecurity/Base System Configuration** menu. The **JSON Definitions** screen appears.



```
                                  JSON Definitions              16/02/14 12:28:37

 Type choices, press Enter.

 Type  . . . . . . . . . .   2              1=UPD, 2=TCP
 Port  . . . . . . . . . .    1468
 Destination address . . .   1.1.1.221


 Convert data to CCSID . .       0          0=Default, 65535=No conversion









 F3=Exit   F12=Cancel
```

Figure 16: JSON Definitions

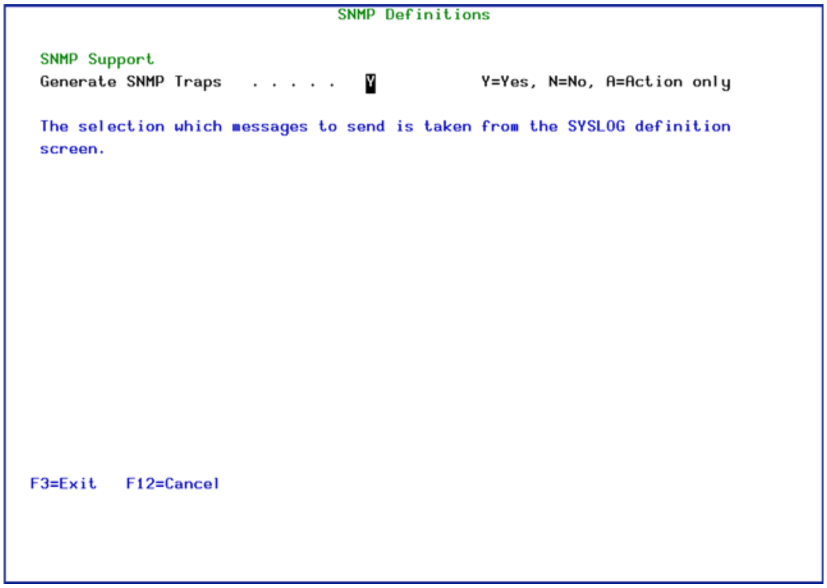
Parameter	Description
Type	1 = UPD 2 = TCP
Port	Enter the JSON port
Destination address	Enter the destination IP address (without quotes)
Convert data to CCSID	0 = Default 65535 = No conversion

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

SNMP Definitions

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

1. Select **`36. SNMP Definitions`** from the **`iSecurity/Base System Configuration`** menu. The **`SNMP Definitions`** screen appears.



```
                        SNMP Definitions

 SNMP Support
 Generate SNMP Traps  . . . . .  Y          Y=Yes, N=No, A=Action only

 The selection which messages to send is taken from the SYSLOG definition
 screen.

F3=Exit   F12=Cancel
```

Figure 17: SNMP Definitions

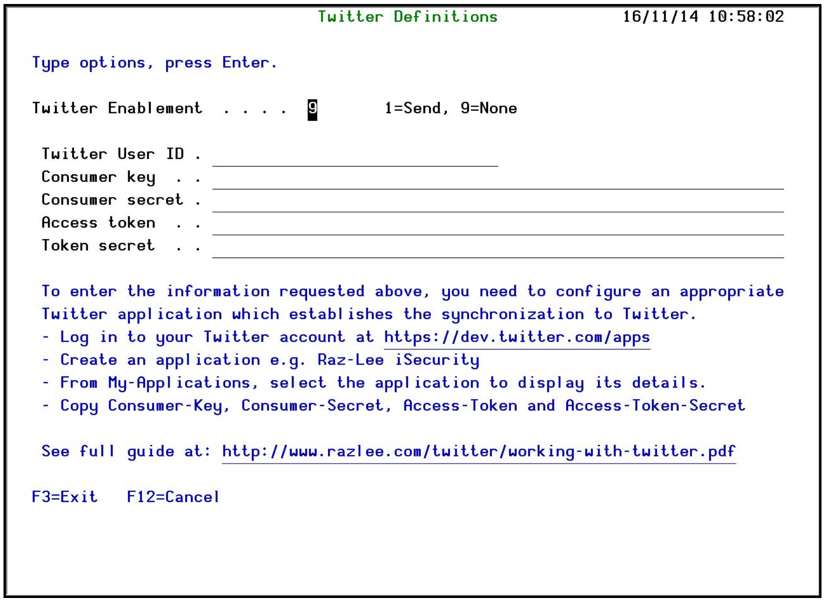
2. Type **`Y`** to generate SNMP traps to monitor network attached devices for conditions that warrant administrative attention.

NOTE: The selection of which messages to send is taken from the SYSLOG definition screen.

To prompt and receive alerts, define an **`Alert Message`** in Action (Use **`31.Work with Actions`** in the Action Main menu).

Twitter Definitions

1. Select **37. Twitter Definitions** from the **iSecurity/Base System Configuration** menu. The **Twitter Definitions** screen appears.



```
                          Twitter Definitions          16/11/14 10:58:02

 Type options, press Enter.

 Twitter Enablement  . . . . 9       1=Send, 9=None

  Twitter User ID . ______________________________
  Consumer key  . . ____________________________________________________________
  Consumer secret . ____________________________________________________________
  Access token  . . ____________________________________________________________
  Token secret  . . ____________________________________________________________

  To enter the information requested above, you need to configure an appropriate
  Twitter application which establishes the synchronization to Twitter.
  - Log in to your Twitter account at https://dev.twitter.com/apps
  - Create an application e.g. Raz-Lee iSecurity
  - From My-Applications, select the application to display its details.
  - Copy Consumer-Key, Consumer-Secret, Access-Token and Access-Token-Secret

  See full guide at: http://www.razlee.com/twitter/working-with-twitter.pdf

 F3=Exit   F12=Cancel
```

Figure 18: Twitter Definitions

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

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

To enter the information requested above, you need to configure an appropriate Twitter application that establishes the synchronization to Twitter.

3. If necessary, create a Twitter account.
4. Log in to your Twitter account at https://dev.twitter.com/apps.
5. Create an application.

6. From **My applications**, select the application to display its details.
7. Copy the **Consumer-Key**, **Consumer-Secret**, **Access-Token**, and **Access-Token-Secret** fields.

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

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

Chapter 3: Working with Rules and Actions

This chapter discusses the concepts of real-time detection and procedures for creating real-time detection rules and actions. Real-Time detection is implemented by several monitor subsystems that examine events as they occur. For each event that it detects, **Action** checks to see if a real time detection rule exists for this event.

If such a rule exists, **Action** records the event in the history log and triggers one or more actions as specified by the rule. An action may consist of alert messages sent to designated personnel and/or a pre-defined command script that runs automatically. You can send alerts via e-mail, IBM i (OS/400) system messages, network messages, SMS messages to cellular telephones, or pager (beeper) messages. **Action** command scripts may include multiple statements that execute IBM i commands or run programs.

The following diagram illustrates the real-time detection rule process.

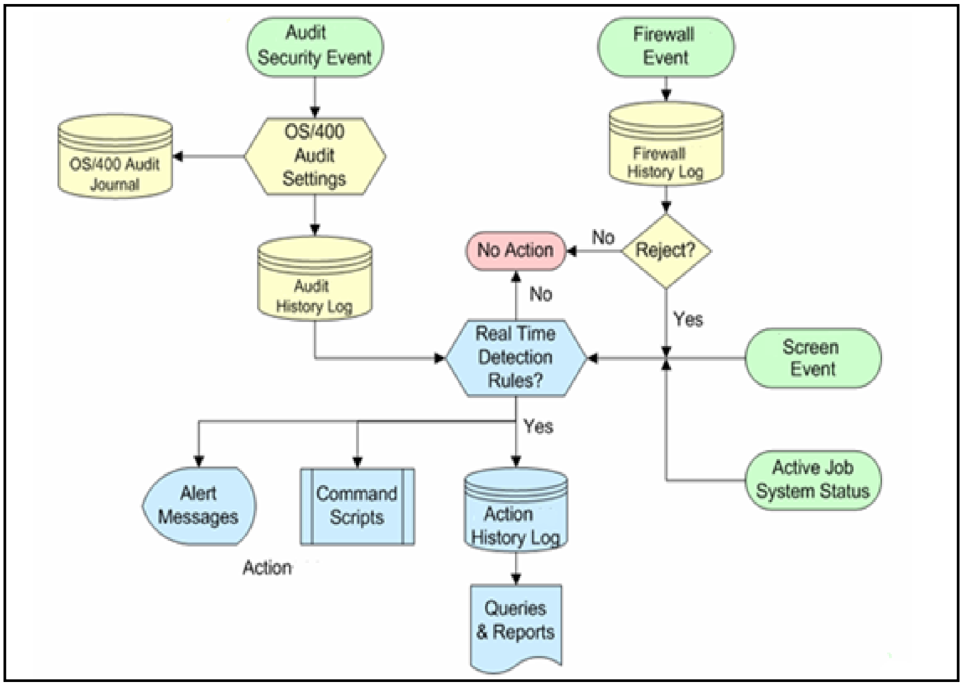


Figure 19: Action Real-Time Detection Rule process

Working with Real-Time Detection Rules

Overview

- Real-time detection rules are based on one of the following event types:
- Events detected by **Audit** based on IBM i (OS/400) audit journal entry types
- Transactions rejected by **Firewall** network security rules
- Terminal screens locked/released and jobs terminated by **Screen**
- Active job information, including rules for jobs that are not presently active
- Current system and memory pool status, including rules for pools that are not presently active

You may create several different rules for a single event type. User-defined sequence numbers determine the order of rule processing within a given type.

Basic Steps

The procedure for defining a real-time detection rule may seem a bit complex at first, but in fact, it is quite easy and intuitive. There are seven basic steps for creating rules.

1. Ensure that settings are properly defined to capture events as follows:
    - Define IBM i (OS/400) audit settings and **Audit** detection rules to record events
    - Define **Firewall** rules to reject the appropriate transaction
    - Define **Screen** timeout periods and job termination rules
    - Determine the appropriate parameters for active jobs and system status
2. Create a new real-time detection rule or select an existing rule to work with.
3. Set basic rule parameters using the **`Selection Rule`** screen.
4. Define filter conditions limiting application of the rule to specific conditions.
5. Define alert message actions as required.
6. Define command script actions as required.
7. Test and debug your rule.

The balance of this chapter presents instructions for defining real-time detection rules and actions. Although the screen examples presented herein refer to audit rules, the procedures themselves apply to all rule types.

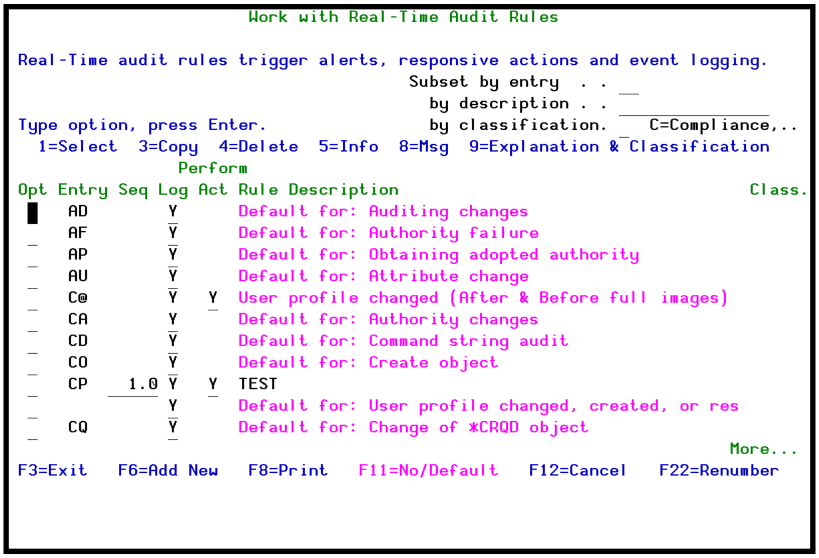
Action provides you with a set of powerful but easy-to-use tools to help you create rules that precisely define the circumstances governing the recording of an event in the history log and/or performing a responsive action. Concise explanations for data elements and options as well as pop-up selection windows are only a key press away.

You can copy existing rules, making minor changes to save definition effort. You may use existing action definitions with any number of rules. Precise filter criteria may be applied to any or all fields in the history log records using powerful criteria selection operators. A single, user-friendly screen supports this process. The unique Time Group feature enables you to apply rules only during (or outside of) predefined time periods.

Creating and Modifying Rules

To create or modify real time detection rules:

1. Select **11. Real – Time Auditing** from the **Action** Main menu. The **Work with Real-Time Audit Rules** screen appears.

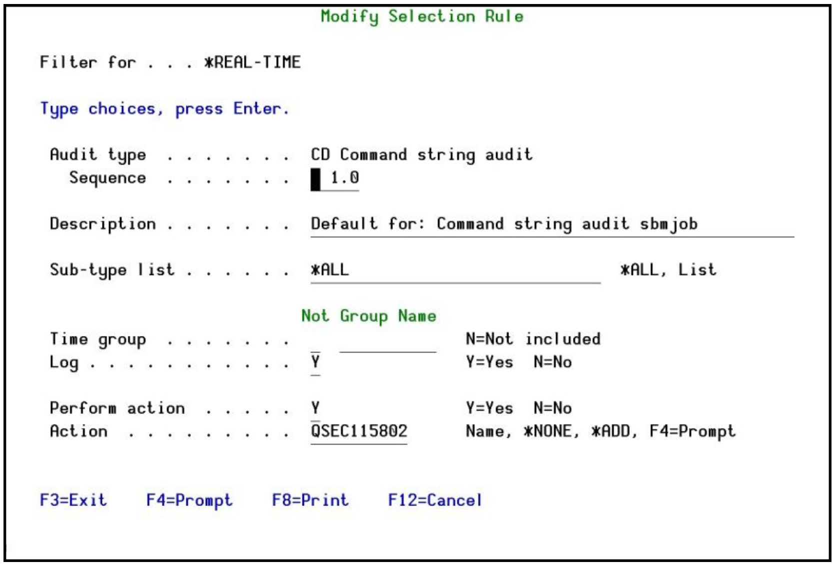


```
                        Work with Real-Time Audit Rules

Real-Time audit rules trigger alerts, responsive actions and event logging.
                                       Subset by entry  . .  __
                                         by description . .  ________________
Type option, press Enter.                by classification.  _  C=Compliance,..
  1=Select  3=Copy  4=Delete  5=Info  8=Msg  9=Explanation & Classification
                Perform
Opt Entry Seq Log Act Rule Description                                  Class.
 █   AD        Y      Default for: Auditing changes
 _   AF        Y      Default for: Authority failure
 _   AP        Y      Default for: Obtaining adopted authority
 _   AU        Y      Default for: Attribute change
 _   C@        Y   Y  User profile changed (After & Before full images)
 _   CA        Y   _  Default for: Authority changes
 _   CD        Y      Default for: Command string audit
 _   CO        Y      Default for: Create object
 _   CP    1.0 Y   Y  TEST
 _             Y   _  Default for: User profile changed, created, or res
 _   CQ        Y      Default for: Change of *CRQD object
                                                                      More...
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber
```

Figure 20: Work with Real-Time Audit Rules

Parameter or Option	Description
Option	1 = Select rule to modify 3 = Copy rule 4 = Delete rule 5 = Info 8 = Message – define a message that will be sent when the action occurs 9 = Explanation & Classification - type an explanation that will be appear on any report that includes this rule
Entry	IBM i (OS/400) Audit journal entry type
Sequence	Rules for a given audit type are applied in sequential order according to the sequence number
Log	**Y** = Log this event in the history log
Action	**Y** = This rule triggers an action
F6	Create a new rule
F11	No / Default
F22	Recalculate rule sequence numbers

2. Select a rule from the list (**`option 1`**) or press **`F6`** to create a new rule.
3. The **`Add Selection Rule`** or **`Modify Selection Rule`** screen appears, enabling you to set basic rule parameters (each screen contains the same parameters).



```
                              Modify Selection Rule

  Filter for . . . *REAL-TIME

  Type choices, press Enter.

   Audit type  . . . . . . .  CD Command string audit
     Sequence  . . . . . . .   1.0

   Description . . . . . . .  Default for: Command string audit sbmjob

   Sub-type list . . . . . .  *ALL                            *ALL, List

                            Not Group Name
   Time group  . . . . . . .                  N=Not included
   Log . . . . . . . . . . .  Y               Y=Yes  N=No

   Perform action  . . . . .  Y               Y=Yes  N=No
   Action  . . . . . . . . .  QSEC115802      Name, *NONE, *ADD, F4=Prompt


  F3=Exit    F4=Prompt    F8=Print    F12=Cancel
```

Figure 21: Modify Selection Rule

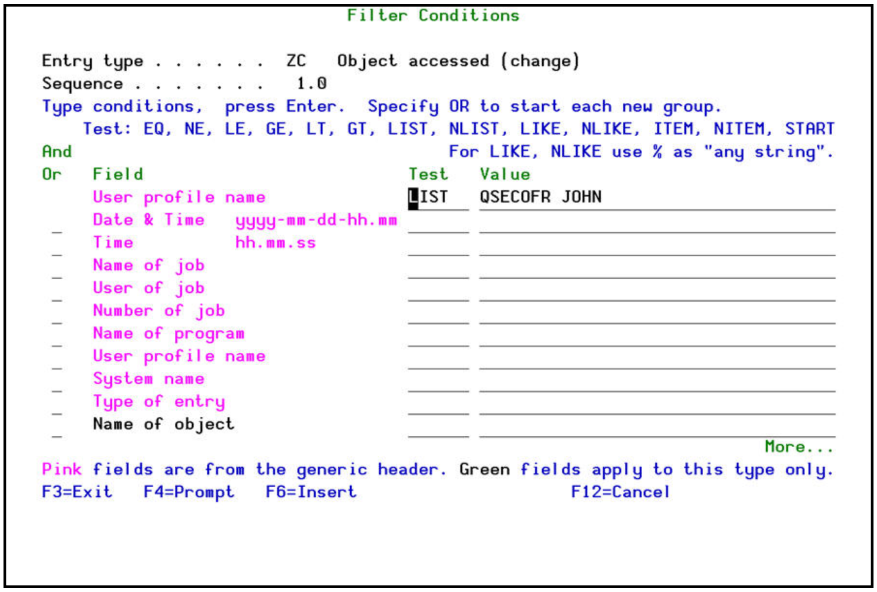
Parameter or Option	Description
Audit Type	IBM i (OS/400) Audit journal entry type **F4** = Choose from a list of available types
Sequence	Enter a sequence number or accept the default as presented. The sequence number determines the order of rule processing when there is more than one rule for a given audit type.
Description	Enter a meaningful description of the rule.
Sub-Type list	You may restrict this rule to one or more sub-types only: **Sub-Type** = One character sub-type code **F4** = Choose a sub-type from the list **List** = Enter several sub-type codes separated by a space ***ALL** = All sub-types within this entry type
Time Group – Not	You may optionally limit this group only to a specific Time Group. **Blank** = Apply rule only to events occurring during time group **N** = Apply rule only to events occurring outside the times defined in the time group
Time Group – Group Name	**Name** = Time Group name **F4** = Choose Time Group name from list **Blank** = Do NOT use Time Group name for rule selection
Log	**Y**= Record this event in the history log **N** = Do NOT Record this event in the history log
Perform Action	**Y**= Perform this action according to the rule **N** = Do NOT perform this action
Action	Optionally trigger an action (the Action module must be installed) **Name** = Name of the action to trigger by this rule **F4** = Select an action from list **Add** = Define a new action for this rule ***NONE** = No actions are triggered by this rule

4. Enter parameters and data as described in the table. Press **Enter** when finished to define filters. The **Filter Conditions** screen appears. Filter criteria enable you to limit application of real-time detection rules to certain specific conditions.

Defining Filter Conditions

Each filter condition consists of a comparison test applied against one of the fields in the journal record.

Below are the **Filter Conditions** screen and a table of explanation.



```
                         Filter Conditions

 Entry type . . . . . .  ZC   Object accessed (change)
 Sequence . . . . . . .   1.0
 Type conditions,  press Enter.  Specify OR to start each new group.
    Test: EQ, NE, LE, GE, LT, GT, LIST, NLIST, LIKE, NLIKE, ITEM, NITEM, START
 And                                 For LIKE, NLIKE use % as "any string".
 Or   Field                                Test   Value
      User profile name                    LIST   QSECOFR JOHN
  _   Date & Time     yyyy-mm-dd-hh.mm     ______ ________________________
  _   Time            hh.mm.ss             ______ ________________________
  _   Name of job                          ______ ________________________
  _   User of job                          ______ ________________________
  _   Number of job                        ______ ________________________
  _   Name of program                      ______ ________________________
  _   User profile name                    ______ ________________________
  _   System name                          ______ ________________________
  _   Type of entry                        ______ ________________________
  _   Name of object                       ______ ________________________
                                                                    More...
 Pink fields are from the generic header. Green fields apply to this type only.
 F3=Exit   F4=Prompt   F6=Insert                    F12=Cancel
```

Figure 22: Filter Conditions

Parameter or Option	Description
And/Or	**A or Blank** = And O = Or
Field	Data field in the journal record: Pink fields are part of the generic header common to all journal types Green fields represent data specific to this journal type
Test	Comparison test type – see table on the following page for details
Value	Comparison value text; this field is case sensitive.
F4	Displays explanatory information/options applicable to the data field on the line where the cursor is located
F6	Select another comparison test from a pop-up window and insert it at the current cursor position
F8	Change Caps Lock from lower to upper case. An indicator appears on the screen.

Filter conditions are optional. If you do not define any filter conditions, the rule will incorporate all events for the specified audit type or types. When you have defined your filters, press **Enter** and you return to the calling screen.

Comparison Test Operators

Several different types of comparison test operators are available as shown in the following table.

Test	Description	Value Field Data
EQ,NE	Equal to, Not equal to	Value
LT, LE	Less than, Less than or equal to	Value
GT, GE	Greater than, Greater than or equal to	Value
LIST, NLIST	Included in list, Not included in list	Values separated by a space
LIKE, NLIKE	Substring search	Value preceded and/or followed by %. **NLIKE is true if the value given is not in the field.**
ITEM/NITEM	Checks if the value of the field is (or is not) an item inside the named group.	*USER – Check that the value is a user in a %GROUP of users *GRPPRF – Check that the value is a user in an OS/400 Group Profile *USRGRP – USER and all user profiles which are members of same user groups as USER *ALL – For both *GRPPRF and *USRGRP cases If the TYPE is missing, *USER or *USRGRP is assumed based on the appearance of the % sign as the first character in the GROUP. *SPCAUT – Check that the value is in the users Special-Authority NAME – The name of a customized group
START	Starts with	Starting characters of a string
PGM, NPGM	Calls a specific user program to conduct a comparison which replies with True or False If you use NPGM, then a returned value of False means that the condition is True.	The user program name (library/program)

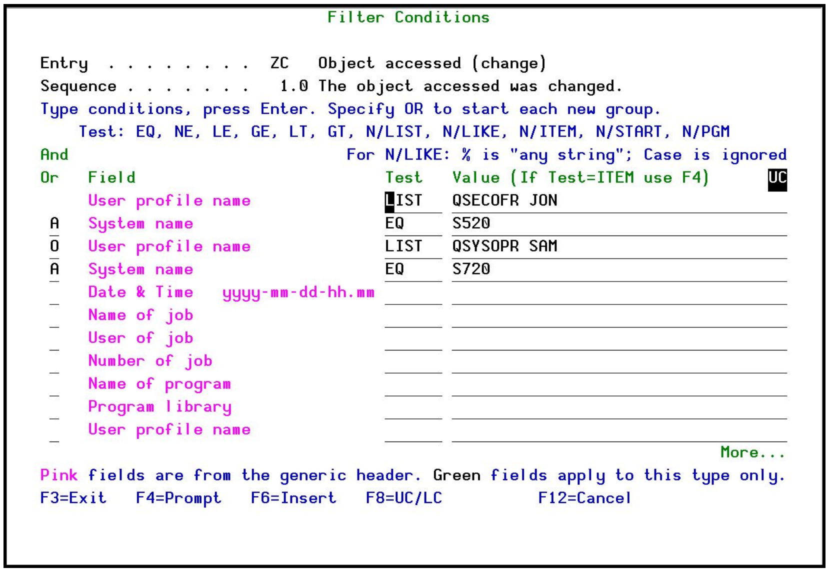
And/Or Boolean Operators

You can combine multiple filter conditions in one rule using Boolean AND/OR operators. This enables you to create complex rules that produce precise results.

When using OR operators in your filter conditions, the order in which each condition appears in the list of conditions is critical. The OR operator enables you to group several conditions together because it includes all the AND conditions that follow it until the next OR operator or until the end of the list.

The AND condition groups the OR condition which was defined before it.

The following example illustrates this principle. This rule will apply to all events meeting **either** the conditions listed in the first two lines **or** the conditions listed in the second two lines. The second group includes the ‘Or’ condition and all of the ‘And’ conditions that follow it.



```
                              Filter Conditions

 Entry  . . . . . . . .  ZC   Object accessed (change)
 Sequence . . . . . . .   1.0 The object accessed was changed.
 Type conditions, press Enter. Specify OR to start each group.
    Test: EQ, NE, LE, GE, LT, GT, N/LIST, N/LIKE, N/ITEM, N/START, N/PGM
 And                            For N/LIKE: % is "any string"; Case is ignored
 Or   Field                           Test   Value (If Test=ITEM use F4)      UC
      User profile name               LIST   QSECOFR JON
  A   System name                     EQ     S520
  O   User profile name               LIST   QSYSOPR SAM
  A   System name                     EQ     S720
  _   Date & Time   yyyy-mm-dd-hh.mm
  _   Name of job
  _   User of job
  _   Number of job
  _   Name of program
  _   Program library
  _   User profile name
  _                                                                  More...
 Pink fields are from the generic header. Green fields apply to this type only.
 F3=Exit   F4=Prompt   F6=Insert   F8=UC/LC          F12=Cancel
```

Figure 23: Filter Conditions

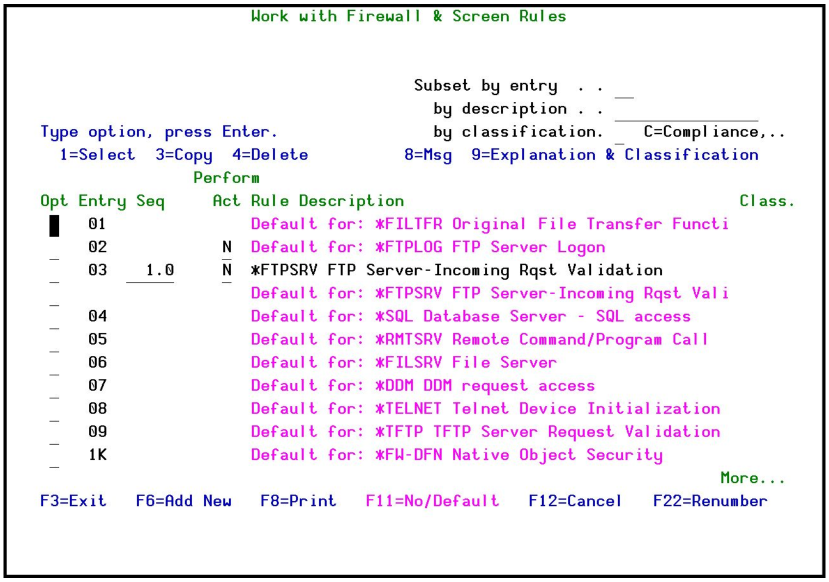
This rule applies only to commands that changed the accessed object only if the User Profile was QSECOFR or JON and on System S520 **OR** if the User Profile was QSYSOPR or SAM and on System S720.

If you intend that your rule will trigger an action, the action definition screens appear automatically. If this is not the case, the rule definition process is complete and the **Real-Time Audit Rules** screen re-appears.

Firewall/Screen

Use this feature to add and modify rules to work with active jobs (*WRKACTJOB*) and work with system status.

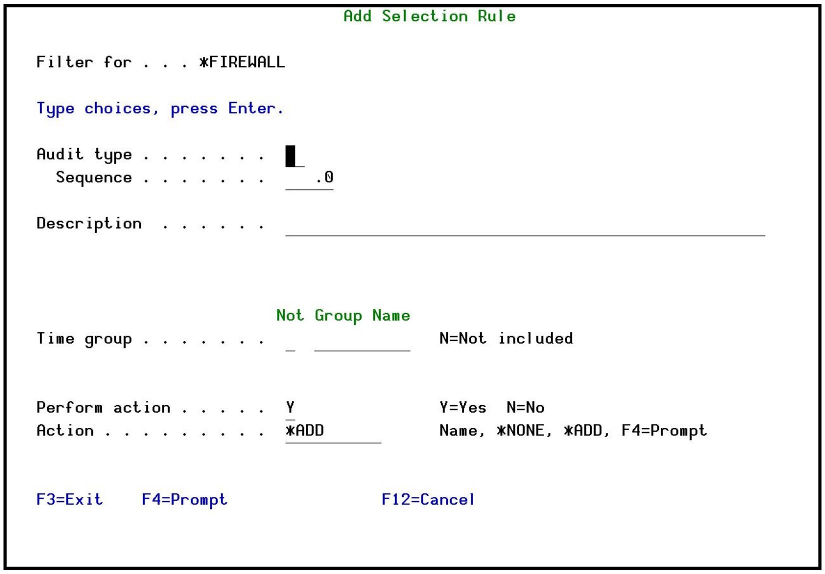
1. Select **12. Firewall/Screen** from the **Action** Main menu. The **Work with Firewall & Screen Rules** screen appears.



```
                         Work with Firewall & Screen Rules


                                              Subset by entry  . .  __
                                                by description . .  ______________
Type option, press Enter.                       by classification.  _  C=Compliance,..
  1=Select  3=Copy  4=Delete          8=Msg  9=Explanation & Classification
                Perform
Opt Entry Seq     Act Rule Description                                       Class.
 █    01              Default for: *FILTFR Original File Transfer Functi
 _    02            N Default for: *FTPLOG FTP Server Logon
 _    03   __1.0    N *FTPSRV FTP Server-Incoming Rqst Validation
 _                  _ Default for: *FTPSRV FTP Server-Incoming Rqst Vali
 _    04              Default for: *SQL Database Server - SQL access
 _    05              Default for: *RMTSRV Remote Command/Program Call
 _    06              Default for: *FILSRV File Server
 _    07              Default for: *DDM DDM request access
 _    08              Default for: *TELNET Telnet Device Initialization
 _    09              Default for: *TFTP TFTP Server Request Validation
 _    1K              Default for: *FW-DFN Native Object Security
                                                                          More...
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber
```

Figure 24: Work with Firewall & Screen Rules

2. Select **1** to modify an existing rule or **F6** to create a new rule. The **Add Selection Rule** screen appears.



```
                              Add Selection Rule

Filter for . . . *FIREWALL

Type choices, press Enter.

Audit type . . . . . . .   █_
  Sequence . . . . . . .   ___.0

Description  . . . . . .   __________________________________________________



                         Not Group Name
Time group . . . . . . .   _  __________      N=Not included


Perform action . . . . .   Y                  Y=Yes  N=No
Action . . . . . . . . .   *ADD______         Name, *NONE, *ADD, F4=Prompt


F3=Exit    F4=Prompt                F12=Cancel
```

Figure 25: Add Selection Rule for Firewall screen

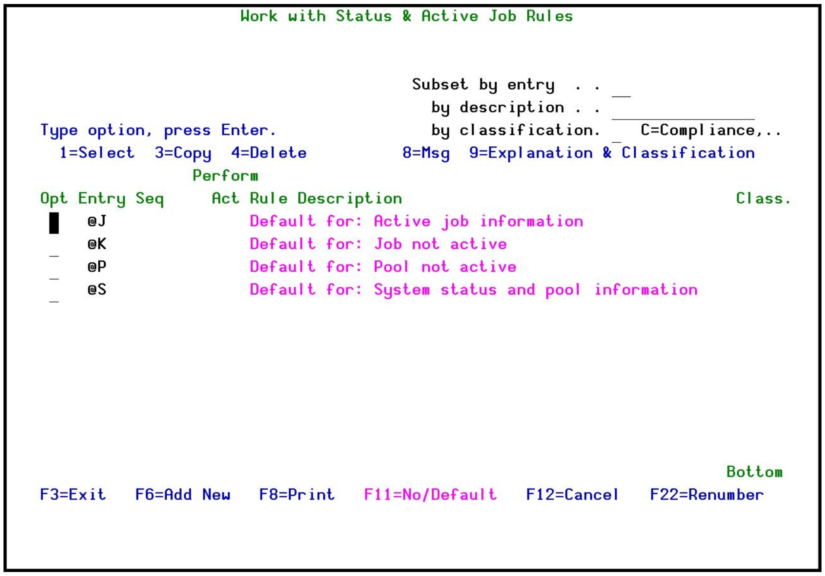
Parameter or Option	Description
Audit Type	IBM i (OS/400) Audit journal entry type **F4** = Choose from a list of available types
Sequence	Enter a sequence number or accept the default as presented. The sequence number determines the order of rule processing when there is more than one rule for a given audit type.
Description	Enter a meaningful description of the rule.
Time Group – Not	You may optionally limit this group only to a specific Time Group. **Blank** = Apply rule only to events occurring during time group **N** = Apply rule only to events occurring outside the times defined in the time group
Time Group – Group Name	**Name** = Time Group name **F4** = Choose Time Group name from list **Blank** = Do NOT use Time Group name for rule selection
Perform Action	**Y**= Perform this action according to the rule **N** = Do NOT perform this action
Action	Optionally trigger an action (the Action module must be installed) **Name** = Name of the action to trigger by this rule **F4** = Select an action from list **Add** = Define a new action for this rule ***NONE** = No actions are triggered by this rule

3. Enter parameters and data as described in the table. Press **Enter** when finished. The **Filter Conditions** screen appears. Filter criteria enable you to limit application of real-time detection rules to certain specific conditions.

Status and Active Jobs

Use this feature to add and modify rules to work with active jobs (*WRKACTJOB*) and work with system status.

1. Select **13. Status & Active Job (SysCtl)** from the Action Main menu. The **Work with Status & Active Job Rules** screen appears. The table below describes the four standard entries that are included with the product.

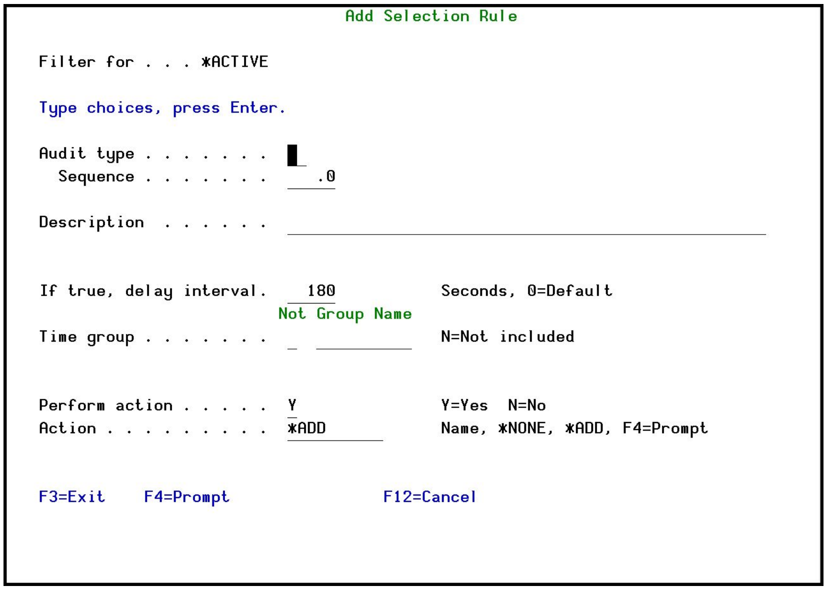


```
                         Work with Status & Active Job Rules


                                          Subset by entry  . .  __
                                            by description . .  ______________
   Type option, press Enter.                by classification.  _  C=Compliance,..
     1=Select  3=Copy  4=Delete           8=Msg  9=Explanation & Classification
                    Perform
   Opt Entry Seq      Act Rule Description                                 Class.
   _    @J                Default for: Active job information
   _    @K                Default for: Job not active
   _    @P                Default for: Pool not active
   _    @S                Default for: System status and pool information




                                                                          Bottom
   F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber
```

Figure 26: Work with Status & Active Job Rules

Entry	Rule Description
@J	Compares every line in the *WRKACTJOB* to the rule that uses it.
@K	Performs a check to verify whether the job is active.
@P	Performs a check to verify whether a particular pool is active.
@S	Checks filter conditions to verify if response criteria are met, thus activating that response

2. Select **1** to modify an existing rule or **F6** to create a new rule. The **Add Selection Rule** screen appears.



```
                         Add Selection Rule

Filter for . . . *ACTIVE

Type choices, press Enter.

Audit type . . . . . . .  _
  Sequence . . . . . . .     .0

Description  . . . . . .  


If true, delay interval.   180          Seconds, 0=Default
                         Not Group Name
Time group . . . . . . .  _            N=Not included


Perform action . . . . .  Y             Y=Yes  N=No
Action . . . . . . . . .  *ADD          Name, *NONE, *ADD, F4=Prompt


F3=Exit    F4=Prompt                F12=Cancel
```

Figure 27: Add Selection Rule for Active Jobs screen

Parameter or Option	Description
Audit Type	IBM i (OS/400) Audit journal entry type **F4** = Choose from a list of available types
Sequence	Enter a sequence number or accept the default as presented. The sequence number determines the order of rule processing when there is more than one rule for a given audit type.
Description	Enter a meaningful description of the rule.
If true, delay interval	Define the number of seconds to wait before performing the action. The default is 0.
Time Group – Not	You may optionally limit this group only to a specific Time Group. **Blank** = Apply rule only to events occurring during time group **N** = Apply rule only to events occurring outside the times defined in the time group
Time Group – Group Name	**Name** = Time Group name **F4** = Choose Time Group name from list **Blank** = Do NOT use Time Group name for rule selection
Perform Action	**Y**= Perform this action according to the rule **N** = Do NOT perform this action
Action	Optionally trigger an action (the Action module must be installed) **Name** = Name of the action to trigger by this rule **F4** = Select an action from list **Add** = Define a new action for this rule ***NONE** = No actions are triggered by this rule

3. Enter parameters and data as described in the table. Press **Enter** when finished. The **Filter Conditions** screen appears. Filter criteria enable you to limit application of real-time detection rules to certain specific conditions.

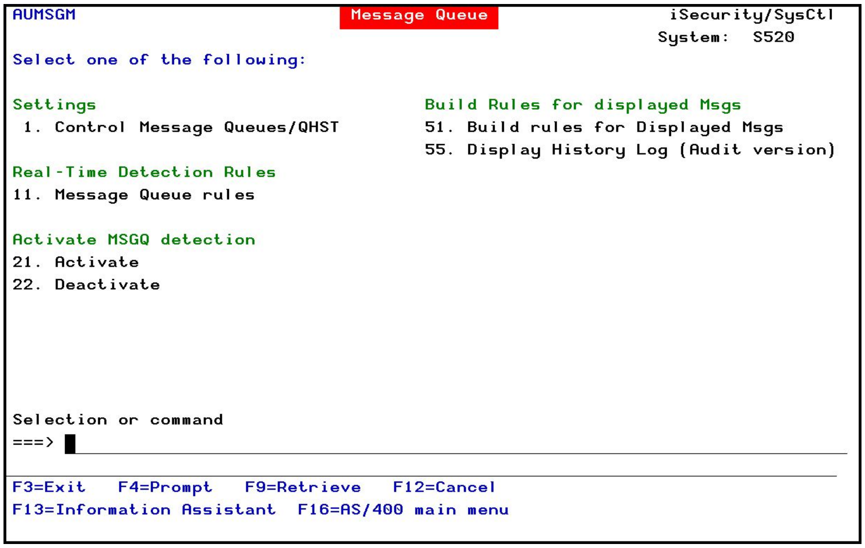
Working with Message Queues

This unique solution enables real-time auditing on message queues. Users have the option to:

- Modify rules according to all the message queue parameters
- Respond to the message by alerting the user (emails, SMS) and by reacting to it directly (send auto response).

To work with message queues:

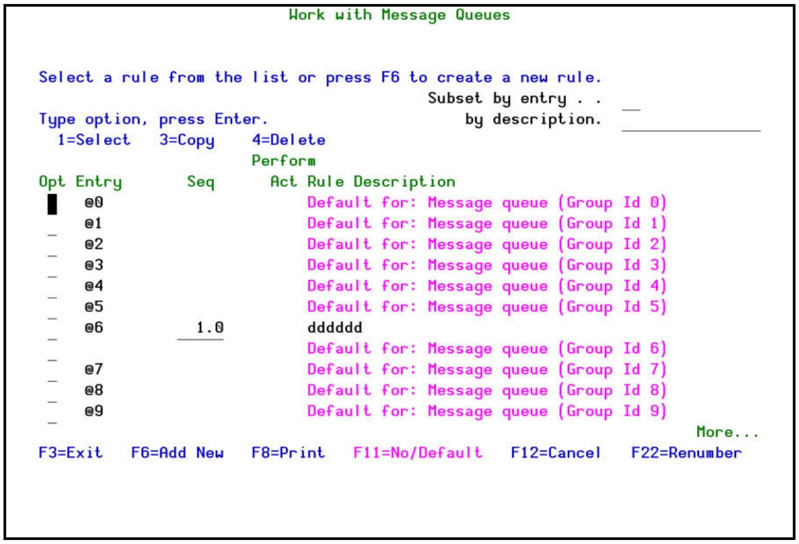
1. Select **`14. Message Queue (SysCtl)`** from the **Action** Main menu. The **`Message Queue`** menu appears.



```
AUMSGM                         Message Queue                iSecurity/SysCtl
                                                            System:   S520
Select one of the following:

Settings                                 Build Rules for displayed Msgs
 1. Control Message Queues/QHST          51. Build rules for Displayed Msgs
                                         55. Display History Log (Audit version)
Real-Time Detection Rules
11. Message Queue rules

Activate MSGQ detection
21. Activate
22. Deactivate




Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 28: Message Queue

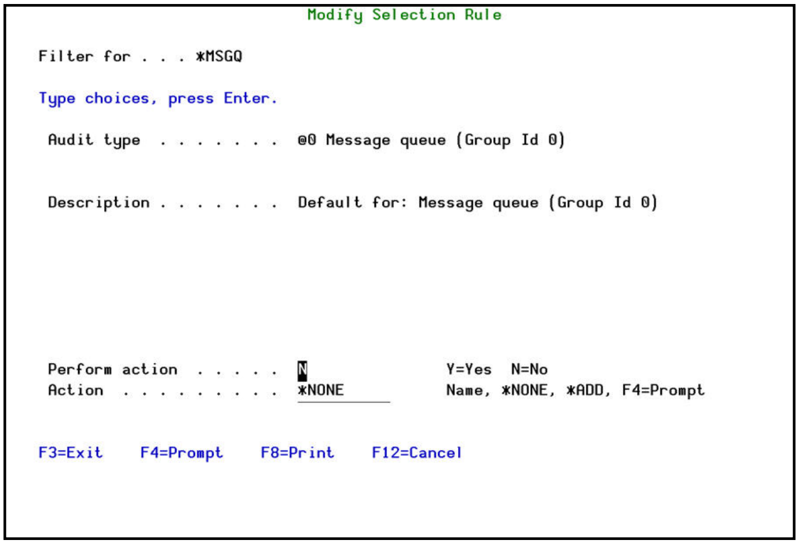
2. Select option **`11. Message Queue rules`**. A table message queues appears



```
                           Work with Message Queues


Select a rule from the list or press F6 to create a new rule.
                                           Subset by entry . .  __
Type option, press Enter.                     by description.  _______________
  1=Select   3=Copy    4=Delete
                      Perform
Opt Entry       Seq      Act Rule Description
 █   @0                       Default for: Message queue (Group Id 0)
 _   @1                       Default for: Message queue (Group Id 1)
 _   @2                       Default for: Message queue (Group Id 2)
 _   @3                       Default for: Message queue (Group Id 3)
 _   @4                       Default for: Message queue (Group Id 4)
 _   @5                       Default for: Message queue (Group Id 5)
 _   @6           1.0         dddddd
 _                            Default for: Message queue (Group Id 6)
 _   @7                       Default for: Message queue (Group Id 7)
 _   @8                       Default for: Message queue (Group Id 8)
 _   @9                       Default for: Message queue (Group Id 9)
 _                                                                    More...
F3=Exit   F6=Add New    F8=Print   F11=No/Default   F12=Cancel   F22=Renumber
```

Figure 29: Work with Message Queues

3. Type 1 to select a message to modify.



```
                             Modify Selection Rule

Filter for . . . *MSGQ

Type choices, press Enter.

 Audit type  . . . . . . .  @0 Message queue (Group Id 0)


 Description . . . . . . .  Default for: Message queue (Group Id 0)








 Perform action  . . . . .  N               Y=Yes  N=No
 Action  . . . . . . . . .  *NONE           Name, *NONE, *ADD, F4=Prompt


F3=Exit    F4=Prompt    F8=Print    F12=Cancel
```

Figure 30: Modify Selection Rule

Option	Description
Audit Type	Audit types are `@0-@9`. All choices have the same parameters. The ID numbers are only for organizational purposes.
Seq (Sequence)	The order in which the rule will be checked in this audit type (**1** = first rule checked, and so on).
Time Group	Find time group
Perform Action	**Y** = Perform this action according to rule **N** = Do not perform this action
Action	Optionally trigger this action **Name** = name of action to trigger by this rule **F4** = Select an action from the list **ADD** = Define a new action for this rule ***NONE** = No actions are triggered by this rule

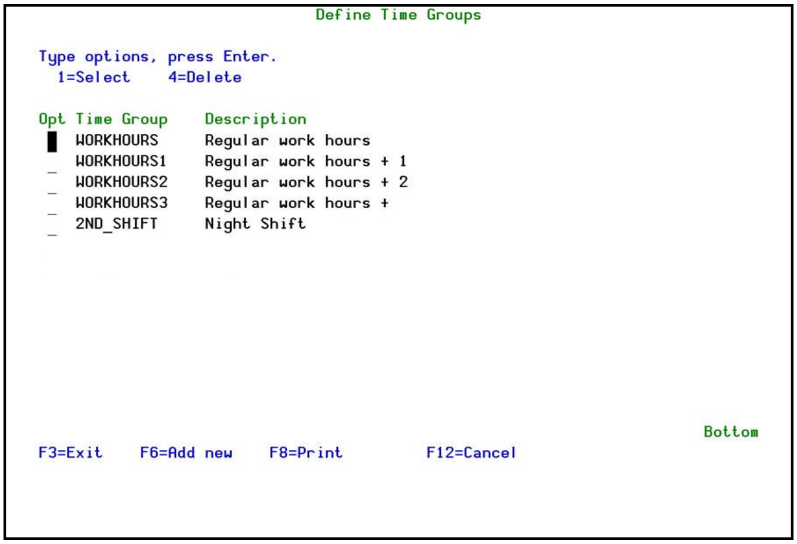
Working with Time Groups

Time groups are user-defined sets of time and day of the week parameters that you can use as filter criteria when working with real time detection rules, queries, reports and the history log. Time group filters can either be:

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

To define a time group:

1. Select **31** from the Audit Main menu or **51** from Action Main menu. The **Define Time Groups** window appears.



```
                        Define Time Groups

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

 Opt Time Group    Description
  █  WORKHOURS     Regular work hours
  _  WORKHOURS1    Regular work hours + 1
  _  WORKHOURS2    Regular work hours + 2
  _  WORKHOURS3    Regular work hours +
  _  2ND_SHIFT     Night Shift
  _














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

Figure 31: Define Time Groups

2. Type 1 to 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.

Parameter or Option	Description
Description	Text description of the time group
Start and End	Starting and ending times for each period using 24 hour notation
F13	Copy starting and ending times from 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.

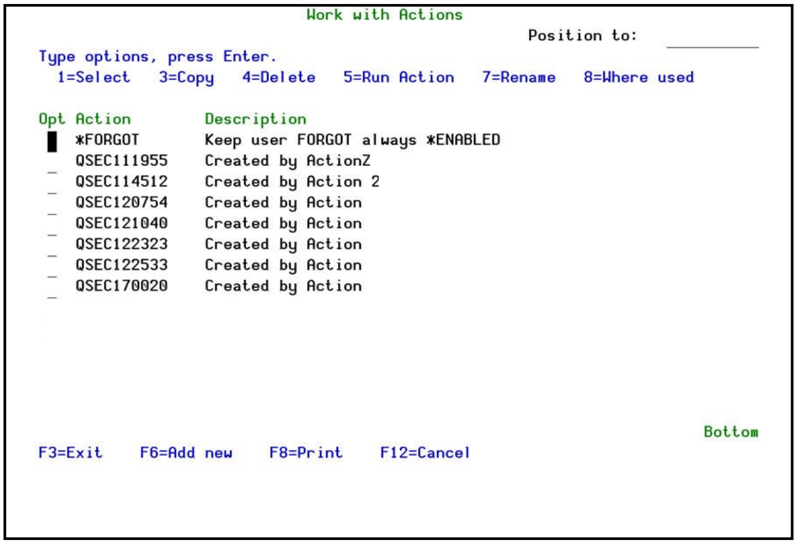
Working with Actions

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

If your rule includes actions (the **Action** parameter on the **Selection Rule** screen is not set to ***NONE**), the action definition screens appear automatically. You can also define and modify actions separately from the rule definition process.

To work with actions separately from rules:

1. Select **31** from the **Action** Main menu.



```
                              Work with Actions
                                                   Position to:  __________
 Type options, press Enter.
   1=Select   3=Copy   4=Delete   5=Run Action   7=Rename   8=Where used

 Opt Action        Description
  █  *FORGOT       Keep user FORGOT always *ENABLED
  _  QSEC111955    Created by ActionZ
  _  QSEC114512    Created by Action 2
  _  QSEC120754    Created by Action
  _  QSEC121040    Created by Action
  _  QSEC122323    Created by Action
  _  QSEC122533    Created by Action
  _  QSEC170020    Created by Action
                                                                     Bottom
 F3=Exit    F6=Add new    F8=Print    F12=Cancel
```

Figure 32: Work with Actions

2. Select an action to modify from the list or press **F6** to create a new action. The definition screens for alert messages and command scripts appear in sequence.

Defining Alert Messages

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

- E-mail over the Internet
- Local workstation message queue using the ***SNDMSG TOMSGQ*** command
- Local user message queue using the ***SNDMSG TOUSER*** command
- Remote user on another System i system over the SNADS network using the ***SNDNETMSG*** command
- SMS service to a cellular telephone
- Pager (beeper) message

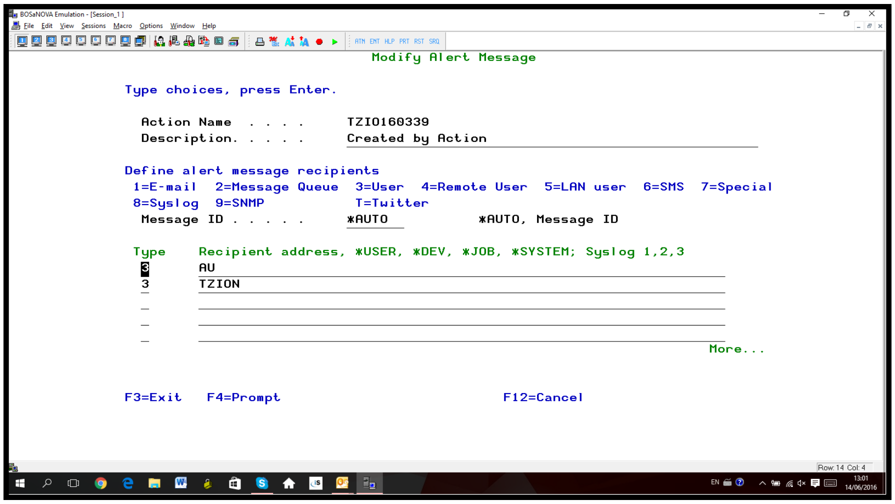
None of the above requires any special hardware (although you may implement hardware if your system is not linked to the internet). Sending Email requires you to have an active Email. SMS and Pager require you to be a user of an external service provider of such services as well. For details, call your distributor.

Some points:

- The exact interface to the Email, SMS and Pager can be adjusted by the user as needed.
- The message definition consists of a pre-defined message together with one or more recipient addresses. You may choose to use the default message text or you may select a user-defined message.
- The exact interface can be found in file ***SMZ4DTA/AUSOURCE***, programs ***AUALR1R*** (Email), ***AUALR6R*** (SMS), ***AUALR7R*** (Special)
- Up to 60 characters of the original log entry that is emailed by Action are inserted automatically to its subject.

To activate the user changes to the interface, follow this short procedure.

1. Modify the relevant program and compile into library ***SMZ4DTA***.
2. To define alert messages, select **31** from the **Action** Main menu.



BOSaNOVA Emulation - [Session_1]
File Edit View Sessions Macro Options Window Help
ATN ENT HLP PRT RST SRQ
Row: 14 Col: 4
EN
13:01
14/06/2016

```
                          Modify Alert Message

 Type choices, press Enter.

   Action Name  . . . .      TZI0160339
   Description. . . . .      Created by Action

 Define alert message recipients
  1=E-mail  2=Message Queue  3=User  4=Remote User  5=LAN user  6=SMS  7=Special
  8=Syslog  9=SNMP           T=Twitter
   Message ID . . . . . .    *AUTO           *AUTO, Message ID

  Type     Recipient address, *USER, *DEV, *JOB, *SYSTEM; Syslog 1,2,3
   3       AU
   3       TZION
   _
   _
   _
                                                                  More...

 F3=Exit   F4=Prompt                          F12=Cancel
```

Figure 33: Modify Alert Message

3. The message definition consists of a predefined message together with one or more recipient addresses. You may choose to use the default message text or you may select a user-defined message. An example of alert message modifications follows, in addition to an explanatory table.

Option	Description
Description	Description of the action
Message ID	Predefined message text to be sent ***AUTO** –Use the default message text **Message ID** – Name of a pre-defined alert message **F4** – Select pre- defined message from list or create new message
Type	Recipient type **1** – E-mail message **2** – Any specific message queue (*SNDMSG TOMSGQ*) **3** – User message queue (*SNDMSG TOUSR*) **4** – Remote system user (*SNDNETMSG*) **5** – Users or workstations on a LAN (*SNDNWSMSG*) **6** – SMS message to cellular telephone **7** – Message to beeper or pager**8** – Syslog 1/2/3 **9** – SNMP **T** – Twitter
Recipient Address	Recipient address formatted according to message type (See following table)

Recipient Addresses

The following table lists the valid recipient address types and formats.

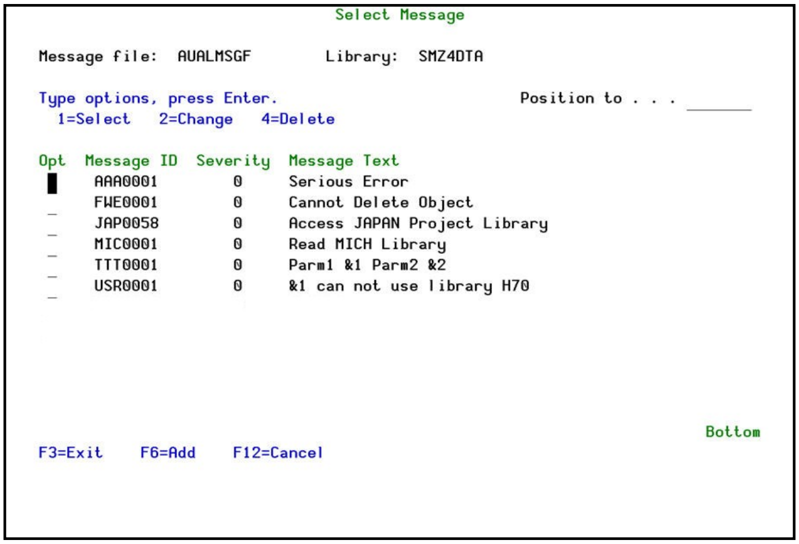
Message Type	Recipient Address Format
1 - E-mail	E-mail address in standard e-mail format (recipient@address)
2 - Message Queue	Fully qualified name of the message queue or **SYSOPR*
3 - User	User profile or IBM i (OS/400) group profile
4 - Network User	User profile & SNA address separated by a space (for example, USER SYSTEM)
5 - LAN User	Valid network user name or **DOMAIN* for all users on your domain
6 - SMS	Phone number including country code and area code as necessary
7 - Pager	Phone number and access codes for the pager service
8 - Syslog	Leave blank, the **SYSLOG** message will be sent according to the definitions in option 31. **Syslog Definitions**
9 - SNMP	Leave blank, the **SNMP** message will be sent according to the definitions in option 32. **SNMP Definitions**
T - Twitter	Leave blank, the **Twitter** message will be sent according to the definitions in option 33. **Twitter Definitions**

Predefined Messages

You have the option to send an alert message containing a pre-defined text message instead of the default message text. Pre-defined messages are stored in a special message file and are identified by a unique message ID.

Selecting Predefined Messages

1. Move the cursor to the **`Message ID`** field in the **`Alert Message`** screen and press **`F4`**. The **`Select Message`** screen appears.



```
                              Select Message

 Message file:  AUALMSGF        Library:  SMZ4DTA

 Type options, press Enter.                           Position to . . . _______
   1=Select   2=Change   4=Delete

 Opt  Message ID  Severity  Message Text
  _     AAA0001        0     Serious Error
  _     FWE0001        0     Cannot Delete Object
  _     JAP0058        0     Access JAPAN Project Library
  _     MIC0001        0     Read MICH Library
  _     TTT0001        0     Parm1 &1 Parm2 &2
  _     USR0001        0     &1 can not use library H70
  _









                                                                        Bottom
 F3=Exit    F6=Add    F12=Cancel
```

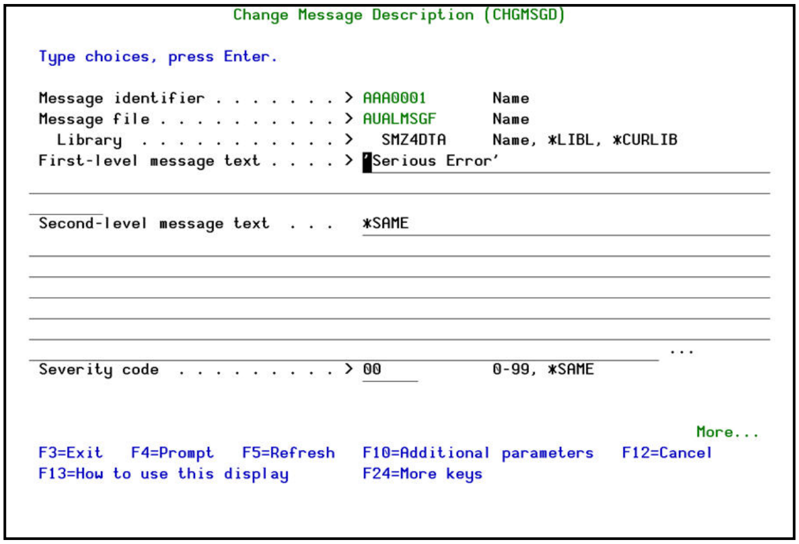
Figure 34: Select Message

2. Type **`1`** next to the desired message ID and press Enter. Press Enter a second time to confirm and continue.

Creating or Modifying Predefined Messages

1. Move the cursor to the **Message ID** field in the **Alert Message** screen.
2. Press **F4**. The **Select Message** screen appears.
3. Type **2** next to a pre-defined message to modify it, or press **F6** to create a new message. If you are modifying a message, you may have to select it a second time from the **Work with Message Description** screen.

The Change Message Description screen appears. This is the standard parameter screen for the *IBM i (OS/400)ADDMSGD* or *CHGMSGD* commands.



```
                     Change Message Description (CHGMSGD)

 Type choices, press Enter.

 Message identifier . . . . . . . > AAA0001       Name
 Message file . . . . . . . . . . > AVALMSGF      Name
   Library  . . . . . . . . . . . >   SMZ4DTA     Name, *LIBL, *CURLIB
 First-level message text . . . . > 'Serious Error'


 Second-level message text  . . .   *SAME





                                                                        ...
 Severity code  . . . . . . . . . > 00            0-99, *SAME


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

Figure 35: Change Message Description

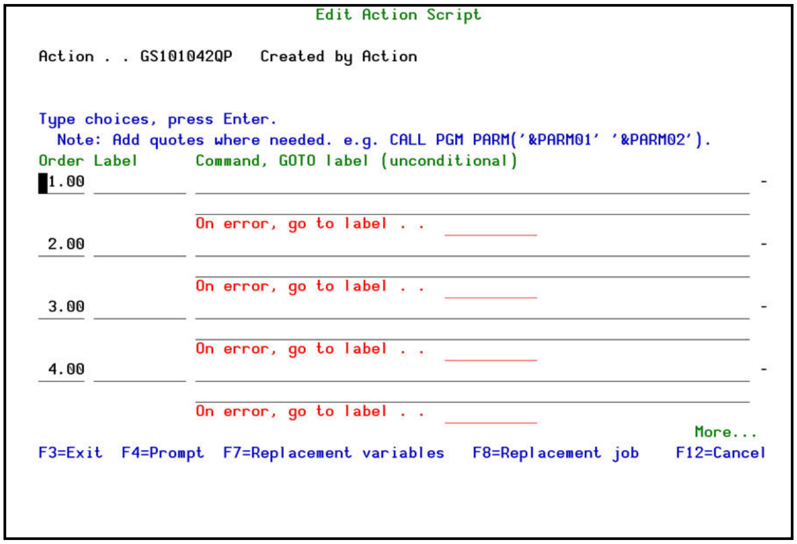
4. Type the parameters as listed in the following table. Only the listed parameters are relevant to this product. It is recommended that you do not modify any other parameters.

Parameter or Option	Description
Message Identifier	Unique message ID – Must be in the format AAA9999, where: **A** = Any alphabetic character (A-Z) **9** = Any number (0-9)
First Level Message Text	Message text up to 132 alphanumeric characters One or more substitution variables can be embedded in the message text string to indicate positional replacement fields that substitute variable data into the message text. Variables must be specified in the form &n, where n is a 1 or 2 digit number identifying the journal data field that is to be substituted (**1** for first field, **2** for the second, and so on.). NOTE: This feature is intended for advanced users only. Please refer to IBM documentation for detailed instructions on the use of variables in messages.
Message Data Field Formats	If you have defined any replacement variables, you must define the data type and length for each variable. This is for advanced users only.

5. Press **Enter** twice.
6. Type **1** to the left of the new or modified message to select it and press **Enter** again to continue.

Defining Command Scripts

Once you have finished defining alert messages, the **Action Script** screen appears automatically.



```
                              Edit Action Script

 Action . . GS101042QP   Created by Action


 Type choices, press Enter.
   Note: Add quotes where needed. e.g. CALL PGM PARM('&PARM01' '&PARM02').
 Order Label      Command, GOTO label (unconditional)
  1.00 __________ ____________________________________________________________ -
                  ____________________________________________________________
                  On error, go to label . . __________
  2.00 __________ ____________________________________________________________ -
                  ____________________________________________________________
                  On error, go to label . . __________
  3.00 __________ ____________________________________________________________ -
                  ____________________________________________________________
                  On error, go to label . . __________
  4.00 __________ ____________________________________________________________ -
                  ____________________________________________________________
                  On error, go to label . . __________
                                                                       More...
 F3=Exit  F4=Prompt  F7=Replacement variables   F8=Replacement job    F12=Cancel
```

Figure 36: Edit Action Script

1. Use this screen to define one or more command scripts to run whenever the rule conditions are met.
2. Press **Enter** to confirm

Commands execute sequentially according to a user-defined order. Commands may include replacement variables that extract data from the history log record and insert it as command parameters. **Action** also supports conditional branching in the event that an error occurs during script execution.

The following table summarizes the options and parameters contained in the **Action Script** screen.

Parameter	Description
Order	Order in which the commands execute
Label	Optional alphanumeric label for the current line Used for the **On Error Go To** feature
Command	Command text including all parameters
On error, go to label	Conditional branch to the line indicated by the label in the event a script error results from the command on the current line
F4	Open prompt window for command parameters and options
F7	Select a variable from pop-up window and insert it at the current cursor position Variables insert contents of journal entry data fields as command parameters

Replacement Variables

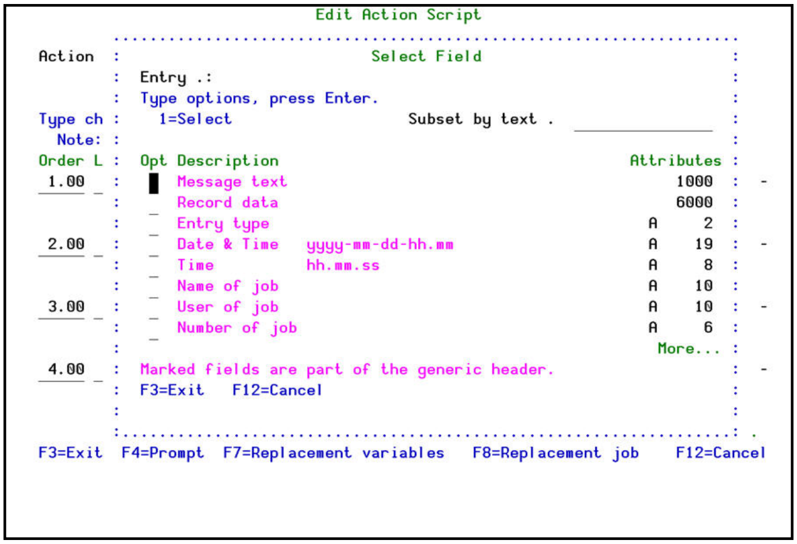
Replacement variables enable you to extract data from the history log record and insert it into command scripts as parameters. For example, in a command script intended to terminate a suspicious job, the ***Job Name***, ***Job User*** and ***Job Number*** information would be extracted from the journal entry and inserted into the appropriate parameter fields for the ***ENDJOB*** command. The command with replacement values would appear as follows:

ENDJOB JOB(&ZRJOB/&ZRUSER/&ZRNBR) OPTION(*IMMED)

Replacement variables are always preceded by the '**&**' character. If you select the data field from a list using **F7**, this character is inserted automatically.

To insert a replacement parameter, follow this procedure.

1. Move the cursor to the appropriate location in your command script in the **Action Script** window.
2. Press **F7** to display the **Select Field** popup window.



```
                             Edit Action Script
          ..................................................................
 Action   :                        Select Field                            :
          :  Entry .:                                                      :
          :  Type options, press Enter.                                    :
 Type ch  :    1=Select                   Subset by text .  _______________ :
   Note:  :                                                                :
 Order L  :  Opt Description                                   Attributes :
  1.00 _  :  █   Message text                                       1000  :  -
          :  _   Record data                                        6000  :
          :  _   Entry type                                    A       2  :
  2.00 _  :  _   Date & Time    yyyy-mm-dd-hh.mm               A      19  :  -
          :  _   Time           hh.mm.ss                       A       8  :
          :  _   Name of job                                   A      10  :
  3.00 _  :  _   User of job                                   A      10  :  -
          :  _   Number of job                                 A       6  :
          :                                                      More...  :
  4.00 _  :  Marked fields are part of the generic header.                :  -
          :  F3=Exit   F12=Cancel                                         :
          :                                                               :
          :...............................................................: .
 F3=Exit  F4=Prompt  F7=Replacement variables   F8=Replacement job    F12=Cancel
```

Figure 37: Replacement variables

3. Select the desired field from which you would like to extract data, and press **Enter**.

Conditional Branching

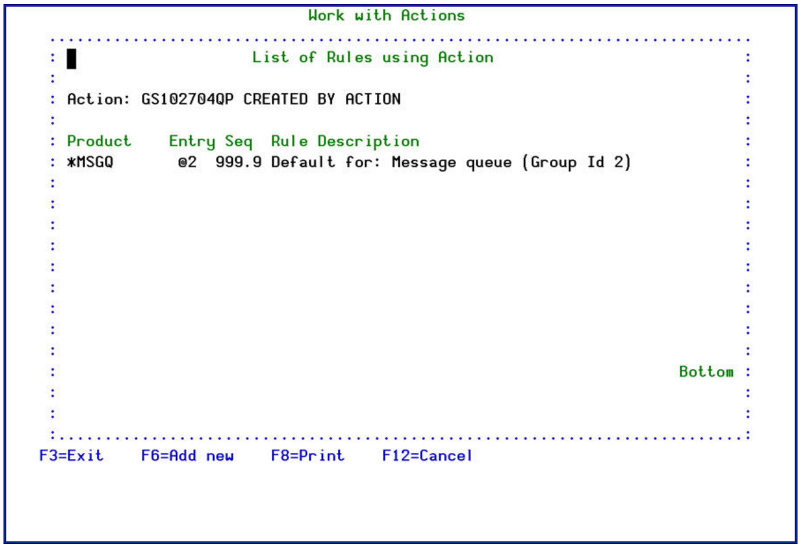
Action command scripts support conditional branching in the event of a script error. The **`Label`** field identifies a command line for branching purposes. The **`On Error Go To Label`** field instructs the script to branch to the line indicated by the label in the event that an error is generated by the command.

To end script processing in the event of a script error, insert a label on a blank line following the last command. Enter that label in the **`On Error Go To Label`** field on each active command line.

Delete an action

To delete an action make sure it's not being used.

1. To check that, type **`8=Where used`** in the **`Opt`** field of the action from a list at the **`Work with Actions`** screen. The **`List of Rules using Action`** screen appears.



```
                          Work with Actions
  ............................................................................
  :                        List of Rules using Action                        :
  :                                                                          :
  : Action: GS102704QP CREATED BY ACTION                                     :
  :                                                                          :
  : Product    Entry Seq  Rule Description                                   :
  : *MSGQ         @2  999.9 Default for: Message queue (Group Id 2)          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                          :
  :                                                                   Bottom :
  :                                                                          :
  :                                                                          :
  :..........................................................................:
 F3=Exit    F6=Add new    F8=Print    F12=Cancel
```

Figure 38: List of Rules using Action

2. Change the action definitions in the rule to be:
   - Perform action . . . . . N Y=Yes N=No
   - Action . . . . *NONE Name, *NONE, *ADD, F4=Prompt
3. Type **`4`** at the **`Work with Actions`** screen to delete the action from the list.

Testing and Debugging Your Rules

Real-time detection rules are, in fact, small programs. They require testing, debugging and maintenance to ensure that they work properly. The following suggestions will help you with this process.

- Make sure that the all actions and events that you wish to include in your rule are captured by the IBM i (OS/400) audit settings (current setting, user activity auditing, and object auditing). If you create a real-time detection rule for an event that is not captured by the IBM i (OS/400) audit settings, it will not function.
- Enable logging for all real-time rules. The history log provides you with a complete audit trail for your rules. This information is invaluable when testing and debugging complex rules.
- Test the filter conditions in your rules before adding actions (alert messages and command scripts). Use the **Query** and/or **Display Audit Log** features to examine the history log entries. Verify that the log contains all the events that you wish to capture and only those events that you wish to capture.
- Create and test your actions before including them in a rule.
- Temporarily disable any other rules that include the same events or otherwise conflict with the rule that you are testing. Set the **Log** parameter to '**N**' and the Action parameter to ***NONE*** to accomplish this.

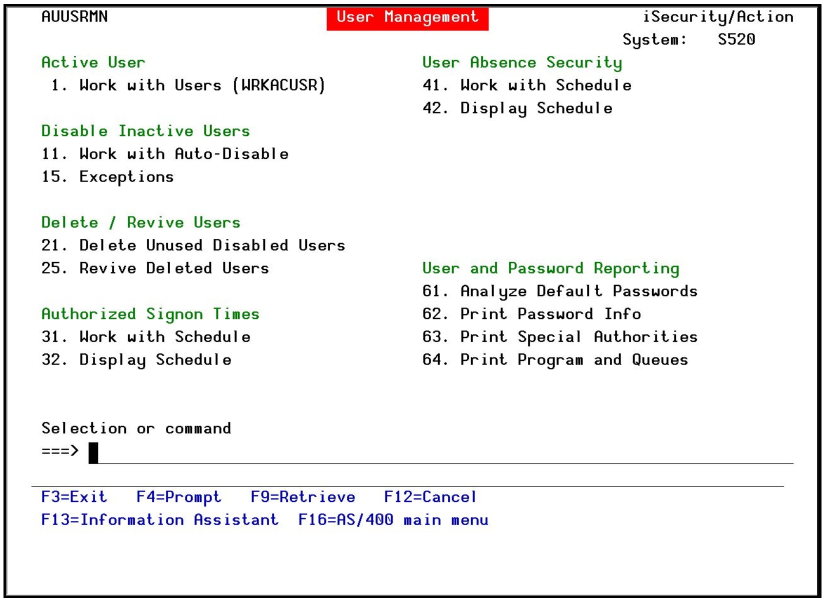
NOTE: Do not forget to re-activate your rules after you finish testing!

Chapter 4: User Management

This chapter presents several powerful security tools that control the ability of users to signon to the system. These tools enhance active system security by enabling you to perform the following tasks:

- View and modify security parameters in user profiles using a convenient wizard interface
- Automatically disable inactive users
- Restrict user signon to specific hours and days
- Prevent user signon during planned absences or following termination
- Analyze default passwords for effectiveness

These options are accessed directly from Action by selecting **`21. User Management`** from the main screen. The **`User Management`** menu appears.



```
AUUSRMN                         User Management                 iSecurity/Action
                                                               System:    S520
Active User                                User Absence Security
 1. Work with Users (WRKACUSR)             41. Work with Schedule
                                           42. Display Schedule
Disable Inactive Users
11. Work with Auto-Disable
15. Exceptions

Delete / Revive Users
21. Delete Unused Disabled Users
25. Revive Deleted Users                   User and Password Reporting
                                           61. Analyze Default Passwords
Authorized Signon Times                    62. Print Password Info
31. Work with Schedule                     63. Print Special Authorities
32. Display Schedule                       64. Print Program and Queues


Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 39: User Management Menu

Working with Users

-

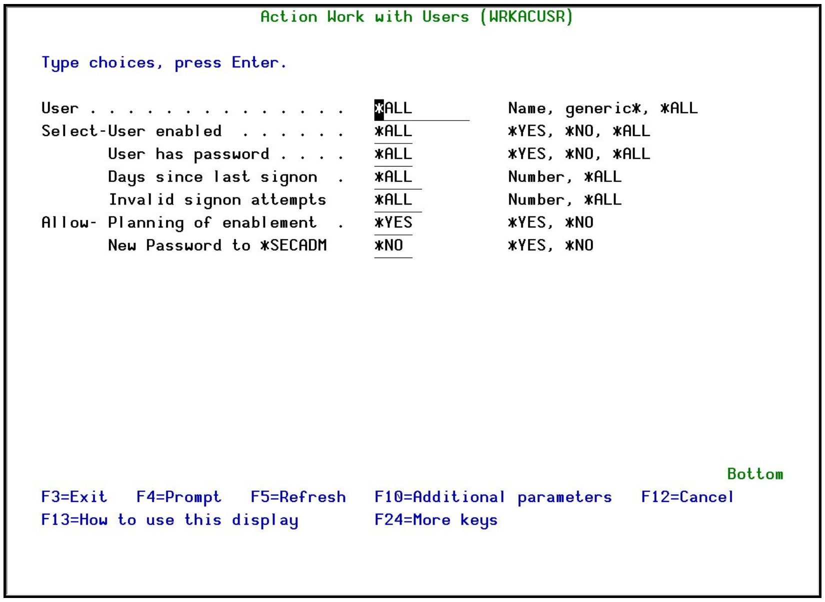
Overview

The **`Work with Users Wizard`** enables you to view and modify several security-related parameters in the user profile by using a user-friendly wizard interface. You can view and work with many different users at once and compare settings between different users.

The security officer can use this tool to review all users at-a-glance and immediately disable suspicious users. One-key access is provided to many of the other user signon tools.

Working with Users Wizard

1. To start the **Work with Users** wizard, select **1** from the **User Management** menu. The **Work with Users** screen appears, offering you several options to display filtered subsets of users.



```
                          Action Work with Users (WRKACUSR)

 Type choices, press Enter.

 User . . . . . . . . . . . . . .   *ALL          Name, generic*, *ALL
 Select-User enabled  . . . . . .   *ALL          *YES, *NO, *ALL
        User has password . . . .   *ALL          *YES, *NO, *ALL
        Days since last signon  .   *ALL          Number, *ALL
        Invalid signon attempts     *ALL          Number, *ALL
 Allow- Planning of enablement  .   *YES          *YES, *NO
        New Password to *SECADM     *NO           *YES, *NO

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

Figure 40: Working with Users

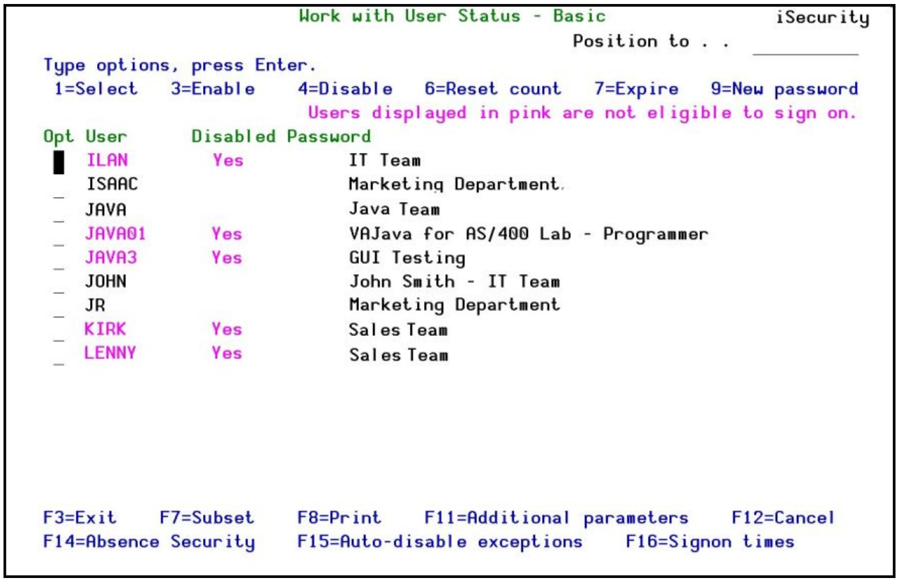
2. Set parameters according to the following options.

Parameter	Description
User	***ALL** = Display all users **Generic*** = Display all users beginning with text preceding the * **Name** = Display a specific user profile
User enabled	***YES** = Display enabled users, with passwords, who can signon ***NO** = Display disabled users and those who cannot signon ***ALL** = Display users irrespective of status
User has password	***YES** = Display only users whose password has expired ***NO** = Display only users whose password has not expired ***ALL** = Display users irrespective of password expiration
Days since last signon	***Number** = Display only users who have not signed on for at least the specified number of days ***ALL** = Display users irrespective days since last signon
Invalid signon attempts	***Number** = Display only users who have not signed on for at least the specified number of days ***ALL** = Display users irrespective of days since last signon
Allow Planning of enablement	***YES** = ***NO** =
Allow New Password to *SECADM	***YES** = ***NO** =

The **Work with Users** Wizard consists of several screens, each containing several related parameters. The same function key options are available on all screens. On each of these screens, users that cannot signon to the system are displayed in pink.

Screen 1: Working with User Status - Basic

The first screen shows whether individual users can signon to the System i system. To signon, users must be enabled and have a valid, non-expired password.

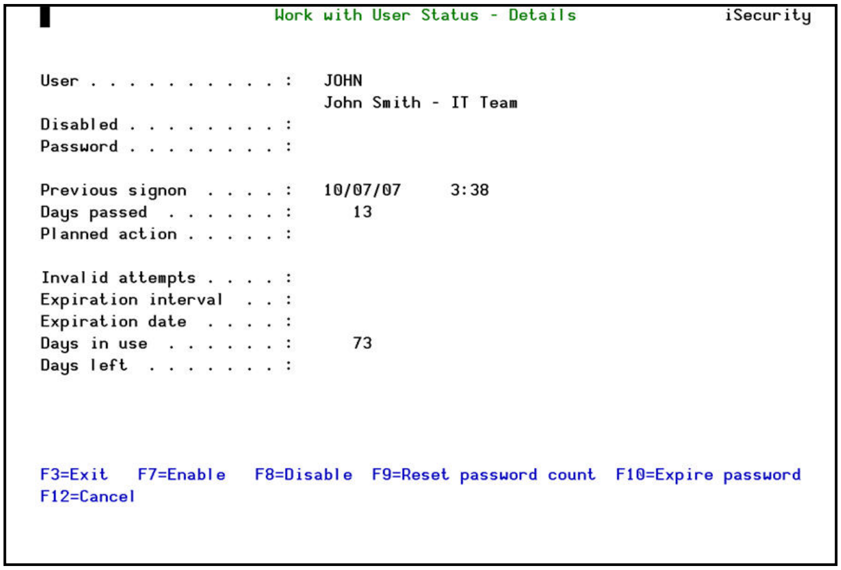


```
                           Work with User Status - Basic               iSecurity
                                                        Position to . .  __________
 Type options, press Enter.
  1=Select   3=Enable    4=Disable   6=Reset count   7=Expire   9=New password
                        Users displayed in pink are not eligible to sign on.
 Opt User        Disabled Password
  █  ILAN         Yes          IT Team
  _  ISAAC                     Marketing Department
  _  JAVA                      Java Team
  _  JAVA01       Yes          VAJava for AS/400 Lab - Programmer
  _  JAVA3        Yes          GUI Testing
  _  JOHN                      John Smith - IT Team
  _  JR                        Marketing Department
  _  KIRK         Yes          Sales Team
  _  LENNY        Yes          Sales Team






 F3=Exit    F7=Subset    F8=Print    F11=Additional parameters    F12=Cancel
 F14=Absence Security    F15=Auto-disable exceptions    F16=Signon times
```

Figure 41: Working with User Status – Basic

Parameter	Description
Opt	**1** = Display all parameters for the selected user profile (see below) **3** = Enable user profile **4** = Disable user profile **6** = Reset invalid signon attempt counter – prevents automatic disabling of this user due to excessive signon errors **7** = Set password to 'expired' – this user must change password at next signon
Disabled	**Blank** = User profile is enabled **Yes** = User profile is disabled
Password	**Blank** = User profile has a valid password and can signon **None** = No password is associated with this user profile and he cannot signon
F7	Display a subset of user profiles filtered according to status parameters (available on all screens)
F11	Display the next of the three parameter screens for the currently displayed user profiles
F14	Temporarily disable users during planned absences (for example, vacation, sick, leave of absence), or permanently delete users leaving the organization
F15	Specify users that should never be disabled automatically, even if they have not signed on for a long period of time (inactive user)
F16	Restrict user signon to predefined working hours

To display all parameters for a single user, type **1** in the **Opt** field for the required user. The **Work with User Status - Details** screen appears. Use the function keys to modify parameters as described in the table.



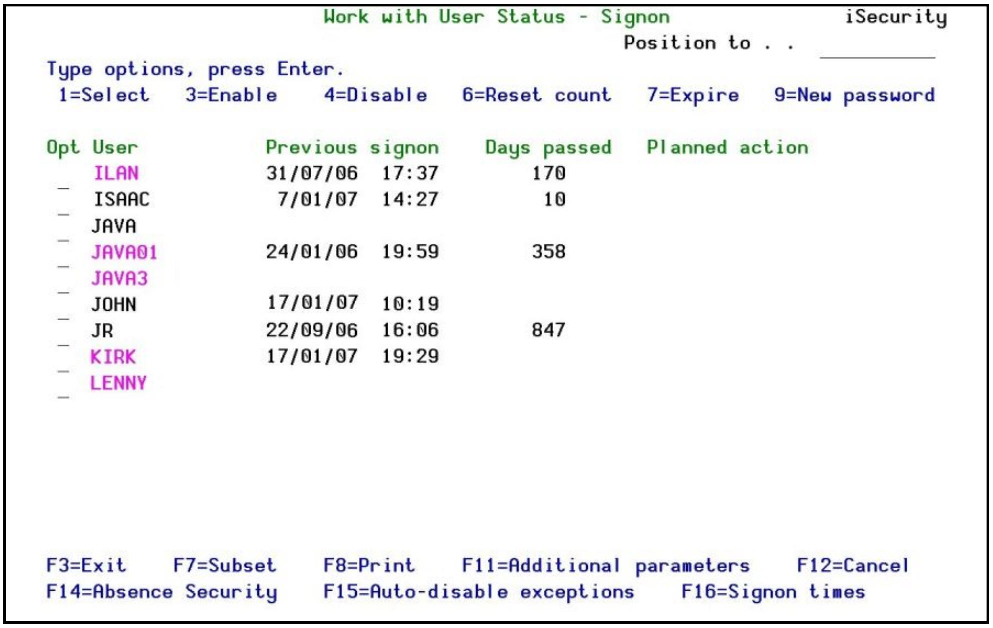
```
                         Work with User Status - Details              iSecurity


 User . . . . . . . . . . . :   JOHN
                                John Smith - IT Team
 Disabled . . . . . . . . . :
 Password . . . . . . . . . :

 Previous signon  . . . . . :   10/07/07     3:38
 Days passed  . . . . . . . :      13
 Planned action . . . . . . :

 Invalid attempts . . . . . :
 Expiration interval  . . . :
 Expiration date  . . . . . :
 Days in use  . . . . . . . :      73
 Days left  . . . . . . . . :




 F3=Exit   F7=Enable   F8=Disable  F9=Reset password count  F10=Expire password
 F12=Cancel
```

Figure 42: Working with User Status - Details

Parameter	Description
F7	Enable user profile
F8	Disable user profile
F9	Reset invalid signon attempt counter – prevents automatic disabling of this user due to excessive signon errors
F10	Set password to ‘expired’ – user must change password at next signon

Screen 2: Working with User Status - Signon

This screen displays recent signon statistics for each user profile. In addition, the scheduled date of any automatic actions (disable or delete) by the **Action** absence control feature is displayed.



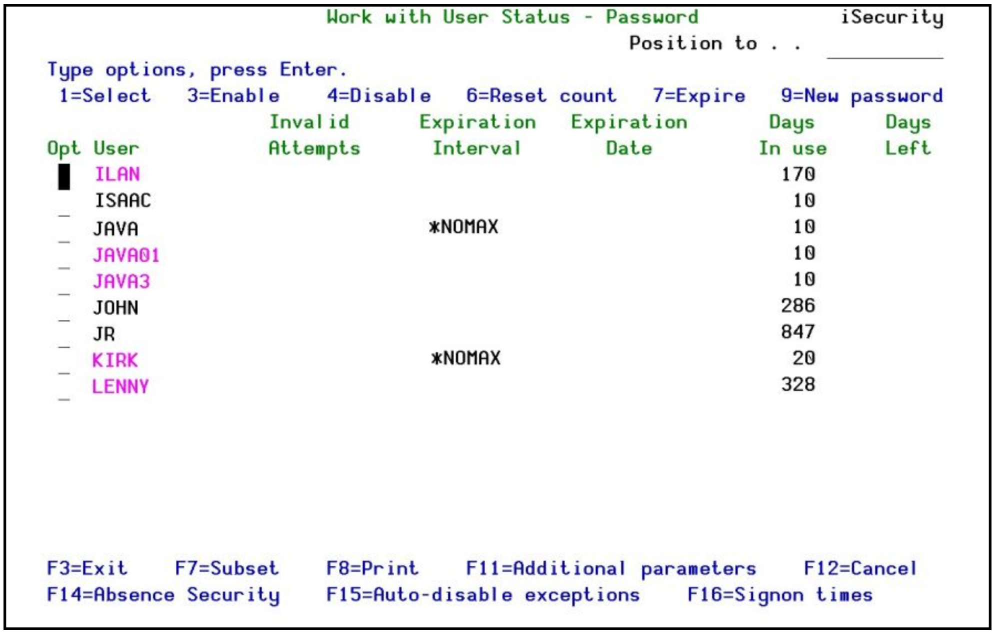
```
                        Work with User Status - Signon           iSecurity
                                                   Position to . .  __________
 Type options, press Enter.
  1=Select   3=Enable   4=Disable   6=Reset count   7=Expire   9=New password

 Opt User            Previous signon    Days passed   Planned action
  _  ILAN            31/07/06  17:37       170
  _  ISAAC            7/01/07  14:27        10
  _  JAVA
  _  JAVA01          24/01/06  19:59       358
  _  JAVA3
  _  JOHN            17/01/07  10:19
  _  JR              22/09/06  16:06       847
  _  KIRK            17/01/07  19:29
  _  LENNY

 F3=Exit   F7=Subset   F8=Print   F11=Additional parameters   F12=Cancel
 F14=Absence Security   F15=Auto-disable exceptions   F16=Signon times
```

Figure 43: Working with User Status - Signon

Parameter	Description
Opt	**1** = Display all parameters for selected user profile **3** = Enable user profile **4** = Disable user profile **6** = Reset invalid signon attempt counter – prevents automatic disabling of this user due to excessive signon errors **7** = Set password to 'expired' – this user must change password at next signon
Previous Signon	Date and time of previous signon for this user profile
Days Passed	Days since previous signon for this user profile
Planned Action	Displays the date of planned absence control actions (Delete or disable) for this user profile

Screen 3: Working with User Status - Password

This screen displays the number of invalid signon attempts and the expiration status of user passwords. This information makes it possible for the security officer to verify that users change their passwords in accordance with the security policy.



```
                          Work with User Status - Password          iSecurity
                                                     Position to . .  __________
 Type options, press Enter.
  1=Select   3=Enable   4=Disable   6=Reset count   7=Expire   9=New password
                     Invalid      Expiration   Expiration        Days     Days
 Opt User            Attempts     Interval       Date            In use   Left
 _   ILAN                                                         170
 _   ISAAC                                                         10
 _   JAVA                          *NOMAX                          10
 _   JAVA01                                                        10
 _   JAVA3                                                         10
 _   JOHN                                                         286
 _   JR                                                           847
 _   KIRK                          *NOMAX                          20
 _   LENNY                                                        328





 F3=Exit    F7=Subset    F8=Print    F11=Additional parameters    F12=Cancel
 F14=Absence Security    F15=Auto-disable exceptions    F16=Signon times
```

Figure 44: Working with User Status - Password

Parameter	Description
Opt	**1** = Display all parameters for selected user profile **3** = Enable user profile **4** = Disable user profile **6** = Reset invalid signon attempt counter – prevents automatic disabling of this user due to excessive signon errors 7 = Set password to 'expired' – this user must change password at next signon
Invalid Attempts	**Blank** = User profile is enabled **No** = User profile is disabled
Expiration Interval	Number of days between required password changes
Expiration Date	Next password expiration date
Days in Use	Number of days the current password has been in use
Days Left	Number of days before the current password expires

Disable Inactive Users

The presence of valid but inactive user profiles can pose a potentially serious security threat. Hackers can exploit these profiles to gain access to critical data via FTP, ODBC connectivity or other methods even without knowing the password.

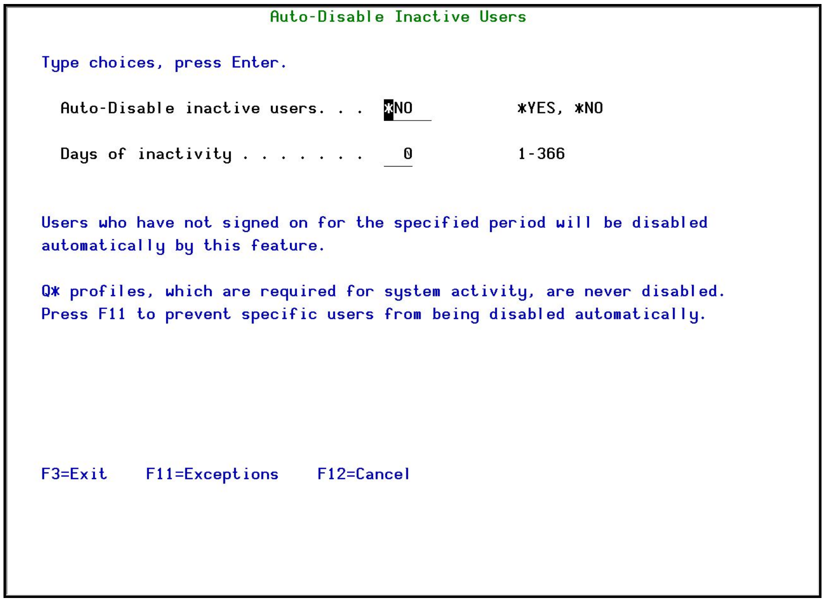
For this reason, it is always a good idea to periodically audit your system and disable any users who have not signed on recently. The Working with Users Wizard, discussed in the previous section, is an excellent tool for performing such a review and manually disabling inactive users.

Audit includes the **`Auto-Disable`** feature, which enables you to disable inactive user profiles automatically after a specified period. Automatic disabling applies to any user who has not signed on for the specified number of days. You can also designate specific users as exceptions, who cannot be disabled automatically. IBM i (OS/400) system generated profiles (Prefixed by the letter '**`Q`**') are never automatically disabled.

Working with Auto-Disable

To define when to disable inactive users:

1. Select **11. Work with Auto-Disable** from the **User Management** menu. The **Auto-Disable Inactive Users** screen appears.



```
                         Auto-Disable Inactive Users

 Type choices, press Enter.

   Auto-Disable inactive users. . .  *NO            *YES, *NO

   Days of inactivity . . . . . . .    0            1-366


 Users who have not signed on for the specified period will be disabled
 automatically by this feature.

 Q* profiles, which are required for system activity, are never disabled.
 Press F11 to prevent specific users from being disabled automatically.




 F3=Exit    F11=Exceptions    F12=Cancel
```

Figure 45: Auto-Disable Inactive Users screen

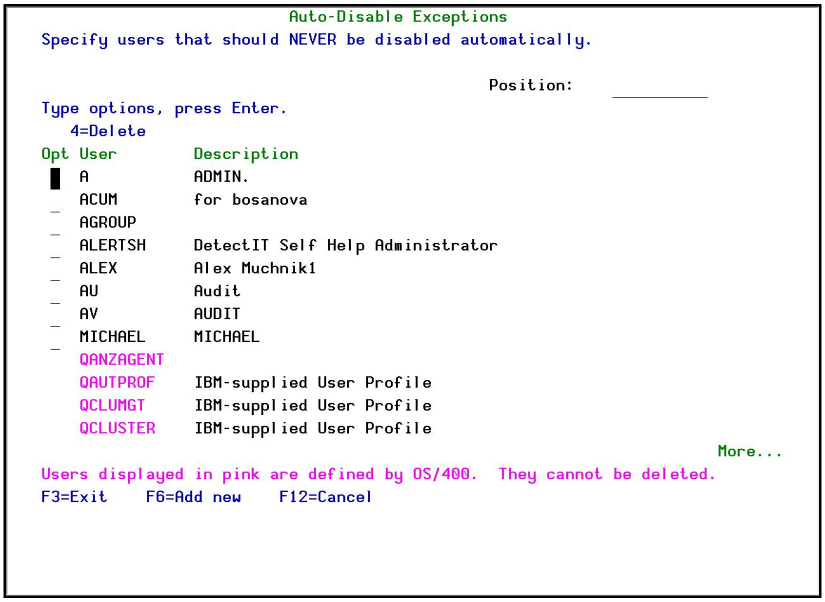
Parameters	Description
Auto-Disable inactive users	***NO** = Inactive users are not automatically disabled. ***YES** = Inactive Users are automatically disabled after they have been inactive for the number of days in the **Days of inactivity** parameter.
Days of inactivity	Enter a number between 1 -366.

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

Exceptions

To define the exceptions for inactive user disabling:

1. Select **`12. Disable Exceptions`** from the **`User Management`** menu. The **`Auto-Disable Exceptions`** screen appears.



```
                          Auto-Disable Exceptions
Specify users that should NEVER be disabled automatically.

                                              Position:    __________
Type options, press Enter.
   4=Delete
Opt User        Description
█   A           ADMIN.
_   ACUM        for bosanova
_   AGROUP
_   ALERTSH     DetectIT Self Help Administrator
_   ALEX        Alex Muchnik1
_   AU          Audit
_   AV          AUDIT
_   MICHAEL     MICHAEL
    QANZAGENT
    QAUTPROF    IBM-supplied User Profile
    QCLUMGT     IBM-supplied User Profile
    QCLUSTER    IBM-supplied User Profile
                                                                More...
Users displayed in pink are defined by OS/400.  They cannot be deleted.
F3=Exit    F6=Add new    F12=Cancel
```

Figure 46: Auto-Disable Exceptions screen

2. Press **`F6=Add`** new. The **`Add Users to Exception List`** appears.
3. Enter the profiles not to disable and press **`Enter`**.

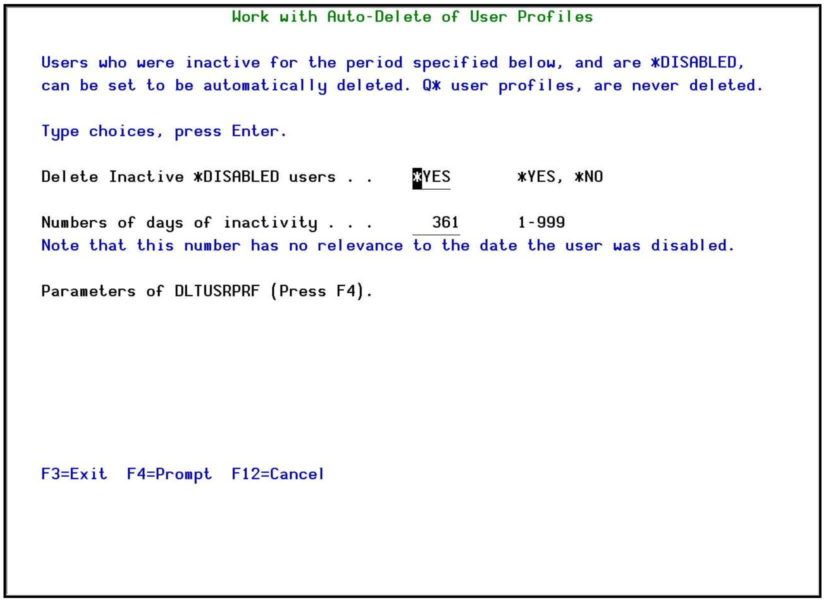
Delete/Revive Users

You can set a time period after which disabled, inactive users are automatically deleted. If a user is deleted by mistake, you can revive the user.

Delete Unused Disabled Users

To define when to delete disabled, inactive users:

1. Select **`26. Delete Unused Disabled Users`** from the **`User Management`** menu. The **`Work with Auto-Delete of User Profiles`** screen appears.



```
                    Work with Auto-Delete of User Profiles

 Users who were inactive for the period specified below, and are *DISABLED,
 can be set to be automatically deleted. Q* user profiles, are never deleted.

 Type choices, press Enter.

 Delete Inactive *DISABLED users . .    *YES       *YES, *NO

 Numbers of days of inactivity . . .      361      1-999
 Note that this number has no relevance to the date the user was disabled.

 Parameters of DLTUSRPRF (Press F4).






 F3=Exit  F4=Prompt  F12=Cancel
```

Figure 47: Working with Auto-Delete of User Profiles screen

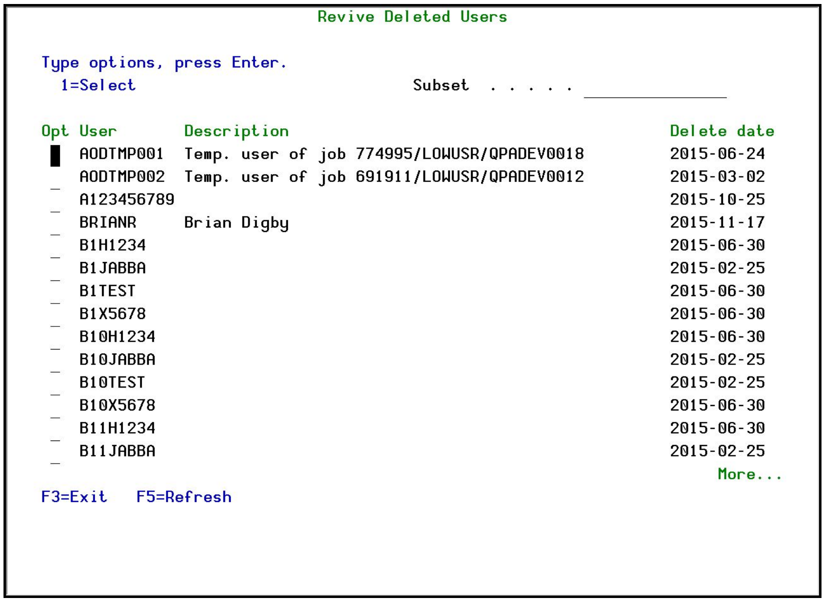
Parameters	Description
`Delete Inactive *DISABLED users`	**`*NO`** = Inactive disabled users are not automatically deleted. **`*YES`** = Inactive disabled users are automatically deleted after they have been inactive for the number of days in the **`Number of days of inactivity`** parameter.
`Number of days of inactivity`	Enter a number between 1 -999. This parameter and the **`Days of inactivity`** parameter in the **`Auto- Disable Inactive Users`** screen start counting from the same date. So, for example, if you want to disable a user after 60 days and then delete the user after a further 30 days, set this parameter to 90.
`Parameters of DLTUSRPRF (Press F4)`	Press **`F4`** to open the **`DLTUSRPRF`** screen and set the parameters for when the inactive, disabled users are deleted.

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

Revive Deleted Users

To restore a deleted user:

1. Select **25. Revive Deleted Users** from the **User Management** menu. The **Revive Deleted Users** screen appears.



```
                              Revive Deleted Users

 Type options, press Enter.
   1=Select                             Subset  . . . . .  _______________

 Opt User       Description                                         Delete date
  █  AODTMP001  Temp. user of job 774995/LOWUSR/QPADEV0018          2015-06-24
  _  AODTMP002  Temp. user of job 691911/LOWUSR/QPADEV0012          2015-03-02
  _  A123456789                                                     2015-10-25
  _  BRIANR     Brian Digby                                         2015-11-17
  _  B1H1234                                                        2015-06-30
  _  B1JABBA                                                        2015-02-25
  _  B1TEST                                                         2015-06-30
  _  B1X5678                                                        2015-06-30
  _  B10H1234                                                       2015-06-30
  _  B10JABBA                                                       2015-02-25
  _  B10TEST                                                        2015-02-25
  _  B10X5678                                                       2015-06-30
  _  B11H1234                                                       2015-06-30
  _  B11JABBA                                                       2015-02-25
                                                                         More...
 F3=Exit   F5=Refresh
```

Figure 48: Revive Deleted Users screen

2. Select the User to be restored and press **1=Select**. The **Create User Profile** screen appears.
3. Press **Enter**. The user is restored.

Authorized Signon Times

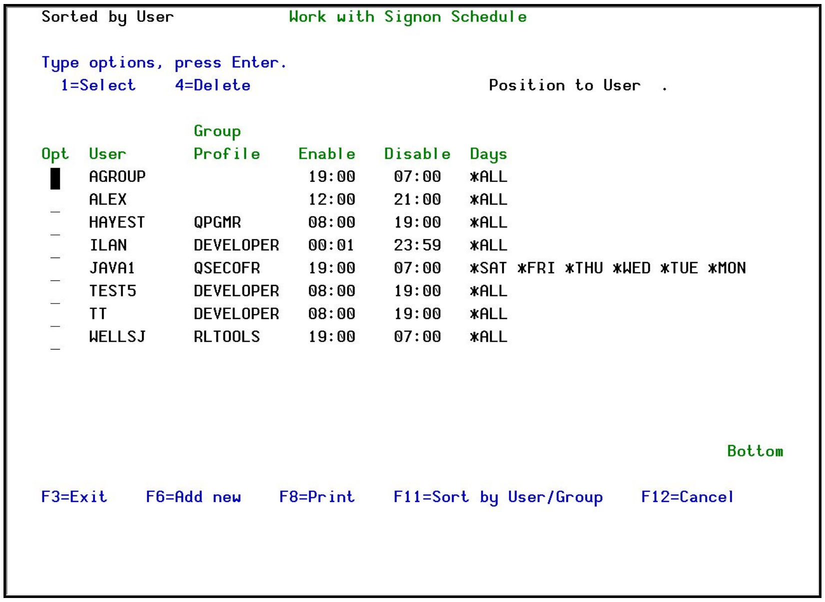
Even valid user profiles have the potential for abuse. A common hacker trick is to obtain a user’s password and use it to signon after the user has left work to access programs and data with that user’s authorities. With this method, a dishonest employee can bypass object level security and remain invisible to subsequent audit.

An effective defense against this scenario would be to restrict user signon to authorized working hours. **Audit** includes a user-friendly tool for defining authorized signon periods for users, by time and day of the week.

Working with Signon Schedule

To define the permitted signon times for users:

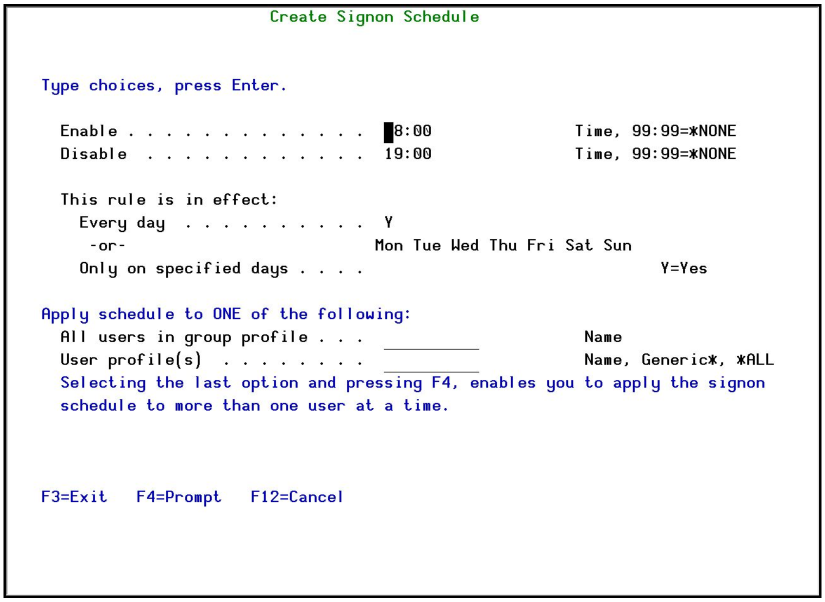
1. Select **31. Work with Schedule** from the **User Management** menu. The **Work with Signon Schedule** screen appears.



```
Sorted by User             Work with Signon Schedule

Type options, press Enter.
  1=Select     4=Delete                          Position to User   .

               Group
Opt  User      Profile     Enable    Disable   Days
_    AGROUP                 19:00     07:00    *ALL
_    ALEX                   12:00     21:00    *ALL
_    HAYEST    QPGMR        08:00     19:00    *ALL
_    ILAN      DEVELOPER    00:01     23:59    *ALL
_    JAVA1     QSECOFR      19:00     07:00    *SAT *FRI *THU *WED *TUE *MON
_    TEST5     DEVELOPER    08:00     19:00    *ALL
_    TT        DEVELOPER    08:00     19:00    *ALL
_    WELLSJ    RLTOOLS      19:00     07:00    *ALL

                                                                    Bottom

F3=Exit    F6=Add new    F8=Print    F11=Sort by User/Group    F12=Cancel
```

Figure 49: Working with Signon Schedule screen

2. Press **F6=Add** new. The **Create Signon Schedule** appears.



```
                         Create Signon Schedule


Type choices, press Enter.

  Enable . . . . . . . . . . . . .  8:00                Time, 99:99=*NONE
  Disable  . . . . . . . . . . . .  19:00               Time, 99:99=*NONE

  This rule is in effect:
    Every day  . . . . . . . . . .  Y
     -or-                          Mon Tue Wed Thu Fri Sat Sun
    Only on specified days . . . .                             Y=Yes

Apply schedule to ONE of the following:
  All users in group profile . . .  __________          Name
  User profile(s)  . . . . . . . .  __________          Name, Generic*, *ALL
  Selecting the last option and pressing F4, enables you to apply the signon
  schedule to more than one user at a time.



F3=Exit   F4=Prompt   F12=Cancel
```

Figure 50: Create Signon Schedule screen

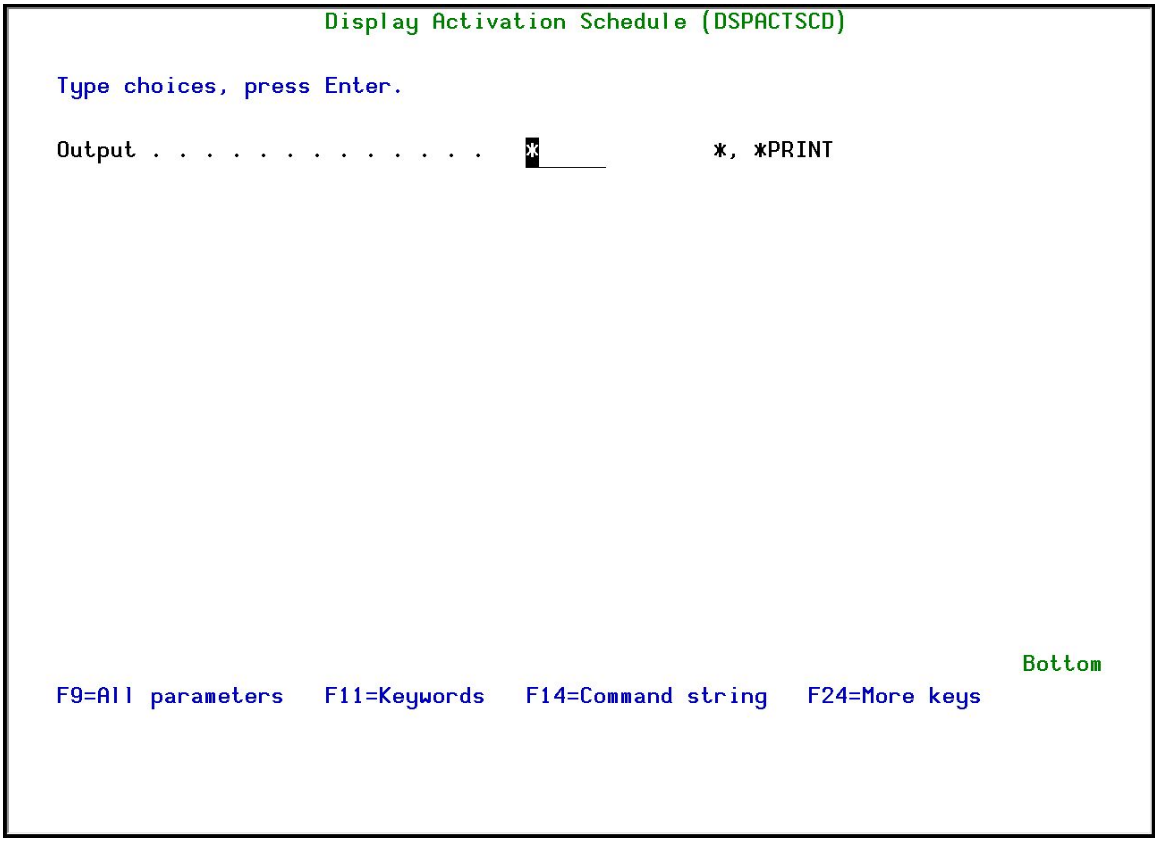
Parameters	Description
Enable/Disable	Enter the time range when the user can sign on. The day starts at 00:00 and finishes at 23:59. If the enable time is before the disable time (for example enable at 22:00 and disable at 05:00), then the disable time is for the following day.
Rule is in effect every day	**Y** = the sign on rule is valid for all days of the week.
Rule is in effect only on specified days	Enter **Y** for each specific day for which the signon rule is valid.
All users in group profile	If you enter a Group Profile, all users that belong to the Group Profile will have this signon schedule. If you enter a Group Profile, do not enter a User Profile name.
User profile (s)	Enter a user profile. **Name** = The sign on schedule is only for this specific profile **Generic*** = The sign on schedule is for this group of profiles ***ALL** = The sign on schedule is for all users

3. Enter your parameters and press Enter. The updated schedule appears in the **Work with Signon Schedule** screen.

Display Signon Schedule

To display the signon schedule:

1. Select **32. Display Schedule** from the **User Management** menu. The **Display Activation Schedule** screen appears.



```
                    Display Activation Schedule (DSPACTSCD)

 Type choices, press Enter.

 Output . . . . . . . . . . . . .   *____         *, *PRINT

                                                                        Bottom
 F9=All parameters   F11=Keywords   F14=Command string   F24=More keys
```

Figure 51: Display Activation Schedule screen

2. Select either ***** to display the report or ***PRINT** to send the report to a printer and press **Enter**. The report is produced.

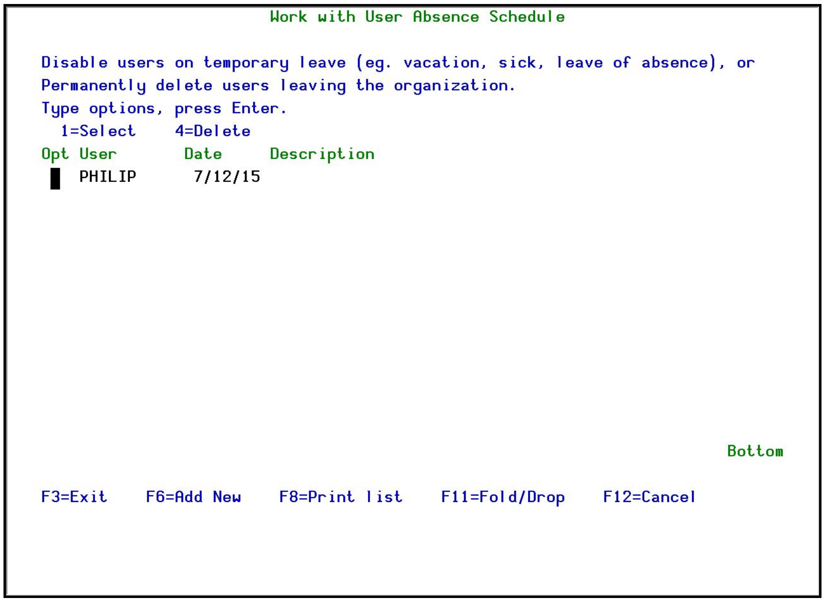
User Absence Security

Another common security risk occurs when an authorized user is away on temporary leave (for example, vacation, sick leave, maternity leave, business trips, and so on.) or leaves the organization. Action enables you make certain that nobody can signon with specific user profiles during such scheduled absences by disabling or deleting user profiles automatically on a specific date.

Working with Absence Schedule

To define absences:

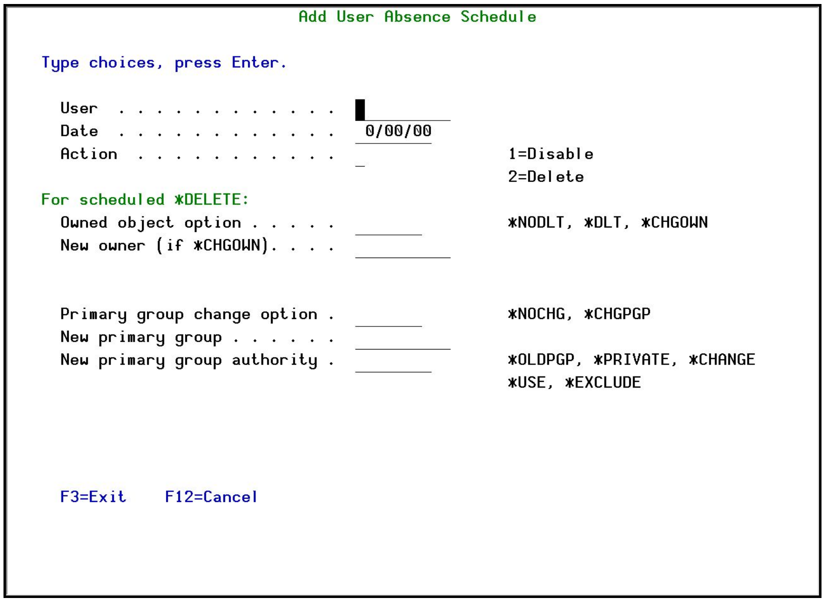
1. Select **41. Work with Schedule** from the **User Management** menu. The **Work with User Absence Schedule** screen appears.



```
                          Work with User Absence Schedule

 Disable users on temporary leave (eg. vacation, sick, leave of absence), or
 Permanently delete users leaving the organization.
 Type options, press Enter.
   1=Select    4=Delete
 Opt User       Date     Description
  █  PHILIP      7/12/15

                                                                        Bottom

 F3=Exit    F6=Add New    F8=Print list    F11=Fold/Drop    F12=Cancel
```

Figure 52: Working with User Absence Schedule screen

2. Press **F6=Add** new. The **Add User Absence Schedule** appears.



```
                          Add User Absence Schedule

 Type choices, press Enter.

   User  . . . . . . . . . . . .  _________
   Date  . . . . . . . . . . . .   0/00/00
   Action  . . . . . . . . . . .  _               1=Disable
                                                  2=Delete
 For scheduled *DELETE:
   Owned object option . . . . .  _______         *NODLT, *DLT, *CHGOWN
   New owner (if *CHGOWN). . . .  __________


   Primary group change option .  _______         *NOCHG, *CHGPGP
   New primary group . . . . . .  __________
   New primary group authority .  ________        *OLDPGP, *PRIVATE, *CHANGE
                                                  *USE, *EXCLUDE




   F3=Exit    F12=Cancel
```

Figure 53: Add User Absence Schedule screen

Parameters	Description
User	The user who will be absent
Date	The date from which the user will be absent
Action	1=Disable The user will be disabled from the date entered. 2=Delete The user will be deleted from the date entered. If you disable a profile, you must manually re-enable the profile using the *CHGUSRPRF* command.
For scheduled *DELETE	The parameters below are only relevant if you set Action to **2** (Delete).
Owner Object Option	***NODLT** = The owned objects for the user profile are not changed, and the user profile is not deleted if the user owns any objects. ***DLT** = The owned objects for the user profile are deleted. The user profile is deleted if the deletion of all owned objects is successful. ***CHGOWN** = The owned objects for the user profile have ownership transferred to the specified user profile. The user profile is deleted if the transfer of all owned objects is successful.
New Owner	When ***CHGOWN** is specified, a user profile name must be specified for the new user profile. Specify the name of the user profile.
Primary group change option	***NOCHG** = The objects the user profile is the primary group for do not change, and the user profile is not deleted if the user is the primary group for any objects. ***CHGPGP** = The objects the user profile is the primary group for are transferred to the specified user profile. The user profile is deleted if the transfer of all objects is successful.
New primary group	When ***CHGPGP** is specified, a user profile name or ***NONE** must be specified. The name of the user profile. The user profile specified must have a group ID number (gid).
New primary group authority	***OLDPGP** = The new primary group has the same authority to the object as the old primary group. ***PRIVATE** = If the new primary group has a private authority to the object, it will become the primary group for that object and the primary group authority will be what the private authority was. If the new primary group does not have a private authority to the object, it becomes the primary group but does not have any authority to the object.

-

Parameters	Description
	***ALL** = The new primary group has ***ALL** authority to the object. ***CHANGE** = The new primary group has ***CHANGE** authority to the object. ***USE** = The new primary group has ***USE** authority to the object. ***EXCLUDE** = The new primary group has ***EXCLUDE** authority to the object.

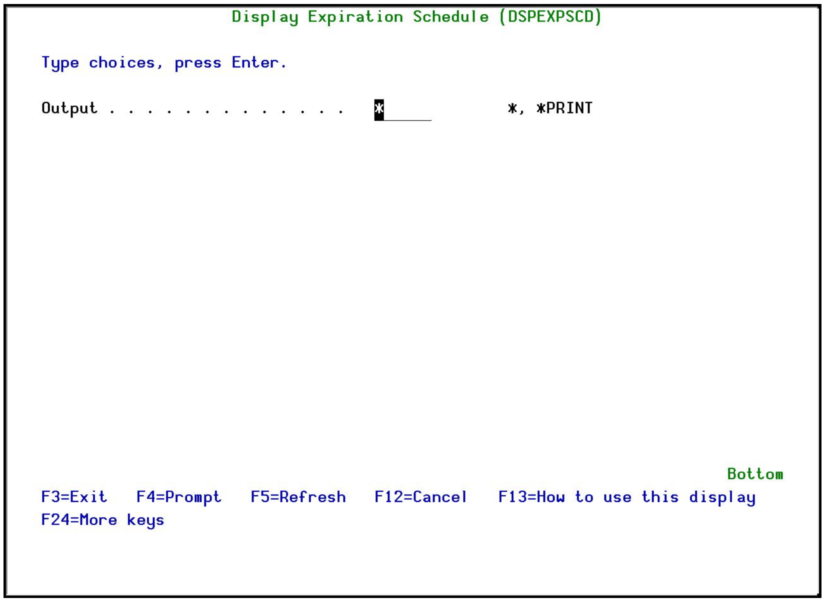
3. Enter your parameters and press Enter. The updated schedule appears in the **Work with Signon Schedule** screen.

NOTE: Refer to IBM documentation for a complete discussion regarding the concepts of object ownership and primary groups.

Display Absence Schedule

To display the absence schedule:

1. Select **42. Display Schedule** from the **User Management** menu. The **Display Expiration Schedule** screen appears.



```
                  Display Expiration Schedule (DSPEXPSCD)

 Type choices, press Enter.

 Output . . . . . . . . . . . . .   *          *, *PRINT


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

Figure 54: Display Expiration Schedule screen

2. Select either ***** to display the report or ***PRINT** to send the report to a printer and press **Enter**. The report is produced.

User and Password Reporting

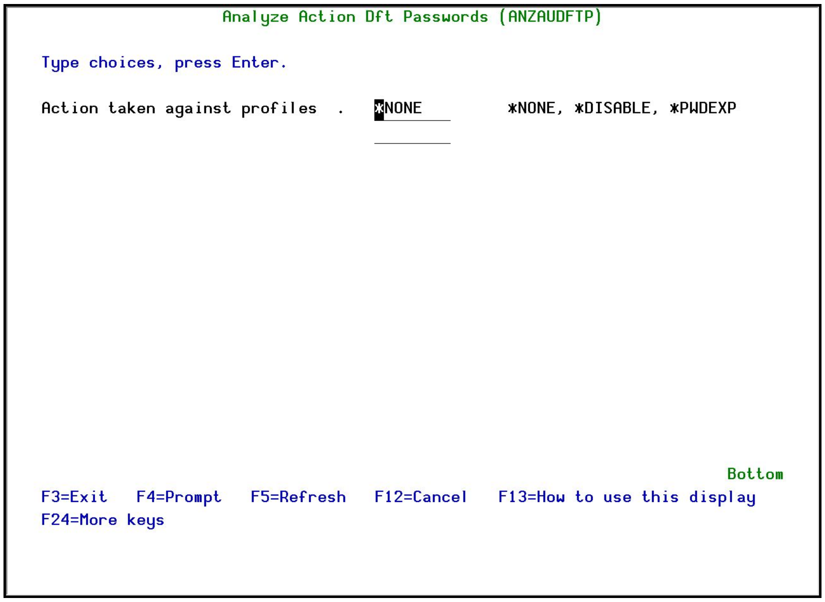
User management has a group of reports that enables you to analyze password usage.

Analyze Default Passwords

A profile is said to have a default password whenever the password is the same as the profile name. Obviously, this is dangerous because it is so easy to guess. This feature enables you to print a report of all the user profiles on the system that have a default password, and optionally disable those profiles or expire their passwords.

To analyze default passwords:

1. Select **61. Analyze Default Passwords** from the **User Management** menu. The **Analyze Action Dft Passwords** screen appears.



```
                      Analyze Action Dft Passwords (ANZAUDFTP)

 Type choices, press Enter.

 Action taken against profiles  .   *NONE       *NONE, *DISABLE, *PWDEXP



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

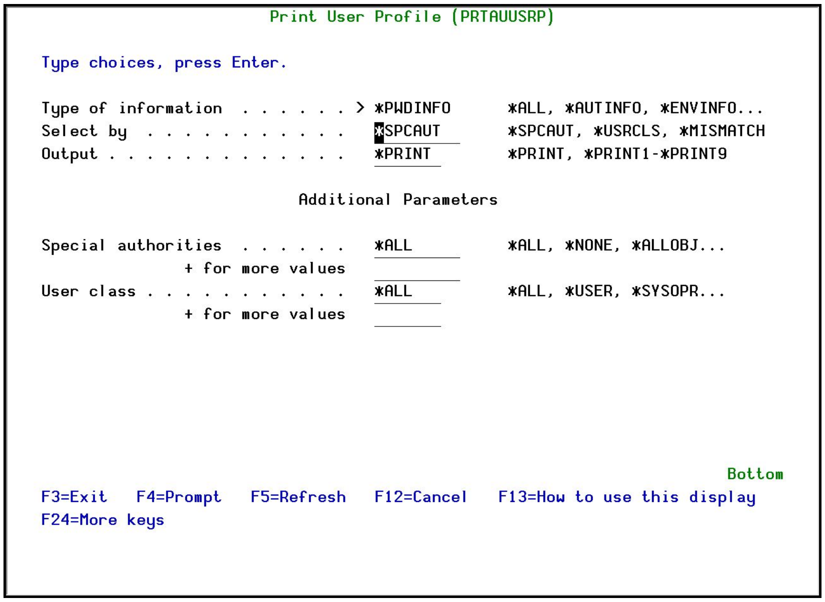
Figure 55: Analyze Action Dft Passwords screen

2. Select to display the report either for no action taken against the password (***NONE**), or for disabled passwords (***DISABLE**) or for expired passwords (***PWDEXP**), and press **Enter**. The report is produced.

Print Password Info

To print password information:

1. Select **62. Print Password Info** from the **User Management** menu. The **Print User Profile** screen appears.



```
                          Print User Profile (PRTAUUSRP)

 Type choices, press Enter.

 Type of information  . . . . . . > *PWDINFO      *ALL, *AUTINFO, *ENVINFO...
 Select by  . . . . . . . . . . .   *SPCAUT       *SPCAUT, *USRCLS, *MISMATCH
 Output . . . . . . . . . . . . .   *PRINT        *PRINT, *PRINT1-*PRINT9

                              Additional Parameters

 Special authorities  . . . . . .   *ALL          *ALL, *NONE, *ALLOBJ...
               + for more values
 User class . . . . . . . . . . .   *ALL          *ALL, *USER, *SYSOPR...
               + for more values







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

Figure 56: Print User Profile – Password Info screen

Parameters	Description
Type of Information	***PWDINFO** A report containing the password type information for the selected user profiles is printed. You cannot change this parameter.
Select by	***SPCAUT** = User profiles will be selected for the report based on special authorities. ***USRCLS** = User profiles will be selected for the report based on user class. ***MISMATCH** = User profiles will be selected for the report based on their special authorities not being the default values assigned to their user class.
Output	Where to send the output. ***PRINT** ***PRINT1 - 9**
Special Authorities	If *SPCAUT was specified for the Select by prompt (SELECT parameter), it specifies which special authorities should be used to select users. User profiles with any of the special authorities specified for this parameter will be included in the report. A maximum of 9 special authorities can be specified. ***ALL** = All user profiles will be included in the report. Alternatively you can select up to 9 of the following ***ALLOBJ** = User profiles with *ALLOBJ special authority will be included in the report. ***AUDIT** = User profiles with *AUDIT special authority will be included in the report. ***JOBCTL** = User profiles with *JOBCTL special authority will be included in the report. ***IOSYSCFG** = User profiles with *IOSYSCFG special authority will be included in the report. ***SAVSYS** = User profiles with *SAVSYS special authority will be included in the report. ***SECADM** = User profiles with *SECADM special authority will be included in the report. ***SERVICE** = User profiles with *SERVICE special authority will be included in the report. ***SPLCTL** = User profiles with *SPLCTL special authority will be included in the report.

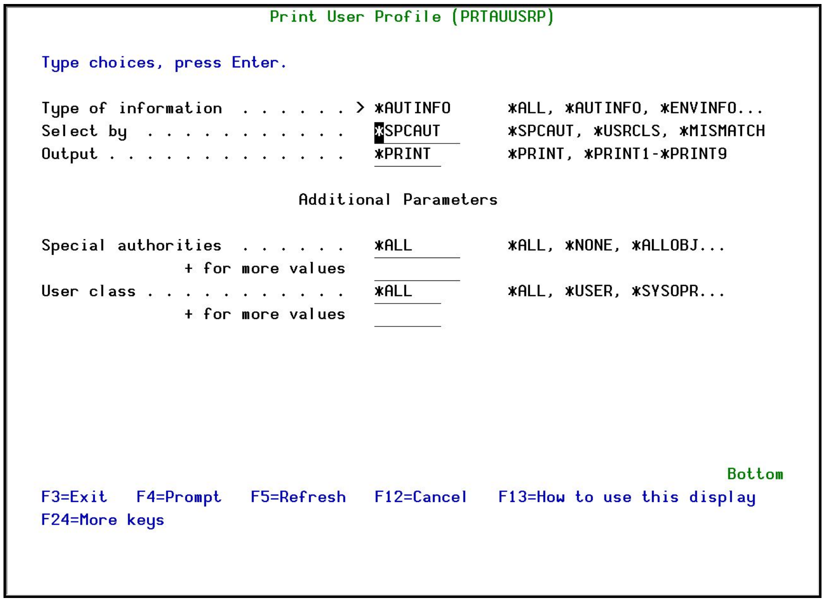
Parameters	Description
	***NONE** = User profiles with no special authorities will be included in the report.
User Class	If *USRCLS was specified for the Select by prompt (SELECT parameter), it specifies that user classes should be used to select users. User profiles with a user class that is specified for this parameter will be included in the report. A maximum of 5 user classes can be specified. ***ALL** = All user profiles will be included in the report. ***USER** = User profiles with *USER user class will be included in the report. ***SYSOPR** = User profiles with *SYSOPR user class will be included in the report. ***PGMR** = User profiles with *PGMR user class will be included in the report. ***SECADM** = User profiles with *SECADM user class will be included in the report. ***SECOFR** = User profiles with *SECOFR user class will be included in the report.

2. Enter the required parameters and press **Enter**. The report is produced.

Print Special Authorities

To print special authorities information:

1. Select **63. Print Special Authorities** from the **User Management** menu. The **Print User Profile** screen appears.



```
                         Print User Profile (PRTAUUSRP)

 Type choices, press Enter.

 Type of information . . . . . . > *AUTINFO      *ALL, *AUTINFO, *ENVINFO...
 Select by . . . . . . . . . . .   *SPCAUT       *SPCAUT, *USRCLS, *MISMATCH
 Output . . . . . . . . . . . . .  *PRINT        *PRINT, *PRINT1-*PRINT9

                            Additional Parameters

 Special authorities . . . . . .   *ALL          *ALL, *NONE, *ALLOBJ...
               + for more values
 User class . . . . . . . . . . .  *ALL          *ALL, *USER, *SYSOPR...
               + for more values




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

Figure 57: Print User Profile – Special Authorities screen

Parameters	Description
Type of Information	***AUTINFO** A report containing the authority type information for the selected user profiles is printed. You cannot change this parameter.
Select by	***SPCAUT** = User profiles will be selected for the report based on special authorities. ***USRCLS** = User profiles will be selected for the report based on user class. ***MISMATCH** = User profiles will be selected for the report based on their special authorities not being the default values assigned to their user class.
Output	Where to send the output. ***PRINT** ***PRINT1 - 9**
Special Authorities	If *SPCAUT was specified for the Select by prompt (SELECT parameter), it specifies which special authorities should be used to select users. User profiles with any of the special authorities specified for this parameter will be included in the report. A maximum of 9 special authorities can be specified. ***ALL** = All user profiles will be included in the report. Alternatively you can select up to 9 of the following ***ALLOBJ** = User profiles with *ALLOBJ special authority will be included in the report. ***AUDIT** = User profiles with *AUDIT special authority will be included in the report. ***JOBCTL** = User profiles with *JOBCTL special authority will be included in the report. ***IOSYSCFG** = User profiles with *IOSYSCFG special authority will be included in the report. ***SAVSYS** = User profiles with *SAVSYS special authority will be included in the report. ***SECADM** = User profiles with *SECADM special authority will be included in the report. ***SERVICE** = User profiles with *SERVICE special authority will be included in the report. ***SPLCTL** = User profiles with *SPLCTL special authority will be included in the report.

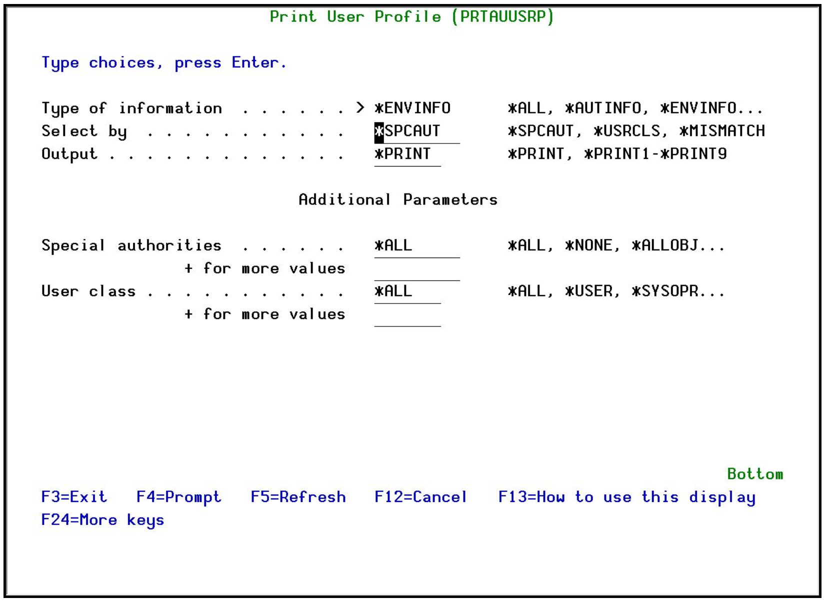
Parameters	Description
	***NONE** = User profiles with no special authorities will be included in the report.
User Class	If *USRCLS was specified for the Select by prompt (SELECT parameter), it specifies that user classes should be used to select users. User profiles with a user class that is specified for this parameter will be included in the report. A maximum of 5 user classes can be specified. ***ALL** = All user profiles will be included in the report. ***USER** = User profiles with *USER user class will be included in the report. ***SYSOPR** = User profiles with *SYSOPR user class will be included in the report. ***PGMR** = User profiles with *PGMR user class will be included in the report. ***SECADM** = User profiles with *SECADM user class will be included in the report. ***SECOFR** = User profiles with *SECOFR user class will be included in the report.

2. Enter the required parameters and press **Enter**. The report is produced.

Print Programs and Queues

To print environment information:

1. Select **64. Print Program and Queues** from the **User Management** menu. The **Print User Profile** screen appears.



```
                          Print User Profile (PRTAUUSRP)

 Type choices, press Enter.

 Type of information . . . . . . > *ENVINFO      *ALL, *AUTINFO, *ENVINFO...
 Select by . . . . . . . . . . .   *SPCAUT       *SPCAUT, *USRCLS, *MISMATCH
 Output . . . . . . . . . . . . .  *PRINT        *PRINT, *PRINT1-*PRINT9

                            Additional Parameters

 Special authorities . . . . . .   *ALL          *ALL, *NONE, *ALLOBJ...
               + for more values
 User class . . . . . . . . . . .  *ALL          *ALL, *USER, *SYSOPR...
               + for more values

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

Figure 58: Print User Profile – Program and Queues screen

Parameters	Description
Type of Information	***ENVINFO** A report containing the environment type information for the selected user profiles is printed. You cannot change this parameter.
Select by	***SPCAUT** = User profiles will be selected for the report based on special authorities. ***USRCLS** = User profiles will be selected for the report based on user class. ***MISMATCH** = User profiles will be selected for the report based on their special authorities not being the default values assigned to their user class.
Output	Where to send the output. ***PRINT** ***PRINT1 - 9**
Special Authorities	If *SPCAUT was specified for the Select by prompt (SELECT parameter), it specifies which special authorities should be used to select users. User profiles with any of the special authorities specified for this parameter will be included in the report. A maximum of 9 special authorities can be specified. ***ALL** = All user profiles will be included in the report. Alternatively you can select up to 9 of the following ***ALLOBJ** = User profiles with *ALLOBJ special authority will be included in the report. ***AUDIT** = User profiles with *AUDIT special authority will be included in the report. ***JOBCTL** = User profiles with *JOBCTL special authority will be included in the report. ***IOSYSCFG** = User profiles with *IOSYSCFG special authority will be included in the report. ***SAVSYS** = User profiles with *SAVSYS special authority will be included in the report. ***SECADM** = User profiles with *SECADM special authority will be included in the report. ***SERVICE** = User profiles with *SERVICE special authority will be included in the report. ***SPLCTL** = User profiles with *SPLCTL special authority will be included in the report.

Parameters	Description
	`*NONE` = User profiles with no special authorities will be included in the report.
`User Class`	If *USRCLS was specified for the Select by prompt (SELECT parameter), it specifies that user classes should be used to select users. User profiles with a user class that is specified for this parameter will be included in the report. A maximum of 5 user classes can be specified. **`*ALL`** = All user profiles will be included in the report. **`*USER`** = User profiles with *USER user class will be included in the report. **`*SYSOPR`** = User profiles with *SYSOPR user class will be included in the report. **`*PGMR`** = User profiles with *PGMR user class will be included in the report. **`*SECADM`** = User profiles with *SECADM user class will be included in the report. **`*SECOFR`** = User profiles with *SECOFR user class will be included in the report.

2. Enter the required parameters and press **`Enter`**. The report is produced.

Chapter 5: Authority Adoption Control

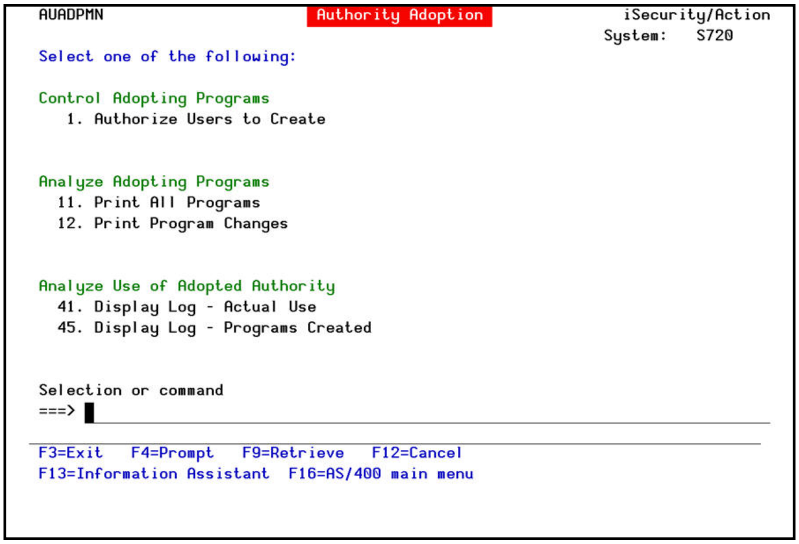
One of the most critical components of IBM i (OS/400) security is the ability to restrict the authority to perform actions and to access objects to specific individual users. Data entry clerks cannot work with payroll data or change program source code. Programmers cannot update the customer master file or record cash receipts.

Unfortunately, IBM i (OS/400) also provides that ability for programs run by one user to “adopt” the authorities of another user. A user with some programming knowledge could create a program that adopts authority to gain access to critical databases. Under this scenario, programmer could use his or her knowledge to get into the customer master file.

Authority adoption is an intentional waiver of control. Action provides several tools that enable administrators to control who can create programs that adopt authority, and which programs may adopt which specific authorities. Several reports and queries are provided to facilitate a complete audit trail of activities related to the creation and use of adopted authority.

Authority Adoption

To work with authority adoption, select **22. Authority Adoption** from the **Action** Main menu.



```
AUADPMN                  Authority Adoption              iSecurity/Action
                                                        System:   S720
Select one of the following:

Control Adopting Programs
   1. Authorize Users to Create


Analyze Adopting Programs
  11. Print All Programs
  12. Print Program Changes


Analyze Use of Adopted Authority
  41. Display Log - Actual Use
  45. Display Log - Programs Created


Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 59: Authority Adoption

Controlling Program Authority Adoption

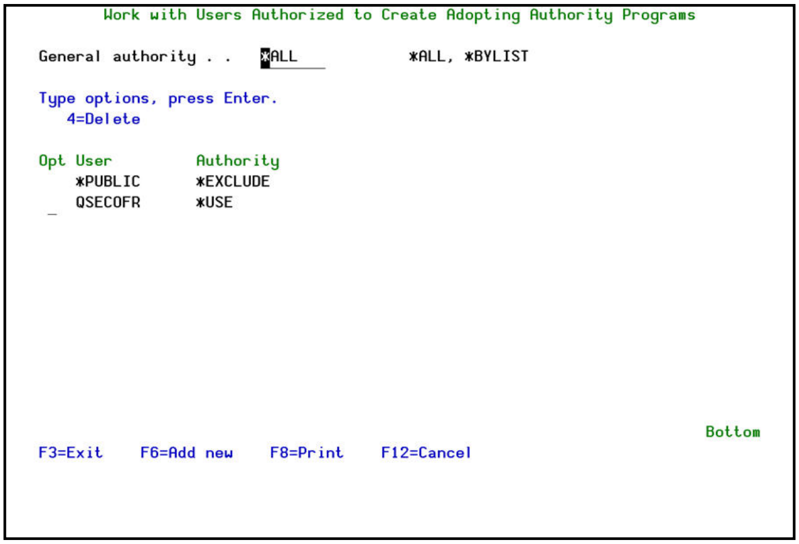
Controlling program authority adoption is implemented at two levels:

- Controlling User Program Authority Adoption
- Adopting specific authorities authorization

Authorizing Users for Program Authority Adoption

Audit enables you to restrict the program adoption for specific users. To work with the list of authorized users:

1. Select **Authorize Users to Create** from the **Authority Adoption** menu.
2. Set the **General Authority** parameter to ***BYLIST***.
3. Press **F6** to add users to the list. Enter authorized user profile names. Press **Enter** when finished.



```
        Work with Users Authorized to Create Adopting Authority Programs

General authority . .   *ALL          *ALL, *BYLIST

Type options, press Enter.
   4=Delete

Opt User          Authority
    *PUBLIC       *EXCLUDE
 _  QSECOFR       *USE

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

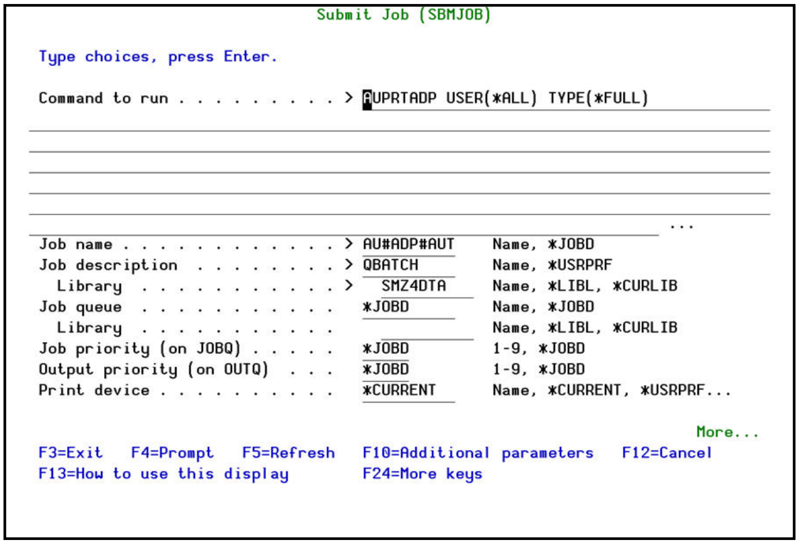
Figure 60: Working with Users Authorized to Adoption Programs

Parameter	Description
General authority	***ALL** = All users have authorization to adopt program authority (Not recommended) ***BYLIST** = Only users listed are authorized to adopt program authority
Opt	**4** = Delete user profile from list
F8	Print list of authorized users

Analyze Programs that Use Adopt Authority

Print all programs using Action or Print programs changes only.

1. Select **`Print All Programs`** from the **`Authority Adoption`** menu. The following screen appears.



```
                              Submit Job (SBMJOB)

 Type choices, press Enter.

 Command to run . . . . . . . . . > AUPRTADP USER(*ALL) TYPE(*FULL)






                                                                    ...
 Job name . . . . . . . . . . . . > AU#ADP#AUT    Name, *JOBD
 Job description  . . . . . . . . > QBATCH        Name, *USRPRF
   Library  . . . . . . . . . . . >   SMZ4DTA     Name, *LIBL, *CURLIB
 Job queue  . . . . . . . . . . .   *JOBD         Name, *JOBD
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
 Job priority (on JOBQ) . . . . .   *JOBD         1-9, *JOBD
 Output priority (on OUTQ)  . . .   *JOBD         1-9, *JOBD
 Print device . . . . . . . . . .   *CURRENT      Name, *CURRENT, *USRPRF...
                                                                    More...
 F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
 F13=How to use this display        F24=More keys
```

Figure 61: Programs Authorized to Adopt Authority

2. Set the parameters and press **`Enter`** to print.
3. Select Print Program Changes to view the programs changes.

Analyze Use of Adopted Authority

The menu provides means to display the audit history log showing:

- creation of/changes to programs that adopt authority
- activity/transactions that use adopted authority

To use this feature, you must have **Audit** installed and properly configured to record these activities in the log. Instructions for using the display log feature appear in the **Audit** User manual.

Chapter 6: Displaying the History Log

You can use the **`Display Log`** feature to display the contents of the history log quickly and easily in a standard format using basic filter criteria. You can even use previously defined Audit queries as filter criteria for the log display. This feature is best suited for investigating immediate problems such as program failures, errors or suspicious activity.

The "Quick Look Back" Feature

This unique feature lets you look at the last several minutes of activity without the need to define specific time or date parameters. Just enter how long a period (in minutes) you wish to look at, press **`Enter`**, and your data is instantly displayed. **`Quick Look Back`** really comes in handy when assisting users with that nasty error message that just popped up or verifying that a batch job was successfully completed.

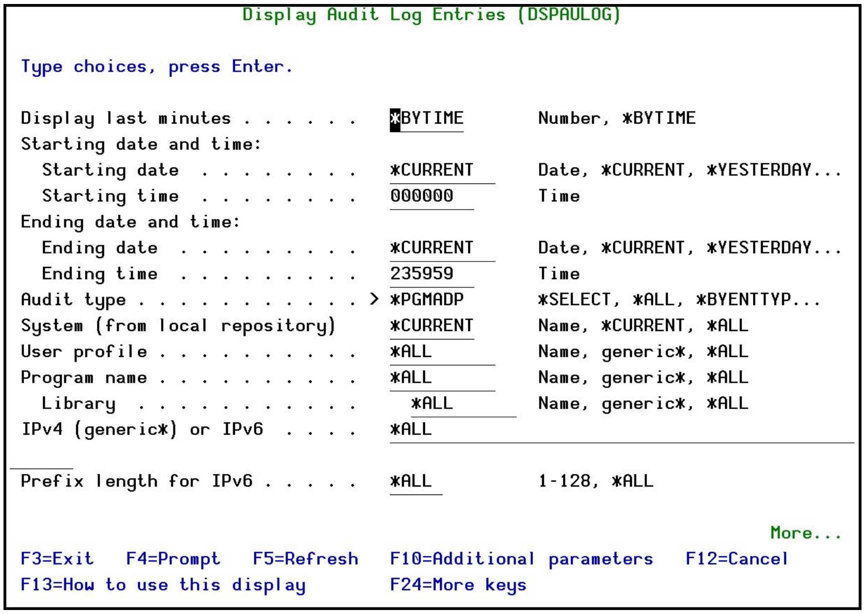
Using Time Groups

The history log feature makes full use of the convenient time group feature. This timesaving option further enhances your ability to get to your critical data rapidly.

Basic Procedure

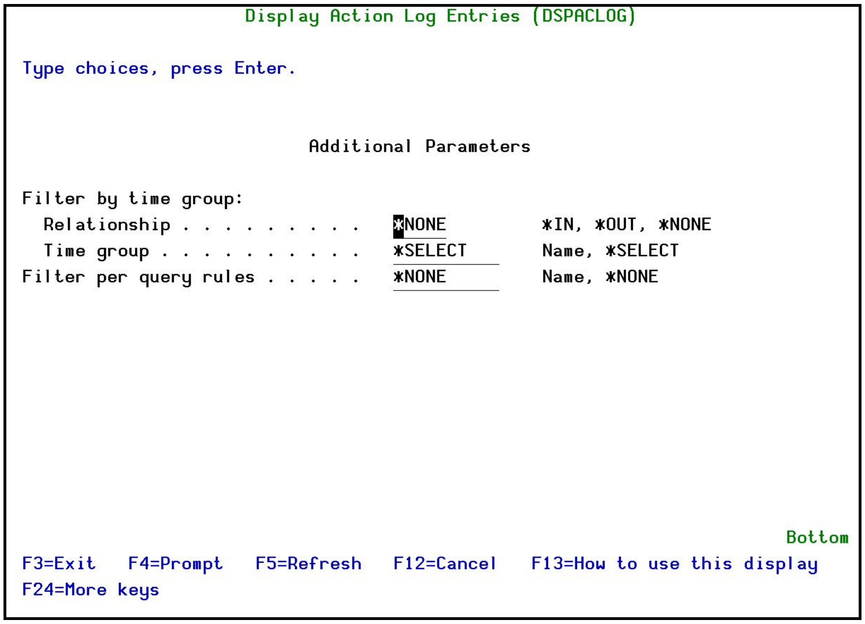
A few simple steps are all that is necessary to view your data:

1. Select **`22 > 41. Display Log`**. The **`Display Audit Log Entries`** screen appears.



```
                     Display Audit Log Entries (DSPAULOG)

 Type choices, press Enter.

 Display last minutes . . . . . .   *BYTIME       Number, *BYTIME
 Starting date and time:
   Starting date  . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
   Starting time  . . . . . . . .   000000        Time
 Ending date and time:
   Ending date  . . . . . . . . .   *CURRENT      Date, *CURRENT, *YESTERDAY...
   Ending time  . . . . . . . . .   235959        Time
 Audit type . . . . . . . . . . . > *PGMADP       *SELECT, *ALL, *BYENTTYP...
 System (from local repository)     *CURRENT      Name, *CURRENT, *ALL
 User profile . . . . . . . . . .   *ALL          Name, generic*, *ALL
 Program name . . . . . . . . . .   *ALL          Name, generic*, *ALL
   Library  . . . . . . . . . . .     *ALL        Name, generic*, *ALL
 IPv4 (generic*) or IPv6  . . . .   *ALL

 Prefix length for IPv6 . . . . .   *ALL          1-128, *ALL

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

Figure 62: Display Action Log Entries



```
                     Display Action Log Entries (DSPACLOG)

 Type choices, press Enter.


                              Additional Parameters

 Filter by time group:
   Relationship . . . . . . . . .   *NONE         *IN, *OUT, *NONE
   Time group . . . . . . . . . .   *SELECT       Name, *SELECT
 Filter per query rules . . . . .   *NONE         Name, *NONE









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

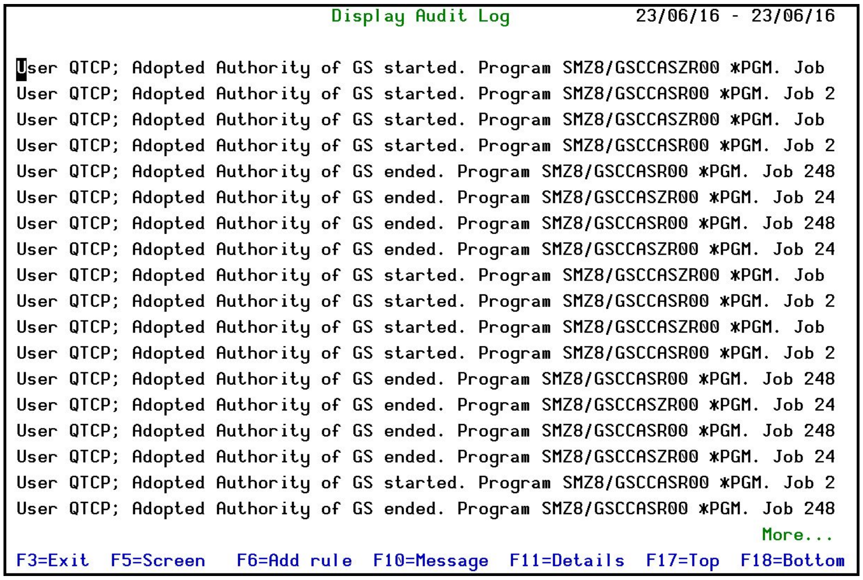
Figure 63: Additional Parameters - Display Action Log Entries

Parameter	Description
Display last minutes	Selects only those events occurring within the previous number of minutes as specified by the user **Number** = Enter the desired number of minutes ***BYTIME** = According to starting and ending times specified below
Starting date & time **Ending date & time**	Selects only those events occurring within the range specified by the starting and ending date/time combination **Date and time** = Enter the appropriate date or time ***CURRENT** = Current day ***YESTERDAY** = Previous day ***WEEKSTR/*PRVWEEKS** = Current week/Previous week ***MONTHSTR/ *PRVMONTH** = Current month/Previous month ***YEARSTR/ *PRVYEARS** = Current year/ Previous year ***SUN -*SAT** = Day of week
Audit Type	***PGMADP** = Adopted Authority
System (from local repository)	The system/s from which to obtain the information for the log
User profile	Selects a subset of records by use profiler
Program name	***ALL** = Include all
Program Name - Library	***ALL** = Include all
IPv4 (generic*) or IPv6	***ALL** = Include all
Prefix length for IPv6	Prefix of 1-128 or ***ALL** = Include all
Job name	Selects a subset of records by IBM i (OS/400) job name
Job - User	Selects a subset of records by IBM i (OS/400) user
Job - Number	Selects a subset of records by IBM i (OS/400) number
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	Use an existing query to filter history log entries. This is useful for

-

Parameter	Description
query rules	applying complex filter criteria. **Name** = Name of an existing query ***None** = Do not use query rules (Default)
Number of records to Process	Maximum number of records to process ***NOMAX** = No maximum (Default)
Output	**PRINT1-*PRINT9* are special values which can be entered in the **OUTPUT** parameter of all commands that are capable of printing. These special print options are handled by the user exit program named on the previous screen. Initially **PRINT1* and **PRINT2* are set to print on remote system.**PRINT2* prints also on the local system. To achieve this result you should modify the special Output Queue, which are spool files that are automatically sent to the remote system. Modify this Output Queue using the following command: **PRINT1* causes the print to be sent to the local system output queue. **PRINT2* will print on both systems (local and remote). **PRINT3* creates an excel file. **PRINT3-9* are user modifiable NOTE: See *Chapter 8* for more details.
Object	***ALL** = Include all
Object Library	***ALL** = Include all
Object Type	***ALL** = Include all

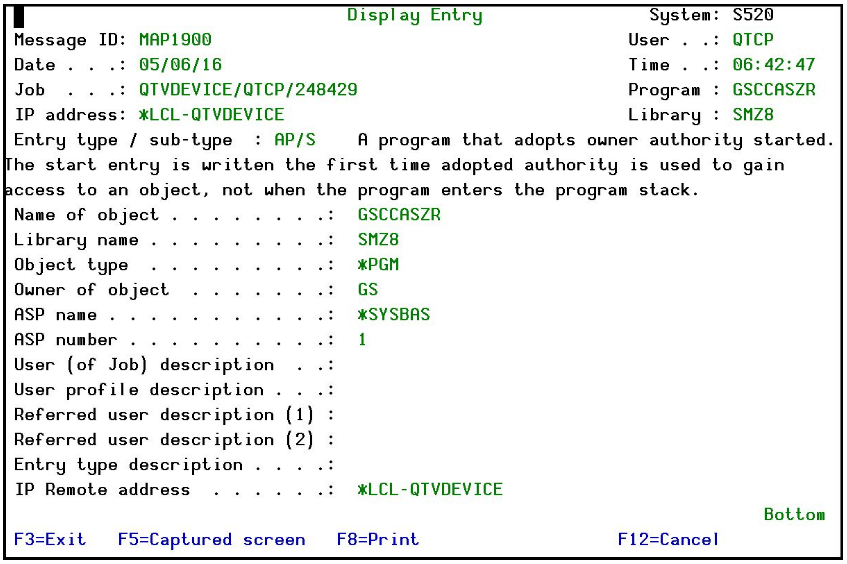
2. Enter run-time filter conditions and other parameters on the **Display Action Log Entries** screen and press **Enter** to display the history log. An example of the audit log display appears below.



```
                             Display Audit Log          23/06/16 - 23/06/16

User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASZR00 *PGM. Job
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASR00 *PGM. Job 2
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASZR00 *PGM. Job
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASR00 *PGM. Job 2
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASR00 *PGM. Job 248
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASZR00 *PGM. Job 24
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASR00 *PGM. Job 248
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASZR00 *PGM. Job 24
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASZR00 *PGM. Job
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASR00 *PGM. Job 2
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASZR00 *PGM. Job
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASR00 *PGM. Job 2
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASR00 *PGM. Job 248
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASZR00 *PGM. Job 24
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASR00 *PGM. Job 248
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASZR00 *PGM. Job 24
User QTCP; Adopted Authority of GS started. Program SMZ8/GSCCASR00 *PGM. Job 2
User QTCP; Adopted Authority of GS ended. Program SMZ8/GSCCASR00 *PGM. Job 248
                                                                       More...
F3=Exit  F5=Screen   F6=Add rule  F10=Message  F11=Details  F17=Top  F18=Bottom
```

Figure 64: Display Action Log

3. To view the detail of an individual entry, move the cursor to the desired line and press **Enter** or **F11**. An example of a single audit log entry appears below.



```
                               Display Entry              System: S520
 Message ID: MAP1900                                     User . .: QTCP
 Date . . .: 05/06/16                                    Time . .: 06:42:47
 Job  . . .: QTVDEVICE/QTCP/248429                       Program : GSCCASZR
 IP address: *LCL-QTVDEVICE                              Library : SMZ8
 Entry type / sub-type  : AP/S    A program that adopts owner authority started.
The start entry is written the first time adopted authority is used to gain
access to an object, not when the program enters the program stack.
 Name of object . . . . . . . .:  GSCCASZR
 Library name . . . . . . . . .:  SMZ8
 Object type  . . . . . . . . .:  *PGM
 Owner of object  . . . . . . .:  GS
 ASP name . . . . . . . . . . .:  *SYSBAS
 ASP number . . . . . . . . . .:  1
 User (of Job) description  . .:
 User profile description . . .:
 Referred user description (1) :
 Referred user description (2) :
 Entry type description . . . .:
 IP Remote address  . . . . . .:  *LCL-QTVDEVICE
                                                                       Bottom
 F3=Exit   F5=Captured screen   F8=Print                 F12=Cancel
```

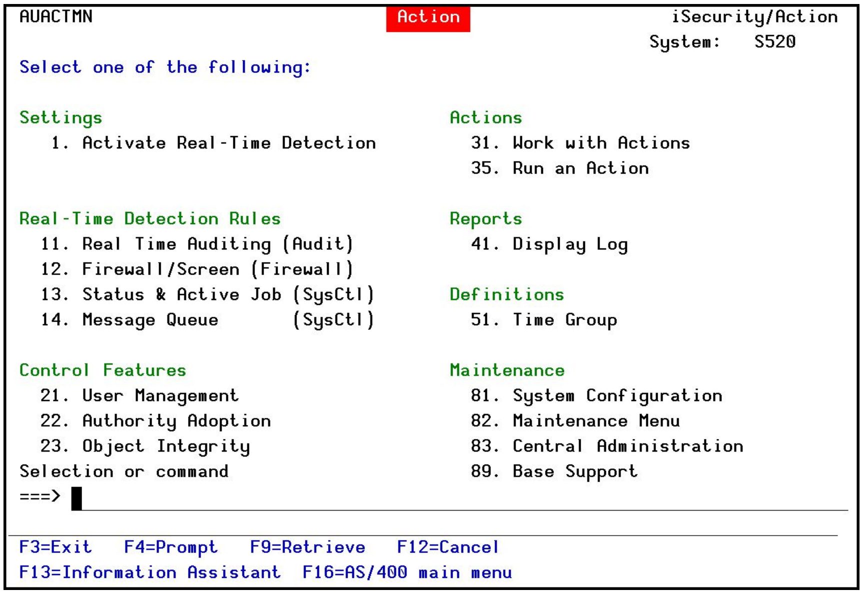
Figure 65: Display Entry

Chapter 7: Maintenance Menu

The **Maintenance Menu** enables you to set iSecurity/Base Global definitions and display them, including:

- Export / Import Definitions
- Import Definitions
- Display Definitions

To access the **Maintenance Menu**, select **82. Maintenance Menu** from the **Action** Main menu.



```
AUACTMN                              Action                 iSecurity/Action
                                                            System:    S520
Select one of the following:

Settings                                      Actions
   1. Activate Real-Time Detection              31. Work with Actions
                                                35. Run an Action

Real-Time Detection Rules                     Reports
  11. Real Time Auditing (Audit)                41. Display Log
  12. Firewall/Screen (Firewall)
  13. Status & Active Job (SysCtl)            Definitions
  14. Message Queue       (SysCtl)              51. Time Group

Control Features                              Maintenance
  21. User Management                           81. System Configuration
  22. Authority Adoption                        82. Maintenance Menu
  23. Object Integrity                          83. Central Administration
Selection or command                            89. Base Support
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 66: Maintenance Menu

Export / Import Definitions

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

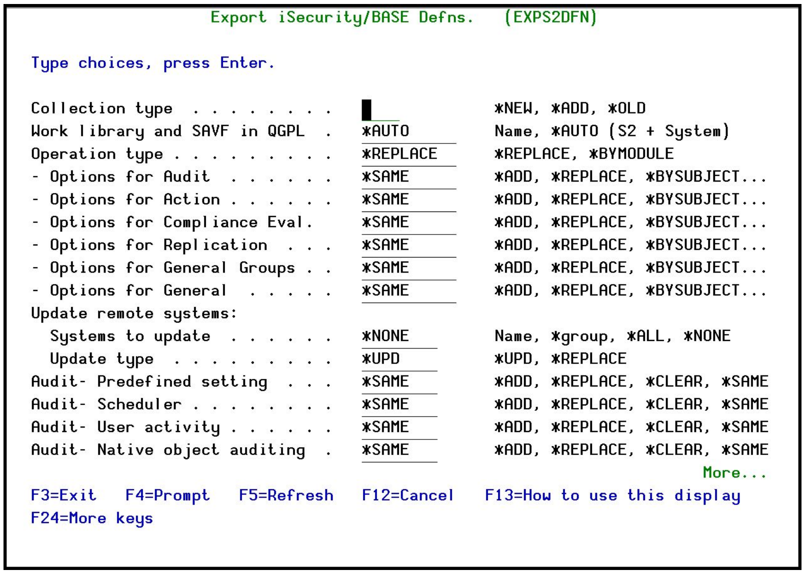
Among the settings and definitions that **Action** can export and import are the following:

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

Export Definitions

Create an SAVF file containing the definitions and setting you want to export.

1. Select **82 >1. Export Definitions**. The **Export iSecurity/BASE Defns.** screen appears.



```
                    Export iSecurity/BASE Defns.   (EXPS2DFN)

 Type choices, press Enter.

 Collection type  . . . . . . . .   █___          *NEW, *ADD, *OLD
 Work library and SAVF in QGPL  .   *AUTO         Name, *AUTO (S2 + System)
 Operation type . . . . . . . . .   *REPLACE      *REPLACE, *BYMODULE
 - Options for Audit  . . . . . .   *SAME         *ADD, *REPLACE, *BYSUBJECT...
 - Options for Action . . . . . .   *SAME         *ADD, *REPLACE, *BYSUBJECT...
 - Options for Compliance Eval.     *SAME         *ADD, *REPLACE, *BYSUBJECT...
 - Options for Replication  . . .   *SAME         *ADD, *REPLACE, *BYSUBJECT...
 - Options for General Groups . .   *SAME         *ADD, *REPLACE, *BYSUBJECT...
 - Options for General  . . . . .   *SAME         *ADD, *REPLACE, *BYSUBJECT...
 Update remote systems:
   Systems to update  . . . . . .   *NONE         Name, *group, *ALL, *NONE
   Update type  . . . . . . . . .   *UPD          *UPD, *REPLACE
 Audit- Predefined setting  . . .   *SAME         *ADD, *REPLACE, *CLEAR, *SAME
 Audit- Scheduler . . . . . . . .   *SAME         *ADD, *REPLACE, *CLEAR, *SAME
 Audit- User activity . . . . . .   *SAME         *ADD, *REPLACE, *CLEAR, *SAME
 Audit- Native object auditing  .   *SAME         *ADD, *REPLACE, *CLEAR, *SAME
                                                                          More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 67: Export iSecurity/BASE Defns. (EXPS2DFN)

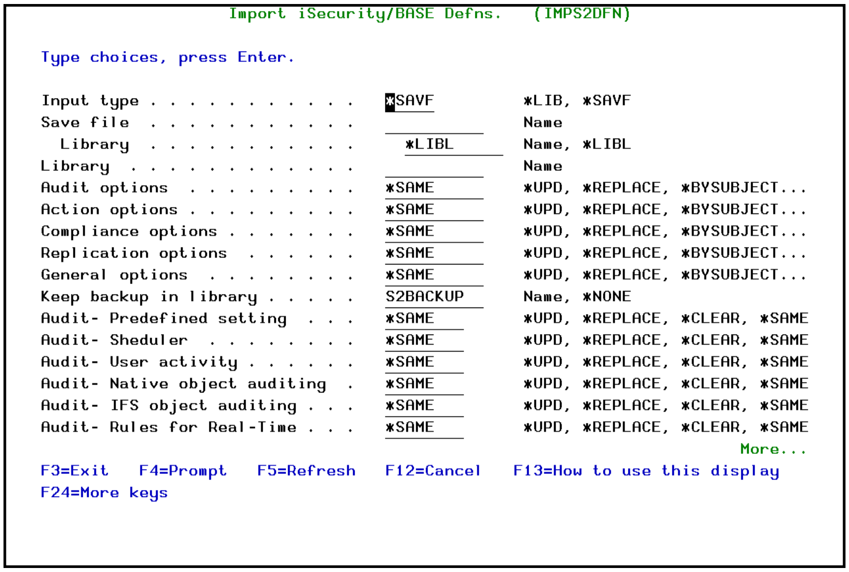
	Description
Work library and SAVF in QGPL	Destination of export library. **S1** (Security One) is default setting **Name=** name of target library.
Firewall /Screen Options	Definitions pertaining to these two applications ***ADD** = add to a previously imported/exported rule ***REPLACE** = replace a previously imported/exported rule ***BYSUBJECT=** import/export rules by subject (IP address, and so on)
Update remote systems	**Systems to update=** When exporting Firewall definitions, the user can choose to export and import immediately by preparing the definitions in a SAVF and send it to a remote system or several remote systems, and automatically import them into it. **Update type** ***UPD** = add new records and replace existing ***REPLACE** = clear the definition file and copy the new
Keep backup in library	**Name=** library where backup definitions are found

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

Import Definitions

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

1. Select **82 > 2. Import Definitions**. The **Import iSecurity/BASE Defns.** screen appears.



```
                        Import iSecurity/BASE Defns.    (IMPS2DFN)

 Type choices, press Enter.

 Input type . . . . . . . . . . .   *SAVF         *LIB, *SAVF
 Save file  . . . . . . . . . . .                 Name
   Library  . . . . . . . . . . .     *LIBL       Name, *LIBL
 Library  . . . . . . . . . . . .                 Name
 Audit options  . . . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 Action options . . . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 Compliance options . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 Replication options  . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 General options  . . . . . . . .   *SAME         *UPD, *REPLACE, *BYSUBJECT...
 Keep backup in library . . . . .   S2BACKUP      Name, *NONE
 Audit- Predefined setting  . . .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
 Audit- Sheduler  . . . . . . . .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
 Audit- User activity . . . . . .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
 Audit- Native object auditing  .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
 Audit- IFS object auditing . . .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
 Audit- Rules for Real-Time . . .   *SAME         *UPD, *REPLACE, *CLEAR, *SAME
                                                                      More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Figure 68: Import iSecurity/BASE Defns. (IMPS2DFN)

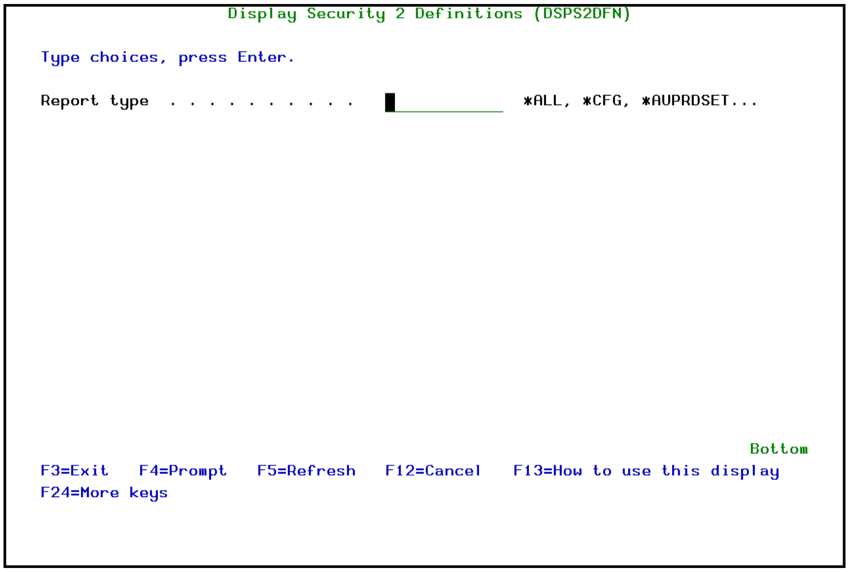
	Description
Work library and SAVF in QGPL	Destination of export library. **S1** (Security One) is default settings **Name=** name of target library.
Firewall /Screen Options	Definitions pertaining to these two applications ***ADD** = add to a previously imported/exported rule ***REPLACE** = replace a previously imported/exported rule ***BYSUBJECT=** import/export rules by subject (IP address, and so on)
Update remote systems	**Systems to update=** When exporting Firewall definitions, the user can choose to export and import immediately by preparing the definitions in a SAVF and send it to a remote system or several remote systems, and automatically import them into it. **Update type** ***UPD** = add new records and replace existing ***REPLACE** = clear the definition file and copy the new
Keep backup in library	**Name=** library where backup definitions are found

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

Display Definitions

This feature enables the user to display and print iSecurity Part One definitions:

1. Select **5. Display Definitions** from the **Maintenance Menu**. The **Display Security 2 Definitions** screen appears.
2. Select the desired **Report type** from the **Display Security 2 Definitions** screen. After selecting the **Report type**, additional parameters appear.
3. Select choices and press **Enter**.



```
                    Display Security 2 Definitions (DSPS2DFN)

 Type choices, press Enter.

 Report type . . . . . . . . . .   _________    *ALL, *CFG, *AUPRDSET...




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

Figure 69: Display Security 2 Definitions (DSPS2DFN)

	Description
Report type	***ALL** = all general definitions ***CFG** = per configuration ***SRVR** = per server ***IPIN** = per IP address
Format	***LIST** = Short form ***DETAILS** = full form
Output	Select correct print option. See **PRINT1-*PRINT9 Setup* at the end of this chapter for details.

Audit

These features that comprise **Audit** are designed for users who have installed this module. **Audit** works hand-in-hand with **Action** by initiating responses to security threats, generating auditing reports, and recording details in a History Log. It includes:

- Start a New Journal Receiver
- Change Journal Receiver Library
- Automatic Translation
- Use English File Descriptions
- Delete Statistic Data

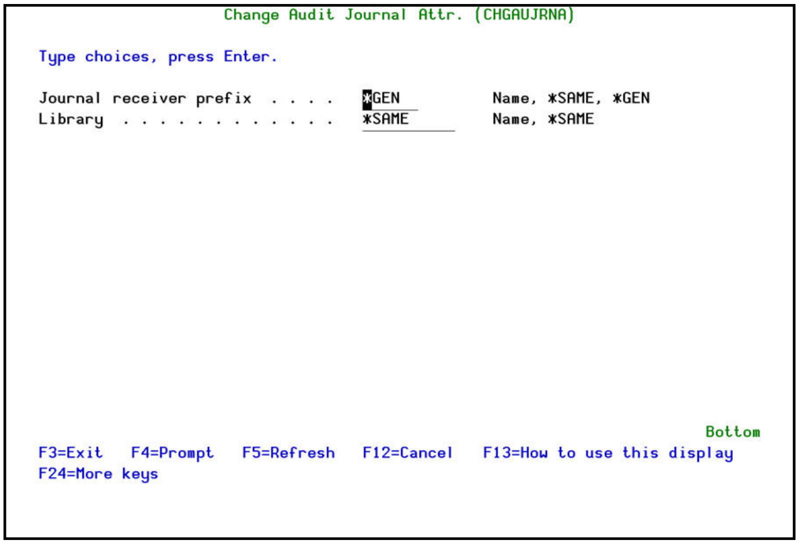
Start a New Journal Receiver

Audit periodically maintains its Journal Receivers according to your configuration (with no intervention). This, and the following features, gives you the option to manually handle all Journal Receiver maintenance.

1. Select **`82 > 21. Start a New QUADJRN Receiver`** to change your Journal Receiver attributes. The **`Change Audit Journal Attr. (CHGAUJRNA)`** screen appears.
2. Select *YES* or *NO* and press **`Enter`**.

Change Journal Receiver Library

1. Select **82 > 22. Change QAUDJRN Receiver Library** to change your Journal Receiver library. The **Change Audit Journal Attr. (CHGAUJRNA)** appears.



```
                        Change Audit Journal Attr. (CHGAUJRNA)

 Type choices, press Enter.

 Journal receiver prefix . . . .   *GEN          Name, *SAME, *GEN
 Library . . . . . . . . . . . .   *SAME         Name, *SAME

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

Figure 70: Change Audit Journal Attr. (CHGAUJRNA)

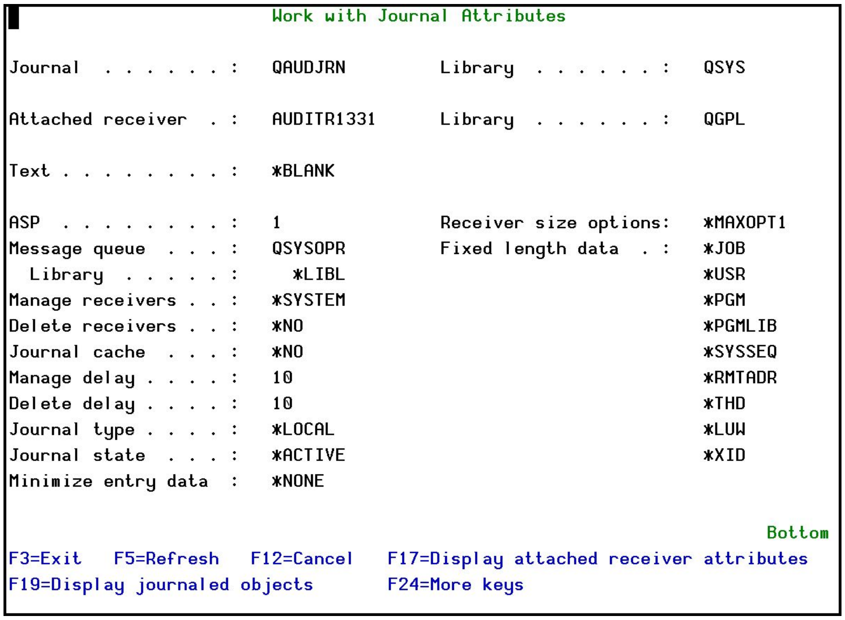
Parameters or Options	Description
Journal Receiver Prefix	**Name** = The name of the Journal Receiver ***Same** = The current journal receiver***Gen** = Generates a new journal receiver and puts it in the new library
Library	**Name** = The name of the library where you want to transfer the Journal receiver ***Same** = The library where the current Journal Receiver is found

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

Viewing Journal Attributes

This option displays the journal and its attached journal receiver information.

1. Select **82 > 23 Work with QAUDJRN Attributes** to view Journal Attributes, and **F3=Exit**.



```
                         Work with Journal Attributes

Journal  . . . . . . :   QAUDJRN         Library  . . . . . . :   QSYS

Attached receiver  . :   AUDITR1331      Library  . . . . . . :   QGPL

Text . . . . . . . . :   *BLANK

ASP  . . . . . . . . :   1               Receiver size options:   *MAXOPT1
Message queue  . . . :   QSYSOPR         Fixed length data  . :   *JOB
  Library  . . . . . :     *LIBL                                  *USR
Manage receivers . . :   *SYSTEM                                  *PGM
Delete receivers . . :   *NO                                      *PGMLIB
Journal cache  . . . :   *NO                                      *SYSSEQ
Manage delay . . . . :   10                                       *RMTADR
Delete delay . . . . :   10                                       *THD
Journal type . . . . :   *LOCAL                                   *LUW
Journal state  . . . :   *ACTIVE                                  *XID
Minimize entry data  :   *NONE

                                                                     Bottom
F3=Exit   F5=Refresh   F12=Cancel   F17=Display attached receiver attributes
F19=Display journaled objects       F24=More keys
```

Figure 71: Viewing with Journal Attributes (WRKJRNA)

Automatic Translation

IBM has translated the audit types into several languages; this feature uses the IBM template to translate automatically the audit type fields into your language.

Select **`82 > 24. Auto-Translate Field Descriptions.`** The translation is generated automatically.

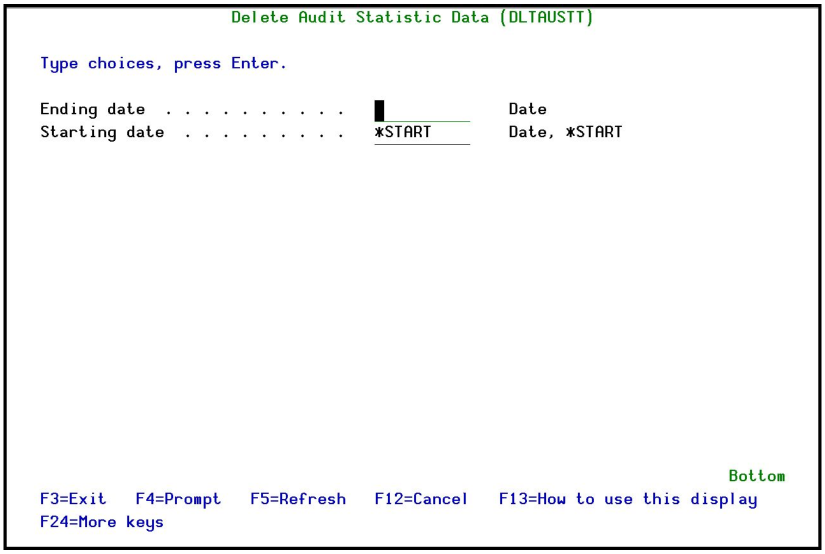
Use English File Descriptions

Select **`82 > 25. Use English File Descriptions.`**

Delete Statistic Data

You can delete the statistical data used in the GUI version of the product.

1. Select **82 > 29. Delete Statistic Data**. The **Delete Audit Statistic Data** screen appears.



```
                    Delete Audit Statistic Data (DLTAUSTT)

 Type choices, press Enter.

 Ending date . . . . . . . . . .   _            Date
 Starting date . . . . . . . . .   *START       Date, *START












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

Figure 72: Delete Audit Statistic Data

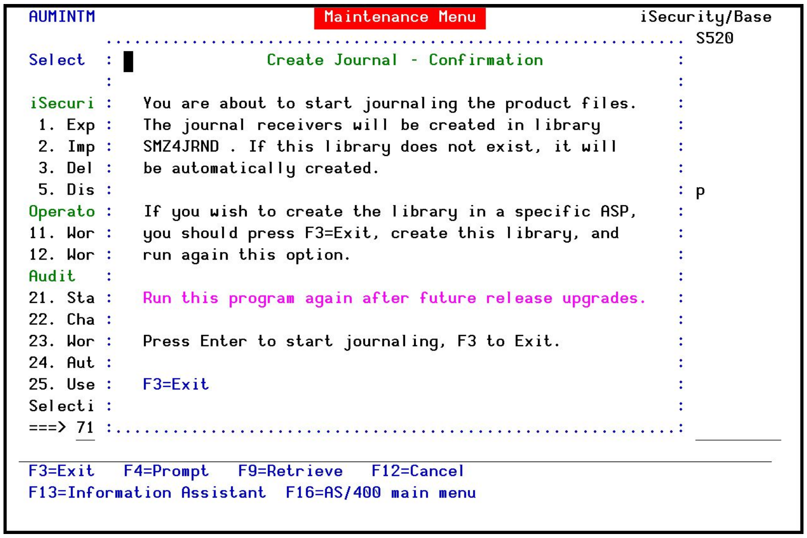
	Description
Ending date	**Enter the range of dates for which you want to delete data. The starting and ending dates are included in the range.**
Starting date	**Enter *START as a starting date to include all data from the beginning of the file.**

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

Trace Definition Modifications

Add Journal

Select **82 > 71. Add Journal** to record the system physical files changes in the data library. The **Create Journal – Confirmation** screen appears. Press **Enter** to confirm.



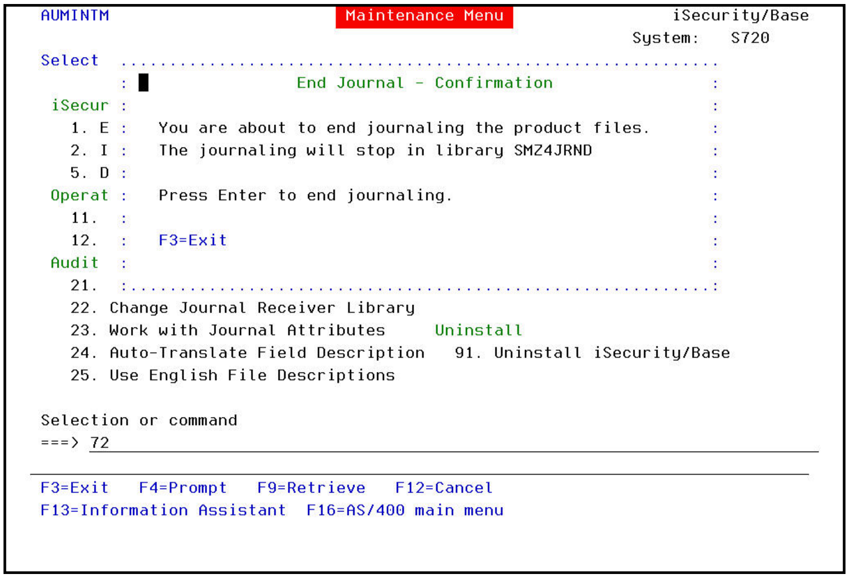
```
AUMINTM                     Maintenance Menu                 iSecurity/Base
        ............................................................ S520
Select  : █               Create Journal - Confirmation            :
        :                                                          :
iSecuri :   You are about to start journaling the product files.   :
 1. Exp :   The journal receivers will be created in library       :
 2. Imp :   SMZ4JRND . If this library does not exist, it will     :
 3. Del :   be automatically created.                              :
 5. Dis :                                                          : p
Operato :   If you wish to create the library in a specific ASP,   :
11. Wor :   you should press F3=Exit, create this library, and     :
12. Wor :   run again this option.                                 :
Audit   :                                                          :
21. Sta :   Run this program again after future release upgrades.  :
22. Cha :                                                          :
23. Wor :   Press Enter to start journaling, F3 to Exit.           :
24. Aut :                                                          :
25. Use :   F3=Exit                                                :
Selecti :                                                          :
===> 71 :..........................................................:

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 73: Create Journal – Confirmation

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

Remove Journal

Select **82 > 72. Remove Journal** to end the journaling of changes in the system physical files. The **End Journal - Confirmation** screen appears. Press **Enter** to confirm.

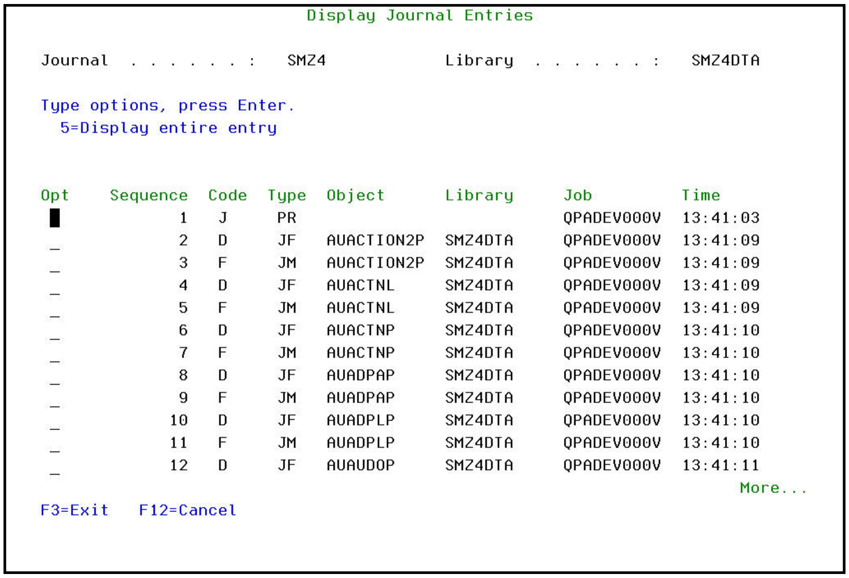


```
AUMINTM                        Maintenance Menu                iSecurity/Base
                                                           System:   S720
Select  ..............................................................
        : █                End Journal - Confirmation                :
 iSecur :                                                            :
   1. E :   You are about to end journaling the product files.       :
   2. I :   The journaling will stop in library SMZ4JRND             :
   5. D :                                                            :
 Operat :   Press Enter to end journaling.                           :
   11.  :                                                            :
   12.  :   F3=Exit                                                  :
 Audit  :                                                            :
   21.  :............................................................:
   22. Change Journal Receiver Library
   23. Work with Journal Attributes     Uninstall
   24. Auto-Translate Field Description   91. Uninstall iSecurity/Base
   25. Use English File Descriptions

Selection or command
===> 72

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 74: End Journal - Confirmation

Display Journal

1. Select **82 >79. Display Journal** to view journaled files. The **Display Journal Entries** screen appears.



```
                           Display Journal Entries

 Journal  . . . . . . . :   SMZ4           Library  . . . . . . . :   SMZ4DTA

 Type options, press Enter.
   5=Display entire entry


 Opt     Sequence  Code  Type  Object      Library     Job         Time
                1    J    PR                           QPADEV000V  13:41:03
  _             2    D    JF   AUACTION2P  SMZ4DTA     QPADEV000V  13:41:09
  _             3    F    JM   AUACTION2P  SMZ4DTA     QPADEV000V  13:41:09
  _             4    D    JF   AUACTNL     SMZ4DTA     QPADEV000V  13:41:09
  _             5    F    JM   AUACTNL     SMZ4DTA     QPADEV000V  13:41:09
  _             6    D    JF   AUACTNP     SMZ4DTA     QPADEV000V  13:41:10
  _             7    F    JM   AUACTNP     SMZ4DTA     QPADEV000V  13:41:10
  _             8    D    JF   AUADPAP     SMZ4DTA     QPADEV000V  13:41:10
  _             9    F    JM   AUADPAP     SMZ4DTA     QPADEV000V  13:41:10
  _            10    D    JF   AUADPLP     SMZ4DTA     QPADEV000V  13:41:10
  _            11    F    JM   AUADPLP     SMZ4DTA     QPADEV000V  13:41:10
  _            12    D    JF   AUAUDOP     SMZ4DTA     QPADEV000V  13:41:11
                                                                       More...
 F3=Exit   F12=Cancel
```

Figure 75: Display Journal Entries

2. Select the entry for which you want to see more details, type **5** and press **Enter**. The **Display Journal Entry** screen appears.

Other Maintenance Options

Refresh STRSEC According to *BASE

Refresh security according to Base menu.

Select **`82 > 92. Refresh STRSEC according to *BASE`** from the **`Maintenance`** menu.

Copy Queries from Backup

Copy Queries from library to library using this option.

Select **`82 > 93. Copy iSecurity Queries (CPYAUQRY)`** from the **`Maintenance`** menu.

Uninstall iSecurity/Base

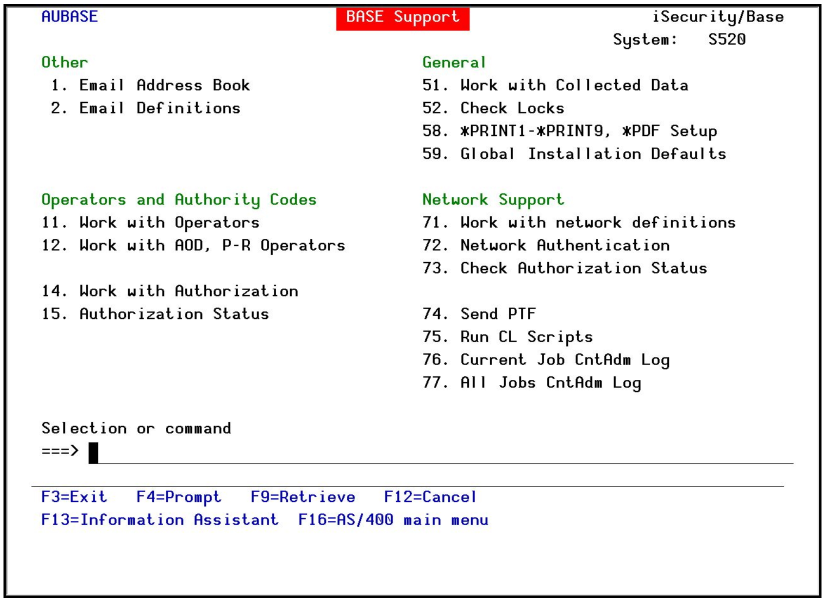
Use this feature to uninstall.

Select **`82 > 98. Uninstall SecurityP2`** from the **`Maintenance`** menu and follow the directions on the **`Uninstall SECURITYP2`** screen.

Chapter 8: Base Support Menu

The **Maintenance Menu** enables you set and display global definitions for iSecurity Part 2.

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 Action Main menu.



```
AUBASE                              BASE Support                     iSecurity/Base
                                                                   System:   S520
Other                                          General
 1. Email Address Book                         51. Work with Collected Data
 2. Email Definitions                          52. Check Locks
                                               58. *PRINT1-*PRINT9, *PDF Setup
                                               59. Global Installation Defaults

Operators and Authority Codes                  Network Support
11. Work with Operators                        71. Work with network definitions
12. Work with AOD, P-R Operators               72. Network Authentication
                                               73. Check Authorization Status
14. Work with Authorization
15. Authorization Status                       74. Send PTF
                                               75. Run CL Scripts
                                               76. Current Job CntAdm Log
                                               77. All Jobs CntAdm Log

Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

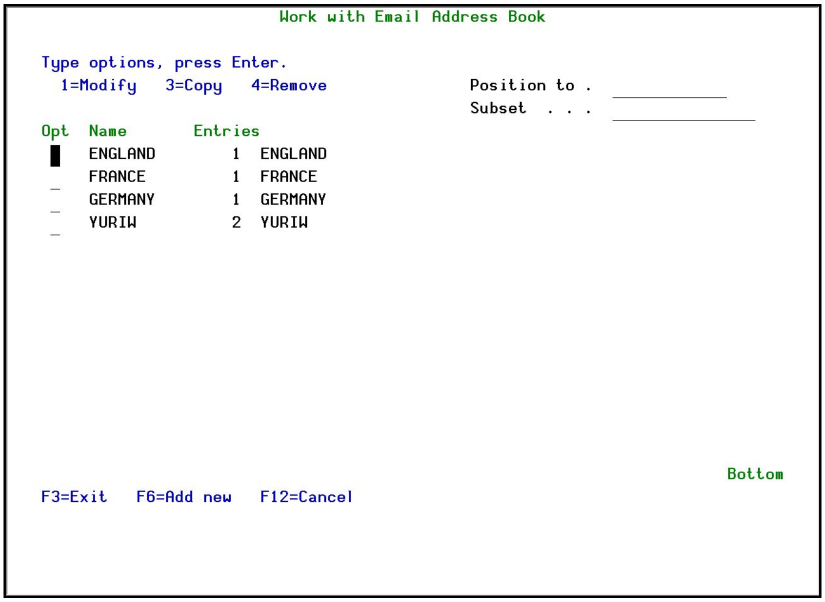
Figure 76: BASE Support

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.

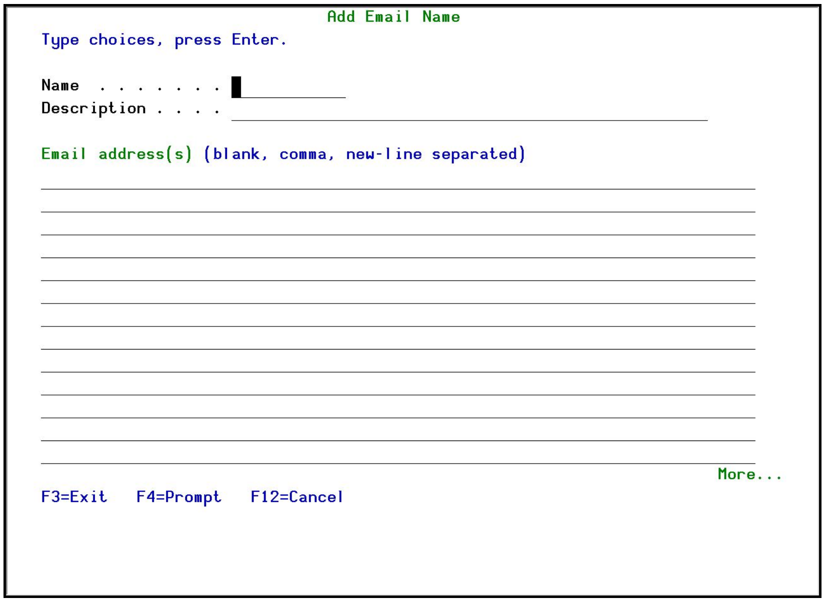
1. Select **89 > 1. Email Address Book** from the **BASE Support** menu. The **Work with Email Address Book** screen appears.



```
                          Work with Email Address Book

 Type options, press Enter.
   1=Modify   3=Copy   4=Remove                  Position to .  ____________
                                                  Subset  . . .  _______________

 Opt  Name        Entries
 █    ENGLAND         1   ENGLAND
 _    FRANCE          1   FRANCE
 _    GERMANY         1   GERMANY
 _    YURIW           2   YURIW









                                                                          Bottom
 F3=Exit   F6=Add new   F12=Cancel
```

Figure 77: Working 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
 Type choices, press Enter.

 Name . . . . . . . ▌__________
 Description . . . . __________________________________________

 Email address(s) (blank, comma, new-line separated)
```

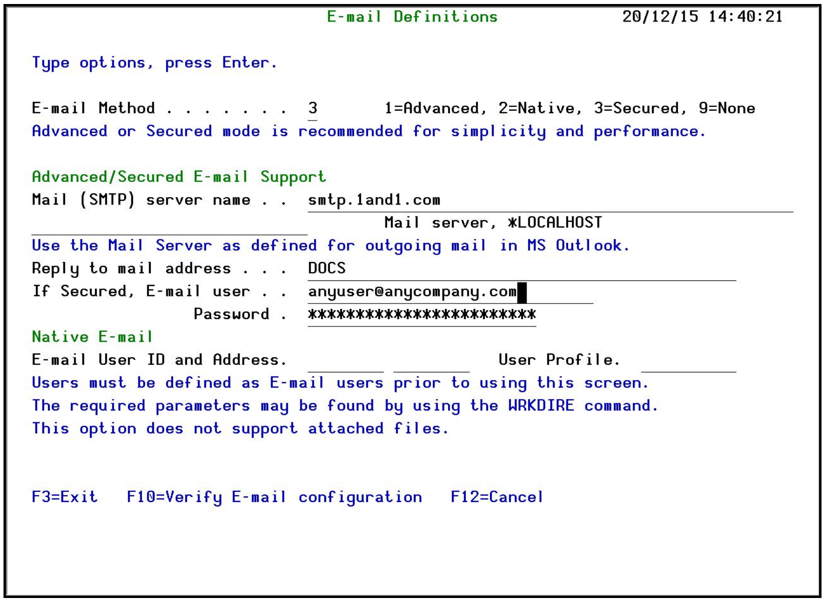
Figure 78: Add Email Name

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

Email Definitions

Action can send out automatic emails according to rules set by you.

1. Select **`89 >2. Email Definitions`** from the **`BASE Support`** menu. The **`E-mail Definitions`** screen appears.



```
                                 E-mail Definitions            20/12/15 14:40:21

  Type options, press Enter.

  E-mail Method . . . . . . .  3       1=Advanced, 2=Native, 3=Secured, 9=None
  Advanced or Secured mode is recommended for simplicity and performance.

  Advanced/Secured E-mail Support
  Mail (SMTP) server name . .  smtp.1and1.com
                                       Mail server, *LOCALHOST
  Use the Mail Server as defined for outgoing mail in MS Outlook.
  Reply to mail address . . .  DOCS
  If Secured, E-mail user . .  anyuser@anycompany.com
                   Password .  ************************
  Native E-mail
  E-mail User ID and Address.                      User Profile.
  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.


  F3=Exit   F10=Verify E-mail configuration   F12=Cancel
```

Figure 79: 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.
F10=Verify E-mail configuration	Press **F10** to open a dialog that enables you to confirm the change to email definitions and sends a confirmation email to the **Reply to mail address**. You should check that the confirmation email is received. If it is not received, there is a problem with your email definitions.

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

Operators and Authority Codes

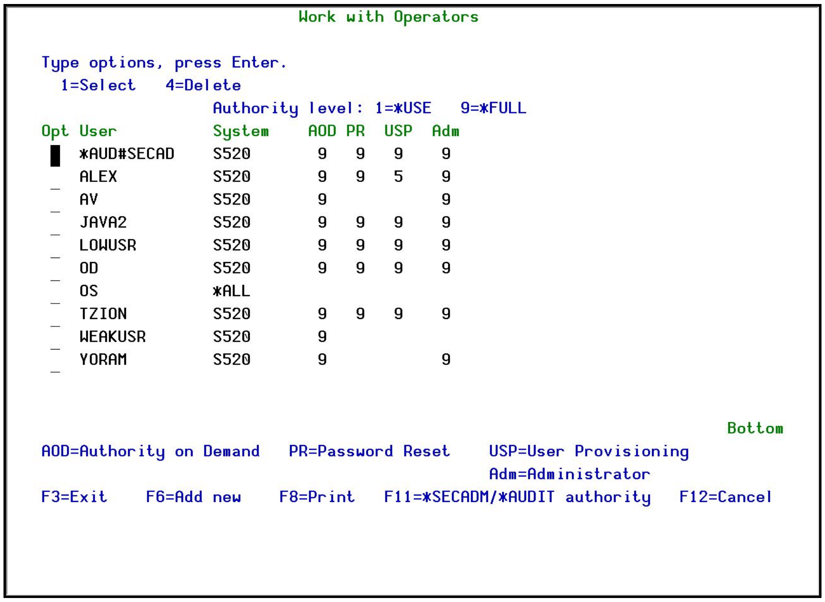
Working with Operators

For a detailed explanation of this feature, see *Modifying Operators' Authorities*.

Working 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.

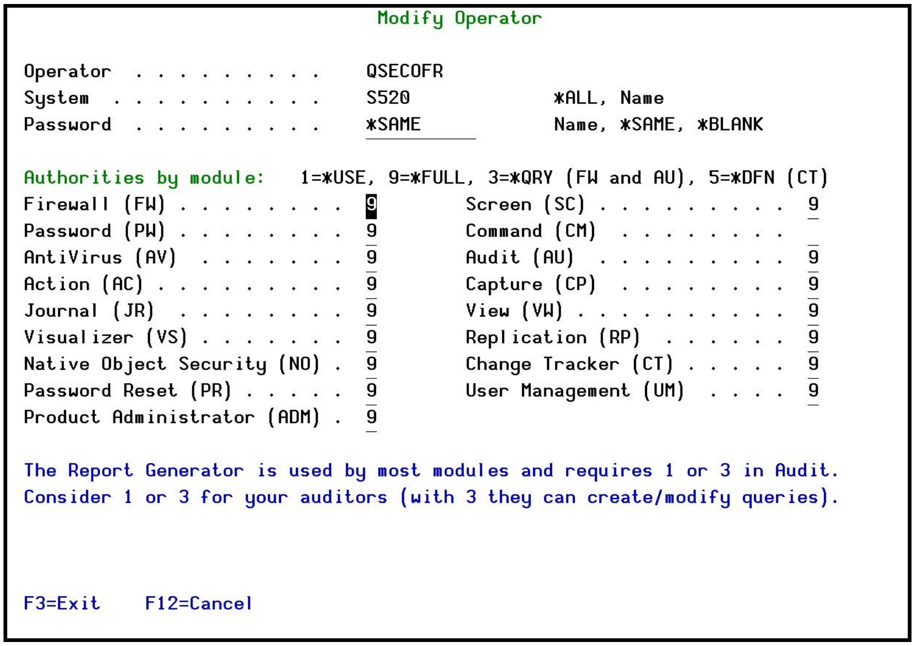
1. Select **89 >12. Work with AOD, P-R Operators** from the **BASE Support** menu. The **Work with Operators** screen appears.



```
                              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
```

Figure 80: Working 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

Operator  . . . . . . . . .    QSECOFR
System  . . . . . . . . . .    S520             *ALL, Name
Password  . . . . . . . . .    *SAME            Name, *SAME, *BLANK

Authorities by module:   1=*USE, 9=*FULL, 3=*QRY (FW and AU), 5=*DFN (CT)
Firewall (FW) . . . . . . . .  9       Screen (SC) . . . . . . . . .  9
Password (PW) . . . . . . . .  9       Command (CM)  . . . . . . . .  _
AntiVirus (AV)  . . . . . . .  9       Audit (AU)  . . . . . . . . .  9
Action (AC) . . . . . . . . .  9       Capture (CP)  . . . . . . . .  9
Journal (JR)  . . . . . . . .  9       View (VW) . . . . . . . . . .  9
Visualizer (VS) . . . . . . .  9       Replication (RP)  . . . . . .  9
Native Object Security (NO) .  9       Change Tracker (CT) . . . . .  9
Password Reset (PR) . . . . .  9       User Management (UM)  . . . .  9
Product Administrator (ADM) .  9

The Report Generator is used by most modules and requires 1 or 3 in Audit.
Consider 1 or 3 for your auditors (with 3 they can create/modify queries).



F3=Exit    F12=Cancel
```

Figure 81: Modify Operator

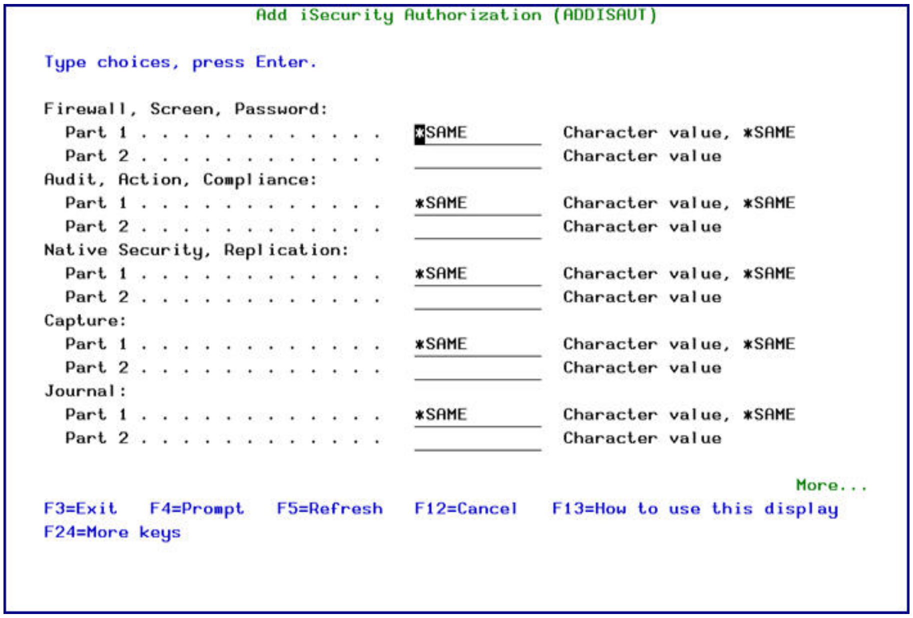
	Description
Password	**Name** = Password **Same** = Same as previous password when edited **Blank** = No password
1 = *USE	Read authority only
9 = *FULL	Read and Write authority
3 = *QRY	Run Queries. For auditor use.
5 = *DFN	For Change Tracker use.

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.

Working with Authorization

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

1. Select **89 > 14. Work with Authorization** from the **BASE Support** menu. The **Add iSecurity Authorization** screen appears.



```
                    Add iSecurity Authorization (ADDISAUT)

 Type choices, press Enter.

 Firewall, Screen, Password:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Audit, Action, Compliance:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Native Security, Replication:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Capture:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value
 Journal:
   Part 1 . . . . . . . . . . . .   *SAME         Character value, *SAME
   Part 2 . . . . . . . . . . . .                 Character value

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

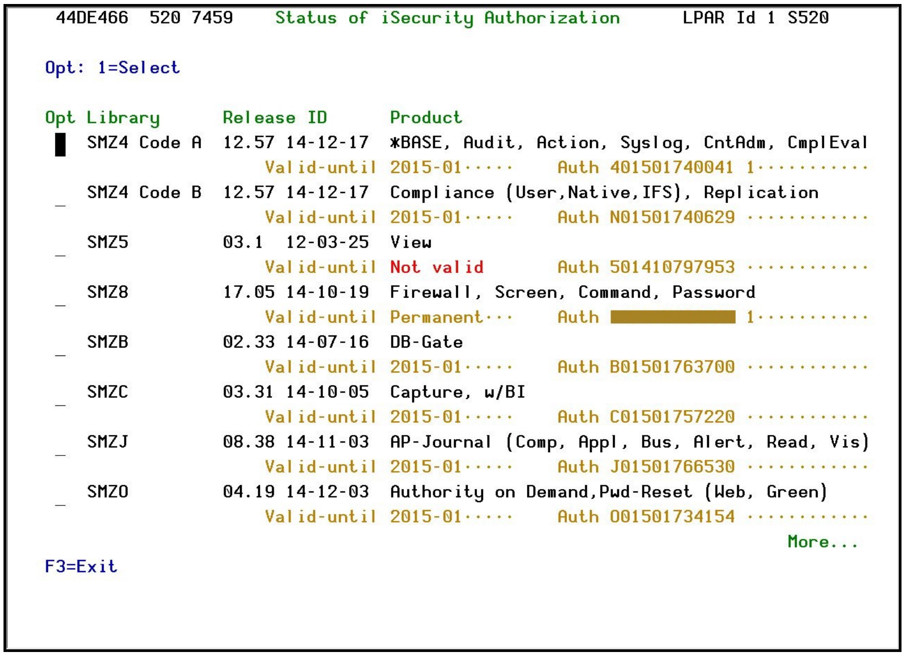
Figure 82: Add iSecurity Authorization (ADDISAUT)

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 **89 >15. Authorization Status** from the **BASE Support** menu. The **Status of iSecurity Authorization** screen appears.



```
  44DE466  520 7459    Status of iSecurity Authorization      LPAR Id 1 S520

 Opt: 1=Select

 Opt Library      Release ID      Product
  █  SMZ4 Code A  12.57 14-12-17  *BASE, Audit, Action, Syslog, CntAdm, CmplEval
                      Valid-until 2015-01·····     Auth 401501740041 1···········
  _  SMZ4 Code B  12.57 14-12-17  Compliance (User,Native,IFS), Replication
                      Valid-until 2015-01·····     Auth N01501740629 ············
  _  SMZ5         03.1  12-03-25  View
                      Valid-until Not valid        Auth 501410797953 ············
  _  SMZ8         17.05 14-10-19  Firewall, Screen, Command, Password
                      Valid-until Permanent···     Auth [redacted] 1···········
  _  SMZB         02.33 14-07-16  DB-Gate
                      Valid-until 2015-01·····     Auth B01501763700 ············
  _  SMZC         03.31 14-10-05  Capture, w/BI
                      Valid-until 2015-01·····     Auth C01501757220 ············
  _  SMZJ         08.38 14-11-03  AP-Journal (Comp, Appl, Bus, Alert, Read, Vis)
                      Valid-until 2015-01·····     Auth J01501766530 ············
  _  SMZO         04.19 14-12-03  Authority on Demand,Pwd-Reset (Web, Green)
                      Valid-until 2015-01·····     Auth O01501734154 ············
                                                                        More...
 F3=Exit
```

Figure 83: 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

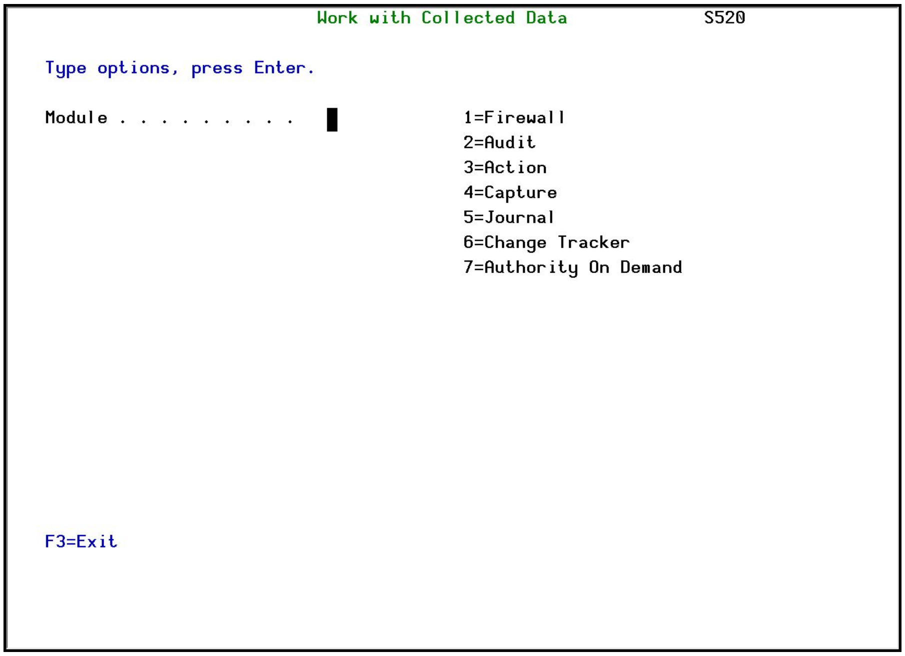
Permanent codes have deliberately been hidden in this screenshot.

General

Working 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.

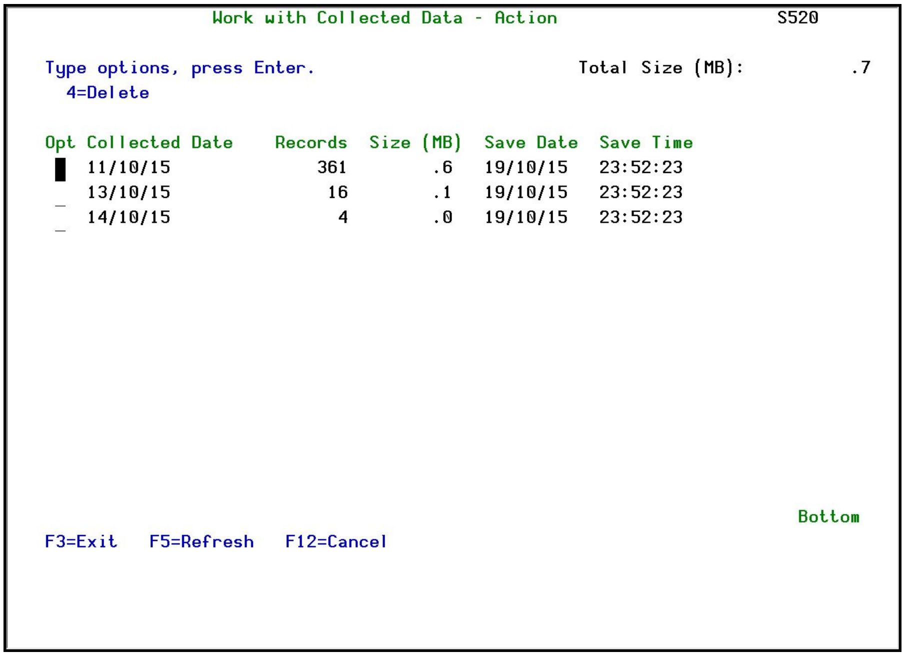
1. Select **`89 > 51. Work with Collected Data`** from the **`BASE Support`** menu. The **`Work with Collected Data`** screen appears.



```
                              Work with Collected Data             S520

   Type options, press Enter.

   Module . . . . . . . . .                   1=Firewall
                                              2=Audit
                                              3=Action
                                              4=Capture
                                              5=Journal
                                              6=Change Tracker
                                              7=Authority On Demand

   F3=Exit
```

Figure 84: Working with Collected Data

2. Enter **3** (Action) and press **`Enter`**. The **`Work with Collected Data – Action`** screen appears.



```
                   Work with Collected Data - Action                    S520

 Type options, press Enter.                           Total Size (MB):          .7
   4=Delete

 Opt Collected Date     Records  Size (MB)  Save Date  Save Time
     11/10/15               361        .6   19/10/15   23:52:23
  _  13/10/15                16        .1   19/10/15   23:52:23
  _  14/10/15                 4        .0   19/10/15   23:52:23













                                                                           Bottom
 F3=Exit   F5=Refresh   F12=Cancel
```

Figure 85: Working with Collected Data - Audit

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

Purging all ACTION data

You can use the following command to purge all **Audit** data:

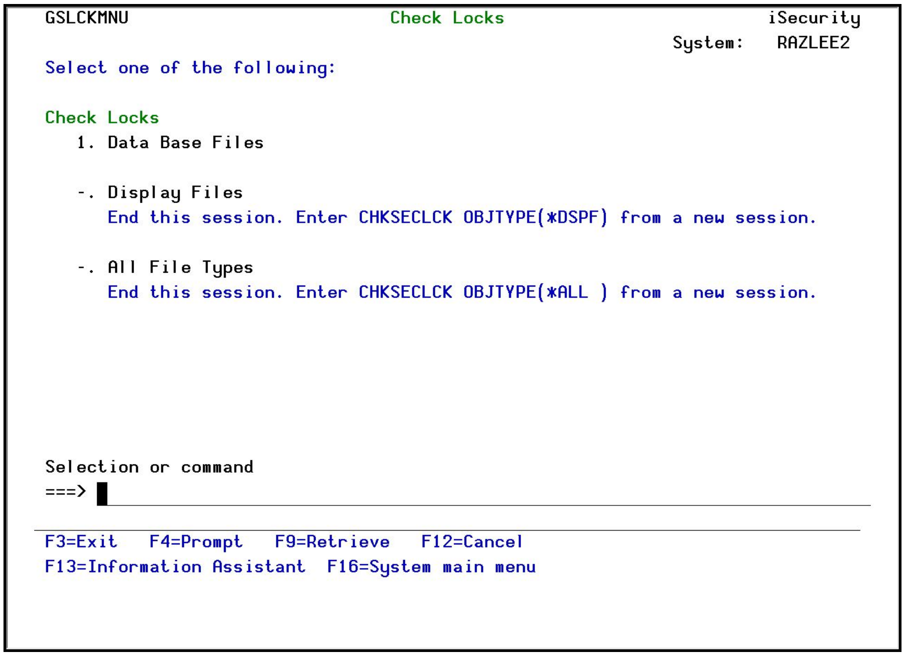
*RMVM SMZ4DTA/AUCC *ALL*

Before you run these commands, you should back up the **Action** data to offline storage.

Check Locks

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

1. Select **`89 > 52. Check Locks`** from the **`BASE Support`** menu. The **`Check Locks`** screen appears.



```
 GSLCKMNU                        Check Locks                       iSecurity
                                                          System:   RAZLEE2
 Select one of the following:

 Check Locks
    1. Data Base Files

    -. Display Files
       End this session. Enter CHKSECLCK OBJTYPE(*DSPF) from a new session.

    -. All File Types
       End this session. Enter CHKSECLCK OBJTYPE(*ALL ) from a new session.





 Selection or command
 ===>

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

Figure 86: Check Locks

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

*PRINT1-*PRINT9 Setup

Audit enables 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.

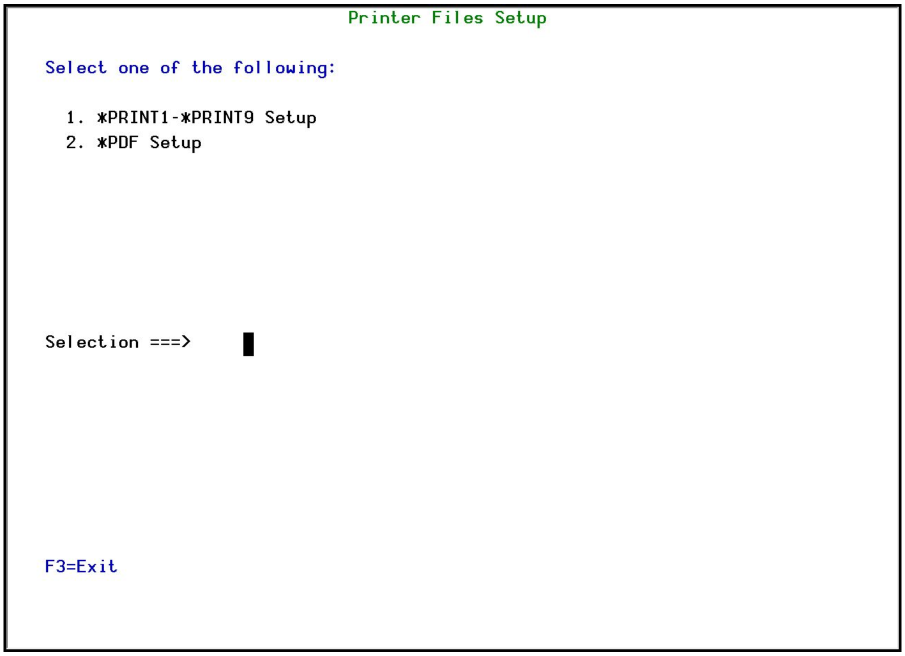
Output to one of the nine remote printers is directed to a special output queue specified on the ***PRINT1-*PRINT9 User Parameters** screen, which, in turn, directs the output to a print queue on the remote system. You use the *CHGOUTQ* command to specify the IP address of the designated remote location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

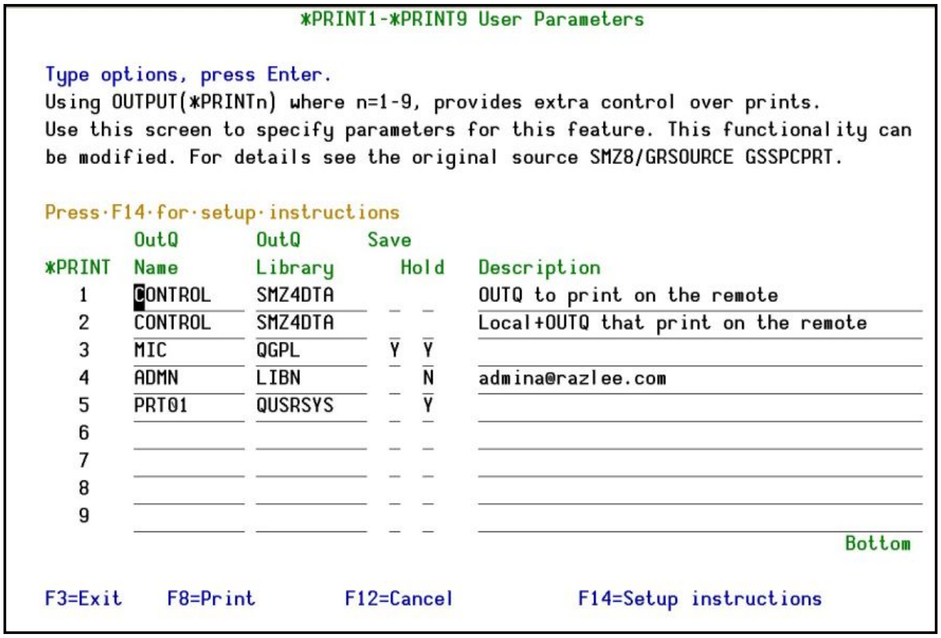
1. Select **89 > 58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



```
                                Printer Files Setup

 Select one of the following:

   1. *PRINT1-*PRINT9 Setup
   2. *PDF Setup




 Selection ===>



 F3=Exit
```

Figure 87: Printer Files Setup

2. Enter **1** and press **Enter**. The ***PRINT1 - *PRINT9 Setup** screen appears.



```
                    *PRINT1-*PRINT9 User Parameters

Type options, press Enter.
Using OUTPUT(*PRINTn) where n=1-9, provides extra control over prints.
Use this screen to specify parameters for this feature. This functionality can
be modified. For details see the original source SMZ8/GRSOURCE GSSPCPRT.

Press·F14·for·setup·instructions
         OutQ          OutQ         Save
*PRINT   Name          Library        Hold    Description
   1     CONTROL       SMZ4DTA        _  _    OUTQ to print on the remote
   2     CONTROL       SMZ4DTA                Local+OUTQ that print on the remote
   3     MIC           QGPL           Y  Y
   4     ADMN          LIBN           _  N    admina@razlee.com
   5     PRT01         QUSRSYS        _  Y
   6                                  _  _
   7                                  _  _
   8                                  _  _
   9                                  _  _
                                                                          Bottom

F3=Exit     F8=Print        F12=Cancel           F14=Setup instructions
```

Figure 88: 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.

	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')

	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:

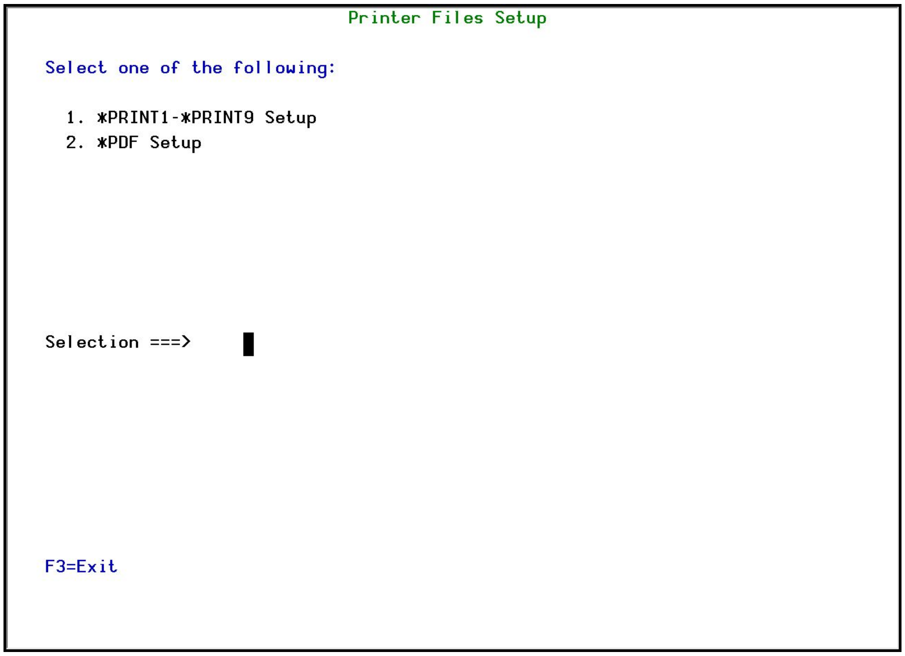
```
CHGOUTQ OUTQ(CONTROL/SMZTMPA) RMTSYS(*INTNETADR)
+  RMTPRTQ(MYOUTQ) AUTOSTRWTR(1) CNNTYPE(*IP) TRANSFORM(*NO)
+  INTNETADR(1.1.1.100)
```

*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:

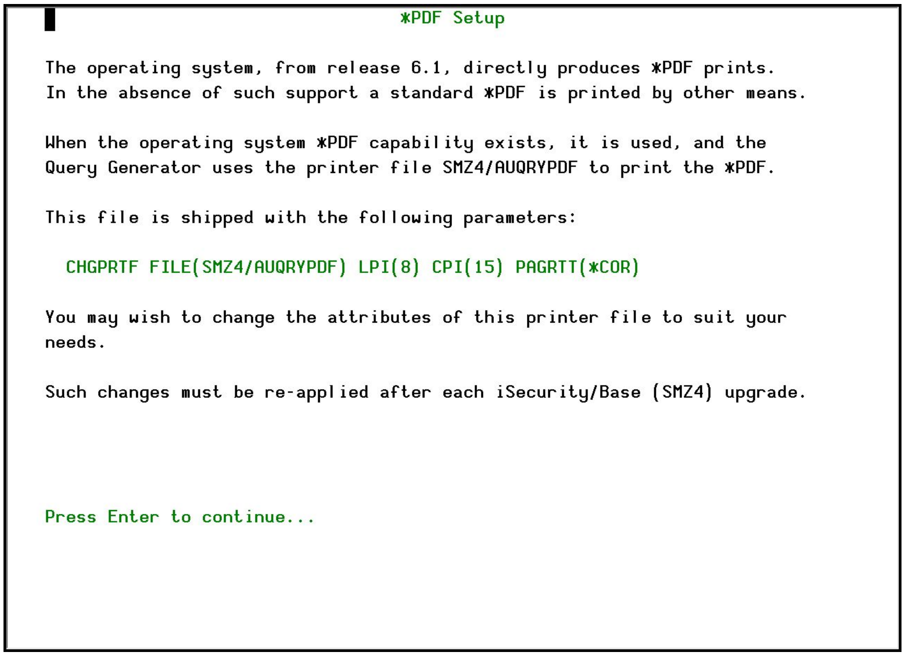
1. Select **89 > 58. *PRINT1 - *PRINT9, PDF Setup** from the **BASE Support** menu. The **Printer Files Setup** screen appears.



```
                              Printer Files Setup

 Select one of the following:

   1. *PRINT1-*PRINT9 Setup
   2. *PDF Setup







 Selection ===>





 F3=Exit
```

Figure 89: Printer Files Setup

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



```
                                  *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.

When the operating system *PDF capability exists, it is used, and the
Query Generator uses the printer file SMZ4/AUQRYPDF to print the *PDF.

This file is shipped with the following parameters:

  CHGPRTF FILE(SMZ4/AUQRYPDF) LPI(8) CPI(15) PAGRTT(*COR)

You may wish to change the attributes of this printer file to suit your
needs.

Such changes must be re-applied after each iSecurity/Base (SMZ4) upgrade.



Press Enter to continue...
```

Figure 90: *PDF Setup

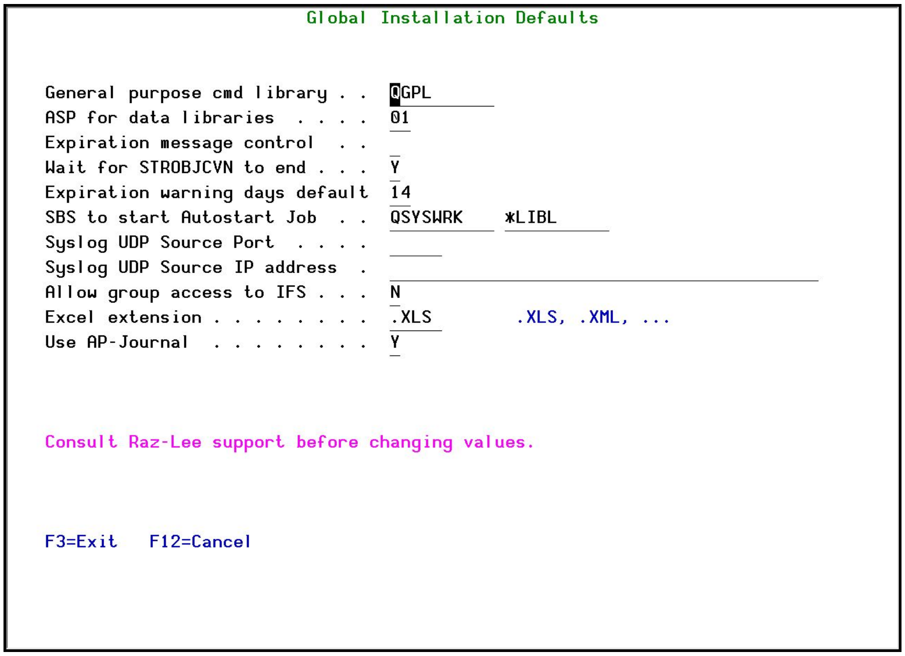
3. Follow the instructions on the screen.

NOTE: You must re-perform this task after every upgrade of **Audit**.

Global Installation Defaults

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

1. Select **89 > 59. Global Installation Defaults** from the **BASE Support** menu. The **Global Installation Defaults** screen appears.



```
                          Global Installation Defaults


   General purpose cmd library . .  QGPL
   ASP for data libraries  . . . .  01
   Expiration message control  . .  _
   Wait for STROBJCVN to end . . .  Y
   Expiration warning days default  14
   SBS to start Autostart Job  . .  QSYSWRK    *LIBL
   Syslog UDP Source Port  . . . .  _____
   Syslog UDP Source IP address  .  ________________________________________
   Allow group access to IFS . . .  N
   Excel extension . . . . . . . .  .XLS       .XLS, .XML, ...
   Use AP-Journal  . . . . . . . .  Y



   Consult Raz-Lee support before changing values.



   F3=Exit   F12=Cancel
```

Figure 91: 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
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	**Y**=Yes

Parameter	Description
access to IFS	**N**=No Allow access to IFS from group profiles.
Excel extension	
Use AP-Journal	

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

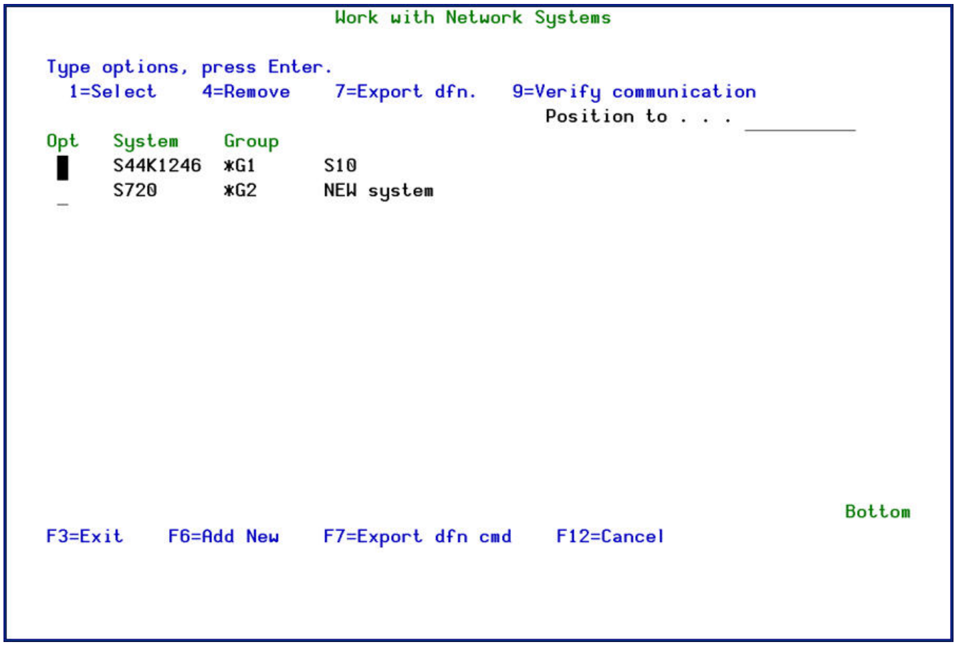
NOTE: You should not change any of the values in this screen without first consulting with Raz-Lee support staff at support@razlee.com.

Network Support

Working 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.

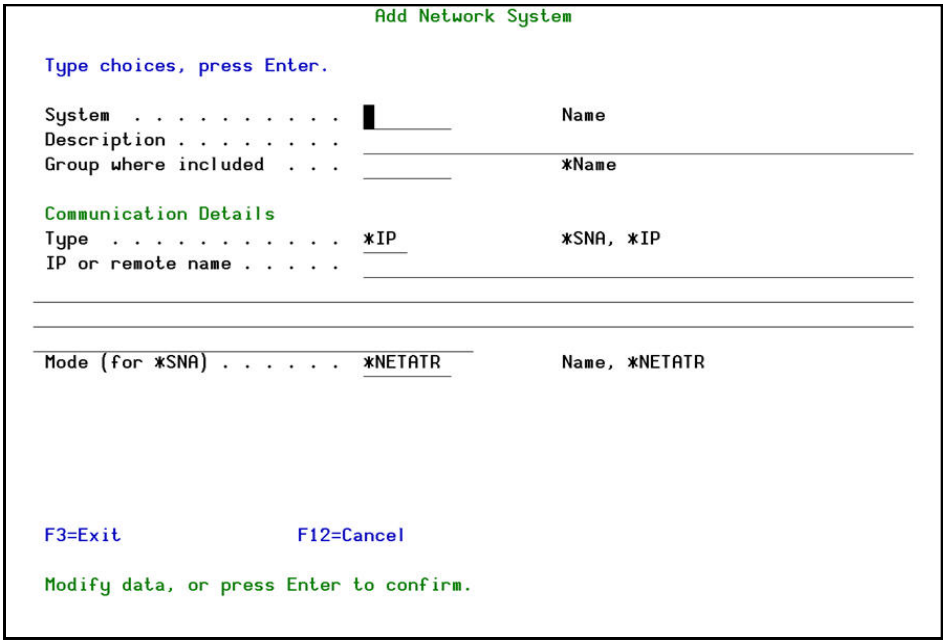
1. Select **`89 > 71. Work with network definitions`** from the **`BASE Support`** menu. The **`Work with Network Systems`** screen appears.



```
                              Work with Network Systems

 Type options, press Enter.
   1=Select     4=Remove     7=Export dfn.    9=Verify communication
                                                  Position to . . .  __________

 Opt    System     Group
 █      S44K1246   *G1        S10
        S720       *G2        NEW system
 _














                                                                          Bottom
 F3=Exit     F6=Add New     F7=Export dfn cmd     F12=Cancel
```

Figure 92: Working with Network Systems

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



```
                              Add Network System

 Type choices, press Enter.

 System . . . . . . . . . .   _______        Name
 Description . . . . . . .    ________________________________________
 Group where included . . .   _______        *Name

 Communication Details
 Type . . . . . . . . . . .   *IP            *SNA, *IP
 IP or remote name . . . . .  ________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________
 Mode (for *SNA) . . . . . .  *NETATR        Name, *NETATR






 F3=Exit              F12=Cancel

 Modify data, or press Enter to confirm.
```

Figure 93: Add Network System

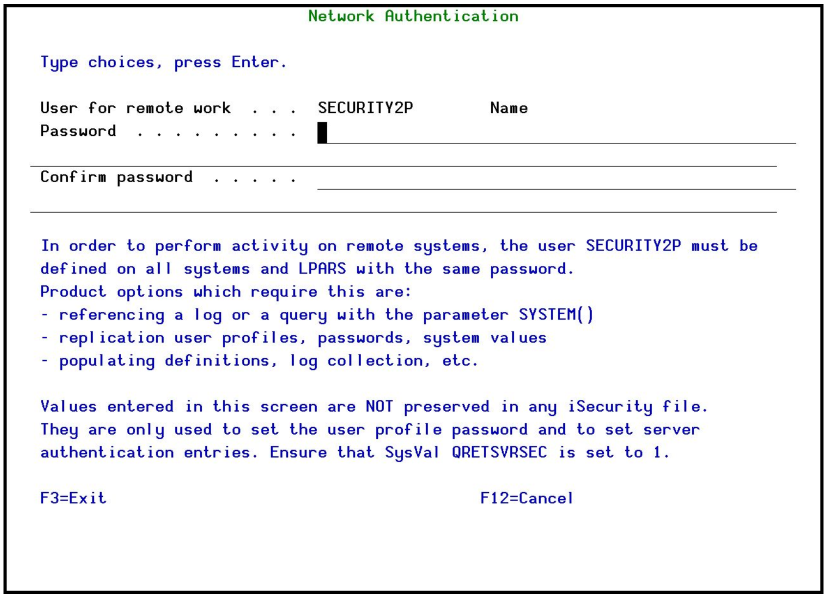
Parameter	Description
`System`	The name of the system
`Description`	A meaningful description of the system
`Group where included`	Enter the name of the group to which the system is assigned
`Where is QAUDJRN analyzed`	Give the name of the System where QAUDJRN is analyzed. Enter **`*SYSTEM`** if it is 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 **89 > 72. Network Authentication** from the **BASE Support** menu. The **Network Authentication** screen appears.



```
                          Network Authentication

 Type choices, press Enter.

 User for remote work  . . .   SECURITY2P        Name
 Password  . . . . . . . . .   █

 Confirm password  . . . . .

 In order to perform activity on remote systems, the user SECURITY2P must be
 defined on all systems and LPARS with the same password.
 Product options which require this are:
 - referencing a log or a query with the parameter SYSTEM()
 - replication user profiles, passwords, system values
 - populating definitions, log collection, etc.

 Values entered in this screen are NOT preserved in any iSecurity file.
 They are only used to set the user profile password and to set server
 authentication entries. Ensure that SysVal QRETSVRSEC is set to 1.

 F3=Exit                                      F12=Cancel
```

Figure 94: Working with Network Systems

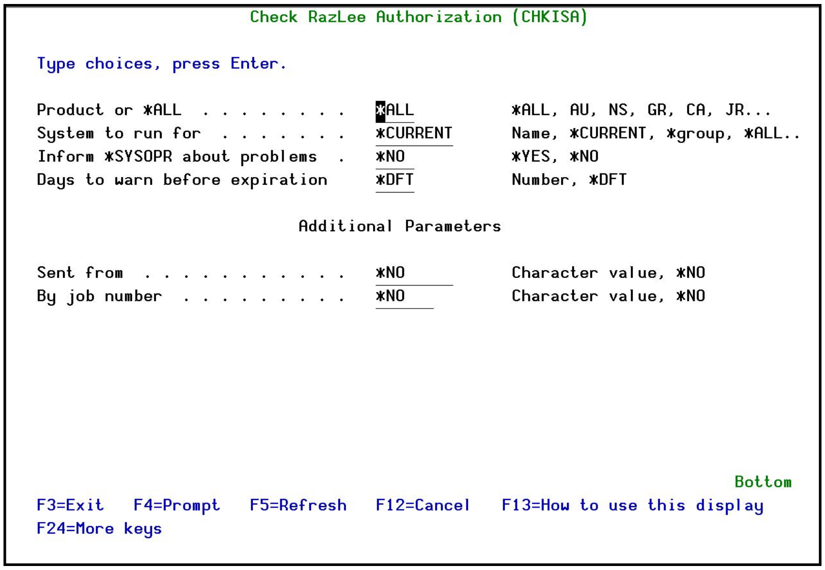
2. Enter the .SECURITY2P user password twice and press **Enter**.

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 enable the system to run network commands and scripts. See *Network Support*, for more details.

1. Select **89 > 73. Check Network Authority Status** from the **BASE Support** menu. The **Check Razlee Authorization** screen appears.



```
                         Check RazLee Authorization (CHKISA)

 Type choices, press Enter.

 Product or *ALL  . . . . . . . .   *ALL          *ALL, AU, NS, GR, CA, JR...
 System to run for  . . . . . . .   *CURRENT      Name, *CURRENT, *group, *ALL..
 Inform *SYSOPR about problems  .   *NO           *YES, *NO
 Days to warn before expiration     *DFT          Number, *DFT

                           Additional Parameters

 Sent from  . . . . . . . . . . .   *NO           Character value, *NO
 By job number  . . . . . . . . .   *NO           Character value, *NO





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

Figure 95: 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**

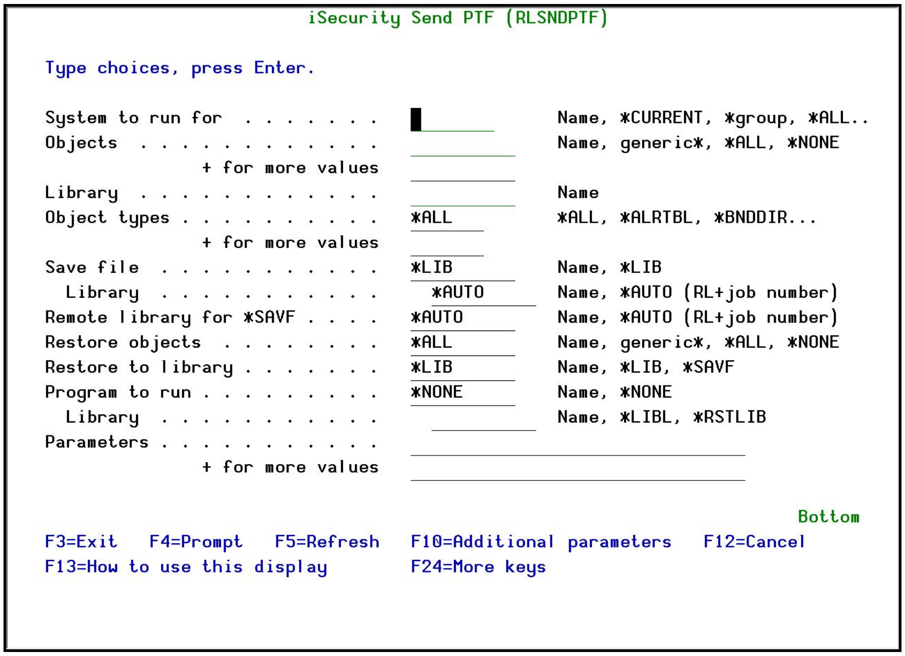
2. Select the correct options and press **Enter**.

Send PTF

This option enables 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 *Working with network definitions* on page *202*, and that you define user SECURITY2P on all nodes, using the same password, as described in *Network Authentication* on page *204*.

1. Select **89 > 74. Send PTF** from the **BASE Support** menu. The **iSecurity Send PTF (RLSNDPTF)** screen appears.



```
                          iSecurity Send PTF (RLSNDPTF)

 Type choices, press Enter.

 System to run for  . . . . . . .                Name, *CURRENT, *group, *ALL..
 Objects  . . . . . . . . . . . .                Name, generic*, *ALL, *NONE
               + for more values
 Library  . . . . . . . . . . . .                Name
 Object types . . . . . . . . . .   *ALL         *ALL, *ALRTBL, *BNDDIR...
               + for more values
 Save file  . . . . . . . . . . .   *LIB         Name, *LIB
   Library  . . . . . . . . . . .     *AUTO      Name, *AUTO (RL+job number)
 Remote library for *SAVF . . . .   *AUTO        Name, *AUTO (RL+job number)
 Restore objects  . . . . . . . .   *ALL         Name, generic*, *ALL, *NONE
 Restore to library . . . . . . .   *LIB         Name, *LIB, *SAVF
 Program to run . . . . . . . . .   *NONE        Name, *NONE
   Library  . . . . . . . . . . .                Name, *LIBL, *RSTLIB
 Parameters . . . . . . . . . . .
               + for more values

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

Figure 96: 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>
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 enables 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

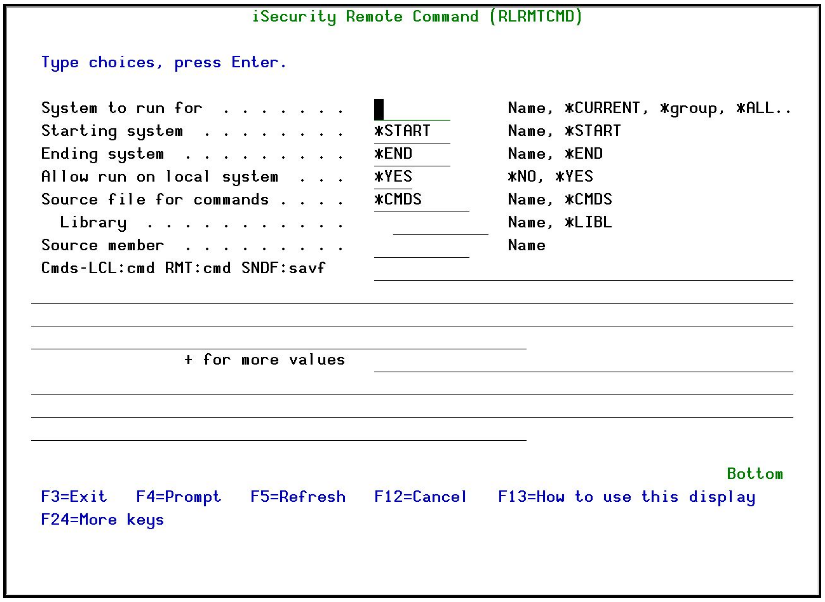
RMT: Run the following command on the remote system

SNDF: Send the save file (format: library/file) to RLxxxxxxxx/file (xxxxxxxx is the local system name)

You can use this option to define check system authorities, as described in *Check Authorization Status*.

Before you can use this option, ensure that you define the entire network, as described in *Network Support*, and that you define user SECURITYP2 on all nodes, using the same password, as described in *Working with Users*.

1. Select **89 > 75. Run CL Scripts** from the **BASE Support** menu. The **iSecurity Remote Command (RLRMTCMD)** screen appears.



```
                    iSecurity Remote Command (RLRMTCMD)

 Type choices, press Enter.

 System to run for  . . . . . . .                 Name, *CURRENT, *group, *ALL..
 Starting system  . . . . . . . .  *START         Name, *START
 Ending system  . . . . . . . . .  *END           Name, *END
 Allow run on local system  . . .  *YES           *NO, *YES
 Source file for commands . . . .  *CMDS          Name, *CMDS
   Library  . . . . . . . . . . .                 Name, *LIBL
 Source member  . . . . . . . . .                 Name
 Cmds-LCL:cmd RMT:cmd SNDF:savf

                + for more values

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

Figure 97: 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
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 **89 > 76. Current Job CntAdm Log** from the **BASE Support** menu to display the current job log.

All Jobs Central Administration Messages

Select **89 > 77. All Jobs CntAdm Log** from the **BASE Support** menu to display the job log for all jobs.