iSecurity Audit

User Guide
Version 14.27

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

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

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

Native IBM i (OS/400) User Interface

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

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

Conventions Used in the Document

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

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

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

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

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRAUD **`> 81 > 32`**

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

Menus

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

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

Data Entry Screens

Data entry screens include many convenient features such as:

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

The following describes the different data entry screens.

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

The following function keys may appear on data entry screens.

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

Legal Notice

Manual Revised: Sunday, May 28, 2023

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)

Preface

In today's increasingly complex business environment, security auditing is a key component of an organizational IT security program. Simply creating a security policy and purchasing security software tools is not enough. Management should ensure that security policies and procedures are properly implemented and enforced. In addition, managers must be able to evaluate and test the effectiveness of these policies on a continuing basis.

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

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

Powerful and flexible auditing tools are required to meet these requirements.

Traditionally, IBM i systems have offered the strongest security features in the industry. These features, however, are effective only for stand-alone, terminal based computing environments that have all but passed from the scene. The contemporary environment is highly interconnected, based on multiple computing platforms, and incorporates a high degree of data sharing.

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

Over the past several years, IBM has begun to take IBM i security auditing seriously. The current version of the IBM i operating IBM includes over

seventy different audit types and a large number of sub-classifications. Each individual audit type covers a particular event or transaction, and specific information relating to that event is stored in an audit database (QAUDJRN, also called the security audit journal by IBM). As well as objects, user profiles and security, many of these new audit types relate to connectivity, communication protocols, and distributed database issues.

This security audit journal is difficult and inefficient to use without assistance. Audit allows you to use this information efficiently.

Overview

Audit enhances native IBM i (OS/400) auditing by adding several powerful new features and by providing a user-friendly interface for working with the large number of system values and parameters. All of these new features are based on data written to the IBM i security audit journal (QAUDJRN). Today, QUADJRN sub-types can be both M-moved and R-renamed according to either library or file name, thereby simplifying the filtering process of data fields.

The following flow chart illustrates the relationship and data flow between IBM i and Audit.

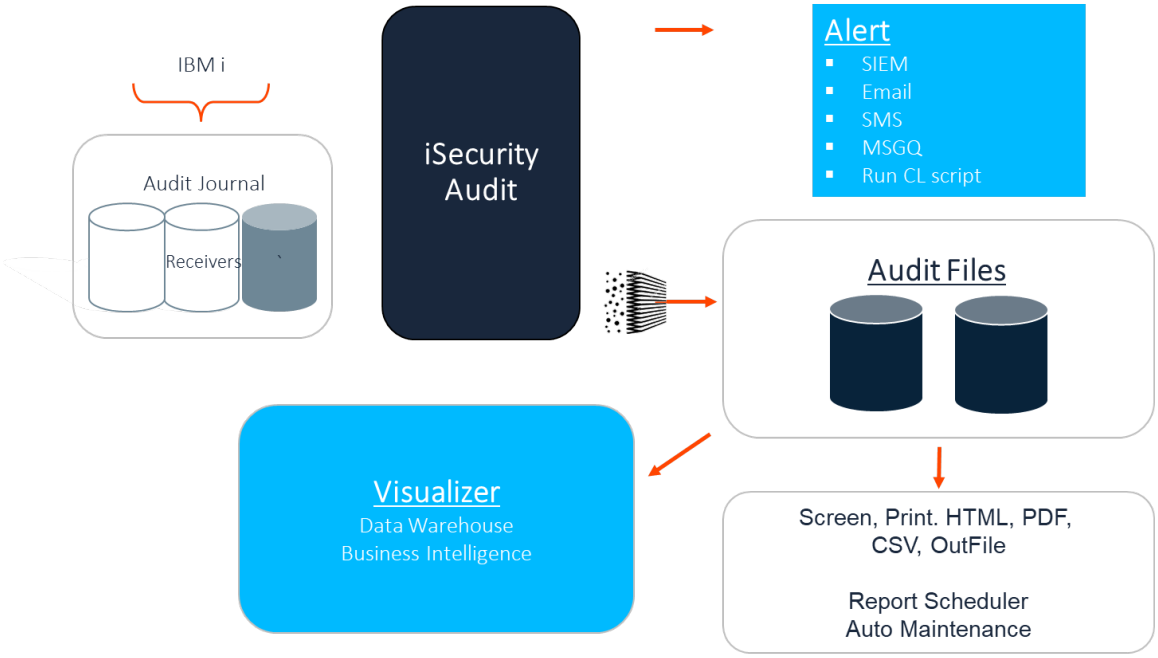


Figure 1: IBM i (OS/400) & Audit Flow Chart

IBM i (OS/400) Audit Settings Made Easy

You should use Audit to define the IBM i (OS/400) system values, user profile parameters and object parameters that make up the audit settings. All of these parameters are available from the IBM i Audit Features menu in Audit. You should never again have to use the IBM i commands to maintain audit settings.

IBM i records user activities and object access attempts to the security audit journal according to the audit settings currently in force. This is referred to as the Current Setting. You can create and save groups of settings for future use.

If the IBM i audit is not working and is activated after activating real-time [[[Undefined variable Audit.ProductName]]], the result will include:

- IBM i (OS/400) audit according to the selected audit level
- Real-time Audit
- Actions based on the real time Audit
- The disk-space consumed by both the IBM i (OS/400) system journal and by the real-time Audit logs

Some of the entries (for example, object auditing: ZR=read object) influence performance and disk space. Use the Visualizer to recognize what are the largest entry types in the organization and how to minimize the performance impact. To learn how to define the Audit settings according to your organization's needs, see IBM i (OS/400) Audit Settings.

Real-Time Detection

The most important feature of [[[Undefined variable Audit.ProductName]]] is the ability to examine security events in real time. When IBM i (OS/400) detects an event covered by the current audit settings, it writes an entry in the security audit journal. At the same time, Audit checks whether a real time detection rule exists for this event. If such a rule exists, the system may then record the event in the Audit history log and may trigger an action as specified by the rule definition. Responsive actions are performed by Action, a companion product that is sold separately.

A series of user-defined rules and actions govern real-time detection. Rules identify which specific events trigger actions and under what conditions the response should occur. Actions define those specific responsive actions that take place whenever rule conditions are met.

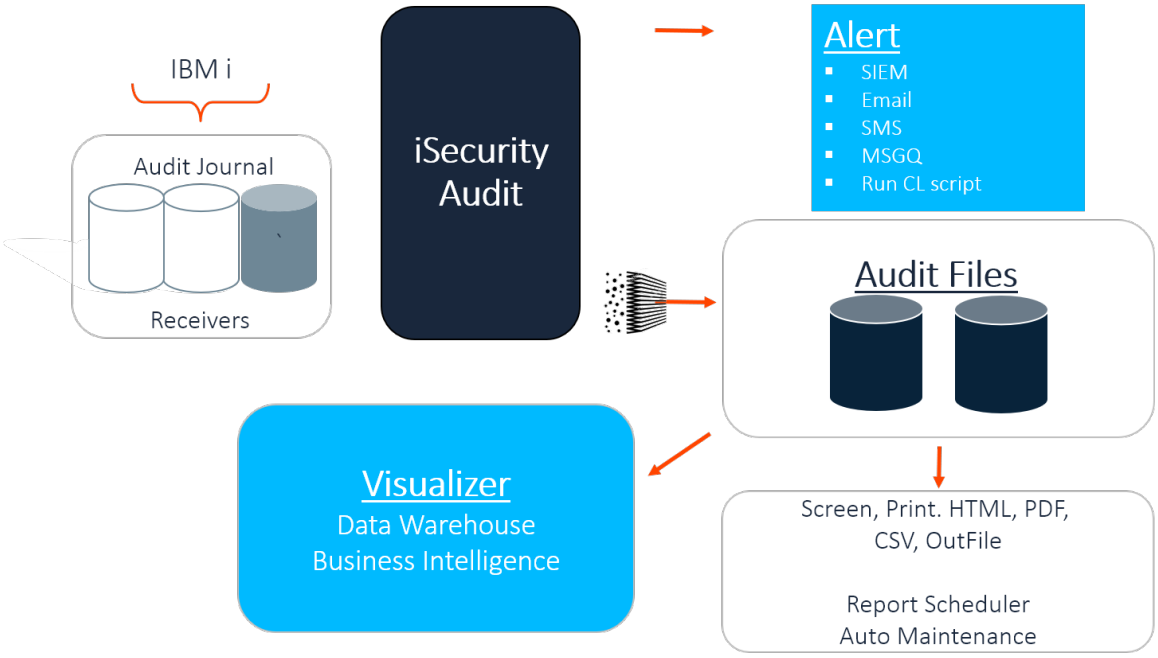


Figure 2: Audit's Real-Time Detection Process

Integration with Action

As you can see from the above chart, one of the main advantages of real-time detection lies in its integration with the Action product. Action physically sends the alert messages and executes command scripts triggered by Audit.

Rules

Rules determine which conditions trigger an action and/or are recorded in the history log. For example, you can create a rule that triggers a message whenever a specific user modifies any **`*FILE`** object, located in the **`ACCOUNTING`** folder, on or after 05-January-2019.

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.

Audit incorporates a Rule Wizard to assist users in defining complex conditions.

Actions

An action may be an alert message sent to designated personnel or a predefined command script that runs automatically. You can configure [[[Undefined variable Audit.ProductName]]] to send alert messages as email, IBM i (OS/400) system messages, network messages, SMS messages to cellular telephones, or beeper (pager) messages.

History Log

[[[Undefined variable Audit.ProductName]]] maintains a separate history log in addition to the security audit journal. The primary purpose of the log is to facilitate the powerful query and reporting features without the need to extract data from the security audit journal.

[[[Undefined variable Audit.ProductName]]]records event data in the history log, only when instructed to do so by real-time detection rules. Therefore, the log typically contains only a subset of the events recorded in the security audit journal. You should create rules only for those events that you wish to track using the query and reporting features.

There is an option that allows you to copy all events to the log, unless a rule specifically excludes it. However, we do not recommend this feature because of performance degradation and disk space requirements.

- Neither **QSECOFR** nor any other user can update or delete records from the file that contains the log. This is true even when using the *SQL*, *DFU*, *CHGFC* or other commands.
- Users authorized as Administrators for the **Work with Operators** option in the BASE Support menu (*STRAUD*> **89 > 11**) can set the number of days that data is kept online.
- Users authorized as Administrators for the **Work with Operator**s option in the BASE Support menu (*STRAUD*> **89 > 11**) can use the **Work with Collected Data** option in the BASE Support menu (*STRAUD* **> 89 > 51**) to remove data of full days.
- To know what user **QSECOFR** has done in the product log files (for example, *RMVM* or *CLRPFM*), use the **Add Journal** option in the **Maintenance Menu** (*STRAUD* **> 82 > 71)**. Every operation with the definition file is recorded. To control the logs, use the *STRJRNPF* command for files **SMZ4DTA/AUXX**, **SMZ4DTA/AUCC**, and **SMZTMPA/GSCALP**.

  NOTE: This will extend the data space requirements.

- **SECOFR** as well as any other authorized user can use the **Real Time Auditing** option (*STRAUD* **> 11**) to change the logging option per any audit type or the combination of field values in audit type.

Creating and Running Queries and Reports

Audit includes powerful tools for creating and viewing queries, reports, and logs. Many of these tools are also available within other iSecurity products, giving a consistent experience in using them.

You can use several powerful and user-friendly tools to create output that contains only the data that you need to see, in a format that is useful to you.

The reporting features are:

- Display of log – showing the collected information of logs in either a message format which looks similar to a job log, or in a tabular view
- Query generator – a comprehensive report generator which has tremendous filtering capabilities and can create reports for one or more systems without copying the report definition
- Compliance Evaluator – score cards type reports to verify compliance with predefined targets
- Report Scheduler - enabling automatic run of groups of reports and logs
- Visualizer – BI (Business Intelligence) for activity logs. It uses a data warehouse with compressed information, making it possible to keep information for long periods. This is available in the GUI interface only.

Possible outputs for reports include display on the Green or GUI screen, HTML, PDF, CSV (Excel), and OUTFILE (Output file). When using the GUI, the results of a query can also be directed to the Visualizer to enabling using BI methods to deal with the results.

Once a report is defined on a system, it can be run on information on the current system, any other system, or any group of systems. There is no need to copy the definition to any other system.

Result files are named and stored in a proper order to ensure that they all run.

The output can be sent by email, either one report at a time, or as a group of reports together. Optional zip and password are available.

If the information that is sent contains one or more empty reports, this is denoted in the subject of the email. Customers can set the product to either eliminate or send empty reports. (Some auditors prefer to keep all reports,

even if they are empty, to ensure that the definition of the report did not change.)

The product collects information about each query that is run. This information includes the full command used to run the report, the time that it ran, how long it took to run it, and the name of the output that it produced.

An effective security policy relies on queries and reports to provide traceability for system activity. Audit queries and reports contain information from an extremely wide range of sources, (as shown in "Appendix A: Raz-Lee Information Sources" on page 384) including:

- Activity data collected from sources such as QHST, QAUDJRN (the system audit journal), QIPFILTER, QIPNAT, QACGJRN, QQOS, QSNMP, QDSNX, QVPN, and QZMF
- Activity data collected by iSecurity/Firewall from security related exit points
- Activity of the Antivirus and Anti-Ransomware modules of iSecurity
- Information from the system about Users, Groups, Native and IFS Objects, System values, PTFs, Authorization lists, and other categories
- Information that shows current activity status such as Active Jobs, NETSTAT, Disk, and System Status
- Summarized activity information which is kept in the internal Data Warehouse that is the base of the GUI Visualizer.
- Database changes, filtered, collected and reported by iSecurity/AP-Journal
- Activity about elevated authority, collected and reported by Authority-On-Demand
- Activities with objects in product libraries, collected and reported by Change-Tracker
- Activities of users on emulated screens collected and reported by Capture
- Activity of Password-Reset, MFA, and other products, also collected and reported.

To work with these features, select **41. Queries and Reports** from the **Audit Main Menu**. The **Queries** screen appears:

```
AUQRYMN                              Queries                    iSecurity/Audit
                                                              System:   S520
Select one of the following:

  Query Wizard                          Report Scheduler
   1. Work with Queries                 51. Work with Report Scheduler
                                        52. Run a Report Group

  Run a Query                           Baseline Setup
  11. Display                           61. System Values
  12. Print                             62. Network Attributes
  13. Submit as Batch Job               63. Counts in Compliance Query

  Log                                   Network reporting        SYSTEM()
  21. Display Log                       71. Network description
                                        75. Current Job CntAdm Messages
                                        76. All Jobs CntAdm Messages

Selection or command
===> ____________________________________________________________________________

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

To work with queries:

To create and modify queries,

select **1. Work with Queries**. The Work with Queries screen appears, as shown in "Creating and Running Queries" on page 169.

To run existing queries,

select the following items. For each the Run Audit Query (RUNAUQRY) screen appears, as shown in "Running Queries" on page 192, with the relevant ways of running the query selected:

- **11. Display**
- **12. Print**
- **13. Submit as Batch Job**

To work with logs:

To display Audit log entries,

select **21. Display Log**. The Display Firewall Log (DSPFWLOG) screen appears, as shown in Displaying Firewall Logs.

To work with reports

To schedule reports to run,

select **51. Work with Report Scheduler**. The Work with Report Scheduler screen appears, as shown in "Scheduling Reports" on page 195.

To run groups of reports,

select **52. Run a Report Group**. The Run Report Group (RUNRPTGRP) screen appears, as shown in "Running Report Groups On Demand" on page 212.

To view other network and system information ,

To ping and test DDM connections for network systems,

select **71. Network Description**. The standard Display Network Systems screen appears.

To view Central Administration messages for current jobs ,

select **75. Current Job CntAdm Messages**. The Display Messages screen appears, showing the job log for the current job.

To view Central Administration messages for all jobs ,

select **76. All Jobs CntAdm Messages**. The Display Messages screen appears, showing the job log for all jobs.

To exit the screen, press the F3 or F12 key.

IBM and Raz-Lee Entry Types

The OS/400 System Journal (**QAUDJRN**) logs all system activities involving Jobs, Objects, User Profiles, Authorities and much more. The activities are classified as “entry types”, many of which have associated subtypes in order to differentiate between different occurrences of the entry type; as an example, entry type JS, which records actions relating to jobs, has eight subtypes, two of which differentiate between batch and interactive jobs.

IBM entry types are associated with “audit types” which are simply IBM-defined auditing categories. A comprehensive table listing all Audit Types, their corresponding Entry Types and all Subtypes, including a description for each category, can be found in *STRAUD* **> 1 > 9**.

To set which IBM Entry types are logged in QAUDJRN:

- Use *STRAUD* **> 1 > 1**.

To set which IBM Entry types are logged in iSecurity Audit log:

- Use *STRAUD* **> 11**.

See Working with Current Setting and Setting up the Audit Scheduler, and see Working with Status and Active Job Rules.

For more information regarding **QAUDJRN** and the IBM-supplied Entry Types, see https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_73/rzarl/rzarlf04.htm .

Other Related Modules

Audit is a comprehensive product that controls the configuration and management of newer iSecurity products designed to meet specific auditing and tracking needs. Access these products and supplementary Audit modules directly from Audit by selecting ***STRAUD* > 69. Other Related Modules** in the Main menu. This opens the following **Related Modules** screen.

In addition, the following options have their own chapters within this manual:

- Working with Native Object Security
- Replication

Getting Started

This chapter guides you through the steps necessary to begin using [[[Undefined variable Audit.ProductName]]] for the first time and the basic procedures for configuring the product for day-to-day use.

Starting Audit for the First Time

To use this product, the user must have *AUDIT special authority. An additional product password may also be required to access certain functions. The default product password is QSECOFR. We recommend that you change this password as soon as possible.

To start Audit:

- In the command line, type ***STRAUD***. The Main menu appears.

```
AUAUDMN                                Audit                        iSecurity/Audit
 System:  S520
 Settings                                     Analysis
  1. OS/400 Audit Features                    41. Queries and Reports
  2. Activation                               42. Display Log

 Real-Time Filtering and Alerts               Related Modules/Options
 11. Audit (QAUDJRN, QIPFILTER...)            61. Work With Actions
 12. Firewall/Screen                          62. User Management
 13. Status & Active Job  (SysCtl)            68. Compliance
 14. Message Queue & QHST (SysCtl)            69. Other Related Modules
 15. IFS Logs

 Definitions                                  General
 31. Time Groups                              81. System Configuration
 35. General Groups                           82. Maintenance Menu
 89. Base Support

 Selection or command
 ===> ____________________________________________________________________________
_
 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
 F13=Information Assistant  F16=AS/400 main menu
```

System Configuration

Audit is ready-to-run right out of the box. Before using the product for the first time, you should review the system configuration parameters that control important features.

Security products such as Audit do not have a “typical” or “optimal” configuration. Each installation or application has different operational criteria and security needs. The auditing requirements for a large manufacturing environment differ from those for a bank, a software developer or a service organization.

To start configuring your system:

1. Select *STRAUD* **`> 81. System Configuration`** from the Main menu.
2. Perform the steps on the following pages. After finishing, press **Enter** again to save your changes and leave this menu.

WARNING: If you press **F3**, you will lose any changes that you have made.

The following is an overview of the System Configuration process:

NOTE: After you modify any of the parameters accessible from this menu, the message

`Modify data, or press Enter`

appears when the menu returns.

Step 1: Setting General Definitions

Five important parameters are located on the **Audit General Definitions** screen.

1. Select **`1. General Definitions`** from the **System Configuration** menu (*STRAUD* **`> 81 > 1`**), shown in "Starting Audit for the First Time" on page 36. The **Audit General Definitions** screen appears.

```
                          Audit General Definitions          23/07/19 11:46:47

Type options, press Enter.

  Enable Audit Scheduling . . . . . .  Y              Y=Yes, N=No
  Audit can automatically replace the OS/400 audit setting with pre-defined
  settings according to the time and day of the week. Y enables this feature.

  "Field changed" symbol (print). . .  #
  This symbol is printed before each user profile attribute that has been
  changed.

  Use *N to represent empty fields  .  Y              Y=Yes, N=No
  Empty fields can be displayed as *N when the log is displayed. If you select
  N=No, the system will use less disk space.

  Start log display . . . . . . . .  N              N=New, O=Old
  Start query display . . . . . . .  N              N=New, O=Old



 F3=Exit   F12=Cancel
```

Parameter or Option	Description
Enable Audit Scheduling	Allows you to change the IBM i (OS/400) setting automatically according to the day of the week and the time of day. **Y**=Yes **N**=No
"Field changed" symbol (print)	Audit can compare "before" and "after" images of records. You can define a symbol to appear by each changed field on printed reports. Choose any character you want. The default character is #.
Use *N to represent empty fields	When displaying a log, empty fields can be displayed as `*N`. If you do not represent empty fields, you will save disk space. **Y**=Yes **N**=No
Start log display	Sort order for displaying a log. **N**=Newest item appears first. **O**=Oldest item appears first.
Start query Display	Sort order for displaying query results. **N**=Newest item appears first. **O**=Oldest item appears first.

Step 2: Setting Log and Journal Retention Parameters

To preserve disk storage capacity and improve query response time, retain transactions for no more than the minimum period necessary to maintain an effective audit program.

Define how long to retain the Audit logs and journals for, and define whether to run a backup program that will run automatically before the logs and journals are deleted at the end of the retention period.

NOTE: The IBM i (OS/400) journal receiver may contain data not recorded in the Audit history log. Therefore, it is highly recommended that you retain and backup the journal in addition to the history log.

1. Select **`9. Log Retention`** from the **Audit Main Menu** (*STRAUD* **`> 81 > 9`**), shown in "Starting Audit for the First Time" on page 36. The **Log & Journal Retention** screen appears. The recommended initial settings are displayed below.

```
                          Log & Journal Retention          23/07/19 11:39:11

Log retention period (days) . . . . . . .   7          Days, 9999=*NOMAX
Backup program for logs . . . . . . . . .  *NONE       Name, *STD, *NONE
Backup program library  . . . . . . . . .  __________
A specified backup program may run before deleting old logs. It will backup
all data deleted after the retention period expires.  The *STD backup
program source is in SMZ4/AUSOURCE AULOGBKP.

Keep deleted users for revival (days) . .  10          Days, 999=*NOMAX

The following parameters apply to the audit journal receivers.  This is
the primary data source for Audit. You should always backup the journal
receiver because it may contain data not logged in Audit.
QAUDJRN receivers retention period (days)   5          Days, 9999=*NOMAX
Backup program for journal  . . . . . . .  *NONE       Name, *STD, *NONE
Backup program library  . . . . . . . . .  __________
A specified backup program may run before deleting old journal receivers.
It will backup data deleted after the retention period expires. The *STD
program is SMZ4/AUSOURCE AUJRNBKP.

F3=Exit   F12=Cancel
```

2. Enter the required fields as defined below and press **Enter**.

Parameter	Description
Log retention period (days)	Transactions are retained for the specified number of days. At the end of this period, transactions are purged from the log. Enter **9999** to retain all data indefinitely.
Backup program for logs	Enter the name of the backup program to use to back up logs. Type ***STD** to use the Audit standard backup program or ***NONE** for no backup. You must ensure the appropriate backup media is loaded before the automatic backup program runs.
Backup program library	Enter the name of the library where the Backup program is stored.
Keep deleted users for revival (days)	Enter the number of days for which deleted users are stored on the system. Enter **999** to keep all users indefinitely.
QAUDJRN receivers retention period (days)	Transactions are retained for the specified number of days. At the end of this period, transactions are purged from the journal. Enter **9999** to retain all data indefinitely.
Backup program for journal	Enter the name of the backup program to use to back up journals. Type ***STD** to use the Audit standard backup program or ***NONE** for no backup. You must ensure the appropriate backup media is loaded before the automatic backup program runs.
Backup program library	Enter the name of the library where the Backup program is stored.

Step 3: Setting Action General Definitions

This option enables you to take full advantage of the integration between IBM®Audit and Action.

1. Select **`11. General Definitions`** from the **Audit Main Menu** (*STRAUD* **`> 81 > 11`**), shown in "Starting Audit for the First Time" on page 36. The **Action General Definitions** screen appears.

```
                          Action General Definitions         23/07/19 14:17:48

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 . . . . . . . . . 1200    Seconds
  Prevent action for same rule (default).    20     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
```

The following table provides an explanation for some of the options:

Option	Description
Enable FYI Simulation Mode	FYI is an acronym for "For Your Information". In this mode, security rules are fully operational, but no action is actually taken. This enables you to review your History Log for analysis, and thereby later create valid security rules. **Y**= Enable FYI **N** = Do not enable FYI
Log CL Script Commands	This option enables you to save a log of CL commands that run in a particular action in the job log of the real-time processor. **1**= Do not save to the log **2** = Save only failed commands **3** = Save all commands
Status & Active jobs detection	Actions are not repeated for the same rule until the specified period has elapsed. This prevents unnecessary repetition of actions.

Option	Description
	Interval between checks= the time between Action checks (in seconds) Prevent action for same rule for = this option avoids repetition of the same rule (in seconds)
For events processed a long time after they occurred	Do not perform actions for events if the time passed since they have occurred has passed the specified limits (in minutes).

2. Select **`5. Auto start activities in ZAUDIT`** from the System Configuration menu (*STRAUD* **`> 81 > 5`**). The **`Auto start activities in ZAUDIT subsystem`** screen appears.
3. Type **`Y`** for system activities that you want to start automatically after you activate the ZAUDIT subsystem in Action.

```
                    Auto Start Activities in ZAUDIT Subsystem  22/07/19 17:30:46

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) . . . . . . . . . .  Y          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
```

Step 4: Language Support

Use this option to replace characters when creating HTML files.

In some languages, the keyboard settings are different. When creating an HTML file via one of the commands, such as ***DSPAULOG*** or ***DSPFWLOG***, the machine writes to a text file that the HTML translator understands.

For example, a keyword for HTML might have to be between square brackets, as in `[keyword]`, but in input to be processed, the key word might look like `!keyword^` , with the word between an exclamation mark (`!`) and a caret (`^`). Setting the replacement fields as follows:

```
Replacement of special characters.    !^

(original value)
[]@#$....1....+....2....+....3....+....4
```

converts the string into `[keyword]` , which will the HTML translator will understand. Each character in the upper field is converted to the character directly beneath it in the lower field.

To **configure Action Language Definitions**, select ***STRAUD*** **> 81 > 91. Lanuage Support**. The **Action Language Definitions** screen appears.

```
                        Action Language Definitions          1/08/19 15:39:01

Type options, press Enter.

  Right to left language system . .  Y                Y=Yes, N=No
  DBCS system . . . . . . . . . . .  N                Y=Yes, N=No


  Override HTML, CSV etc. Attributes
  Target CCSID (Windows ASCII)  . .   ____0           Place cursor and press:
  HTML Character set  . . . . . . .  _______________  - F4 for selection
                                                      - F5 for auto set
  Special consideration for DBCS/non-Latin languages
  CCSID to use as origin of data  .   ___37


  Replacement of special characters  ________________________________________
  (original value)                   []@#${}..1....+....2....+....3....+....4



F3=Exit   F4=Prompt   F5=Autoset   F12=Cancel
```

Step 5: Activating Real Time Detection

You must activate real-time detection on your system to enable triggering actions and posting events in the Audit history log. It is recommended that you allow IBM i (OS/400) to activate real-time detection automatically at IPL. You can de-activate real-time detection at any time.

To manage real-time detection after installation, select **`2. Activation`** in the Audit main menu (*STRAUD* **> 2**). The **Activation** menu appears.

```
AUSETMN                          Activation                    iSecurity/Audit
 System:  S520

 Activation                                Manual Activation (Local/Remote)
  1. Activate ZAUDIT subsystem              31. Start Real-Time Auditing
  2. De-activate ZAUDIT subsystem           32. End Real-Time Auditing
  5. Work with Active Jobs                  33. Set/Add Start of Auditing
 STRAUD, 81, 5 to set activities           35. Work with Active Journals
 For QHST/MsgQ see STRAUD, 14

 Auto-Activation at IPL                    Analyzing QAUDJRN on another system
 11. Activate ZAUDIT subsystem at IPL      41. Setup
 12. Do Not Activate ZAUDIT sbs at IPL

 Selection or command
 ===> ____________________________________________________________________
_
 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
 F13=Information Assistant  F16=AS/400 main menu
```

To **activate real-time auditing manually**:

1. Select **`31. Start Real-Time Auditing`**.
2. In the **Start Real-Time Auditing** (*STRRTAUD*)screen that appears, enter the required starting date and time (and if relevant, enter the required ending date and time), then press **Enter**.

To **end real-time auditing**,

1. Select **`32. End Real-Time Auditing`**.
2. Specify which system to stop auditing.

To **set a specific time and date** to begin auditing:

1. Select **`35. Set Start of Auditing Time`**.
2. In the **`Set Start of Auditing Time (SETRTAUD)`** screen that appears, enter the required starting date and time, then press Enter.

To enable automatic activation at IPL, select **`11. Activate ZAUDIT subsystem at IPL`**.

To manually activate or add additional message queue detection:

1. Select **`14. Message Queue (SysCtl)`** in the Audit main menu
2. Select **`21. Activate`** in the Message Queue menu.

Detailed Change User Profile Audit Type

[[[Undefined variable Audit.ProductName]]] presents a new unique solution in auditing User Profile changes. This solution allows you to receive detailed information on any changes made on the IBM i user profiles:

- Exact user attributes that were changed
- Their former value
- Their current value

To reach this detailed information, [[[Undefined variable Audit.ProductName]]] uses a special artificial audit type, `C@ - Change User Profile`. This audit type, unique to iSecurity, writes to the [[[Undefined variable Audit.ProductName]]] log file when user profiles change and contains user profile data from before and after the change.

This audit type can be used both for real-time detection and for queries and reports. The queries from this audit-type show the “before and after” values only of the fields changed.

Working with Operators' Authorities

Operators' authority management for all iSecurity modules is now maintained in a single place.

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.

Use **Password = *BLANK** for the default entries. Use *DSPPGM GSIPWDR* to verify. The default for other users 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 **`11. Work with Operators`** in the **Base Support** menu (*STRAUD* **`> 89 > 11`**). 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,SU), 5=*DFN(CT,EN,SU), 9=*FULL
   User       System  FW SC PW CD AV AU AC CP JR SU VS RP CO CT PR UM EN AD
_  *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
_  ALEX3      S520     9  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
_  AVRAHAM    S520     9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9  9
_  DB         S520     9  9  9  9  9  9  9  9  9  9  9  9  9  3  9  9  9  9
_  EVGPRVD    S520     9  9  9  9  9     9  9  9  9  9  9  9  9  9  9  9  9
_  GS         S520     9  9  9  9  9  9  9  9  9  5  9  9  9  9  9  9  9  9
_  JAVA       S520                                            3         5
                                                                       More...
FW=Firewall    SC=Screen   PW=Password   CM=Command     AU=Audit      AC=Action
AV=Antivirus   CA=Capture  JR=Journal    VS=Visualizer  UM=User Mgt.  AD=Admin
RP=Replication CO=Compliance            CT=Chg Tracker PR=Pwd Reset
EN=Encryption  SU=SafeUpd

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

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  . . . . . . . . . .    ALEX3
System  . . . . . . . . . . .    S520              *ALL, Name
Password  . . . . . . . . . .    *SAME             Name, *SAME, *BLANK

Auth.level: 1=*USE, 3=*QRY(FW,AU,CT,SU), 5=*DFN(CT,EN,SU), 9=*FULL
Firewall  . . . . . . . . . . FW 9        Screen  . . . . . . . . . . . SC 9
Password  . . . . . . . . . . PW 9        Command . . . . . . . . . . . CD 9
AntiVirus . . . . . . . . . . AV 9        Audit . . . . . . . . . . . . AU 9
Action  . . . . . . . . . . . AC 9        Capture . . . . . . . . . . . CA 9
Journal . . . . . . . . . . . JR 9        Safe Update . . . . . . . . . SU 9
Visualizer  . . . . . . . . . VS 9        Replication . . . . . . . . . RP 9
Compliance  . . . . . . . . . CO 9        Change Tracker  . . . . . . . CT 9
Password Reset  . . . . . . . PR 9        User Management . . . . . . . UM 9
Encryption  . . . . . . . . . EN 9        Administrator . . . . . . . . AD 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).
*APR=Approver.


F3=Exit    F12=Cancel
```

Set the **Password** field to a valid password, to ***SAME** to keep it the same as the previous password when edited, or to ***BLANK** to have no password.

The **AuthLevel** field for each item can have the values:

- **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 or modifying queries.

3. Set authorities and press **Enter**. A message appears stating that the user being added or 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 or release upgrade process. The **`SECURITY_P`** user profile is granted Authority **`*ALL`** while 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.

Initial IBM i (OS/400) Audit Settings

Effective security auditing demands a balance between preserving historical data and system performance. The process of capturing events and recording them in both the IBM-provided security audit journal and the Audit history log can consume system resources and large amounts of disk space. Performance degradation can result when you capture and record too many events.

Which specific events you choose to track is a function of your organization's overall security objectives and potential exposures. When working with Audit for the first time, we recommend certain all-purpose settings that will allow you to examine security exposures and to develop historical data that will be useful when creating real-time detection rules.

In the following section, several generic setting scenarios help get you started with security data collection, while minimizing performance burden and disk space. Modify these settings as soon as possible, in accordance with your organizational and system requirements. In any case, you should carefully monitor system performance and disk space.

After analyzing audit data generated by this initial process, you will be able to narrow your audit scope and use real-time detection rules to build a more efficient audit program.

However, for your initial settings, we recommend that you follow these procedures as described. For the step-by-step tutorials, together with detailed explanations for the parameter settings see IBM i (OS/400) Audit Settings.

To begin working with IBM i audit settings:

1. Select **`1. OS/400 Audit Features`** in the Audit main menu (*STRAUD* **`> 1`**). The **`OS/400 Audit Features`** menu appears.
2. Perform the following procedures:
   - Working with Current Setting
   - Working with User Activity Auditing
   - Working with Object Auditing

Working with Current Setting

The current audit setting determines which events you track for all users on a global basis and whether object auditing is active for all users.

1. Select **`1. Work with Current Setting`** from the Audit Main menu (*STRAUD* **`>1 >1`**). The **Work with Current Setting** screen appears.

```
                          Work with Current Setting
Use this screen to view or modify the current global audit setting.
The Audit Scheduler may change this setting automatically when active.

Type choices, press Enter.
   Y=Yes
  Current Modified  Parameter  Description
Main Audit Control Parameters (QAUDCTL)
     Y       Y      *AUDLVL    Activity auditing (as selected below)
     Y       Y      *OBJAUD    Object access auditing
     Y       Y      *NOQTEMP   Do not audit QTEMP objects
Action Auditing Values (in effect only if *AUDLVL = "Y")
     Y       Y      *CREATE    Create objects
     Y       Y      *DELETE    Delete objects
     Y       Y      *JOBDTA    Start, End, Hold, Release, Change job
     Y       Y      *NETCMN    Network and communication functions
             _      *NETBAS    | Network base functions
             _      *NETCLU    | Cluster and cluster resource group
             _      *NETFAIL   | Network failures are audited.
             _      *NETSCK    | Socket tasks
                                                                  More...
F3=Exit   F4=Prompt   F8=Print  F12=Cancel
```

2. Place a **`Y`** or space in the `Modified` column next to the setting parameters as shown below. You will need to press **Page Down** to scroll the lower section of the screen to see all of the settings.
3. Press **Enter** to return to the menu.

Working with User Activity Auditing

The following settings apply to the security officer (QSECOFR)and any other users with similar authority.

1. Select **31. User Activity Auditing** from the OS/400 Audit Features menu (*STRAUD* **> 1 > 31**). The Set User Auditing screen appears.

```
                                Set User Auditing


Select User or Group Profile, press Enter:

User profile  . . . . . . .  __________       Name
 -or-
Group profile . . . . . . .  __________       Name
Enables setting of all User Profiles in the group profile.

Retrieve auditing of User .  __________       Name
Sets the default of the Audit values as per those of the specified User.









F3=Exit   F4=Prompt
```

2. In **Group Profile**, enter the user profile **QSECOFR**.
3. Set the parameters as shown below:

```
                              Set User Auditing

Group Profile:  QSECOFR    Security Officer

Apply for all GrpPrf users.  Y            Y=Yes, N=No

Object access auditing  . .  1            1=*ALL, 2=*CHANGE, 3=*NONE, 4=*SAME
User activity auditing  . .  2            1=*ALL, 2=*LIST,   3=*NONE, 4=*SAME

Type Y to select.
 Y Commands          Y Security events
 Y Create objects    Y Service tools
 Y Delete objects    Y Spool files
 Y Job tasks         Y Sys management
 Y Obj Move/Rename
 _ Office services
 Y Optical volumes
 Y Auth adoption
 Y Save/Restore
                                                                      Bottom

F3=Exit   F11=Display Keywords      F18=Outcoming Audit Types (by cursor)
```

Use the same methods to set User Auditing settings for other users and groups, as appropriate.

Working with Object Auditing

You should identify those objects that are critical to your organization and then create settings to capture all attempts to access these objects. There are separate wizards for auditing native IBM i objects or IFS (any non-native IBM i objects). The procedures are similar for both object types.

At first, you should capture all changes to critical objects. When you have analyzed the data, you can define settings and real-time detection rules to capture a much smaller sample to provide an effective audit trail.

1. For native objects, select **`41. Native Object Auditing`** from the **OS/400 Audit Features** menu (*STRAUD* **`> 1 > 41)`**. For IFS objects, select **`42. IFS Object Auditing`**.
2. Select a library and object combination from the list, or press **F6** to create a new entry.
3. Enter parameters on the appropriate **Add Object Auditing**screen as displayed (example is for native IBM i (OS/400) objects).

```
                              Add Object Auditing

Type choices, press Enter.

  Object  . . . . . . . . . .  __________        Name, generic*, *ALL
    Library . . . . . . . . .  __________        Name, *LIBL, *ALL, *ALLUSR

  Object type . . . . . . . .  _______           *ALL, *ALRTBL, *AUTHLR...


  Object auditing option  . .  _                 1=*NONE
                                                 2=*USRPRF
                                                 3=*CHANGE
                                                 4=*ALL


  Apply immediately . . . . .  B                 Y=Yes, B=in Batch, N=No
  This might be a long running procedure. Batch run is recommended.



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

4. Repeat this process for other critical objects.

IBM i (OS/400) Audit Settings

This Chapter discusses the concepts and procedures for working with the IBM i (OS/400) auditing features using [[[Undefined variable Audit.ProductName]]]. The topics in this chapter cover the most commonly used audit features and parameters.

Working with the Current Settings

The term Current Setting refers to those parameters governing events that are currently in effect and will be recorded in the IBM i security audit journal for all users on a global basis. Two separate audit modes comprise the current setting, user activity auditing and object access auditing

You can enable or disable either of these modes and specify which types of user activities are audited for all users. You use the User Audit Settings and Object Audit Settings to record specific user activities and object access events for audit in addition to those specified in the current setting.

Audit includes several features that make working with the IBM i (OS/400) current setting more efficient:

- **Current Setting Screen** – This screen allows you to quickly review the current setting parameters and make changes on the fly. You no longer have to worry about all those system values and other parameters.
- **Predefined Settings** – You can create and store groups of current setting parameters for future use. This allows you to change the settings quickly with only a few keystrokes.
- **Audit Scheduler** – This feature allows you to change the current setting automatically according to the time of day and the day of the week.

All of these features involved in Current Settings are accessible in the **OS/400 Audit Features** menu.

To open the OS/400 Audit Features menu and begin working:

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **OS/400 Audit Features** screen appears.
2. Select **`1. Work with Current Settings`**. The **`Work with Current Setting`** screen appears.

Use the **Page Up** and **Page Down** keys to scroll the user activity auditing values.

```
                          Work with Current Setting
Use this screen to view or modify the current global audit setting.
The Audit Scheduler may change this setting automatically when active.

Type choices, press Enter.
   Y=Yes
  Current Modified  Parameter  Description
Main Audit Control Parameters (QAUDCTL)
     Y        Y      *AUDLVL    Activity auditing (as selected below)
     Y        Y      *OBJAUD    Object access auditing
     Y        Y      *NOQTEMP   Do not audit QTEMP objects
Action Auditing Values (in effect only if *AUDLVL = "Y")
     Y        Y      *CREATE    Create objects
     Y        Y      *DELETE    Delete objects
     Y        Y      *JOBDTA    Start, End, Hold, Release, Change job
     Y        Y      *NETCMN    Network and communication functions
              _      *NETBAS    | Network base functions
              _      *NETCLU    | Cluster and cluster resource group
              _      *NETFAIL   | Network failures are audited.
              _      *NETSCK    | Socket tasks
                                                                   More...
F3=Exit   F4=Prompt   F8=Print  F12=Cancel
```

Parameter or Option	Description
*AUDLVL	Toggles user activity auditing (enabled/disabled). **Y** = user activity auditing enabled (recommended) **Blank** = User activity auditing is disabled
*OBJAUD	Toggles object access auditing (enabled/disabled). **Y** = object access auditing enabled (recommended) **Blank** = object access auditing is disabled
*NOQTEMP	Toggles auditing of objects in the QTEMP library (enabled/disabled). **Y** = Do not audit objects in the QTEMP library (recommended) **Blank** = Enable auditing of objects in the QTEMP library
Action Auditing Values	Toggles user auditing of various types of objects in the QTEMP library (enabled/disabled) **Y** = Enable auditing **Blank** = Disable auditing

Current Setting Strategies

In general, you should try to minimize the number of records posted to the security audit journal to preserve disk space and lessen the impact on system performance. Since the current setting applies globally to all users, it is best to avoid capturing routine user activity that will create many entries. The current setting is best employed to capture exceptional occurrences, such as serious errors, program failures, changes to security definitions and changes to important system parameters.

You can also use the current setting to track routine activity for very limited periods to analyze user activities, assess security risks, and evaluate system performance.

Current Setting Suggestions

- Always enable the `Do not audit QTEMP objects` option. Many objects are located in this library and they are rarely important.
- Enable user activity auditing, but only include extraordinary activity in the current setting such as:
    - Authority failures (*AUTFAIL)
    - Program failures (*PGMFAIL)
    - Security definitions (*SECURITY)
    - System service operations (*SERVICE)
- Use the User Activity and Object Access features to audit routine activities for specific users and objects.

Example: Typical Production System

The following example illustrates the procedure for defining the global audit setting for a typical production environment.

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **`OS/400 Audit Features`** menu appears.
2. Select **`1. Work with Current Settings`**. The **`Work with Current Setting`** screen appears.
3. Type **`Y`** to the left of the following options:
    - *AUDLVL User activity auditing

- *OBJAUD Object access auditing
- *NOQTEMP Do not audit QTEMP objects
- ***AUTFAIL Authority failures**
- ***NETCMN Violations detected by the APPN filter**
- Security definitions (*SECURITY)
- System service operations (*SERVICE)

4. Press **Enter** to return to the Main menu.

Predefined Audit Settings

This feature allows you to create and save predefined audit settings for future use. You can then substitute the predefined setting for current setting at any time. The audit scheduler automatically substitutes a predefined setting for the current setting at a specific time.

Creating and Modifying Predefined Audit Settings

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **OS/400 Audit Features** menu appears.
2. Select **`2. Work with Pre-Defined Settings`**. The **Work with Pre-Defined Settings** screen appears.

```
                        Work With Pre-defined Settings

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

Opt Setting    Description
 _  ALON_QA    checking audinting of all NO except Create objects
 _  SHIFT1     SHIFT1
 _  SHIFT2     SHIFT2
 _  SHIFT3     SHIFT3

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

3. Select an existing setting to modify, or press **F6** to create a new setting.
4. Modify or create new settings as described in "Working with the Current Settings" on page 60.
5. Press **Enter** to return to the **`Work with Predefined Settings`** screen.
6. Work with another setting, or press **Enter** to return to the **OS/400 Audit Features** menu.

Activating a Predefined Setting

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **`OS/400 Audit Features`** screen appears.
2. Select **`3. Activate Predefined Setting`**. The **`Activate Predefined Setting (SETAUDOPT)`** screen appears.

```
                    Activate Pre-defined Setting (SETAUDOPT)

Type choices, press Enter.

Name of pre-defined setting  . .   *SELECT      Character value, *SELECT

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

3. Type a setting name, or enter **`*Select`** to choose a setting in the **Work with Pre-defined Settings** window.
4. Press **Enter** to continue.

Example: Three Shift Production Scenario

The following example describes the creation of four predefined settings for a hypothetical production scenario. The settings shown here are for demonstration purposes only, and do not represent typical or recommended settings. Your settings should represent the operational characteristics and security exposure for your organization.

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **OS/400 Audit Features screen** appears.
2. Select **2**. The **Work With Pre-defined Settings** screen appears.
3. Press **F6** to create a new setting.
4. For each of the four settings:
   a. Type the value **`SHIFT1`** in the first Set field.
   b. Type a description in the field to the right.
   c. Type the setting parameters as shown in the **`SHIFT1`** column in the table below and press **Enter** twice.
5. Press **F12** to return to the **OS/400 Audit Features** menu.
6. Select **3**.
7. Press **Enter** to accept the **`*SELECT`** parameter.
8. Select one of the newly defined settings. Press **Enter** to continue.
9. Select `1` in the **OS/400 Audit Features** menu. Note that the current setting parameters have changed accordingly.

Using the Audit Scheduler

The Audit Scheduler feature automatically replaces the current audit setting with a predefined setting at specific days and times. Some useful applications of this feature may include:

- More intensive system activity auditing at night or on weekends when users are more likely to attempt unauthorized activity
- Tracking of scheduled backups, program installations or system maintenance
- Performing “system snapshot” audit samples of routine activity for short periods of time during peak hours for analysis purposes

Setting up the Audit Scheduler

You set up the Audit Scheduler by specifying predefined settings to replace the current setting at specific times for each day of the week. For more information about creating predefined settings, see Predefined Audit Settings, on page 64.

1. Select **`1. OS/400 Audit Features`** in the Main menu (**`STRAUD > 1`**). The **OS/400 Audit Features**menu appears.
2. Select **`11. Work with Audit Scheduler`**. The **Work with Audit Scheduler**screen appears.

```
                          Work with Audit Scheduler

Type choices, press Enter.

   Activate Audit Scheduler  . .  Y    (Y/N)

 Change pre-defined settings at:
   Time . . . .   :15      :49     9:00     14:55     19:50      :00

 Pre-defined settings to be activated at the above times:
   Monday . . .  ________ ________ ________ ________ ________ ________
   Tuesday  . .  ________ ________ ________ ________ ________ ________
   Wednesday  .  ________ ________ ________ ________ ________ ________
   Thursday . .  ________ ________ ________ ________ ________ ________
   Friday . . .  ________ ________ ________ ________ ________ ________
   Saturday . .  ________ ________ ________ ________ ________ ________
   Sunday . . .  ________ ________ ________ ________ ________ ________


F3=Exit    F4=Prompt    F8=Print     F12=Cancel     F13=Copy daily schedule
```

3. Make sure that the **Activate Audit Scheduler** field is set to **`Y`**.
4. You can specify up to six times each day at which settings can automatically change. Type the times for settings to change in the Time fields using 24-hour notation (HH:MM)

5. For each day of the week, to change to a different scheduler setting at any of the times that you entered in the Time field, enter the name of the predefined setting in the column under that Time setting in the row for that day. Press **F4** in any setting field to choose from a list of available predefined settings. To copy the schedule from one day to another day or days, press the **F13=Copy daily schedule** key. For more details, see "Copying a Daily Audit Schedule" on the facing page.
6. When you are finished, press **Enter** to return to the **OS/400 Audit Features** menu. The current setting changes to the appropriate scheduled setting.

Copying a Daily Audit Schedule

When working with the Audit Scheduler, you can save time by copying a given day's schedule to another day or days.

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* > 1). The **`OS/400 Audit Features`** menu appears.
2. Select **`11. Work with Audit Scheduler`**. The **`Work with Audit Scheduler`** screen appears.
3. In the **`Work with Audit Scheduler`** screen, after entering pre-defined settings to at least one day of the week, press **F13**. The **Duplicate Day Scheduling**screen appears.

```
                          Duplicate Day Scheduling

Copy from source day:  . .   _        1=Monday
                                      2=Tuesday
                                      3=Wednesday
                                      4=Thursday
                                      5=Friday
                                      6=Saturday
                                      7=Sunday
To Target day:
  Monday . . . . . . . . .   _        Y=Yes
  Tuesday  . . . . . . . .   _
  Wednesday. . . . . . . .   _
  Thursday . . . . . . . .   _
  Friday . . . . . . . . .   _
  Saturday . . . . . . . .   _
  Sunday . . . . . . . . .   _


F3=Exit     F12=Cancel
```

4. Enter the number corresponding to the day of the week to copy in the Copy from source day field.
5. Enter **`Y`** for all days in the To Target day list that will receive the copied schedule.
6. Press **Enter**. The schedule is copied.

Example: Three-Shift Production Environment

The following example portrays a scenario for a hypothetical three-shift production environment, in which the majority of clerical, data entry and reporting functions take place during the first (daytime) shift.

This example uses the settings that you created in the Activating a Predefined Setting example shown in "Example: Three Shift Production Scenario" on page 67

1. Select *STRAUD* **> 1. OS/400 Audit Features** in the Main menu (*STRAUD* > 1). The OS/400 Audit Features menu appears.
2. Select **11. Work with Audit Scheduler**. The Work with Audit Scheduler screen appears.
3. Type the values **0600**, **1600**, and **2300** in the first three Time fields.
4. Move the cursor to the first Setting field on the Monday line and press F4. The Work with Predefined Settings screen appears.
5. Type **1** to the left of the SHIFT1 line and press Enter.
6. On the Work with Audit Scheduler screen, move the cursor to the second and third Setting fields on the `Monda`y line, then use F4 to select **SHIFT2** and **SHIFT3**.
7. Press F13. The `Duplicate Day Scheduling` screen appears.
8. In the Copy from source day field, type **1**.
9. In the To Target day field, type **Y** in the field to the right of `Tuesday` through `Friday`.
10. Press Enter to confirm and return to the **OS/400 Audit Features** menu.

Audit will now automatically change the settings each day at the indicated times. If you check the current settings after the indicated times, you can verify that this has occurred.

User Activity Auditing

User activity auditing covers specific user activities that are written to the security audit journal in addition to those activities specified in the current setting. User activity rules contain the parameters regarding specific activities to be audited for a given user as well as for object access attempts by that user.

Creating and Modifying User Activity Audit Rules

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **`> 1`**). The **OS/400 Audit Features** menu appears.
2. Select **`31. User Activity Auditing`**. The **Set User Auditing** screen appears.

```
                              Set User Auditing


Select User or Group Profile, press Enter:

User profile  . . . . . . .  _________       Name
 -or-
Group profile . . . . . . .  _________       Name
Enables setting of all User Profiles in the group profile.

Retrieve auditing of User .  _________       Name
Sets the default of the Audit values as per those of the specified User.









F3=Exit   F4=Prompt
```

3. Enter the User profile or Group profile you want to create or change the rules for. A second **Set User Auditing** screen appears.

```
                              Set User Auditing

User Profile .: ALEX       Alex - Supporteam strong user



Object access auditing  . .  2            1=*ALL, 2=*CHANGE, 3=*NONE, 4=*SAME
User activity auditing  . .  1            1=*ALL, 2=*LIST,   3=*NONE, 4=*SAME

Type Y to select.
 Y Commands         Y Security events
 Y Create objects   Y Service tools
 Y Delete objects   Y Spool files
 Y Job tasks        Y Sys management
 Y Obj Move/Rename
 Y Office services
 Y Optical volumes
 Y Auth adoption
 Y Save/Restore
                                                                        Bottom

F3=Exit   F11=Display Keywords      F18=Outcoming Audit Types (by cursor)
```

4. Create or modify the rules as desired.

Parameter or Option	Description
User	Existing valid user profile
Object Access Auditing	Determines the auditing action when object auditing is defined according to user profile. **1 (*ALL)** = Audit all object access attempts (read, change, delete) **2 (*CHANGE)** = Audit only access attempts for change object **3 (*NONE)** = No object access auditing for this user **4 (*SAME)** = Retain existing setting
User Activity Auditing	Determines the user activity auditing action for this user. **1 (*ALL)** = Audit all activity for this user **2 (*LIST)** = Only audit activities specified in the Activity List **3 (*NONE)** = No auditing for this user **4 (*SAME)** = Retain existing setting
Activity List	Type **Y** next to the activities to audit for this user. • Commands • Create objects • Delete objects • Job tasks (Start, end, hold, release, change jobs) • Obj Move/Rename • Office services (Sys distribution directory, Office mail) • Optical volumes • Auth adoption • Save/Restore (Save and restore operations) • Security events • Service tools • Spool files (Operations on spooled files) • Sys activities

User Activity Audit Strategies

The following best practices will help you balance the need to capture sufficient historical data without generating an excessive amount of raw data.

- Create a unique user profile for each individual user; do not use generic departmental user profiles. Define rules for all active users.
- Avoid defining rules using the `*ALL` parameter for object access and user activity auditing. This will only generate a large volume of irrelevant journal entries. These options should be used only to trace suspicious activity or troubleshooting system problems.
- Avoid continuous auditing of routine activities for high volume users, such as data entry clerks and programmers. The following activities will likely generate an enormous quantity of journal entries for this type of user.
    - Commands (`*CMD`)
    - Create objects (`*CREATE`)
    - Delete objects (`*DELETE`)
    - Spool files (`*SPLFDTA`)

As an alternative, you can choose to audit these activities for short time periods on a random basis.

- Audit the Commands (`*CMD`) activity sparingly. Programs typically generate numerous other programs, commands and batch jobs. Each of these is a separate activity, generating its own audit journal entries. Consequently, a single job can create hundreds of journal entries, most of which are irrelevant for effective security auditing.
- Do not audit IBM i internal user profiles (such as QSYS, QUSER, QTCP) regularly. They generate a large volume of journal entries that are of little value for security auditing. Never allow users to sign-on using these profiles.

- Use object access auditing instead of the **Create Objects** and **Delete Objects** user audit activities. This greatly reduces the volume of journal entries by allowing you to audit only specific user accesses to specific objects.
- Use the `*CHANGE` object access audit parameter instead of `*ALL`. You rarely need to audit who reads or uses an object.

Examples of User Activity Auditing

This section presents examples of user activity auditing settings for several user types. Please note that the settings shown here are for demonstration purposes only, and do not represent “typical” or “recommended” settings. Your settings should represent the operational characteristics and security exposure for your organization.

These examples also illustrate the Subset and Copy features provided by the user interface.

Use the following command to create temporary user profiles: ***CRTUSRPRF USRPRF (XXXXX) LMTCPB (*YES)***, where ‘***XXXXX***’ represents the user profile names appearing in the table below (XDATA and so on).

You will use these temporary user profiles for other tutorial examples as well. You should only delete these profiles when you have completed all the examples in this manual.

1. Follow these steps for users named XDATA, XPROG, XSY, and XSECO:
    a. Select **31. User Activity Auditing** in the **OS/400 Audit Features** menu (*STRAUD* **> 1 > 31**).
    b. Press **F6** to create a new user audit rule.
    c. Type the value **XDATA** in the User field.
    d. Type the values as shown in the table in the Object access auditing, User activity auditing and activity list fields.
    e. Then press **Enter** to continue.
2. To demonstrate the Subset feature, press **F7**. The **Subset Selection** screen appears.
3. Type the value **X*** in the User Profile field and press **Enter**. Note that only user profiles beginning with the letter X appear. (See the table following this procedure.)
4. Next, you need to copy a user profile and modify it. This feature saves time when defining rules for many similar profiles. Type **3** next to the **XSECO** profile to copy it and then press Enter.
5. Type **XSUSP** in the **To User** field and press **Enter**.
6. Type **1** next to the **XSUSP** profile to modify it.

7. Enter the parameters as shown in the last column of the table and press **Enter**.

We suggest you sign-on with these user profiles and perform some routine activities to create entries in the security audit journal.

Activity	Data Entry XDATA	Programmer XPROG	System Operator XSYS	Security Officer XSECO	Suspicious User XSUSP
Object access auditing	2	2	2	2	2
User activity auditing	2	2	2	2	2
Commands			Y	Y	Y
Create objects					Y
Delete objects					Y
Job tasks		Y	Y	Y	Y
Object management		Y	Y	Y	Y
Office services			Y	Y	
Optical volumes					
Authority adoption		Y		Y	Y
Save / restore		Y	Y	Y	Y
Security events	Y	Y	Y	Y	Y
Service tools			Y	Y	Y
Spool files			Y		
System management	Y		Y	Y	Y

Object Access Auditing

IBM i (OS/400) allows you to audit all attempts to access certain critical objects, such as database files, source code files or key libraries. You can choose to audit the contents of entire libraries or only specific object types within those libraries, such as data files, job queues or program source files. Auditing can cover all access attempts, changes only or as specified in the user profile.

For example, you can choose to audit all attempts to modify program sources by users whose user class is not *PGMR.

Creating and Modifying Object Access Audit Rules

Separate menu options exist for Native IBM i (OS/400) objects and objects native to other computer platforms (known as Integrated File System (IFS) Objects).

NOTE: The procedures for working with both object types are virtually identical.

To work with Native Object Audit rules:

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD* **> `1`**). The **`OS/400 Audit Features`** menu appears.
2. Select **`41. Native Object Auditing`**. The **Work with Object Auditing** screen appears.

```
                          Work with Object Auditing

Type options, press Enter.
  1=Select   3=Copy   4=Delete   5=Display Objects   8=Apply


Opt  Library      Object       Type      Option     Previous Change
 _   ALEX         DEMOPF       *FILE     *NONE      31/07/19  16:32
 _   ALEX         DEMOPFF      *FILE     *ALL       30/04/19  15:25
 _   ALEX         DEMOPF1      *FILE     *NONE      30/04/19  15:24
 _   ALEX         DEMOPF2      *FILE     *NONE      30/04/19  15:25
 _   ANLIB        A*           *ALL      *NONE      17/07/19  10:41
 _   ANLIB        AUFF*        *ALL      *USRPRF    15/04/18  15:00
 _   ANLIB        AUFFX*       *ALL      *NONE      15/04/18  15:00
 _   ANLIB        AUS*         *FILE     *USRPRF    17/07/19  13:06
 _   DLT          A*           *ALL      *ALL       15/04/18  15:01
 _   DLT          TES*         *DTAARA   *NONE       2/12/18  15:21
 _   QSYS         ANLIB        *LIB      *NONE      17/01/18  10:16
 _   YOEL         DEMOPF       *FILE     *CHANGE    17/07/19  12:11
                                                                   More...
List is of activities done by this option. It does not represent current status
F3=Exit   F6=Add new   F7=Subset   F8=Print        F12=Cancel
```

3. Enter **1** in the Opt column for the object that you want to change. The **Apply Object Auditing** screen appears.

```
                         Apply Object Auditing

Type choices, press Enter.

  Object  . . . . . . . . . .  DEMOPF            Name, generic*, *ALL
    Library . . . . . . . . .  ALEX              Name, *LIBL, *ALL, *ALLUSR

  Object type . . . . . . . .  *FILE             *ALL, *ALRTBL, *AUTHLR...


  Object auditing option  . .  1                 1=*NONE
                                                 2=*USRPRF
                                                 3=*CHANGE
                                                 4=*ALL



  This might be a long running procedure. Batch run is recommended.



F3=Exit               F12=Cancel
```

3. Enter the Object or Library to change audit options for.
4. If desired, enter the Object Type.
5. Select the Object auditing option.
6. Press **Enter**.

Parameter or Option	Description
Object Auditing Options	Define access auditing for this option **1 (*NONE)** = No auditing for this object **2 (*USRPRF)** = Audit according to user profile definition **3 (*CHANGE)** = Audit all changes to this object **4 (*ALL)** = Audit all activity for this object

To work with IFS Object Audit rules:

1. Select *STRAUD* **>1. OS/400 Audit Features** in the Main menu (*STRAUD* **>1**). The **OS/400 Audit Features** menu appears.
2. Select `42. IFS Object Auditing`. The **Work with IFS Object Auditing** screen appears.

```
                         Work with IFS Object Auditing

 Type options, press Enter.
   1=Select   4=Delete   5=Display Object   8=Apply

Opt Object                                          Option   Previous Change
 _  /home/AU/AAAAA                                  *NONE    17/07/19 12:52
 _  /tmp/jhi/QOpenSys/perl/lib/5.8.0/ai*            *USRPRF  26/12/17 17:20

                                                                     Bottom

 List is of activities done by this option. It does not represent current status
 F3=Exit   F6=Add New   F8=Print         F12=Cancel
```

3. Enter **1** in the **`Opt`** column for the object that you want to change. The **Apply Object Auditing** screen appears.

```
                         Apply IFS Object Auditing

 Type choices, press Enter.

   Object  . . . . . . . . .  /home/AU/AAAAA
   You may use *, ?.
   Example:   /dir1      - all sub directories and all objects in all
                           sub directories.
              /dir1/*    - all objects in dir1
              /dir1/abc* - all abc* objects in dir1

   Object auditing option  .  1       1=*NONE
                                      2=*USRPRF
                                      3=*CHANGE
                                      4=*ALL

   Include sub directories .  Y       Y=Yes, N=No



 F3=Exit               F12=Cancel
```

Object Audit Strategies

The following best practices will help you balance the need to capture sufficient historical data without generating an excessive amount of raw data.

- Avoid using the `*ALL` parameter in object audit rules. It is generally unnecessary to audit passive object accesses, such as read attempts, on a routine basis. You can choose to do periodic, short-term audits of certain objects to get an idea of who is using them, but certainly not on an everyday basis.
- Utilize the `*USRPRF` option to restrict auditing of commonly used objects to users who do not need to access such objects routinely. For example, programmers routinely modify program source files. You might not wish to audit every update attempt by these users, but you would certainly want to know if your technical writer is messing around with program sources. This same axiom holds true for data files frequently updated by data entry clerks.
- Make effective use of the Object Type parameter in your rules, for example:
    - If your objective is to audit changes to program files in a library that contains both program and data files, use the `*PGM` object type to avoid cluttering your audit journal with updates of data files.
    - Likewise, use the `*FILE` object type to restrict your auditing to physical files.
    - Use `*AUTL` and `*USRPRF` to see who has been changing user profiles and object authorizations.
    - To discover who deleted your reports, use the `*OUTQ` object type.
    - Use the *CMD object type together with the `*USRPRF` auditing option to audit the use of specific commands by certain users. This creates far fewer journal entries then the user activity `*CMD` audit option.

- Use IFS object auditing. Databases shared with other platforms, such as ODBC databases, are IFS objects that should be audited on a regular basis.

Defaults for Object Creation

1. Select **`1. OS/400 Audit Features`** in the Main menu (*STRAUD*> **`1`**). The **`OS/400 Audit Features`** menu appears.
2. Select **`45`**. The **`Work with New Object Auditing (WRKNEWAUD)`** screen appears.

```
                    Work with New Objects Auditing (WRKNEWAUD)

 Type choices, press Enter.

 Library  . . . . . . . . . . .   __________    Name, generic*, *ALL



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

Parameter	Description
Library	**`Name`** = Display a specific user profile **`Generic*`** = Display all users beginning with text preceding the * **`*ALL`** = Display all users

3. Press Enter. The **Work with New Object Audit Defaults** screen appears.

```
                    Work with New Objects Auditing (WRKNEWAUD)

Type choices, press Enter.

Library  . . . . . .  . . .  __________    Name, generic*, *ALL



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

Working with IFS logs

When an organization is using a Security Information and Event Management (SIEM) system, Raz-Lee Security provides the administrator with an easy and effective tool for sending messages and events to those systems. With special capabilities and advanced features, Raz-Lee allows configuring up to three unique SIEM systems to be handled using the IFS logs mechanism.

NOTE: For more information about SIEM integration and configuration, see "SIEM Support" on page 296.

To access the IFS Logs:

- Select **15. IFS Logs** from the Audit main menu screen (*STRAUD* **> 15)**.

```
AUIFSMN                          IFS Logs                    iSecurity/SysCtl
                                                            System:   S520
Select one of the following:

Settings
 1. Work with Definitions

 5. Work with Activities


Activate IFS Log Detect
21. Activate
22. Deactivate

Note: Apache, WebSphere and other well-known servers can be set to
produce logs in CEF format.


Selection or command
===> ____________________________________________________________________

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

The **IFS Logs** menu allows the administrator to set and configure various types of message sources to be forwarded to SIEM systems such as Apache web server, IBM's WebSphere Application Server (WAS), and various database tools.

Settings

The settings section lets you configure IFS logging, including defining which files are logged.

To work with Definitions:

- Item *STRAUD* **> 15 > 1. Work with Definitions**. from the Settings section allows the administrator to add, remove, display and modify the desired application messages to communicate with the SIEM:

```
                        Work with IFS log Definitions

Type options, press Enter.
  1=Select  4=Delete  5=Display
              Auto   -SIEM-       Subset . .  ____________________________
Opt Subject   Start  1  2  3
 _  AABB             Y  Y  Y FOR TEST FROM JAVA.
 _  APACHEVV            Y    Apache Web Server S520
 _  ARDGATE          Y  Y  Y ArdGate log
 _  TEST50           Y       test dir longer than 50

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Add New   F12=Cancel
```

To change the logging settings on a file:

1. Type 1 next to the item to change, then press Enter.

```
                              Add IFS Log Auditing

 Subject . . . . . . . . . .  _________
 Description . . . . . . . .  ______________________________________________________
 Inform SIEM 1 2 3 . . . . .  _ _ _            Y=Yes
 Auto-start  . . . . . . . .  Y                Y=Yes

 Dir . . . . . . . . . . . .  ______________________________________________________
                              ______________________________________________________
 File prefix . . . . . . . .  ________________________________
 Original input format . . .  _____            *CEF, *LEEF, *FREE
 Severity  . . . . . . . . .  0                0-7
 Add date  . . . . . . . . .  Y                Y=Yes
 Add system  . . . . . . . .  Y                Y=Yes
 Add subject . . . . . . . .  _                Y=Yes




 Maximum message length is 5000.
 F3=Exit   F12=Cancel
```

2. Change the settings as appropriate.
3. Press **F3**. The changes are saved.

To delete the logging settings for a file:

- Type 4 next to the file whose settings are to be deleted, then press **Enter**.

To display the settings for a file:

- Type 5 next to the file, then press **Enter**.

To log settings for a new file:

1. Press **F6**. The **Add IFS Log Auditing** page is displayed.
2. Enter the settings as appropriate.
3. Press **F3**. The file's changes will now be logged.

Parameter	Description
Subject	Indicates the specific server type. Keep this part blank, as the software will fill that part automatically.
Description	Enter the name of the server.
Inform SIEM 1 2 3	Set which SIEM servers to inform. More information, about the different three types can be found under ***STRAUD* > 81 > 30**.
Auto-Start	Choose **Y** next to the Auto-Start section in order for the server to send messages automatically to the desired SIEM system. Note: Choosing **Y** will start automatically the IFS Log transmission when Audit is activated.
Dir	Enter the specific path where the server message log is located. For example: `/tmp/`
File Prefix	Indicate the specific file name containing the messages to be sent to the SIEM system under the desired directory. Normally, the SIEM messaging system works with a specific file. WHen the file fills up, the system renames the file and continues to write the new logs and messages under the same file. Indicating the correct file name will ensure that the messaging activity and sending works flawlessly.
Original input Format	The Original input format indicates which log the Raz-Lee IFS gets from the Apache webserver or the IBM websphere. You can choose `CEF`, `LEEF` or `FREE`.
Severity	Use the severity mechanism to determine the importance level of a message. The possible values are: **`Blank`** = Do not send **0** = Emergency (Default) **1** = Alert **2** = Critical **3** = Error **4** = Warning **5** = Notice **6** = Info **7** = Debug For more information, see "QAUDJRN Type/Sub Severity Setting" on page 294.

Parameter	Description
	You can change the severity level or an SIEM by going to *STRAUD* **> 81. System Configuration, 31/32/33 (SIEM 1,2,3)**.
Facility	There are 24 levels of facilities to be chosen from (levels 0-23). The FREE facility component indicates the type of program or process that is logging the message. It is recommended to keep this section 0 to keep SIEM default Audit's default Facility number is marked as 22 (Local use 6 or Local 6). For more information, see "SIEM Support" on page 296.

Original Input Formats

The following Original Input Formats are supported:

- **CEF** – Common Event Format, an open standard that passes messages over to the communications module that handles the transmission of the messages to the waiting log collection server using either UDP, TCP or TLS protocol.
- **LEEF** – Log Event Extended Format, another open standard for log management and interoperability of security related information from different devices, network components and applications. The LEEF format is a customized event format for IBM security Qradar that contains readable and easily processed events.
- **FREE** - In the FREE format, information and message settings (Severity and Facility) are sent as is (i.e. as configured at the Add/Change IFS Log Auditing menu, shown in "Working with IFS logs" on page 89). If FREE format is chosen, the administrator has to manually indicate Severity and Facility sections, and the subject name would be attached to the log that is sent.

Activate /Deactivate IFS Log Detection

Once the administrator has added and configured all of the desired servers to participate in the SIEM message handling, you can proceed to the **`Activate IFS Log Detect`** section in order to Activate/Deactivate them for transmitting the information to the SIEM system. Use this section in order to activate the servers that were configured at the **Work with IFS logs Auditing** menu page.

To activate Audit IFS Logs (ACTAUIFSL):

1. Select **`21. Activate`** from the **IFS Logs** screen (*STRAUD* **`> 15 > 21`**).

```
                      Activate Audit IFS Logs (ACTAUIFSL)

Type choices, press Enter.

IFS Log Subject  . . . . . . . .   __________     Name, generic*, *ALL
Select Auto-start=Y only . . . .   *NO           *YES, *NO

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

Field	Description
IFS Log Subject	Choose which servers should send their messages to the SIEM system. The administrator can choose between a specific server (Name) and all enabled servers (*ALL).
Select Auto-start=Y only	If set to `*YES`, activate only the servers with that IFS Log Subject for which the Auto-Start field was set to "`Y`" on the **Work with IFS Logs Definition** screen (shown in "Settings" on page 90).

2. Enter the options as appropriate, then press **Enter**.

NOTE: Only the enabled subject at the **Control IFS Logs** menu will be activated.

To deactivate Audit IFS Logs (DCTAUIFSL):

1. Select **`22. Deactivate`** from the **IFS Logs** screen (*STRAUD* **`> 15 > 22`**).

```
                    Deactivate Audit IFS Logs (DCTAUIFSL)

Type choices, press Enter.

IFS Log Subject  . . . . . . . .   __________    Name, generic*, *ALL



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

2. Enter the log subject to deactivate or `*ALL` to deactivate all of them, then press **Enter**.

Real-Time Auditing

This chapter presents a detailed discussion of the real-time auditing features. The discussion begins with a conceptual introduction and continues with the most commonly used features and parameters. Practical examples are presented together with detailed procedures.

Real-Time Detection

The principal feature of [[[Undefined variable Audit.ProductName]]] is its ability to examine and respond to security related events in real time. When the IBM i (OS/400) current audit settings detect an event, an entry is recorded in the security audit journal. At the same time, [[[Undefined variable Audit.ProductName]]] looks for a real time detection rule for this event.

If such a rule exists, [[[Undefined variable Audit.ProductName]]]records the event in a history log and optionally triggers an alert message or command script as specified by the rule definition. Action (sold as a separate product) performs these responsive actions.

The powerful query and reporting features of [[[Undefined variable Audit.ProductName]]]use the contents of the history log. You must define real time detection rules to capture and record events in the history log, even if no responsive action is necessary. In fact, you will likely create most of your real time detection rules solely for the purpose of recording events in the history log for subsequent audit and analysis.

It is important to note that an event must first be detected by the current IBM i (OS/400) audit settings in order for real-time detection to capture and record it in the history log and/or trigger an action.

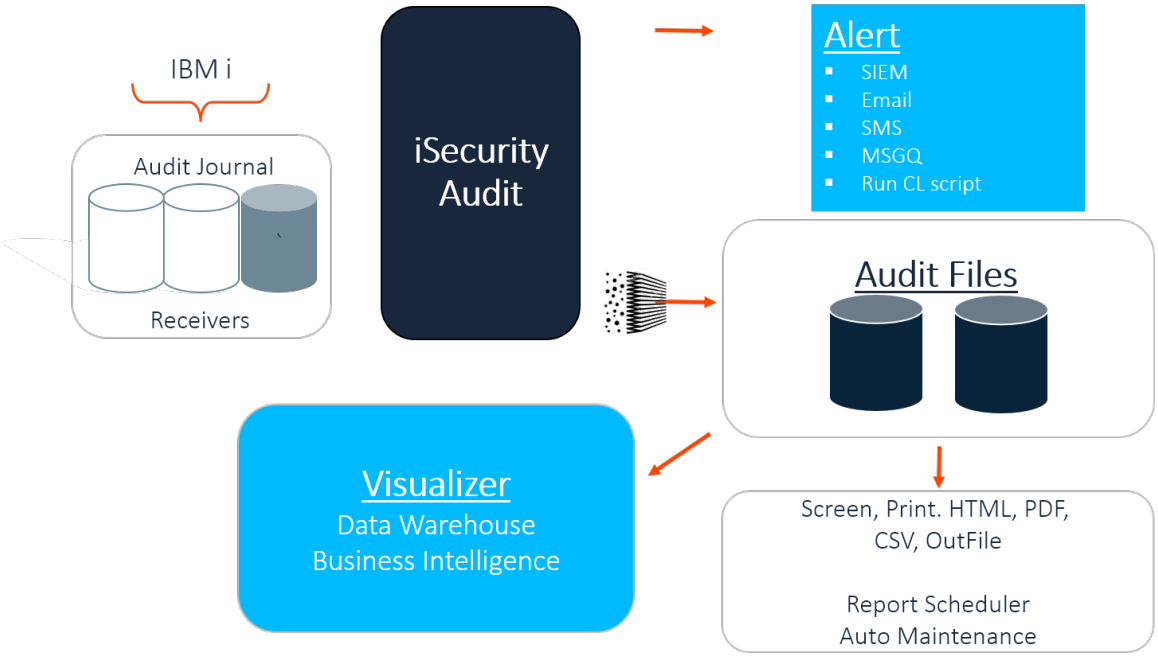


Figure 2: Audit's Real-Time Detection Process

Integration with Action

As you can see from the above chart, one of the main advantages of real-time detection lies in its integration with the Action product. Action physically sends the alert messages and executes command scripts triggered by [[[Undefined variable Audit.ProductName]]].

Rules and Actions

A series of user-defined rules and actions controls real-time detection. Rules identify which specific events trigger actions and under what conditions the response should occur. Actions define specific responsive actions that take place whenever rule conditions are met.

Real-time detection rules are based on IBM i (OS/400) audit journal types. You can create several different rules for a single audit type. User-defined sequence numbers determine the order of rule processing within a given type.

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

1. Ensure that the IBM i (OS/400) audit settings are properly defined to capture events covered by the rule.
2. Create a new real-time detection rule or select an existing rule for modification.
3. Optionally:
    a. Set basic rule parameters using the Selection Rule screen.
    b. Define filter conditions limiting application of the rule to specific conditions.
    c. Define alert message actions as necessary.
    d. Define command script actions as necessary.
4. Test and debug your rule.

Audit provides you with a suite 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 can use existing action definitions with any number of rules.
- You can apply precise filter criteria 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 allows you to apply rules only during (or outside of) predefined periods.

Creating and Modifying Rules

To create or modify real time detection rules:

1. Select `11. QAUDJRN Real-Time Processsing` in the Main menu (*STRAUD>* **11**). The **Work with Real-Time Audit Rules** screen appears.

```
                        Work with Real-Time Audit Rules
                          Rules & Actions for QAUDJRN
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

Opt Entry Seq Log Act Cont. Description
 _   AD  999.9 N   N   N    Default for: Auditing changes AD
 _   AF  999.9 N   N        Default for: Authority failure AF
 _   AP  999.9 N   N        Default for: Obtaining adopted authority AP
 _   AU  999.9 N   N        Default for: Attribute change AU
 _   AX  999.9 N   N   N    Default for: Row and Column Access Control (RCAC)
 _   C@    1.0 Y   N   N    scc@ test x Stephen Laseplan
 _       999.9 Y   N        Default for: User profile changed (After & Previou
 _   CA    1.0 N   N   N    Authority changes
 _       2.0 N   N   N    Authority changes
 _       999.9 N   N   N    Default for: Authority changes CA
 _   CD    1.0 Y   N   N    Command string audit
                                                                       More...
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber

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

Parameter or Option	Description
Opt	**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 displayed 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
Act	**Y** = This rule triggers an action
Cont	**Y** = Continue with the rest of the rule after running the 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.

```
                              Modify Selection Rule
                                  Rules & Actions for QAUDJRN

Entry type . . . . . . .  C@ User profile changed (After & Previous images)
  Sequence . . . . . . .   1.0

Description  . . . . . .  scc@ test x Stephen Laseplan
Sub-type list  . . . . .  *ALL                          *ALL, List
                          N  Name
Check if in Time group .  _  __________

Log  . . . . . . . . . .  Y                     Y=Yes, N=No

Perform action . . . . .  N  VICT202448         Name, *NONE, *ADD
  If event rate exceeds.     ___1 / ___1        Events/Seconds, 1/1=Always
  Run action once per  .     ___0               Seconds, 0=Always
If true, re-check after.     0                  Seconds, 0=Default
If false, re-check after     0                  Seconds
Continue to rule seq . .  N   ___.0             Y=Yes, N=No. 0=Following rule


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

Parameter or Option	Description
EntryType	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 can 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
Check if Time Group	You can 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
If event rate exceeds	Only perform the action if the event occurs more than a given number of times in a given time period. For example, 5 times in every 10 seconds. If you want to run the action always, enter 1/1.

Parameter or Option	Description
Run action once per	The number of seconds between each performance of the action.
Continue to rule seq	Y= After performing the actions, continue to the rule sequence.

4. Enter parameters and data as described in the table, then Press **Enter**.
   The **`Filter Conditions`** screen appears.

Filter criteria allow you to limit the application of real-time detection rules to certain specific conditions.

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.

```
                                Filter Conditions
Entry  . . . . . . . .  ZC   Object accessed (change)
Sequence . . . . . . .   1.0 React to unpermitted changes in prod files
                             Subset by text . . _____________________________
Type conditions, press Enter. Specify OR to start each new 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
     Program library                 ______ ________________________________
 _   Library name                    ______ ________________________________
 _   Date & Time   yyyy-mm-dd-hh.mm  ______ ________________________________
 _   Name of job                     ______ ________________________________
 _   User of job                     LIST   QSECOFR JOHN
 _   Number of job                   ______ ________________________________
 _   Name of program                 ______ ________________________________
 _   Program library                 ______ ________________________________
 _   Current user profile            ______ ________________________________
 _   System name                     ______ ________________________________
 _   IP address family               ______ ________________________________
                                                                      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
```

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 the 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.

5. If desired, add filter conditions, then press **Enter**. The previous screen is displayed.

Comparison Test Operators

You can use these test operators when creating filters.

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	Compare the value of the tested field against a group of values. To select values, place the cursor in the **Values** field and press the F4 key, as shown in the example below.	▪ For **character** fields: • Group Name: The name of a general group (as shown in General Groups). If the name is followed by the keyword ***GENERIC**, items within the group that end in an asterisk ("*****") are treated as generic values. Otherwise, the values, including the asterisk, must be exact matches. Generic searches take much longer than exact matches. Only use them if they are necessary. ▪ For **user profile** fields: • ***GRPPRF**: Check if the User is included in a Group or Supplemental profile. • ***LMTCPB**: Checks the User Limit Capabilities. • ***SPCAUT**: Check if the User has a Special Authority. • ***USRGRP**: Checks if the User is included in an iSecurity/Firewall group (as documented in the Firewall manual). ▪ For **timestamp** fields: • Check if the time is within a Timegroup (as shown in Using Time Groups).

Test	Description	Value Field Data
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)

For example, in this **Filter Conditions** screen, the **`Test`** for the field **`User Profile`** is set to **`ITEM`**.

```
                                Filter Conditions
Entry  . . . . . . . .  $A   User profile information
Sequence . . . . . . .   1.0
                              Subset by text . . _______________________________
Type conditions, press Enter. Specify OR to start each new 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
     *ALLOBJ   (User+Groups) X=Yes   EQ     X
 _   User Profile                    ITEM   ____________________________________
 _   Previous sign-on date: YYMMDD   ______ ____________________________________
 _   Days passed since last sign-on  ______ ____________________________________
 _   Sign-on attempts not valid      ______ ____________________________________
 _   Status                          ______ ____________________________________
 _   Password of *NONE: *YES or *NO  ______ ____________________________________
 _   Password change date: YYMMDD    ______ ____________________________________
 _   Password expiration interval    ______ ____________________________________
 _   Days password is in use         ______ ____________________________________
 _   Block password change           ______ ____________________________________
                                                                        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
```

To select values for the test, place the cursor in the **Value** field for that line and press the **F4** key.

The **Select Subject** window appears:

```
                              Filter Conditions
.........................................................................
:                               Select Subject                          :
:                                                                       :
:  Type options, press Enter.             Position to . . . _________  :
:    1=Select                             Subset  . . . . . ____________ :
:  ** When run for another system, groups on that system are considered. **  :
:  Opt Subject    Description                                           :
:   _  *GRPPRF    User is included in Group/Supplemental profile        :
:   _  *LMTCPB    User Limit Capabilities                               :
:   _  *SPCAUT    User has a Special Authority                          :
:   _  *TIMEGRP   Time group                                            :
:   _  *USRGRP    User is included in iSecurity/Firewall Group          :
:   _  AUD        List for Audit Reporting                              :
:   _  AUDJ       Secondary list for audits                             :
:   _  COMMANDS   Initial commands to run as a group                    :
:   _  COMMANDS2  Secondary commands group                              :
:                                                                More... :
:  F3=Exit   F6=Work with group type   F12=Cancel                      :
:                                                                       :
:.......................................................................:
 F3=Exit   F4=Prompt   F6=Insert   F8=UC/LC          F12=Cancel
```

Each **Subject** on this screen contains one or more groups that can be selected. To select a **Subject**, enter **1** in the **Opt** field next to that **Subject** field.

The **Select Groups of** screen for that **Subject** appears:

```
                                Filter Conditions
..............................................................................
:                                Select Subject
..............................................................................
:                        Select Groups of LIBRARIES                          :
:  Class: Groups of libraries                                                :
:                                                                            :
:  Type options, press Enter.           Position to .  __________          :
:    1=Select                           Subset  . . .  ________________    :
:    2=Select with generic* support                                          :
:  Opt  Group       Description                                             :
:   _   KEYSLIB     List of libraries holding encryption keys               :
:   _   PGMPROD                                                              :
:   2   PRODLIB     List of Production Libraries                            :
:   _   SYSTLIB     List of System Libraries                                :
:                                                                            :
:                                                                            :
:                                                                            :
:                                                                     Bottom :
:                                                                            :
:  F3=Exit   F6=Work with groups   F12=Cancel                                :
:                                                                            :
:............................................................................:
```

For example, this screen shows the groups within the subject **LIBRARIES**.

You can select the groups in two ways.

To select a group with generic* support, enter **2** in the **Opt** field for that group. With generic* support, for each item in the group that ends with an asterisk ("*****"), the test will attempt to match the item with any values that begin with the characters in the item name preceding the asterisk. This can significantly increase the amount of time that the test will take. Only specify this when necessary.

To select a group without generic* support, enter **1** in the **Opt** field for the group. The test will match the items in the group literally.

When you press **Enter**, the **Filter Conditions** screen returns:

```
                              Filter Conditions
Entry  . . . . . . . .  $A   User profile information
Sequence . . . . . . .   1.0
                             Subset by text . . ______________________________
Type conditions, press Enter. Specify OR to start each new 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
     *ALLOBJ   (User+Groups) X=Yes   EQ     X
 _   User Profile                    ITEM   LIBRARIES/PRODLIB *GENERIC
 _   Previous sign-on date: YYMMDD   ______ ______________________________
 _   Days passed since last sign-on  ______ ______________________________
 _   Sign-on attempts not valid      ______ ______________________________
 _   Status                          ______ ______________________________
 _   Password of *NONE: *YES or *NO  ______ ______________________________
 _   Password change date: YYMMDD    ______ ______________________________
 _   Password expiration interval    ______ ______________________________
 _   Days password is in use         ______ ______________________________
 _   Block password change           ______ ______________________________
                                                                     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
```

In this case, the **`Value`** field for **`User Profile`** shows **`LIBRARIES/PRODLIB *GENERIC`**, indicating that you had selected the group **`PRODLIB`** within the subject **`LIBRARIES`**, with **`*GENERIC support`** enabled.

And/Or Boolean Operators

You can combine multiple filter conditions in one rule using Boolean AND/OR operators. This allows 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 allows 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 React to unpermitted changes in prod files
                             Subset by text . . _
Type conditions, press Enter. Specify OR to start each new 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
     Program library                 NITEM  LIBRARIES/PGMPROD
 A   Library name                   ITEM   LIBRARIES/PRODLIB
 _   Date & Time   yyyy-mm-dd-hh.mm
 _   Name of job
 _   User of job
 _   Number of job
 _   Name of program
 _   Program library
 _   Current user profile
 _   System name
 _   IP address family
                                                                        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
```

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

```
                                Message to send

Rule: *REAL-TIME  ZC    1.0 Object accessed (change)

Type message to send. Use F7-F9 to select replacement fields.
*AUTO is the standard message (*AUTO1/*AUTO2 are message first/second levels).

Message text:
Job: &ZCNBR/&ZCUSER/&ZCJOB
Action: &ACTION &SEQID
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________


F7=Replacement fields   F8=Add JOB   F9=Add ACTION   F12=Cancel
 Modify data, or press Enter to confirm.
```

Use **F7** to insert fields to the message, **F8** to add the job information, **F9** to add Action information.

Firewall/Screen

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

To work with system status:

1. Select **`12. Firewall/Screen`** from the Main menu (*STRAUD* **`> 12`**). The **`Work with Firewall/Screen Rules`** screen appears.

```
                        Work with Firewall/Screen Rules
                      Firewall and Screen (after decision)

                                          Subset by entry  . . ___
                                            by description . . _______________
Type option, press Enter.                   by classification. _  C=Compliance,..
  1=Select   3=Copy   4=Delete            8=Msg   9=Explanation & Classification

Opt Entry Seq      Act Cont. Description
 _   01    1.0 Y    N   N    *FILTFR Original File Transfer Function
 _        999.9 Y    N        Default for: *FILTFR Original File Transfer Functi
 _   02   999.9 Y    N        Default for: *FTPLOG FTP Server Logon 02
 _   03    1.0 Y    N   N    *FTPSRV FTP Server-Incoming Rqst Validation
 _        999.9 Y    N        Default for: *FTPSRV FTP Server-Incoming Rqst Vali
 _   04   999.9 Y    N        Default for: *SQL Database Server - SQL access 04
 _   05   999.9 Y    N        Default for: *RMTSRV Remote Command/Program Call 0
 _   06   999.9 Y    N        Default for: *FILSRV File Server 06
 _   07   999.9 Y    N        Default for: *DDM DDM request access 07
 _   08   999.9 Y    N        Default for: *TELNET Telnet Device Initialization
 _   09   999.9 Y    N        Default for: *TFTP TFTP Server Request Validation
                                                                        More...
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber
```

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

```
                              Add Selection Rule
                           Firewall and Screen (after decision)

Entry type . . . . . . .  ___
  Sequence . . . . . . .   .0

Description  . . . . . .  ____________________________________________________
Sub-type list  . . . . .  *ALL                            *ALL, List
                          N  Name
Check if in Time group .  _  __________



Perform action . . . . .  Y  *ADD        Name, *NONE, *ADD
  If event rate exceeds.     0 / 0       Events/Seconds, 1/1=Always
  Run action once per  .     0           Seconds, 0=Always
If true, re-check after.     0           Seconds, 0=Default
If false, re-check after     0           Seconds
Continue to rule seq . .  _   .0         Y=Yes, N=No. 0=Following rule


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

Parameter or Option	Description
Entry 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.
Check if in Time group	You can 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

Parameter or Option	Description
If event rate exceeds	Only perform the action if the event occurs more than a given number of times in a given time period. For example, 10 times in every 5 seconds. If you want to run the action always, enter **1/1**.
Run action once per	The number of seconds between each performance of the action.
If true, recheck after	The number of seconds after which to check again, if true. **0** = Default
If false, recheck after	The number of seconds after which to check again, if false. **0** = Default
Continue to rule seq	**Y**= After performing the actions, continue to the rule sequence.

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

Working with Status and Active Job Rules

IBM and Raz-Lee Entry Types include (see Appendix A: Raz-Lee Entry Types):

- IBM Entry Types – ***STRAUD > 11*** (see Setting up the Audit Scheduler).
- Raz-Lee Entry Types @J, @K, @P, @S - ***STRAUD > 13*** (see Working with Status and Active Job Rules).
- Raz-Lee Entry Types @0…@9 - ***STRAUD > 14*** (see Working with Message Queues).
- Other Raz-Lee Entry Types (see Appendix A: Raz-Lee Entry Types).

The following can be achieved using the Entry Type screens:

- Define rules triggered by specific field contents for each entry type. Resulting actions can generate messages, run command language (CL) commands and more.
- Generate reports using the iSecurity report generator and scheduler which controls, via field filters, which of the collected QAUDJRN entries are to be outputted to e-mail, message queue (MSGQ), Syslog, etc. The report generator can be accessed at ***STRAUD*> 41 > 1**.

To Work with Status & Active Job Rules:

1. Select **13. Status & Active Job (SysCtl)** in the Main menu (***STRAUD*> 13**). 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
                        Rules for WRKACTJOB/WRKSYSSTS

                                          Subset by entry  . . ___
                                            by description . . _______________
Type option, press Enter.                   by classification. _  C=Compliance,..
  1=Select  3=Copy  4=Delete             8=Msg  9=Explanation & Classification

Opt Entry Seq     Act Cont. Description
 _   @J  999.9 N   N        Default for: Active job information @J
 _   @K  999.9 N   N        Default for: Job not active @K
 _   @P  999.9 N   N        Default for: Pool not active @P
 _   @S  999.9 N   N        Default for: System status and pool information @S

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

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

Entry	Rule Description
@J	Logs Active job information, while comparing every line in the *WRKACTJOB* to the rule that uses it.
@K	Logs Inactive Jobs, while performing a check to verify whether the job is active.
@P	Logs Inactive Pools, while performing a check to verify whether a particular pool is active.
@S	Logs System status & pool information, while checking filter conditions to verify if response criteria are met, and activating that response.

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

```
                                Add Selection Rule
                            Firewall and Screen (after decision)

Entry type . . . . . . .  ___
  Sequence . . . . . . .  ___.0

Description  . . . . . .  ____________________________________________________
Sub-type list  . . . . .  *ALL                            *ALL, List
                          N  Name
Check if in Time group .  _  __________



Perform action . . . . .  Y  *ADD       Name, *NONE, *ADD
  If event rate exceeds.     ____0 / ____0  Events/Seconds, 1/1=Always
  Run action once per  .     ____0       Seconds, 0=Always
If true, re-check after.      0          Seconds, 0=Default
If false, re-check after      0          Seconds
Continue to rule seq . .  _  ___.0       Y=Yes, N=No. 0=Following rule


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

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 can 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
If event rate exceeds	Only perform the action if the event occurs more than a given number of times in a given time period. For example, 10 times in every 5 seconds. If you want to run the action always, enter **1/1**.
Run action once per	The number of seconds between each performance of the action.
If true, delay interval	Define the number of seconds to wait before performing the action. The default is 0.
Continue to rule seq	**Y**= After performing the actions, continue to the rule sequence.

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

See Working with Current Setting and Setting up the Audit Scheduler.

Working with Message Queues

There are two fixed IBM message queue types, known as Group ID:

- @9 QHST – IBM provided History queue
- @1 QSYSOPR – IBM provided System Operator queue

In Audit, you can create your own message queues and operate them according to your needs. This unique solution allows real-time auditing on message queues, by:

- Modifying rules according to all the message queue parameters
- Responding to the message by alerting the user (by email and/or text message (SMS)) and by reacting to it directly (send auto response).

To work with message queues:

- Select **14. Message Queue (SysCtl)** in the Main menu (*STRAUD* **> 14**). 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 from Displayed Msgs
                                          55. Display History Log (Audit version)
Real-Time Detection Rules
11. Message Queue rules

Activate MSGQ detection
21. Activate
22. Deactivate

Set Start
35. Set Start of QHST Time


Selection or command
===> ____________________________________________________________________________

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

Create Message Queue Audit Rules

1. To define a message queue to monitor, select **`1. Control Message Queues/QHST`** from the Message Queue menu (*STRAUD*> **`14 > 1`**). The **`Work with Message Queues`** screen appears.

```
                          Work with Message Queues

Type options, press Enter.                    Position to . . . _________
  1=Modify   4=Remove   5=Display messages
                                        Operation            Data      Check
Opt  Msg queue  Library   Group  Active   Mode     Syslog    Queue     Actions
 _   QHST       QSYS       @9      Y       5         Y       *NONE       Y
 _   QSYSOPR    *LIBL      @1      Y       9         N       *NONE       Y

                                                                        Bottom

F3=Exit    F6=Add New    F8=Print    F12=Cancel
```

2. Select **`1=Modify`** to modify an existing message queue or **F6** to create a new message queue. The **`Add Message Queue`** screen appears.

```
                              Add Message Queue

Message queue  . . . . . . . .  __________    Name, QHST
  Library  . . . . . . . . . .    *LIBL      Name, *LIBL
Active definition  . . . . . .  Y            A=Auto start, N=No,
                                             Y=Yes, requires manual activation
Operation mode . . . . . . . .  _            1=Periodic, 5=QHST, 9=Immediate
  For 1, Number of seconds . .   300
  For 9, Break program . . . .  *STD         Name, *STD SMZ4/AUSOURCE AUMSGBRK
    Library  . . . . . . . . .   __________  Name, *LIBL

Send to SIEM . . . . . . . . .  N            Y=Yes, N=No
Send to user Data Queue  . . .  *NONE        Name, *NONE
           Library . . . . . .   __________  Name, *LIBL

Check rules & perform Actions.  Y            Y=Yes, N=No     *NO
  For Check rules, Group Id  .  @1           @1, @2, ..., @9=QHST
Duplicates may appear if Action sends to SIEM/Data Queue, selected above.

QHST requires Operation mode 5, Group @9.

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

Parameter or Option	Description
Message queue/library	The name of message queue being created/modified and the library where it exists
Active Definition	**A** = Automatic start at IPL or restart. You can only choose this if the Message Queues (set to start at *IPL) parameter in the Auto Start Activities screen is set to Yes. For more details, see "Auto start activities in ZAUDIT" on page 284. **Y** = Yes. After activating ZAUDIT, you will need to manually restart the Message Queue. **N** = No
Operation mode	**1** = Periodic **5** = Watch. You must use 5 if you are monitoring QHST. **9** = Immediate
Number of seconds	Only used if Operation Mode = **1**. Define the number of seconds to wait between each application of the rule.
Break program/library	Only used if Operation Mode = **9** Define the name and library of the program to use for break handling. The program source for ***STD** is *SMZ4/AUSOURCE AUMSGBRK*.
Send to SIEM	Define how to send the break information to SIEM: **1** = Syslog **2** = SNMP **N** = No
Send to user data queue/library	Define the name and library of the data queue to use for break handling.
Check rules & perform Actions	**Y** = Yes **N** = No
For check rules, Group Id	The Group ID for the rule definitions. Use option `11`. `Message Queue` rules to create/modify the rule definitions. Use the Group ID to group message queues with similar handling together to reduce the number of rules needed.

3. Enter parameters and data as described in the table, then press **Enter**. The **Filter Conditions** screen appears. Filter criteria allow you to limit application of real-time detection rules to certain specific conditions.

Define a Message Queue Rule

The message queue rule defines what gets filtered when written to the log.

1. Select **`11. Message Queue rules`** from the **Message Queues** menus (*STRAUD* **`> 14 > 11`**). The **`Work with Message Queues`** screen appears.

```
                              Work with Message Queues
                     Rules & Actions for Message Queue

                                          Subset by entry  . . ___
                                            by description . . _______________
Type option, press Enter.                   by classification. _  C=Compliance,..
  1=Select  3=Copy  4=Delete             8=Msg  9=Explanation & Classification

Opt Entry Seq     Act Cont. Description
 _   @0  999.9 N   N   N    Default for: Message queue (Group Id 0) @0
 _   @1   __1.0 Y   Y   N    Message queue (Group Id 1)
 _       999.9 N   N   N    Default for: Message queue (Group Id 1) @1
 _   @2  999.9 N   N        Default for: Message queue (Group Id 2) @2
 _   @3  999.9 N   N        Default for: Message queue (Group Id 3) @3
 _   @4  999.9 N   N        Default for: Message queue (Group Id 4) @4
 _   @5  999.9 N   N        Default for: Message queue (Group Id 5) @5
 _   @6  999.9 N   N        Default for: Message queue (Group Id 6) @6
 _   @7  999.9 N   N        Default for: Message queue (Group Id 7) @7
 _   @8  999.9 N   N        Default for: Message queue (Group Id 8) @8
 _   @9   __1.0 Y   Y   N    Test
                                                                      More...
F3=Exit   F6=Add New   F8=Print   F11=No/Default   F12=Cancel   F22=Renumber

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

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

```
                              Modify Selection Rule
                           Rules & Actions for Message Queue

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

Description  . . . . . .  Message queue (Group Id 1)
Sub-type list  . . . . .  *ALL                            *ALL, List
                          N  Name
Check if in Time group .  _  __________



Perform action . . . . .  Y  ALEX172310          Name, *NONE, *ADD
  If event rate exceeds.     ___1 / ___1         Events/Seconds, 1/1=Always
  Run action once per  .     ___0                Seconds, 0=Always
If true, re-check after.      0                  Seconds, 0=Default
If false, re-check after      0                  Seconds
Continue to rule seq . .  N   ___.0              Y=Yes, N=No. 0=Following rule


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

Option	Description
Entry Type	Audit types are the entries **@1**-**@9**. All choices have the same parameters. These are the rule identifiers you use when setting rules. **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	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 ***NONE** = No actions are triggered by this rule ***ADD** = Define a new action for this rule F4 = Select an action from the list
If event rate exceeds	Only perform the action if the event occurs more than a given number of times in a given time period. For example, 10 times in every 5 seconds. If you want to run the action always, enter **1/1**.
Run action once per	The number of seconds between each performance of the action.
If true, delay interval	Define the number of seconds to wait before performing the action. The default is 0.
Continue to rule seq	**Y**= After performing the actions, continue to the rule sequence.

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

Activate Message Queue Detection

1. Select **21. Activate** from the Message Queues menu (*STRAUD* **>14 >21**). The **Activate Audit Message Queue (ACTAUMSGQ)** screen appears.

```
                    Activate Audit Message Queue (ACTAUMSGQ)

 Type choices, press Enter.

 Message queue  . . . . . . . . .   __________    Name, generic*, *ALL
   Library  . . . . . . . . . . .     *ALL        Name, *ALL, *LIBL
 Select by: Activate at IPL . . .   *ALL          *IPL, *ALL
            Operation mode  . . .   *ALL          *IMMED, *PERIOD, *QHST, *ALL

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

Parameter	Description
Message queue	The name of the message queue you want to activate. **Name** = the name of the specific message queue ***ALL** = All message queues
Library	The name of the library that contains the message queue. **Name** = the name of the specific message queue ***ALL** = All message queues ***LIBL**
Select by: Activate at IPL	***IPL** = Activate at IPL ***ALL**
Operation mode	***IMMED** = Activate the message queue immediately ***PERIOD** = Activate the message queue periodically ***ALL**

2. Enter parameters as described in the table and press **Enter**. The Message Queue is activated according to the input parameters.

Deactivate Message Queue Detection

1. Select **22. Deactivate** from the Message Queues menu (*STRAUD* **> 14 > 22**). The **Deactivate Audit Message Queue (DCTAUMSGQ)** screen appears.

```
                    Deactivate Audit Message Queue (DCTAUMSGQ)

 Type choices, press Enter.

 Message queue  . . . . . . . . .   __________    Name, generic*, *ALL
   Library  . . . . . . . . . . .     *ALL        Name, *ALL, *LIBL
 Handling type  . . . . . . . . .   *ALL          *IMMED, *QHST, *PERIOD, *ALL

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

Parameter	Description
Message queue	The name of the message queue you want to deactivate. **Name** = the name of the specific message queue ***ALL** = All message queues
Library	The name of the library that contains the message queue. **Name** = the name of the specific message queue ***ALL** = All message queues ***LIBL**
Handling type	***IMMED** = Deactivate the message queue immediately ***PERIOD** = Deactivate the message queue periodically ***ALL**

2. Enter parameters as described in the table and press **Enter**. The Message Queue is deactivated according to the input parameters.

Build Rules for Displayed Messages

Define in which order to display messages from a defined message queue; earliest first or latest first.

1. Select **51. Build rules for displayed Msgs** from the **Message Queues** menu (*STRAUD* **> 14 > 51**). The **Display Audit Message Queue (DSPAUMSGQ)** screen appears.

```
                    Display Audit Message Queue (DSPAUMSGQ)

Type choices, press Enter.

Message queue  . . . . . . . . .   __________    Name
  Library  . . . . . . . . . . .    *LIBL       Name, *LIBL
Message queues to display first  . . .  *FIRST    *FIRST, *LAST

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

Parameters or Options	Description
Message queue	The name of the message queue for which you are defining display rules. Name = the name of the specific message queue
Library	The name of the library that contains the message queue. **Name** = the name of the specific message queue ***LIBL**
Messages to display first	***FIRST** = Display the earliest messages first. This is the default choice. ***LAST** = Display the latest messages first.

2. Enter parameters as described in the table and press **Enter**.

Display Message History Log

1. Select **`55. Display History Log (Audit version)`** from the Message Queues menu (*STRAUD* **`> 14 > 55`**). The **Display Log (Audit) (DSPSYSLOG)** screen appears.

```
                        Display Log (Audit) (DSPSYSLOG)

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
Output . . . . . . . . . . . . .   *            *, *PRINT, *PRINT1-*PRINT9



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

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 start and end times specified below
Starting date and time Ending date and time	Selects only those events occurring within the range specified by the start and end 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**/ ***PRVMONTHS** = Current month/Previous month ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year ***SUN** -***SAT** = Day of week
Output	Where to send the output. The default is to the screen. * ***PRINT** ***PRINT1 - 9**
Print format	***SHORT** (default) ***FULL**

2. Enter parameters as described in the table and press **Enter**. The log appears or printed according to the input parameters.

Working with Time Groups

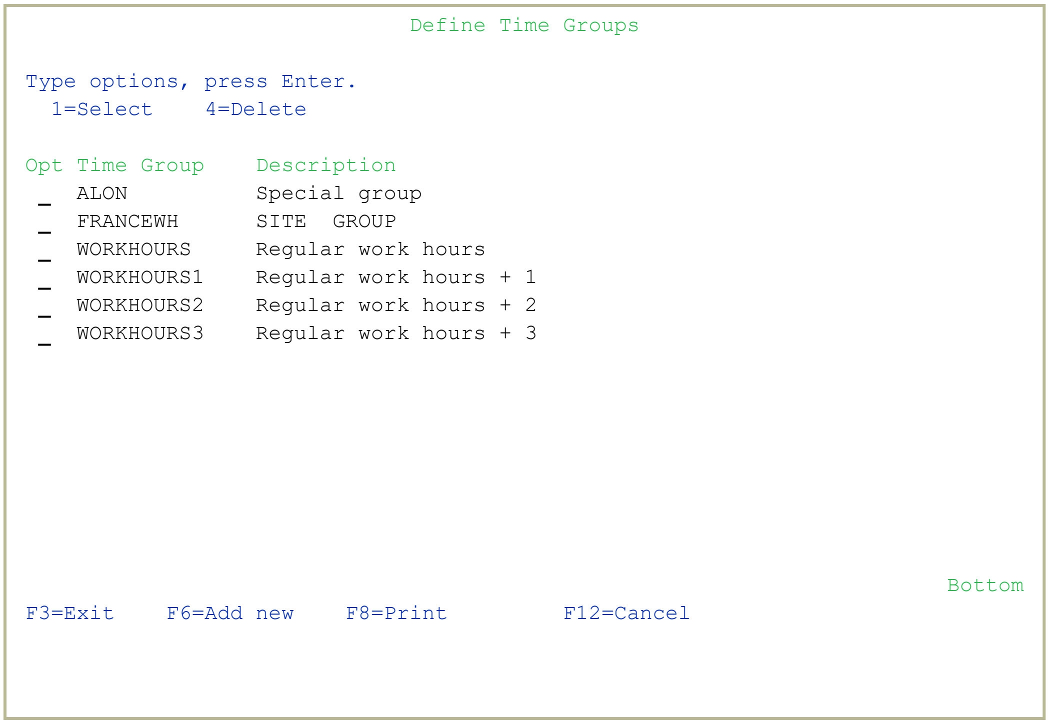
Time Groups

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 auditing rules, as well as for queries, reports and the history log. Time group filters can be either:

- Inclusive – Including activities that occur only during the time group periods
- Exclusive – Excluding all activities that occur during the time group periods.

To define a time group:

1. Select **`31. Time Groups`** in the Audit Main menu (***STRAUD* `> 31`**). The **`Define Time Groups`** screen appears.



```
                               Define Time Groups

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

Opt Time Group    Description
 _  ALON          Special group
 _  FRANCEWH      SITE  GROUP
 _  WORKHOURS     Regular work hours
 _  WORKHOURS1    Regular work hours + 1
 _  WORKHOURS2    Regular work hours + 2
 _  WORKHOURS3    Regular work hours + 3











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

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

```
                              Change Time Group

Time Group . . . ALON
Description  . . Special group

Type choices,  press Enter

           Start  End    Start  End
Monday      8:00 12:00    0:00  0:00
Tuesday     8:00 12:00    0:00  0:00
Wednesday   8:00 12:00    0:00  0:00
Thursday    8:00 12:00    0:00  0:00
Friday      0:00  0:00    0:00  0:00
Saturday    0:00  0:00    0:00  0:00
Sunday      8:00 12:00    0:00  0:00


 Note: An End time earlier than the Start time refers to the following day.
       Example: Monday 20:00-08:00 means from Monday 20:00 until Tuesday 08:00


F3=Exit    F8=Print    F12=Cancel     F13=Repeat time    F14=Clear time
```

Parameter or Option	Description
Time Group	Enter a meaningful name for the Time Group. This field is mandatory.
Description	Type a meaningful description of the time group
Start and End	For each relevant day of the week, enter Start and End Times in the format HH:MM, using the 24-hour clock. Midnight is 00:00. NOTE: An End time earlier than the Start time refers to the following day. For example, Monday 20:00-08:00 means from Monday 20:00 until Tuesday 08:00.
F13	Copy starting and ending times from cursor line to all subsequent days
F14	Erase the starting and ending times from the cursor line and below

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

Copy Time Groups

You can use this feature either to create a new time group that is very similar to an existing one, or to copy the settings of one time group to another time group. You should be careful using this command to copy to an existing time group, as the contents of the copied time group overwrite the contents of the receiving time group.

1. Select **32. Copy Time Groups** in the Main menu (*STRAUD* **> 32**). The **Copy Audit/Firewall Time Group** screen appears.

```
                    Copy Audit/Firewall Time Group (CPYAUTG)

Type choices, press Enter.

From time group  . . . . . . . .   __________    Name
To time group  . . . . . . . . .   __________    Name

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

2. Enter the **From time group** and the **To time group** and press Enter.

For more information, see Using Time Groups.

Working with Actions

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

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

To work with actions separately from rules,

1. Select **`61. Work With Actions`** in the Main menu (*STRAUD* **`> 61`**).
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 can send alert messages to designated personnel via one or more of the following methods:

- Email over the Internet
- Local workstation message queue using the ***SNDMSG MSG (MSGTEXT) TOMSGQ (MSGQNAME)*** command
- Local user message queue using the ***SNDMSG MSG (MSGTEXT) TOUSER (USERNAME)*** command
- Remote user on another IBM i system over the SNADS network using the ***SNDNETMSG*** command
- SMS service to a cellular telephone
- Syslog and SNMP

The message definition consists of predefined message text and one or more recipient addresses. You can opt to have the system send a default message or you can select a predefined message.

```
                              Modify Alert Message

Type choices, press Enter.

  Action Name  . . . .     VICT202448
  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=SIEM  9=SNMP             T=Twitter
  Message ID . . . . .     *AUTO          *AUTO, Message ID

 Type    Recipient address, *USER, *DEV, *JOB, *SYSTEM; SIEM 1/2/3
  1      ALEXM@RAZLEE.COM                                                    
  3      ALEX3                                                               
  8      1                                                                   
  _                                                                          
  _                                                                          
                                                                       More...


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

The following table lists the parameters and options for the Modify Alert Message screen.

Parameter or Option	Description
Action Name	
Description	Type a meaningful description of the action
Message ID	Predefined message text to be sent **`*AUTO`** = Use the default message text **`Msg ID`** = name of a predefined alert message F4 = Select a predefined message from the list or create a new message
Type	Recipient type ▪ **1** = E-mail ▪ **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 *(SNDNWSGMSG*) ▪ **6** = SMS message to a cellular telephone ▪ **7** = Message to beeper or pager ▪ **8** = Syslog ▪ **9** = SNMP
Recipient Address	Recipient address formatted according to the recipient type: ▪ **1** – E-mail Email address in standard email format (recipient@address) ▪ **2** – Message Queue Fully qualified name of the message queue or *SYSOPR ▪ **3** – User profile or IBM i group profile ▪ **4** – Network user profile and 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** – Special Phone number and access codes for the pager service

Predefined Messages

You have the option of using a predefined message instead of the product's default message text. Predefined messages are stored in a special message file and have a unique message ID.

Selecting a Predefined Message

1. Move the cursor to the **`Message ID`** field in the **`Alert Message`** screen, then press **F4**. The **`Select Message`** screen appears.
2. Type **1** next to the desired message ID, then press **Enter**.
3. Press **Enter** a second time to confirm and continue.
4.

```
                                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
 _    VV00001        5     The user was changed, please check.
 _    VV00002        1     Alest User was *DISABLED
 _    VV00003        0     Alest User was *ENABLED









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

Creating or Modifying a Predefined Message

4. Move the cursor to the **`Message ID`** field in the **`Alert Message`** screen and press F4. The **`Select Message`** screen appears.
5. Type **2** next to a predefined message to modify it, or press **F6** to create a new message. If you are modifying a message, you might have to select it a second time in the **`Work with Message Description`** screen.
6. The **`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 . . . . . . . > VV00001       Name
 Message file . . . . . . . . . . > AUALMSGF      Name
   Library  . . . . . . . . . . . >   SMZ4DTA     Name, *LIBL, *CURLIB
 First-level message text . . . . > 'The user was changed, please check.'
_________________________________________________________________________________
_______
 Second-level message text  . . .   *SAME
_________________________________________________________________________________
_________________________________________________________________________________
_________________________________________________________________________________
_________________________________________________________________________________
_________________________________________________________________________________
_________________________________________________________________________ ...
 Severity code  . . . . . . . . . > 05          0-99, *SAME


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

7. Type the parameters as listed in the following table. The table shows only the parameters relevant to this product; you should not modify any other parameters.

Parameters or Options	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 of up to 132 alphanumeric characters. One or more substitution variables can be embedded in the message text string to indicate positional replacement fields that allow the program to substitute variable data in 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 to be substituted (1 is the first field, 2 the second, and so on). 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.

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

Defining Command Scripts

When you have finished defining alert messages, the **Action Script** screen appears automatically. Use this screen to define one or more command scripts to run whenever the rule conditions are met.

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.

```
                              Edit Action Script

Action . . VICT202448   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 __________ RUNAUQRY QRY(SCC@) PRVMIN(5) OUTPUT(*HTML) MAILTO(VV)      -
                 ______________________________________________________________
                 On error, go to label . .  LVL001
 2.00 LVL001     CHGUSRPRF USRPRF(&CPUSPF) STATUS(*DISABLED)                 -
                 ______________________________________________________________
                 On error, go to label . .  LVL002
 3.00 LVL002     MONMSG CPF0000                                              -
                 ______________________________________________________________
                 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
F14=SYSLOG   F15=SNMP   F16=Twitter
```

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

Parameters or Options	Description
Order	The order to execute the commands
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 a 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 allow 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, you can retrieve and extract Job Name, Job User and Job Number information from the journal entry and insert it 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)

NOTE: 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:

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

```
                              Edit Action Script
        ..................................................................
Action  :                          Select Field                          :
        :  Entry .: C@ User profile changed (After & Previous images)    :
        :  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  :
        :   _  Date & Time   yyyy-mm-dd-hh.mm                   A   19  :
 2.00 _ :   _  Date yyyy-mm-dd                                   A   10  :  -
        :   _  Hour of day yyyy-mm-dd.hh                         A   13  :
        :   _  Time HH.MM.SS                                     A    8  :
 3.00 _ :   _  Name of job                                       A   10  :  -
        :   _  User of job                                       A   10  :
        :                                                         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
F14=SYSLOG  F15=SNMP  F16=Twitter
```

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:

1. Insert a label on a blank line following the last command.
2. Enter that label in the **`On Error Go To Label`** field on each active command line.

Testing and Debugging Rules

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

- Make sure that all the actions and events that you want 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. Use the **`Run Action`** feature (*STRAUD*> **`61 > 5`**) to perform the test.

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.

Creating and Running Queries and Reports

Audit includes powerful tools for creating and viewing queries, reports, and logs. Many of these tools are also available within other iSecurity products, giving a consistent experience in using them.

You can use several powerful and user-friendly tools to create output that contains only the data that you need to see, in a format that is useful to you.

The reporting features are:

- Display of log – showing the collected information of logs in either a message format which looks similar to a job log, or in a tabular view
- Query generator – a comprehensive report generator which has tremendous filtering capabilities and can create reports for one or more systems without copying the report definition
- Compliance Evaluator – score cards type reports to verify compliance with predefined targets
- Report Scheduler - enabling automatic run of groups of reports and logs
- Visualizer – BI (Business Intelligence) for activity logs. It uses a data warehouse with compressed information, making it possible to keep information for long periods. This is available in the GUI interface only.

Possible outputs for reports include display on the Green or GUI screen, HTML, PDF, CSV (Excel), and OUTFILE (Output file). When using the GUI, the results of a query can also be directed to the Visualizer to enabling using BI methods to deal with the results.

Once a report is defined on a system, it can be run on information on the current system, any other system, or any group of systems. There is no need to copy the definition to any other system.

Result files are named and stored in a proper order to ensure that they all run.

The output can be sent by email, either one report at a time, or as a group of reports together. Optional zip and password are available.

If the information that is sent contains one or more empty reports, this is denoted in the subject of the email. Customers can set the product to either eliminate or send empty reports. (Some auditors prefer to keep all reports,

even if they are empty, to ensure that the definition of the report did not change.)

The product collects information about each query that is run. This information includes the full command used to run the report, the time that it ran, how long it took to run it, and the name of the output that it produced.

An effective security policy relies on queries and reports to provide traceability for system activity. Audit queries and reports contain information from an extremely wide range of sources, (as shown in "Appendix A: Raz-Lee Information Sources" on page 384) including:

- Activity data collected from sources such as QHST, QAUDJRN (the system audit journal), QIPFILTER, QIPNAT, QACGJRN, QQOS, QSNMP, QDSNX, QVPN, and QZMF
- Activity data collected by iSecurity/Firewall from security related exit points
- Activity of the Antivirus and Anti-Ransomware modules of iSecurity
- Information from the system about Users, Groups, Native and IFS Objects, System values, PTFs, Authorization lists, and other categories
- Information that shows current activity status such as Active Jobs, NETSTAT, Disk, and System Status
- Summarized activity information which is kept in the internal Data Warehouse that is the base of the GUI Visualizer.
- Database changes, filtered, collected and reported by iSecurity/AP-Journal
- Activity about elevated authority, collected and reported by Authority-On-Demand
- Activities with objects in product libraries, collected and reported by Change-Tracker
- Activities of users on emulated screens collected and reported by Capture
- Activity of Password-Reset, MFA, and other products, also collected and reported.

To work with these features, select **41. Queries and Reports** from the **Audit Main Menu**. The **Queries** screen appears:

```
AUQRYMN                              Queries                    iSecurity/Audit
                                                              System:   S520
Select one of the following:

  Query Wizard                          Report Scheduler
   1. Work with Queries                 51. Work with Report Scheduler
                                        52. Run a Report Group

  Run a Query                           Baseline Setup
  11. Display                           61. System Values
  12. Print                             62. Network Attributes
  13. Submit as Batch Job               63. Counts in Compliance Query

  Log                                   Network reporting        SYSTEM()
  21. Display Log                       71. Network description
                                        75. Current Job CntAdm Messages
                                        76. All Jobs CntAdm Messages

Selection or command
===> ____________________________________________________________________________

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

To work with queries:

To create and modify queries,

select **1. Work with Queries**. The Work with Queries screen appears, as shown in "Creating and Running Queries" on page 169.

To run existing queries,

select the following items. For each the Run Audit Query (RUNAUQRY) screen appears, as shown in "Running Queries" on page 192, with the relevant ways of running the query selected:

- **11. Display**
- **12. Print**
- **13. Submit as Batch Job**

To work with logs:

To display Audit log entries,

select **21. Display Log**. The Display Firewall Log (DSPFWLOG) screen appears, as shown in Displaying Firewall Logs.

To work with reports

To schedule reports to run,

select **51. Work with Report Scheduler**. The Work with Report Scheduler screen appears, as shown in "Scheduling Reports" on page 195.

To run groups of reports,

select **52. Run a Report Group**. The Run Report Group (RUNRPTGRP) screen appears, as shown in "Running Report Groups On Demand" on page 212.

To view other network and system information ,

To ping and test DDM connections for network systems,

select **71. Network Description**. The standard Display Network Systems screen appears.

To view Central Administration messages for current jobs ,

select **75. Current Job CntAdm Messages**. The Display Messages screen appears, showing the job log for the current job.

To view Central Administration messages for all jobs ,

select **76. All Jobs CntAdm Messages**. The Display Messages screen appears, showing the job log for all jobs.

To exit the screen, press the F3 or F12 key.

Working with Individual Reports

The next step in the definition process is to define the individual reports that are contained in the report group.

1. To add a new report to a group, type **2** next to the group name, or type **2** next an individual report to modify it. The **`Report Definition`** screen appears. For information, see "Working with Report Groups" on page 1.
2. Define run time parameters for this report. The actual parameters available are specific to the report type.
   - For details regarding query parameters, see "Running Queries" on page 1.
   - For details regarding display log parameters, see "Viewing the logs" on page 1.
3. Press Enter to finish the definition and return to the **`Work with Report Scheduler`** screen.

NOTE: For all parameters that exist at both the group and individual report level (for example, the email address to receive the report), if no entry is made in the individual report, the group parameter is used. All parameters defined in the individual report override the group parameter.

Running Reports

The Report Scheduler submits all scheduled reports as batch jobs automatically on the day and time as specified in the definition. You can also run a report manually at any time.

To run a report manually:

1. Select **`52. Run a Report Group`**. from the **Queries**menu (*STRAUD* **`> 41 > 52`**). The **`Run Report Group`** screen appears.

Parameters	Description
Report Group	Enter the report group name
Job Description	Your batch job subsystem – normally **`QBATCH`**
Library	**`Name`** = Library name **`*Product`** = SMZ4 or the default product library **`*LIBL`** = Current library list **`*CURLIB`** = Current Library

Baseline Setup

There are queries that compare the current situation with a predefined baseline. You can set the Baseline to either the current "System Values" on the facing page or the "Network Attributes" on page 164.

System Values

To define the Baseline as being the system values:

1. Select **61. System Values**. from the Queries screen (*STRAUD* **> 41 > 61**). The **Set Audit Compliance Base-Line** screen appears.

```
                    Set Audit Compliance Base-Line (SETAUCBL)

Type choices, press Enter.

Set current as "Base line" . . . > *SYSVAL       *SYSVAL, *NETATR, *COUNTS
Compliance query . . . . . . . .   *SELECT       Name, *SELECT
Run number . . . . . . . . . . .   *LAST         Number, *LAST, *SELECT

                           Additional Parameters

Called from  . . . . . . . . . .   QRY            REPL, QRY

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

Parameters	Description
SYSVAL	Sets the current system value settings as the baseline.
NETATR	Sets the current values of network attributes as the baseline.

2. Press **Enter**. The Compliance Baseline is set.

Network Attributes

To define the Baseline as being the network attributes:

1. Select **62. Network Attributes**. from the **Queries** screen (*STRAUD*> **41 > 62**). The **Set Audit Compliance Base-Line** screen appears.

```
                    Set Audit Compliance Base-Line (SETAUCBL)

Type choices, press Enter.

Set current as "Base line" . . . > *NETATR       *SYSVAL, *NETATR, *COUNTS
Compliance query . . . . . . . .   *SELECT      Name, *SELECT
Run number . . . . . . . . . . .   *LAST        Number, *LAST, *SELECT

                           Additional Parameters

Called from  . . . . . . . . . .   QRY           REPL, QRY

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
Function key not allowed.
```

Parameters	Description
SYSVAL	Sets the current system value settings as the baseline.
NETATR	Sets the current values of network attributes as the baseline.

2. Press **Enter**. The Compliance Baseline is set.

Network Reporting

You can check the communication between your system and remote systems. You can also see the job messages for both the current job and for all jobs on the remote system.

Network Description

To check the communication between your system and remote systems:

1. Select **71. Network description** from the **Queries**screen (*STRAUD*> **41 > 71**). The **Display Network Systems** screen appears.

```
System type: AS400        Display Network Systems            System: S520
                                                  Position to . . . _
Type options, press Enter.
                                     8=Test DDM  9=Ping

Opt   System    Group
 _    RAZLEE1   *RL      RAZLEE1 machine
 _    RAZLEE2   *G1      RAZLEE2 machine
 _    RAZLEE3   *G1      RAZLEE3 machine
 _    S520      *NONE    S520 computer

                                                                  Bottom
F3=Exit                                        F12=Cancel
```

2. To test DDM communications with the remote system, type **8** in the **Opt** field for the selected system and press **Enter**.

   To ping the remote system, type **9** in the **Opt** field for the selected system and press **Enter**.

   Audit checks communications and displays a result message.

Current Job Central Administration Messages

To display messages for the current job, select **`75. Current Job CntAdm Messages`** from the Queriesmenu (*STRAUD*> **`41 > 75`**).

If there are any relevant message, the IBM supplied Display Messages screen appears and displays them.

If there are no relevant messages, the text "**`Message queue AUCOMLOG in QTEMP not found.`**" appears at the bottom of the screen.

All Jobs Central Administration Messages

To display messages for all jobs:

- Select **`76. All Job CntAdm Messages`** from the **Queries**menu (*STRAUD* **`> 41 > 76`**). The IBM supplied **Display Messages** screen appears.

Creating and Running Queries

The Query Wizard is a powerful tool that allows you to select exactly which events and actions you wish to examine and to specify the format of the printed or displayed output. You create query definitions using a series of parameter screens covering the various components.

To **open the Query Wizard** within Audit, select **`1. Work with Queries`** from the **Queries** menu (*STRAUD* **`> 41 > 1`**).

The **`Work with Queries`** screen appears.

```
                              Work with Queries
                                       Position to  . . . . _________
                                       Subset by type . . . __
                                         by text  . . . . . _______________
Type options, press Enter.               by classification. _  C=Compliance,..
  1=Select  3=Copy  4=Delete  5=Run  6=Print  7=Rename  8=Run as batch job
  9=Explanation  S=Schedule  X=Export  G=Group summary
Opt  Query     Type  Description                                       Class.
 _   AA_DBOPEN  00
 _   AAA        49
 _   AAAAANET   08   TELNET-Telnet Device Initialization
 _   AAAAFSRV   06   FILSRV-File Server
 _   AAFILSRV   06   FILSRV-File Server
 _   CPYCPSGN   32   TCPSGN-TCP Signon Server
 _   EVGENY1    01
 _   MZDBOPEN   00
 _   R6         06
 _   TEST       03
 _   TSTDB      45   Test llllll
 _   T50        50
                                                                      More...
F3=Exit   F4=Prompt   F6=Add New   F7=Un/Fold   F8=Print   F12=Cancel
```

The body of the screen lists existing queries. After the **`Opt`** field for entering options, it has the following fields:

`Query`

A unique name for the query

`Type`

The query information type. Press the **F4** key for a list of available query types.

`Description`

A free-form text description of the query

Class.

Letters or digits for classifications of queries. Predefined values include

- **C**: Compliance (SOX/ISO17799/PCI, etc)
- **U**: User
- **O**: Object
- **S**:System Values
- **N**: Network

You can freely define meanings for the digits **0** through **9**.

To **add** a new query, press the **F6** key. The **Add Query** screen appears, as shown in "Adding and Modifying Queries" on page 172.

To **view or modify further information** on a query, type **1** in the **Opt** field for the query and press **Enter**. The **Modify Query** screen appears, as shown in "Adding and Modifying Queries" on page 172.

To **view or modify the classification and explanation** of a query, type **9** in the **Opt** field for the query and press **Enter**. The **Query Explanation and Classification** screen appears. Enter classification characters (as shown for the **Class** field above) in the **Classification** list field. Enter a free-form explanation of the query in the **Query explanation** field, which is printed on output reports that include headers.

To **view or modify summaries** included in the query output, type **G** (for Group Summary) in the **Opt** field for the query and press **Enter**. The **Modify Query Summary Definitions** screen appears, as shown in "Modifying Query Summary Definitions" on page 188.

To **copy** information from one query to another, type **3** in the **Opt** field for the query and press **Enter**. The **Copy Query** window opens. The read-only **From** field shows the name and description of the original query. Enter the name and a free-form description for the new query in the **To** fields.

To **rename** a query, type **7** in the **Opt** field for the query and press **Enter**. The **Rename Query** window opens. The read-only **From** field shows the name and description of the original query. Enter the new name and description for the query in the **To** fields.

To **delete** a query, type **4** in the **Opt** field for the query and press **Enter**. The **Delete Query** window opens. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

To **run a query interactively**, type **5** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)Run Audit Query (RUNAUQRY)** screen appears (as shown in "Running Queries" on page 192) with the query name in its **Query** field and the Output field set to *****, which immediately sends the output to the screen.

To **run a query interactively and print the output**, type **5** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)Run Audit Query (RUNAUQRY)** screen appears (as shown in "Running Queries" on page 192) with the query name in its **Query** field and the Output field set to ***PRINT**, which immediately sends the output to the screen.

To **run a query as a batch job**, type **8** in the **Opt** field for the query and press **Enter**. The **Run Firewall Query (RUNFWQRY)Run Audit Query (RUNAUQRY)** screen appears (as shown in "Running Queries" on page 192) with the query name in its **Query** field and the Output field set to ***BATCH**, which immediately sends the output to the screen.

To **schedule** a query to run regularly as part of a report group, type **S** in the **Opt** field for the query and press **Enter**. The **Schedule Query** screen appears, as shown in "Scheduling Queries" on page 186.

To **export** a query definition, type **X** in the **Opt** field for the query and press **Enter**. A confirmation line stating that the definition has been exported appears at the bottom of the screen. After you have finished working with this screen and press **F3** to exit, the **Export iSecurity Query Definitions** screen appears. You can specify whether to export the definition to a particular system, a group of systems, or to all. If you set the field to ***NONE**, it is exported to a save file with a name indicated on the last line of that screen.

Adding and Modifying Queries

To **add** a new query, press the **F6** key from the **Work with Queries** screen (*STRAUD* **> 41 > 1**) as shown in "Creating and Running Queries" on page 169.

To **modify** an existing query, enter **1** in the **Opt** field for the query on the **Work with Queries** screen.

The **Add Query** or **Modify Query** screen appears. (The only differences between them are the screen title and that some fields for the **Modify Query** screen are read-only, as noted in their descriptions.)

```
                                Add Query           Last change date  0/00/00
                                                              by user
Type choices, press Enter.

Query name  . . . . .  __________
Description . . . . .  ________________________________________________

Type  . . . . . . . .  __

                      Not Name
Time group  . . . . .  _  __________ N=Not in time group

Output format . . . .  2             1=Tabular and wrap, 2=One line, 9=Log
If Output=1, Wrap on.   __0          Field number, 0=*AUTO

Add Header / Total  .  1             1=Both, 2=Header, 3=Total, 4=Total only,
                                     9=None
Add Filter / Desc.  .  1             1=Filter and description, 2=Filter,
                                     3=Description, 9=None
Action  . . . . . . .  *NONE_____    Name, *NONE, *ADD, F4=Prompt
Password  . . . . . .

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

```
                              Add Query          Last change date  0/00/00
                                                          by user
Type choices, press Enter.

Query name  . . . . .  __________
Description . . . . .  ______________________________________________

Type (00=All) . . . .  00  Generic entry type (00-99 for reporting only)

                      Not Name
Time group  . . . . .  _  __________ N=Not in time group

Output format . . . .  2             1=Tabular and wrap, 2=One line, 9=Log
If Output=1, Wrap on.   __0          Field number, 0=*AUTO

Add Header / Total  .  1             1=Both, 2=Header, 3=Total, 4=Total only,
                                     9=None
Add Filter / Desc.  .  1             1=Filter and description, 2=Filter,
                                     3=Description, 9=None

Password  . . . . . .

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

The screen contains the following fields:

Query name

A unique name for the query. Do not begin the name with the letter "**Z**", which is reserved for queries included with iSecurity products. (For **Modify Query**, this field is read-only.)

Description

A free-form description of the query.

Type (00-All)

A code indicating the type of the query. For a list of possible values, press the **F4** key. (For **Modify Query**, this field is read-only.)

The type **$9** is a special value, with which you can use the output from any command as input for the query. If you set this field to **$9**, the **Spool File Query Selection** screen appears after this screen, in which you can specify the command.

Time group

Restrict information to times within a named time group or, if the first one-character field is set to **N**, to times outside of it. For a list of valid time groups, press the **F4** key.

Output format

The format in which each line of output appears. Possible values are:

- **1**: Display in tabular format. If the data is longer than an output line, wrap on the field of the data indicated on the next field of this screen.
- **2**: Display in tabular format on a single line.
- **9**: Display in log format.

If Output=1, Wrap on

If the **Output format** field is set to **1**, the number of the data field on which to start a new line. If this field is set to **0**, wrap output to the next line at the start of any data field that would cause the output to exceed its maximum line length.

Add Header / Total

Whether the output should include field headers or a summary of totals. Possible values include:

- **1**: Include both the headers and summary.
- **2**: Include only the header.
- **3**: Include the summary.
- **4**: Omit the body of the report and include the summary.
- **9**: Include neither headers nor summary.

Add Filter / Desc.

Whether the output should include a listing of the query's filter conditions or a text description of them. Possible values include:

- **1**: Include both filter and description.
- **2**: Include only the header
- **3**: Description
- **4**: Include neither filter nor description.

Password

Add a password to this query to protect it from being changed. This is a hidden field, without an underline marking its location. It begins on the same line as its label, in the same column as the entry areas for the other fields.

After entering values for the fields, press **Enter**.

If you set the **`Type (00-All)`** field to **`$9`**, the **Spool File Query Selection** screen appears. Specify the command string, then press **Enter**.

The **Filter Conditions** screen appears, as shown in "Setting the Order of Rules" on page 182. Set the filter conditions for the query, then press **Enter**,

The **Select Output Fields** screen appears, as shown in "Selecting Output Fields for Queries and Reports" on page 177. Select the output fields and the order in which they appear on lines of output, then press **Enter**.

The **Select Sort Fields** screen appears, as shown in "Selecting Sort Fields for Queries and Reports" on page 179. Select the order in which the data records will be sorted in the output, then press **Enter**.

The **Exit Query Definition** screen appears:

```
                            Exit Query Definition

Query . . . . . TESTJZ     Test for Documentation
Type  . . . . . 00         Generic entry type (00-99 for reporting only)

Type choices, press Enter.

Summaries . . . . . .  N                Y=Yes, N=No
Explanation . . . . .  N                Y=Yes, N=No

Save  . . . . . . . .  Y                Y=Yes, N=No
Schedule  . . . . . .  N                Y=Yes, N=No

Run . . . . . . . . .  Y                Y=Yes, N=No









F3=Exit   F12=Cancel
```

The screen includes the following fields. For each, enter **`Y`** for "Yes" or **`N`** for "No".

`Summaries`

Whether the output include a summary of totals. If set to **`Y`**, the **Modify Query Summary Definitions** screen appears after you press

Enter, as shown in "Modifying Query Summary Definitions" on page 188.

Explanation

Whether the output should include text description in its header. If set to **Y**, the Query Explanation and Classification screen appears after you press Enter, as shown in "Creating Query Classifications and Explanations" on page 190.

Save

Whether to save the query definition.

Schedule

Whether to add the query to a group to run on a schedule. If set to **Y**, the Schedule Query screen appears after you press Enter, as shown in "Scheduling Queries" on page 186.

Run

Whether to run the query immediately. If set to **Y**, the Run Audit Query (RUNAUQRY)Run Firewall Query (RUNFWQRY) screen appears after you press Enter, as shown in .

To save your selections and exit the screen, press Enter. The additional screens related to your selections appear.

To exit the screen without saving your selections, press the F12 key.

Selecting Output Fields for Queries and Reports

The **Select Output Fields** screen specifies the fields to appear in a query and the order in which they appear in each record.

The screen appears in the process of adding or modifying queries, as shown in "Adding and Modifying Queries" on page 172.

```
                            Select Output Fields

Query  . . . . . TESTJZ     Test for Documentation
Entry  . . . . . 00         Generic entry type (00-99 for reporting only)
                                       Find (F16). ________________________


                                                                    Output
  Seq.   Description                                     Attribute   Length
   1.0   Date & Time   yyyy-mm-dd-hh.mm                      19 A      19
   2.0   Name of job                                         10 A      10
   3.0   User of job                                         10 A      10
         Number of job                                        6 A       6
         Current user profile                                10 A      10
         System name                                          8 A       8
         Object                                              10 A      10
         Object library                                      10 A      10
         Object type                                          7 A       7
         User                                                18 A      18
         *FYI mode (simulation)                               1 A       1
                                                                     More...
Pink fields are generic (all types)   Green fields apply to this type only
F3=Exit  F5=Display values  F12=Cancel  F16=Find   F21=Select all  F23=Invert
```

The read-only **Query** field shows the name and description of the query.

The read-only **Entry** field shows the code and description of the entry type that the query processes.

The body of the screen contains one line for each field defined for the entry type specified for the query (shown in green) as well as one for each of several generic fields that do not depend on the entry type (shown in pink).

Each contains the following fields:

Seq.

A number determining the order in which the fields appear. For example, fields with the **Seq** values **1.0, 1.1, 2.0, 4.0** would appear in that order, regardless of the order in which they appear in the displayed list.

Description

A read-only text description of the field, as defined for that entry type or generic field.

Attribute

A pair of read-only fields showing the length and type of the field, as defined for that entry type or generic field.

Output Length

The number of characters allocated for the field contents in the output.

To **find a field** in the list, enter a string from the field name in the **Find** field and press the **F16** (**Shift+F4**) key. The cursor moves from the current field to the next field with a name that includes that string. If there are no more field names containing the string in the rest of the list, it searches from the beginning.

To **select** all fields, press the **F21** (**Shift+F9**) key.

To **invert** the selection, selecting all fields that are not currently selected and deselecting those that are, press the **F23** (**Shift+F11**) key.

Selecting Sort Fields for Queries and Reports

The **Select Sort Fields** screen specifies the fields by which data is sorted in a query.

The screen appears in the process of adding or modifying queries, as shown in "Adding and Modifying Queries" on page 172.

```
                              Select Sort Fields

Query  . . . . . TESTJZ     Test for Documentation
Entry  . . . . . 00         Generic entry type (00-99 for reporting only)
Order A=Ascending D=Descending  A       Find (F16). ________________________
Break after change of  . . . .  _0      Number of sort fields, 0=No break
Records to include . . . . . .  1       1=All records, 2=One record per key
  Seq.   Description
   _1.0  Date & Time   yyyy-mm-dd-hh.mm
   _2.0  Name of job
   _3.0  User of job
   _____ Number of job
   _____ Current user profile
   _____ System name
   _____ Object
   _____ Object library
   _____ Object type
   _____ User
   _____ *FYI mode (simulation)
                                                                      More...
Pink fields are generic (all types)   Green fields apply to this type only
F3=Exit  F5=Display values  F12=Cancel  F16=Find   F21=Select all  F23=Invert
```

The read-only **Query** field shows the name and description of the query.

The read-only **Entry** field shows the code and description of the entry type that the query processes.

The following fields control the presentation of the records:

Order A=Ascending D=Descending

The order in which the sorted records appear in the output.

Break after change of

The number of changes in sort fields that trigger a break in the output. If set to **0**, there are no breaks.

Records to include

Whether to include only records on which values of sorted fields change. Possible values are:

- **1**: Include all records
- **2**: Include only the records on which values change.

The body of the screen contains one line for each field defined for the entry type specified for the query (shown in green) as well as one for each of several generic fields that do not depend on the entry type (shown in pink).

Each contains the following fields:

Seq.

A number determining the priority with which the records are sorted. For example, fields with the **Seq** values **1.0, 1.1, 2.0, 4.0** would have sort priorities in that order, regardless of the order in which they appear in the displayed list.

Description

A read-only text description of the field, as defined for that entry type or generic field.

To **find a field** in the list, enter a string from the field name in the **Find** field and press the **F16** (**Shift+F4**) key. The cursor moves from the current field to the next field with a name that includes that string. If there are no more field names containing the string in the rest of the list, it searches from the beginning.

To **select all** fields, press the **F21** (**Shift+F9**) key.

To **invert** the selection, selecting all fields that are not currently selected and deselecting those that are, press the **F23** (**Shift+F11**) key.

Setting Filter Conditions

Using the **Filter Conditions** screen, you can combine tests on any number of fields in a record to determine the system's response. Within Audit, for example, you can set tests on events in real-time to determine whether they would trigger events in Action.In Firewall, you can set tests on access requests to various servers to determine whether the system accepts or rejects the request.

Within Firewall, the screen appears when you add or modify a free-style rule for filtering access to servers (*STRFW* **> 15, F6** or **Opt 1**).

```
                              Filter Conditions
Entry  . . . . . . . .  45   *DBOPEN Open Database
Sequence . . . . . . .   2.0 *DBOPEN Open Database
                             Subset by text . . ______________________________
Type conditions, press Enter. Specify OR to start each new 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
     Object library                  EQ     DH
 _   Date & Time   yyyy-mm-dd-hh.mm  ______ ____________________________________
 _   Name of job                     ______ ____________________________________
 _   User of job                     ______ ____________________________________
 _   Number of job                   ______ ____________________________________
 _   Current user profile            ______ ____________________________________
 _   System name                     ______ ____________________________________
 _   Object                          ______ ____________________________________
 _   Object library                  ______ ____________________________________
 _   User                            ______ ____________________________________
 _   Open type                       ______ ____________________________________
                                                                          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
```

The read-only fields at the top of the screen show the entry type of the server, as both a numerical code and a text description, followed by the relative sequence number in which the filter runs and a text description of the filter (or, if that has not been set, a repetition of the server description).

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

And/Or

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

it.)

Field

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

Test

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

Value

The value against which the Field is tested.

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

Setting the Order of Rules

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

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

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

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

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

Test Comparison Operators

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

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

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

Combining Tests with the And/Or Field

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

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

```
                              Filter Conditions
Entry  . . . . . . . .  09   *TFTP TFTP Server Request Validation
Sequence . . . . . . .   1.0 Checking two users for TFTP
                             Subset by text . . ______________________________
Type conditions, press Enter. Specify OR to start each new 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
     IP address                      EQ     192.0.2.1
 A   User of job                     LIST   DAVID EDDIE MICHAEL ALEX
 O   IP address                      EQ     192.0.2.2
 A   User of job                     LIST   JOHN PAUL GEORGE RINGO
 _   Date & Time   yyyy-mm-dd-hh.mm _______ ______________________________
 _   Name of job                     _______ ______________________________
 _   User of job                     _______ ______________________________
 _   Number of job                   _______ ______________________________
 _   Current user profile            _______ ______________________________
 _   System name                     _______ ______________________________
 _   Object                          _______ ______________________________
                                                                     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
```

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

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

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

Scheduling Queries

With the **Schedule Query** screen, you can specify when a query is to run by adding it to schedule groups (as shown in "Defining Groups of Items" on page 208) or removing it from them.

To schedule a query, type **S** in the **Opt** field for that query on the **Work with Queries** screen (*STRAUD* **> 14 > 1**) as shown in "Creating and Running Queries" on page 169.

The screen also appears in the process of adding or modifying queries if the **Schedule Query** field on the **Exit Query Definition** screen is set to **Y** (as shown in "Adding and Modifying Queries" on page 172).

```
                                Schedule Query

Query . . . . . TESTJZ     Test for Documentation

Type options, press Enter.
  1=Add      4=Remove

Opt   Group    Description
 _    A        TEXT FOR A
 _    DAILY    Daily
 _    DAILYGU  Daily, for GUI output (EXCEL like, preformatted)
 _    DAILYML  Daily, in HTML, sent by Email
 _    GUI      TEXT FOR GUI
 _  > QQ       Test
 _    RR       TEXT FOR RR
 _    TELNET   Check of Z6TELNET Quiery
 _    TSTDAY   Daily
 _  > TSTGRP   Test group
                                                                    More...


F3=Exit   F12=Cancel
```

The read-only **Query** field shows the name and text description of the query being scheduled.

The body of the screen contains a line for each of the existing schedule groups. In each, the **Group** field shows the name of the group and the **Description** field shows a text description.

If a group contains the query being scheduled, its **Group** field is preceded by an open-arrow (the "**>**" character).

To **add** the query to a schedule group, type **`1`** in the **`Opt`** field for that group and press **Enter**.

To **remove** the query from a schedule group, type **`4`** in the **`Opt`** field for that group and press **Enter**.

Modifying Query Summary Definitions

With the **Modify Query Summary Definition** screen, you can group together data records to create and modify summaries that appear in query output.

To **create summary groups** for a query, type **G** in the **Opt** field for that query on the **Work with Queries** screen (*STRAUD* **> 41 > 1**) as shown in "Creating and Running Queries" on page 169.

The screen also appears in the process of adding or modifying queries if the **Summaries** field on the **Exit Query Definition** screen is set to **Y** (as shown in "Adding and Modifying Queries" on page 172).

```
                      Modify Query Summary Definitions       User Defined

Query . TESTJZ      Test for Documentation

                               Summary Report 1

Title  . . . . . . . . .  Count of Objects Allowed/Rejected by Library
Group by . . . . . . . .  00OBJ       Object
                          00LIB       Object library
                          00RTCD      Allow (1=Yes)
Sum field or *COUNT  . .  *COUNT
Report if sum is . . . .  _           >=Greater than, <=Less then
  Than . . . . . . . . .   0          Number
  Specified in units of.  _           K=Kilo, M=Mega, G=Giga
Sort by the sum  . . . .  _           A=Asc, D=Dsc
Code to add description.   22         F4 to select based on the Group By fields




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

The screen includes fields for creating up to three summaries. These appear on successive pages, which you can reach by pressing the **Page Down** key.

The fields for each are:

Query

A read-only field showing the name and text description of the query.

Title

A free-form text title for the summary.

Group by

How to group items in the output.

A group of three subfields set the fields by which items in the report are grouped. You can set this via the **Code to add description** field or by pressing the F4 key in each field to select the fields from a list.

Sum field or *COUNT

The field from the record for which the sum of values since the last summary is shown, or ***COUNT** to show the number of records.

Report if the sum is

Whether the summary appears if the sum is greater than the value in the **Than** field or when it is less. Possible values are:

- **>** : Greater than
- **<** : Less than

Than

The value to which the sum is compared.

Specified in units of

Units to which the values are rounded and displayed:

- **K**: Kilo
- **M**: Mega
- **G**: Giga

Sort by the sum

Possible values are:

- **A**: Ascending
- **D**: Descending

Code to add description

A code specifying groups of items to place in the three subfields of the **Group by** field. Press the F4 key to see a list of the field sets.

Creating Query Classifications and Explanations

With the **Query Classification and Explanation** screen, you can create and modify classifications for your query as well as text explanations of the query that can be printed in the header of the output.

To **create classifications and an explanation for a query**, enter **9** in the **`Opt`** field for that query on the **Work with Queries** screen (*STRAUD* **`> 14 > 1`**) as shown in "Creating and Running Queries" on page 169.

The screen also appears in the process of adding or modifying queries if the **`Explanation`** field on the **Exit Query Definition** screen is set to **`Y`** (as shown in "Adding and Modifying Queries" on page 172).

```
                      Query Explanation and Classification

Query:  TESTJZ     Test for Documentation

Type choices, press Enter.
Classification list  . . .  ______          C=Compliance (SOX/ISO17799/PCI...),
(e.g. CU=Compliance+User)                   U=User, O=Object, S=System values,
                                            N=Network, 1-9=User defined
Query explanation: (Printed if Header is requested)
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________

F12=Cancel
```

The body of the screen includes the following fields:

`Classification list`

Letters or digits for classifications of queries. These codes appear in the line for the query on the **Work with Queries** screen (*STRAUD* **`> 14 > 1`**) as shown in "Creating and Running Queries" on page 169.

Predefined values include

- **C**: Compliance (SOX/ISO17799/PCI, etc)
- **U**: User
- **O**: Object
- **S**:System Values
- **N**: Network

You can freely define meanings for the digits **0** through **9**.

Query explanation

A free-form text explanation of the query. The text is printed in the header of the output if the **Add Header / Total** field is set to **1** or **2** on the Add Query or Modify Query screen as shown in "Adding and Modifying Queries" on page 172.

Running Queries

You can run queries from several points within Audit.

To run queries for **display**, for **print**, or as **batch** jobs, select **`11. Display`**, **`12. Print`**, or **`13. Submit as Batch Job`** respectively from the **Queries** menu (*STRAUD***`41`**)

You can also **run queries** by entering **`5`** in the **`Opt`** field for the query in the **Work with Queries** screen (*STRAUD* **`> 41 > 1`**) as shown in "Creating and Running Queries" on page 169.

The **Run Audit Query (RUNAUQRY)** screen appears:

```
                         Run Audit Query (RUNAUQRY)

Type choices, press Enter.

Query  . . . . . . . . . . . . . . > Z$J_CMD       Name, *SELECT
Display last minutes . . . . . .   *BYTIME       Number, *BYTIME
Starting date and time:
  Starting date  . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . . . .   000000       Time
Ending date and time:
  Ending date  . . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . . .   235959       Time
User profile . . . . . . . . . .   *ALL         Name, generic*, *ALL
Run action on each row . . . . .   *NO          Name, *YES, *NO
Run action after end of run  . .   *NO          Name, *NO
System to run for  . . . . . . .   *CURRENT     Name, *CURRENT, *group, *ALL..
Number of records to process . .   *NOMAX       Number, *NOMAX
Output . . . . . . . . . . . . . > *            *, *PRINT, *PDF, *HTML..


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

The screen includes the following fields. Depending on how and from where within Audityou are running the query, some fields may already be filled in with read-only values.

`Query`

The name of the query to run. If you have not yet created the query, you can do so from the **Add Query** screen, as shown in "Adding and Modifying Queries" on page 172.

To choose the query after this screen, set this field to the value ***SELECT**.

Display last minutes

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

Starting data and time

Starting date

The day or date on which the included data begins.

Allowed values include:

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

Starting time

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

Ending date

The day or date on which the included data ends.

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

Ending time

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

User* or '%GROUP'

The name of a user, or the generic* name or %GROUP name of a group of users, whose data the query examines.

Run action after end of run

If the Query Type of the query is **$8**, the name of an action for the Action product to run after the query. For no action, enter ***NO**.

System to run for

Queries can run on information for this system or for others. Possible values include:

- ***CURRENT**: The current system.
- ***ALL**: All systems.
- **Name**: The name of a different system.
- ***group**: A named group of systems.

Number of records to process

The maximum number of records to process. To include all records, enter ***NOMAX**.

Output

The destinations for output. Possible values include:

- ***:** The default output. If running interactively, this is the current screen.
- ***PDF**: Print report to PDF outfile.
- ***HTML**: Print report to HTML outfile.
- ***CSV**: Print report to CSV outfile.
- ***OUTFILE**: Print report as text to an outfile.
- ***PRINT**: Print to default printer.
- ***PRINT[1-9]**: Print to another destination, as defined via the Printer Files Setup screen (*STRAUD* **> 89 > 58**).

If you choose a destination that goes to an outfile, additional fields appear for further information.

Scheduling Reports

With the **Report Scheduler**, you can run predefined report groups automatically, according to a fixed schedule.

Each **report group** contains one or more queries, reports, or history log inquiries that are executed together at a designated time. This is more efficient than running each report on its own, since you only need to define scheduling details and other run-time parameters once for the whole group.

To **create and run report groups** within Firewall, select **`51. Work with Report Scheduler`** from the **Reporting** menu (*STRFW* **`> 41`**), as shown in Creating and Running Firewall Queries and Reports.

The **Work with Report Scheduler** screen appears:

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

Opt Group    Seq  Description                                        Query
 _  A             TEXT FOR A
 _             1  Run FireWall Query                                 A
 _             2                                                     TEST
 _             3  TCPSGN-TCP Signon Server                           CPYCPSGN
 _             4                                                     AA_DBOPEN
 _             5  Run FireWall Query                                 DSPFWLOG
 _  ABTEST        Test for Documentation
 _             2  Run FireWall Query                                 RUNFWQRY
 _             3  Run FireWall Query                                 DSPFWLOG
 _  ADOC2         Documentation run weekly on Tuesday
 _             1  Run FireWall Query AA_DBOPEN                       AA_DBOPEN
 _  ADOC3         Monthly run for Documentation
 _  DAILY         Daily
                                                                       More...
F3=Exit    F5=Refresh    F6=Add New Group   F8=Print     F12=Cancel
```

The body of the screen contains a list of report groups and the reports within them.

The groups are listed in alphabetical order. For each, the **`Group`** field contains the group name, and the **`Description`** field contains a free-form text description.

The reports within the group are listed after the group name. Three fields are shown for each report:

Seq

The order in which the reports run within the group. This corresponds to the order in which they were added.

Description

A free-form text description of the report.

Query

The query that the report runs, as defined in "Adding and Modifying Queries" on page 172.

To **add a new report group**, press the **F6** key. The **Add Report Group** screen appears, as shown in "Adding or Modifying Report Groups" on the facing page.

To **add a report to a report group**, type **2** in the **Opt** field for either the group or another report within it and press **Enter**. The **Add Report Definition** screen appears, as shown in "Adding Reports to Report Groups" on page 202.

To **modify a report group**, type **1** in the **Opt** field for the group or a report within it and press **Enter**. The **Modify Report Groups** screen appears, as shown in "Adding or Modifying Report Groups" on the facing page.

To **copy a report group**, type **3** in the **Opt** field for the group or a report within it and press **Enter**. The **Copy Report Groups** screen appears. The read-only **From Report group** field shows the name and description of the original group. Enter the name of the new group in the **To Report group** field.

To **delete a report group**, type **4** in the **Opt** field for the report group and press **Enter**. The **Delete Report Group** window opens. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

To **delete a report from a group**, type **4** in the **Opt** field for the report and press **Enter**. The **Delete Report Group** window opens. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

To **run a report group on demand**, type **5** in the **Opt** field for the report group and press **Enter**. The **Run Report Group (RUNRPTGRP)** screen appears, as shown in "Running Report Groups On Demand" on page 212.

Adding or Modifying Report Groups

To **add a report group** to the Report Scheduler, press the **F6** key in the **Work with Report Scheduler** screen (*STRAUD* **> 41 > 51**) as shown in "Scheduling Reports" on page 195.

To **modify an existing report group**, enter **1** in the **Opt** field for the report group or a report in it in the **Work with Report Scheduler** screen.

The **Add Report Group** or **Modify Report Group** screen appears. They differ only in their title and an additional read-only field on the **Modify Report Group** screen:

```
                                Add Report Group

Report groups are intended to run pre-defined sets of reports automatically
on a periodic basis.
If ZIP(*YES) is specified, all PDF, HTML, CSV will be sent together.
Other individual reports parameters, if defined, override group parameters.
The use of descriptive date values *YESTERDAY, *WEEKSTR... is recommended.

Type choices, press Enter.
  Report Group name . . .  _______       Name  e.g. DAILY, WEEKLY, MONTHLY etc.
  Description . . . . . .  ______________________________________________________




Press Enter to continue to the Define Parameters screen.

F3=Exit                                F12=Cancel
```

The screen includes the following fields:

Report Group name

The name of the group. It may have up to seven alphanumeric characters, beginning with a letter.

Description

A free-form text description of the report group.

Group parameters

On the **Modify Report Group** screen, a read-only field showing the parameters that have already been entered for the group.

After entering this information, press **Enter** twice to confirm it.

The **Define FW Report Group Details (DFNFWGRPD)Define AU Report Group Details (DFNAUGRPD)** screen appears:

```
                    Define FW Report Group Details (DFNFWGRPD)

 Type choices, press Enter.

 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
 System to run for  . . . . . . .   *CURRENT     Name, *CURRENT, *group, *ALL..
 Output . . . . . . . . . . . . .   *PDF         *, *PRINT, *PDF, *HTML..









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

```
                    Define AU Report Group Details (DFNAUGRPD)

Type choices, press Enter.

Starting date and time:
  Starting date  . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Starting time  . . . . . . . .   000000       Time
Ending date and time:
  Ending date  . . . . . . . . .   *CURRENT     Date, *CURRENT, *YESTERDAY...
  Ending time  . . . . . . . . .   235959       Time
User profile . . . . . . . . . .   *ALL         Name, generic*, *ALL
System to run for  . . . . . . .   *CURRENT     Name, *CURRENT, *group, *ALL..
Output . . . . . . . . . . . . .   *PDF         *, *PRINT, *PDF, *HTML..





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

The screen contains the following fields:

Starting data and time

Starting date

The day or date on which the included data begins.

Allowed values include:

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

- ***SAT**: Saturday
- ***SUN**: Sunday

Starting time

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

Ending date

The day or date on which the included data ends.

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

Ending time

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

User profile

The user or set of users about whom the report group is run. This can be a name, a generic* name, or ***ALL**.

System to run for

Queries can run on information for this system or for others. Possible values include:

- ***CURRENT**: The current system.
- ***ALL**: All systems.
- **Name**: The name of a different system.
- ***group**: A named group of systems.

Output

The destinations for output. Possible values include:

- *****: The default output. If running interactively, this is the current screen.
- ***PDF**: Print report to PDF outfile.
- ***HTML**: Print report to HTML outfile.
- ***CSV**: Print report to CSV outfile.
- ***OUTFILE**: Print report as text to an outfile.
- ***PRINT**: Print to default printer.
- ***PRINT[1-9]**: Print to another destination, as defined via the Printer Files Setup screen (*STRAUD* **> 89 > 58**).

If you choose a destination that goes to an outfile, additional fields appear for further information.

After entering this information, press **Enter**.

The **Add Job Schedule Entry (ADDJOBSCDE)** screen appears, as shown in IBM documentation at https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/cl/addjobscde.htm:

```
                      Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . . . . . . . . > GS@ADOC2      Name, *JOBD
Frequency  . . . . . . . . . . . > *WEEKLY       *ONCE, *WEEKLY, *MONTHLY
Schedule date  . . . . . . . . . > *NONE         Date, *CURRENT, *MONTHSTR...
Schedule day . . . . . . . . . . > *ALL          *NONE, *ALL, *MON, *TUE...
               + for more values   _____
Schedule time  . . . . . . . . . > 230000        Time, *CURRENT

                           Additional Parameters

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




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

After entering values, press **Enter** to return to the **Work with Report Scheduler** screen.

Adding Reports to Report Groups

To **add a report to a report group**, enter **2** in the **Opt**field for either the group or another report within it on the **Work with Report Scheduler** screen (*STRAUD* **> 41 > 51**) as shown in "Scheduling Reports" on page 195. The **Add Report Definition** screen appears:

```
                            Add Report Definition

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

 Group ABTEST     Test for Documentation

 Type choices, press Enter.

 Report Id.  . . . . . .     4
 Description . . . . . .  Run FireWall Query
 Reporting command (F7).  RUNFWQRY       Command, F7 or *SELECT to select
                          Run FireWall Query
 Report parameters (F4)..

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

The screen contains the following fields:

Group

A read-only field showing the name and text description of the report group, as set on the **Define FW Report Group Details (DFNFWGRPD)Define AU Report Group Details (DFNAUGRPD)** screen, as seen in "Adding or Modifying Report Groups" on page 197.

Report ID

A read-only field showing the numeric report identifier.

Description

A free-form text description of the report, as relevant to the report group.

Reporting command

The command that runs the report. By default, this is RUNFWQRYRUNAUQRY. To select other commands, press the **F7** key.

Report parameters

A read-only field showing the parameters for the Reporting command. To set or change these, press the **F4** key. The **Run Firewall Query (RUNFWQRY)** screen appears, as shown in "Running Queries" on page 192.

Defining Time Groups

Many of the Audit rules and reporting features take advantage of the unique **Time Group** feature. With time groups, users can apply predefined sets of time-based filters to different queries without having to define complex criteria for each query. Time groups also work with the **Report Scheduler** and the **Display Activity Log** features.

For example, you may be using different queries and reports to audit the activities of one group employees during normal working hours and a different group of employees during nights and weekends. This can be accomplished with just one time group using the following guidelines:

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

One common use of time groups is as filter criteria in security rules, queries and reports. For example, time groups can be used to restrict the application of a rule to specific times and days of the week.

Time group filters can be either:

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

Generally, an exclusive time group filter is indicated by placing an **N** (NOT) in the field immediately preceding the time group name field on the rule definition or query definition screen.

For example, you can use an exclusive time group filter to apply a rule to any time occurring outside of days and hours specified in the time group.

To **create and modify time groups,** select **`31. Time Groups`** from the **Reporting**screen, as shown in Creating and Running Firewall Queries and Reports.

The **Define Time Groups** screen appears:

```
                              Define Time Groups

Type options, press Enter.
  1=Select  3=Copy  4=Delete

Opt Time Group    Description
 _  ALEXANDRA     TEXT FOR ALEXANDRA
 _  ALON          Special group
 _  ALONPP        Special group
 _  ALON88        Special group
 _  CONF1         TEXT FOR CONF1
 _  FRANCEWH      SITE  GROUP
 _  NEW           TEXT FOR NEW
 _  VB123         Special group
 _  WORKHOURS     Regular work hours
 _  WORKHOURS1    Regular work hours + 1
 _  WORKHOURS2    Regular work hours + 2
 _  WORKHOURS3    Regular work hours + 3


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

Each line in the body of the screen refers to a single time group. After the standard **`Opt`** field, it shows a unique name for the **`Time Group`** and a free-form text **`Description`**.

To **create** a new time group, press the **F6** key. The **Add Time Group** screen appears:

```
                                Add Time Group

Time Group . . . __________
Description  . . ______________________________

Type choices,  press Enter

          From  To      From  To
Monday     0:00  0:00    0:00  0:00
Tuesday    0:00  0:00    0:00  0:00
Wednesday  0:00  0:00    0:00  0:00
Thursday   0:00  0:00    0:00  0:00
Friday     0:00  0:00    0:00  0:00
Saturday   0:00  0:00    0:00  0:00
Sunday     0:00  0:00    0:00  0:00


 Note: If To is less than From it will be considered in the following day .
       Example: Monday 20:00 - 08:00 means Monday 20:00 till Tuesday 08:00.


F3=Exit     F12=Cancel     F13=Repeat time     F14=Clear time
```

Enter a unique name for the time group in the **`Time Group`** field and a free-form description in the **`Description`** field.

The body of the screen has named lines for each day of the week.

Each line has two pairs of fields, with one named **`From`** and the other named **`To`**. Each pair specifies a time period during the day. For example, if workers had a shift from 8 AM to 5 PM, with a lunch break from noon to 1 PM, the line for each weekday would show times from **`8:00`** to **`12:00`** and from **`13:00`** to **`17:00`**.

If the value of the **`To`** field is less than that of the **`From`** field, it signifies that the shift continues into the next calendar day. For example, an overnight shift **`From23:00To7:00`** would run from 11 PM on that day through 7 AM on the next.

To **repeat** the entered times from the line containing the cursor to those for all other days, press the **F13 (Shift+F1)** key.

To **clear** the times from all the lines except for the one containing the cursor, press the **F14 (Shift+F2)** key.

Further Operations from the Define Time Groups Screen

To **modify** the times for an existing time group, enter **1** in the **Opt** field for that group. The **Change Time Group** screen appears, with the same set of fields as the **Add Time Group** screen.

To **copy** the settings from one time group to another, enter **3** in the **Opt** field for that group. The **Copy / Replace Time-Group** screen appears. The Time Group for the existing group appears in read-only **From:** fields. Enter the name of the new group in the **To: Time Group** field. If the group already exists, its settings are overwritten.

To **delete** a time group, enter **4** in the **Opt** field for that group. The **Delete Time Group** screen appears. Press **Enter** to confirm the deletion or the **F12** key to cancel it.

Defining Groups of Items

You can define groups of reports that you can schedule to run together. You can also define classes of groups, so that you can schedule all the groups of reports in the class to run together.

You can also use classes of other types of groups within queries to limit the items on which the query would run. For example, you could create a class **OVERNIGHT** of all Time Groups that work overnight shifts. You could then define a query that only select those users by including a filter with the comparison **ITEM OVERNIGHT** (as shown in "Setting the Order of Rules" on page 182).

You could also create a class **HQIP** of all IP address groups at an organization's headquarters, then create a query that would exclude them by creating a filter with the comparison **NITEM HQIP**.

To create and modify report groups, select **51. Work with Report Scheduler** from the Reporting menu (*STRAUD* **> 41**). The Work with Report Scheduler screen appears, as shown in "Scheduling Reports" on page 195.

To add reports to a group, enter **2** in the **Opt** field for either the group or another report within it in the Work with Report Scheduler screen (*STRAUD* **> 41 > 51**). The Add Report Definition screen appears, as shown in "Adding Reports to Report Groups" on page 202.

To create and modify classes and add groups to them, select **35. Group Items for Selection** from the Reporting menu (*STRAUD* **> 41**).

The Work with Classes of Groups window appears.

```
 GSRPTMNU                          Reporting                          Firewall
.............................................................................
:                          Work with Classes of Groups                      :
:                                                                           :
:  Type options, press Enter.             Position to . . . __________      :
:    1=Work with   2=Edit   4=Remove      Subset  . . . . . ________________ :
:                                                                           :
:  Opt Class      Description                                   Item Length :
:      *GRPPRF    User is included in Group/Supplemental profile      10    :
:      *LMTCPB    User Limit Capabilities                             10    :
:      *SPCAUT    User has a Special Authority                        10    :
:      *TIMEGRP   Time group                                          10    :
:      *USRGRP    User is included in iSecurity/Firewall Group        10    :
:   _  AUD        List for Audit Reporting                            10    :
:   _  AUDJ       Secondary list for audits                           10    :
:   _  COMMANDS   Initial commands to run as a group                  20    :
:   _  COMMANDS2  Secondary commands group                            20    :
:                                                                    More... :
:  *CLASSes are automatically defined by the system. Press F6 for instructions :
:  F3=Exit    F6=Add New (plus instructions)    F8=Print    F12=Cancel      :
:                                                                           :
:............................................................................:
 F13=Information Assistant  F16=AS/400 main menu
```

Each line on the body of the screen refers to a single class. For each class, it shows the these fields:

Class

A unique name for the class.

Description

A free-form text description of the class.

Item Length

The maximum length of item names in the class, from 0 through 20.

The predefined classes at the start of the list, with names that begin with an asterisk (*****), cannot be altered. The lines for the other classes begin with the standard **Opt** field.

To **add a new class**, press the **F6** key. The **Add Class** window appears:

```
 GSRPTMNU                          Reporting                          Firewall
.............................................................................
:                                 Add Class                                 :
:                                                                           :
:  Type choices, press Enter.                                               :
:                                                                           :
:  Class . . . . . . . .  __________      e.g. USERS, IP, COMMANDS, FILES...  :
:                                                                           :
:  Text  . . . . . . . .  ______________________________________________   :
:                                                                           :
:  Maximum item length .  __              1 - 20                            :
:                                                                           :
:  Group-Classes (such as USERS, IPS, FILES) consist of individual Groups.  :
:  For example, Group-Class USERs could consist of groups HR, ERP, etc. These :
:  groups are useful when you want to limit a report or a rule to only the  :
:  USERS listed in USERS/HR who accessed files listed in FILES/SENSITIVE.   :
:  To use, enter ITEM or NITEM ("item of" or "not item of") in the TEST     :
:  column of the report's Filter Conditions; then press F4 in VALUE column. :
:  F3=Exit                 F12=Cancel                                      :
:                                                                           :
:...........................................................................:
 ...........................................................................:
 F13=Information Assistant  F16=AS/400 main menu
```

The window has the same fields as the **Work with Classes of Groups** window. Fill in the values for the new class, then press **Enter**.

The **Work with Groups of** window appears. To add groups, press the **F6** key.

The **Add Group** window appears. Enter the name of the first group and a free-form text description, then press **Enter**.

The **Work with Group Items** window appears. For each item in the group, enter the item name and a free-form text description. After entering items, press **Enter**.The **Work with Groups of** window reappears.

To **modify the list of items within the group**, enter **1** in the **Opt** field for the group.

To **edit the description of a group**, enter **2** in the **Opt** field for the group.

To **remove an item from the group**, enter **4** in the **Opt** field for the group.

More Operations from the Work with Classes of Groups screen

To **modify the list of groups within the class**, enter **1** in the **Opt** field for the class.

To **edit the description or item length of a class**, enter **2** in the **Opt** field for the class.

To **remove a group from the class**, enter **4** in the **Opt** field for the class.

Running Report Groups On Demand

To **run report groups on demand**, select **`52. Run a Report Group`** from the Queries **Reporting** menu (*STRAUD* **`> 41`**), as shown in Creating and Running Firewall Queries and Reports.

To **run a report group on demand** from within the Report Scheduler (as shown in "Scheduling Reports" on page 195), type **`5`** in the **`Opt`** field for the report group and press **Enter**.

```
                         Run Report Group (RUNRPTGRP)

 Type choices, press Enter.

 Product  . . . . . . . . . . . . > FIREWALL      FIREWALL, SCREEN, PASSWORD...
 Report group . . . . . . . . . . > ABTEST        Name
 Job description  . . . . . . . . > QBATCH        Name, *NONE
   Library  . . . . . . . . . . . >   *PRODUCT    Name, *PRODUCT, *LIBL...

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

If you have selected the screen from within the **Reporting** menu, enter the name of the report group (as set within the Report Scheduler) in the **`Report group`** field.

If you have selected the screen from within the Report Scheduler, the name of the product that you are running and the name of the report group appear as read-only values in the **`Product`** and **`Report group`** fields.

The **`Job description`** field contains the name of the program to run. To run the report group interactively, enter **`*NONE`**.

The **`Library`** field contains the name of the library containing the program. This can be a library name or **`*PRODUCT`**, **`*LIBL`**, or **`*CURLIB`**.

iSecurity Multi System Support

As more and more sites worldwide implement multiple IBM i systems, it has become imperative that audit and compliance reports be able to report simultaneously on all local and remote systems simply and efficiently, and that the output be presented so that each IBM system is clearly indicated.

Raz-Lee Security has implemented support for multiple systems which provides maximum flexibility and capabilities for all IBM i shops.

iSecurity's implementation of multiple system support can be performed in one of the following two manners:

Remote Execution

In Remote Execution mode, Audit reports, whether user or scheduler initiated, indicate the remote (yet connected) systems on which the report is to execute. Upon submission, the report is executed in sequence on each of the remote systems with the data for each execution collected at the initiating system.

When all remote executions have completed, the report is executed at the initiating system. At this point, if the appropriate option has been selected, all output files are merged into one output file. Again, depending on the execution option specified, the composite report can be printed on the local system or on any of the remote systems, and can also b sent as an HTML, PDF, or CSV email attachment to one or more email addresses.

Local Execution

In Local Execution mode, the appropriate remote files (such as **SMZ4DTA** for Audit) must first be copied, using whatever facilities are available, to the local system. Accessing the appropriate product menu, the user then selects which remote file should be used as the basis for all subsequent queries submitted on the local system. This selection will remain in effect until changed, and all queries executed on the local system will continue to reference the copied remote data files.

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 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.

Audit includes many ready-to-use log display sets. Just enter a few parameters on a simple data screen and the specified data appears in seconds. You can also choose to print a hard copy of the history log results.

The "Backward Glance" 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 transactions occurring that period of time quickly appear. Backward Glance really comes in handy when assisting users with those nasty error messages that pop up or verifying that a batch job has successfully completed.

If one Audit Type is selected, the output can be directed into a Field Oriented File.

To **direct output to a Field Oriented File**, enter

> ***DSPAULOG AUDTYP(*BYENTTYP) OUTPUT(*OUTFILE) ENTTYP(xx) OUTFILFMT(*BYTYPE) OUTFILE(QTEMP/OUTNAME)***
>
> where ***AUDTYP(*BYENTTYP)*** and ***OUTFILFMT(*BYTYPE)*** are constants,
>
> and ***xx*** must be replaced by a valid Audit Type

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

To **view the logs**:

1. Select **`42. Display Log`** in the Main menu (*STRAUD* **`> 42`**). The **`Log Menu`** appears.

```
AULOGMN                              Log Menu                    iSecurity/Audit
                                                               System:  S520
Select one of the following:

Display Log                                Display Action Log
   1. All                                    61. All
   2. By Entry Type

Display Log by Subject
  11. Authorization Failure                  20. Program Failures
  12. Commands                               21. Printing Functions
  13. Create Object                          22. Restore Operations
  14. Delete Object                          23. Security Tasks
  15. Job Tasks                              24. Service Tasks
  16. Object Management Tasks                25. Spool File Operations
  17. Optical Device Operations              26. System Management Tasks
  18. Network Communications                 27. Office Services
  19. Authority Adoption                     28. Change Object
Selection or command
===> ____________________________________________________________________________

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

2. Choose one of the many predefined log display options.
   - **All** – Display all entries in the history log. This option is useful when examining all activities over a period of time, perhaps in conjunction with the Backward Glance feature.
   - **By Entry Type** – Display history log entries for one or more audit types
   - **By Subject** – Display history log entries according to one of the predefined subjects listed on the menu.
3. Enter run-time filter and other parameters by selecting **1. All** or **2. By Entry Type**. The Display Audit Log Entries screen appears. For screen parameters and explanations, see Running Queries.

```
                         Display Log (Audit) (DSPSYSLOG)

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
Output . . . . . . . . . . . . .   *            *, *PRINT, *PRINT1-*PRINT9









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

4. Press **Enter** to display the history log.
5. Press **Enter** to continue.

   You can press **F18** at any time during the data retrieval process to display a pop-up status window. This window continuously displays the number of records processed and selected. Press **Esc** at any time to halt retrieval and immediately display the query or log.

User Management

This chapter presents several powerful security tools that control the ability of users to sign on to the system. These tools enhance active system security by allowing 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 sign-on to specific hours and days
- Prevent user sign-on during planned absences or following termination
- Analyze default passwords for effectiveness

These options are accessed directly from Audit by selecting **`62. User Management`** in the Main menu (*STRAUD* **>** **62**). The User Management menu appears.

Working with Users

Overview

The **Work with Users** Wizard allows 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 sign-on tools.

Using the Work with Users Wizard

1. Select **`1. Work with Users (WRKACUSR)`** from the **User Management** menu (*STRAUD* **`> 62 > 1`**). The **Action Work with Users (WRKACUSR)** screen appears.

```
                        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
```

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 sign on ***NO** = Display disabled users and those who cannot sign on ***ALL** = Display users irrespective of status
User has password	***YES** = Display only users whose password has not expired ***NO** = Display only users whose password has 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 sign-on
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 sign-on
Allow Planning of enablement	***YES** = Enable user ***NO** = Disable user
Allow New Password to *SECADM	***YES** = New password allowed for SECADM user ***NO** = No new password allowed for SECADM user

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 sign on to the system are displayed in pink.

Screen 1: Work with User Status - Basic

The first screen shows whether individual users can sign on to the IBM i system. To sign on, 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
                         Users displayed in pink are not eligible to sign on.
Opt User      Disabled Password
 _  #RONI       No      Yes
 _  #VV         No      Yes  Victor # weak user
 _  #VVV        No      Yes  Victor # weak user
 _  #01         No      None *NONE
 _  A           No      None *NONE
 _  AAA         No      None *NONE
 _  AAACCC      No      None *NONE
 _  AABBCC      No      None *NONE
 _  ABCDE       No      None *NONE
 _  ACUM        No      Yes  for bosanova
 _  AGROUP      No      None *NONE
 _  ALERTSH     No      Yes  DetectIT Self Help Administrator
 _  ALEX        No      Yes  Alex - Supporteam strong user
 _  ALEX2       No      Yes  Security Officer
                                                                    More...
F3=Exit    F7=Subset    F8=Print    F11=Additional parameters    F12=Cancel
F14=Absence Security    F15=Auto-disable exceptions    F16=Signon times
```

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 sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors 7 = Set password to 'expired' – this user must change password at next sign-on
Enabled	Blank = User profile is enabled No = User profile is disabled
Password	Blank = User profile has a valid password and can sign on None = No password is associated with this user profile and he cannot sign on
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 sign-on 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 . . . . . . . . . . . :   #RONI

Disabled . . . . . . . . . :   No
Password . . . . . . . . . :   Yes

Previous signon  . . . . :    0/00/00
Days passed  . . . . . . :
Planned action . . . . . :   None      0/00/00

Invalid attempts . . . . :
Expiration interval  . . :
Expiration date  . . . . :
Days in use  . . . . . . :      190
Days left  . . . . . . . :



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

Work with User Status - Details

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

Screen 2: Work with User Status - Signon

This screen displays recent sign-on statistics for each user profile. In addition, the scheduled date of any automatic actions (disable or delete) by the Action absence control feature appears.

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

Opt User           Previous signon    Days passed   Planned action
 _  HAYEST         22/11/11  17:29       2799       None      0/00/00
 _  HUSER           0/00/00                         None      0/00/00
 _  IBM             9/02/03  16:28       6007       None      0/00/00
 _  IBOLT           9/08/07   6:10       4365       None      0/00/00
 _  ILAN           26/02/15  15:02       1607       None      0/00/00
 _  ILANR          24/03/19  13:55        120       None      0/00/00
 _  ILAN2           0/00/00                         None      0/00/00
 _  IMPERVA        30/12/12  13:48       2395       None      0/00/00
 _  ISEC           13/11/16  16:17        981       None      0/00/00
 _  ISECAGENT       2/10/18  19:21        293       None      0/00/00
 _  ISRAEL          0/00/00                         None      0/00/00
 _  ITZIK           9/08/07  10:48       4365       None      0/00/00
 _  I304001F11      1/01/19  12:53        202       None      0/00/00
 _  JAVA           20/06/19  10:29         32       None      0/00/00
                                                                   More...
F3=Exit    F7=Subset    F8=Print    F11=Additional parameters    F12=Cancel
F14=Absence Security    F15=Auto-disable exceptions    F16=Signon times
```

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

Screen 3: Work with User Status - Password

This screen displays the number of invalid sign-on 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.

```
 *SUBSET*                Work with User Status - Password            iSecurity
                                                   Position to . .  __________
Type options, press Enter.
 1=Select   3=Enable    4=Disable   6=Reset count   7=Expire
                   Invalid      Expiration   Expiration       Days      Days
Opt User           Attempts      Interval       Date          In use     Left
 _  EVG2912B                                                   1127
 _  EVG2912X                                                   1127
 _  EXODUS
 _  EYAL                        *NOMAX                         1070
 _  FERNANDO                                                   2756
 _  FILESCOPE
 _  FORGOT                      *NOMAX                         1723
 _  FORGOTAUA                   *NOMAX                         1145
 _  FORGOTDEU                   *NOMAX                         1728
 _  FORGOTENG                   *NOMAX                         1728
 _  FORGOTHEB                   *NOMAX                         1728
 _  FORGOTS                     *NOMAX                           46
 _  FORGOTV                      *NOMAX                          307
 _  FORGOTYYY                    *NOMAX                          764
                                                                        More...
F3=Exit    F7=Subset    F8=Print    F11=Additional parameters    F12=Cancel
F14=Absence Security    F15=Auto-disable exceptions    F16=Signon times
```

Work 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 sign-on attempt counter – prevents automatic disabling of this user due to excessive sign-on errors **7** = Set password to 'expired' – this user must change password at next sign-on
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

Disabling Inactive Users

Profiles that have been inactive for a long time need to be disabled.

[[[Undefined variable Audit.ProductName]]] User Management provides this functionality. It is composed of two elements:

- Work with Auto-Disable - by which you can activate the function and provide the number of days to consider
- Disable Exceptions – By which you can provide a list of user which will not be checked and will not be set to disable by this function

[[[Undefined variable Audit.ProductName]]]provides two methods of handling this subject.

- The standard method wraps IBM OS400 functionality and provides. The OS400 activity is based on the commands ***ANZPRFACT***, ***CHGACTPRFL***, and ***DSPACTPRFL***.
- An extended method is also provided. This extends the ability to specify user profiles that will always be considered active, and will be excluded from this process by generic* names.

To switch between the two methods:

1. Select **`Work with Auto-Disable`** and switch off the current used method.
2. Use ***STRAUD*** **`> 89 > 59. Global Installation Defaults`** and change the "**`Standard auto disable . . Y`**" field to**`Y=Yes`** – for the IBM OS400 method; **`E=Extended`** – for the extended method.
3. Copy the **`Disable Exceptions`** list to the new method with the required changes.
4. Select again **`Work with Auto-Disable`** and switch on the activated method.

You can schedule report ZCP_INADIS to see a log of auto-disable activity.

Work with Auto-Disable

To define when to disable inactive users:

1. Select **`11. Work with Auto-Disable`** from the User Management screen (*STRAUD* **`> 62 > 11`**). The **Auto-Disable Inactive Users** screen appears.

```
Extended                Auto-Disable Inactive Users     With generic* support

Type choices, press Enter.

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

  Days of inactivity . . . . . . .  366           1-366, 0-*NOMAX


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
```

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**.

Disable Exceptions

To define the exceptions for inactive user disabling:

1. Select **`12. Exceptions`** from the User Management screen (*STRAUD*> **`62 > 12`**). The **Auto-Disable Exceptions** screen appears.

```
                          Auto-Disable Exceptions

Specify user names or generic* that should NEVER be disabled automatically.
                                                Position:     __________
Type options, press Enter.
  4=Delete
Opt User        Description
 _  AB*
 _  AVRAHAM     Avrohom Notik
 _  IXY*
    QANZAGENT
    QAUTPROF    IBM-supplied User Profile
    QCLUMGT     IBM-supplied User Profile
    QCLUSTER    IBM-supplied User Profile
    QCOLSRV     IBM-supplied User Profile
    QDBSHR      Internal Data Base User Profile
    QDBSHRDO    Internal Data Base User Profile
    QDFTOWN     Default Owner for System Objects
    QDIRSRV     OS/400 Directory Services Server User Profile
                                                                      More...
Users defined in the Auto-Disable exception list, are considered excluded.
F3=Exit    F6=Add new    F12=Cancel
```

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

Deleting/Reviving 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. The Auto-Delete runs as part of the daily standard maintenance job *AU#MAINT*.

For both successful and unsuccessful delete attempts, a message is sent to QSYSOPR. If the attempt was unsuccessful, the reason is included in the message. In addition, a report is sent to *PRINT9. See "Setting up the *PRINT1-*PRINT9 Printers and *PDF Output" on page 356 for details of how to define *PRINT9. You can also run report ZDO_INADLT to see a log of auto-delete activity.

To work with this option, your operating system must be at version 6.1 or later.

NOTE: For a user profile to be deleted:

- It must be *DISABLED
- Their Last Used Date must be old enough
- Their Creation Date must be old enough
- They cannot be a Group Profile
- They may not appear in Disable Exceptions
- They may not appear in Delete Exceptions (includes generic* names)

Deleting Unused Disabled Users

Users who have been in the `*DISABLED` state for a long period of time may be deleted according to their Last used date, Create date, and Sign-on date. User Profiles which are Group Profiles will never be deleted.

Exceptions may be added to generic* names list and excluded from delete even if `*DISABLED`.

NOTE: Users in the disable exceptions list cannot be deleted.

NOTE: During Auto-Deletion, some messages are sent to QSYSOPR.

To define when to delete disabled, inactive users:

1. Select **`21. Delete Unused Disabled Users`** from the **User Management** screen (*STRAUD* **`> 62 > 21`**). 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 . . .     999       1-999, 0=*NOMAX
Note that this number has no relevance to the date the user was disabled.

Delete pending distributions  . . .    *YES       *YES, *NO
Pending distributions must be deletd before a DLTUSRPRF runs.

Parameters of DLTUSRPRF (Press F4).



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

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**.

Auto-Delete Reports Available

Some reports accompany the Auto-Delete function:

- ZDO_INADLT DO Users that were DELETED due to inactivity. This is a standard report
- Z$@_INADLT $@ Log of Auto-Delete activity. This includes info both on users that could be deleted and those who for some reason could not be deleted. This is a textual report that includes 2 types of messages:

- `Auto-Delete: User XXXX could not be deleted: MsgId + MsgText of the reason.`
- `Auto-Delete: User XXXX inactive since YYYY-MM-DD deleted.`

During Auto-Deletion, these messages are also sent to QSYSOPR.

Deleting Exceptions

To delete exceptions:

1. Select **`22. Delete Exceptions`** from the **User Management** menu (*STRAUD* **`> 62 > 22`**). The **Auto-Delete Exceptions** screen appears.

```
                          Auto-Delete Exceptions

Specify user names or generic* that should NEVER be deleted automatically.
                                                   Position:    __________
Type options, press Enter.
  4=Delete
Opt User*       Description
    *EXC_DISAB  All the users in Auto-Disable Exception list

                                                                      Bottom
Users in pink are excluded by OS/400, and cannot be deleted from this list.
F3=Exit    F6=Add new    F12=Cancel
```

2. Enter **4** next to the User to be deleted, then press Enter. The Auto-Delete Exceptions are deleted.

Reviving Deleted Users

To restore a deleted user:

1. Select **`26. Revive Deleted Users`** from the **User Management** menu (*STRAUD* **`> 62 > 26`**). The **Revive Deleted Users** screen appears.

```
                              Revive Deleted Users

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

Opt User       Description                                        Delete date
 _  ALEX5      Alex - Supporteam strong user                      2019-07-21
 _  AODTMP001  Temp. user of job 559777/LOWUSR/QPADEV000W         2019-07-21
 _  DB2        DB-Gate                                            2019-07-23

                                                                        Bottom
F3=Exit   F5=Refresh
```

2. Enter **1** next to the User to be restored. The **Create User Profile**screen appears.
3. Press **Enter**. The user is restored.

Authorizing Sign-on 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 sign on 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 a subsequent audit.

An effective defense against this scenario would be to restrict user sign-on to authorized working hours. [[[Undefined variable Audit.ProductName]]] includes a user-friendly tool for defining authorized sign-on periods for users, by time and day of the week.

Working with Sign-on Schedule

To define the permitted sign-on times for users:

1. Select **`31. Work with Schedule`** from the **User Management** menu (*STRAUD* **`> 62 > 31`**). The **Work with Signon Schedule** screen appears.

```
Sorted by Group           Work with Signon Schedule

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

                Group
Opt  User       Profile    Enable   Disable  Days
 _   #RONI                  08:00    19:00   *ALL
 _   #VV                    08:00    19:00   *ALL
 _   #VVV                   08:00    19:00   *ALL
 _   ALEX                   08:00    19:00   *ALL
 _   ALEX2                  08:00    19:00   *ALL
 _   AMIR                   08:00    19:00   *ALL
 _   AZ                     08:00    19:00   *ALL
 _   AVRAHAM    JR          08:00    19:00   *ALL



                                                                    Bottom

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

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

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 sign-on 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 sign-on 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 Sign-on Schedule

To display the signon schedule:

1. Select **`32. Display Schedule`** from the **User Management** menu (*STRAUD* **`> 62 > 32`**). The **Display Activation Schedule (DSPACTSCD)** screen appears.

```
                    Display Activation Schedule (DSPACTSCD)

Type choices, press Enter.

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

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

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 (such as vacation, sick leave, maternity leave, or business trips) or leaves the organization. You can make certain that nobody can sign on with specific user profiles during such scheduled absences by disabling or deleting user profiles automatically on a specific date.

Working with Absence Schedule

Predefine absences of personnel to ensure secure access or delete personnel who no longer belong to the organization.

To define absences:

1. Select **`41. Work with Schedule`** from the **User Management** menu (*STRAUD* **`> 62 > 41`**). 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
 _  ALEX       31/12/19 Alex - Supporteam strong user

                                                                      Bottom

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

2. Press **F6=Add New**. The **Add User Absence Schedule** screen 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
```

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).

Parameters	Description
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. ***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`** in the **User Management** menu (*STRAUD* **`> 62 > 42`**). 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
```

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 allows you to analyze password usage.

Analyzing 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 allows 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 (*STRAUD* **`> 62 > 61`**). The **Analyze Action Dft Passwords (ANZAUDFTP)** 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
```

2. Select
    - ***DISABLE** to disable accounts with default passwords,
    - ***PWDEXP** to expire default passwords, or
    - ***NONE** to list the accounts with default passwords but take no action.
3. Press **Enter**. The report is produced. If the selected option was ***NONE**, a line at the bottom of the screen reports the number of accounts found with default passwords and the number of those that are enabled.

Printing User Profile Information

The following options from the **User Management** Menu (***STRAUD*** > 62):

```
62. Print Password Info
63. Print Special Authorities
64. Print Programs and Queues
```

use the OS/400 Print User Profile (***PRTUSRPRF***) command. They are placed here for convenience and to enable authorized users of iSecurity to use them even if their authority is insufficient for the IBM command. In addition, the print is enhanced to support output to *PRINT1 through *PRINT9, in addition to the standard *PRINT.

Replication

The recent trend of consolidating servers has led to the increasing prevalence of multi-system and multi-LPAR shops. Companies have found it mandatory that system administrators and users alike synchronize user profile definitions, user passwords and system values between the different systems, allowing for exceptions as needed in Production, Test or Development systems. Such synchronization should be accomplished with minimum overhead to both the actual systems and the personnel mandated with managing user profile information.

Because of the growing demand for data synchronization, Raz-Lee created User and System Value Replication, allowing the user to replicate security settings such as user profile definitions, user passwords and system values across multiple servers or LPARs, allowing for the exceptions needed in Production, Test or Development systems.

Replication includes the following features:

- Flexible user-defined replication rules defining user profiles, passwords and parameters to be replicated
- Definition of destination systems for replication
- Bulk updates of user profiles
- Setting of System Values to optimal value or site-defined baseline values
- Replication of all, group or individual system values
- Collection and display of network-wide replication results
- Revival of deleted users, with an option to modify parameters
- Can be initiated from any IBM in the environment and does not require special commands

Activation

1. Select **`71. Enable User/Password Replication`** from the **Replication** menu (*STRAUD* **`> 69 > 25 > 71`**). The Call Program screen appears.

```
                              Call Program (CALL)

 Type choices, press Enter.

 Program  . . . . . . . . . . . . > AURPUEP      Name
   Library  . . . . . . . . . . . >   SMZ4        Name, *LIBL, *CURLIB
 Parameters . . . . . . . . . . . > *ADD
_____
                + for more values
_____

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

2. Press **Enter**. This option adds an exit program to the system registration facility.

Network Definitions

To work with Replication, you must define destination systems.

1. Select **`71. Work with Network Definitions`** from the **Base Support** menu (*STRAUD* **`> 89`**). The **Work with Network Systems** screen appears.

```
System type: AS400        Work with Network Systems           System: RLDEV
                                                Position to . . . __________
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Test DDM  9=Ping

Opt   System    Group
 _    RLDEMO    *TT      Demo system Audit release 14.16
 _    RLDEV     *NONE    Razlee Develop
 _    RLG       *TT      RL Germany
 _    RLMED     *TT      RLEMD
 _    RLPRV     *TT      Razlee Production
 _    RL74A     *VVVV    Demo system
 _    RL74B     *NONE    Test Yoel
 _    VERDE     *NONE    verde





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

2. Press **F6** to add a new system to the list or type `1` to modify an existing

system. The **Modify Network System** screen appears.

```
System type: AS400          Modify Network System            System: S520

System  . . . . . . . . . .  RAZLEE1
Description . . . . . . . .  RAZLEE1 machine
Group where included  . . .  *RL                  *Name

Communication Details
IP or remote name . . . . .  251.236.56.124

                             ___________________________
Type  . . . . . . . . . . .  *IP                   *SNA, *IP
Entry of *LOCAL on System .  C205307W              Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed .  *SYSTEM               Name, *SYSTEM
Extension Id on remote  . .  D__


Note: After adding a system, run again "Network Authentication".

F3=Exit   F12=Cancel
```

Parameters	Description
System	The name of the system you are defining.
Description	Enter a meaningful description.
Group where included	You can create groups of system. The group name must begin with an asterisk (*).
Default extension	
Type	***SNA** or ***IP**
IP or remote name	If type = ***SNA**, enter the name of the remote system. If Type = ***IP**, enter the IP address of the remote system.

3. Type the appropriate parameters and press **Enter**.

NOTE: When you define both source and target systems, you must define each system on both the systems. Both systems must have the same version of Base Support installed.

System Values

You can replicate the System Values from this system to another system, you can set the current system values and network attributes as a baseline, and you can set a baseline to be the current system values.

Set System Values as a Baseline

1. Select **`39. Set Current SysVal as Baseline`** in the **Replication** menu (*STRAUD* **`> 69 > 26 > 39`**). The **Set Audit Compliance Base-Line** screen appears.

```
                    Set Audit Compliance Base-Line (SETAUCBL)

Type choices, press Enter.

Set current as "Base line" . . . > *SYSVAL       *SYSVAL, *NETATR, *COUNTS

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

2. Type either **`*SYSVAL`** or **`*NETATR`** and press Enter.

Set Baseline Values to be System Values

1. Select **35. Change System Value to Baseline** in the **Replication** menu (*STRAUD* > **69** > **25** > **35**). The **Change (Audit) System value** screen appears.

```
                    Change (Audit) System value (CHGAUSV)

Type choices, press Enter.

System value . . . . . . . . . .   __________     Name, *ALL, *ALC, *DATTIM...
To value . . . . . . . . . . . . > *BASELINE      *BASELINE, *OPTIMAL, *VALUE
System to run for  . . . . . . . > *CURRENT       Name, *CURRENT, *group, *ALL..

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

Parameters	Description
System value	***ALL** = All system values ***ALC** = Allocation ***DATTIM** = Date and time ***EDT** = Editing ***LIBL** = Library list ***MSG** = Message and Logging ***SEC** = Security ***STG** = Storage ***SYSCTL** = System control
Confirm group change	***YES**, ***NO**

2. Type the appropriate parameters and press **Enter**.

Replicate System Values to Another System

1. Select **`31. System Value Replication`** in the **Replication** menu (**`STRAUD > 69 > 25 > 31`**). The **Change (Audit) System value** screen appears.

```
                    Change (Audit) System value (CHGAUSV)

Type choices, press Enter.

System value . . . . . . . . . .   __________    Name, *ALL, *ALC, *DATTIM...
To value . . . . . . . . . . . .   *OPTIMAL      *BASELINE, *OPTIMAL, *VALUE
System to run for  . . . . . . .   *CURRENT      Name, *CURRENT, *group, *ALL..

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

Parameters	Description
System value	***ALL** = All system values ***ALC** = Allocation ***DATTIM** = Date and time ***EDT** = Editing ***LIBL** = Library list ***MSG** = Message and Logging ***SEC** = Security ***STG** = Storage ***SYSCTL** = System control
To value	***BASELINE** = the current system as defined in option 39. Set System Values Baseline. ***OPTIMAL** = defined in the Compliance Evaluator ***VALUE**
System to run for	Replicate system values to a specific system name, the current system or a group of systems
Confirm group change	***YES**,***NO**

2. Type the appropriate parameters and press **Enter**.

Test RDB Connection

Before you use Replication over IP, you should run a simple test to check the RDB connection existence (Full SQL access from an RPG program to remote databases from all IBM i high- level languages). This check is a pre-condition for Replication based over IP.

In the following example, there are two computers, a Local computer, and a Target computer whose IP address is 10.20.30.40

1. Type the following command on the Local computer:
   ADDRDBDIRE RDB(TTT) RMTLOCNAME('10.20.30.40' *IP)
2. Type the following command on the Target computer:
   CRTDTAQ DTAQ(QGPL/DTAQTTT) MAXLEN(32000)
3. Type the following commands on the Local computer:
   ADDSVRAUTE USRPRF(*CURRENT) SERVER(TTT) USRID(QSECOFR) PASSWORD(xxxxx)
   CRTDTAQ DTAQ(QGPL/DTAQLLL) TYPE(*DDM) RMTDTAQ (QGPL/DTAQTTT) RMTLOCNAME(*RDB) RDB(TTT)
   call qsnddtaq (DTAQLLL QGPL x'00010F' 'aaaaaaaaaaaaaaaaaaaa')

   If this stage fails, the following message will appear (and may also be found in the sent JOBLOG):

   CPF9155 Cannot communicate with DDM target system.

   CPF9510 Operation on DDM data queue DTAQAAA in QGPL failed.
4. When this step succeeds, the contents of DTAQ can be read on the Target computer:
   QSH CMD('dataq -r /QSYS.LIB/QGPL.LIB/DTAQTTT.DTAQ')

User/Password

Replication duplicates user profiles and their parameters in their latest and most updated version. Replication does not copy the actual password but an encrypted version of the password.

Replication Rules

Before you can replicate anything, you must define the rules of what to replicate.

1. Select **`51. Work with Replication Rules`** in the **Replication** menu (*STRAUD* **`> 69 > 25 > 51`**). The **Work with Replication Rules** screen appears.

```
                          Work with Replication Rules

Type options, press Enter.                Position to . . . _________
  1=Select   4=Remove    5=Display        Subset  . . . . . _______________
                --Systems--        --Replicate--
Opt  User*      From     To        CRT  CHG  DLT
 _   *ALL       *ALL     *ALL       Y    Y    Y
 _   AB*        RAZLEE2  *ALL       Y    Y    Y

                                                                      Bottom
 If CRT, CHG and DLT are blanks, no replication occurs.

 F3=Exit    F6=Add New                        F8=Print    F12=Cancel
```

2. Press **F6** to add a new rule or type `1` to modify an existing rule. The **Modify Replication Rules 1/2** screen appears.

```
Screen 1/2                Modify Replication Rules

Type choices, press Enter.

User . . . . . . . . . . . .  AB*                Name, generic*, *ALL
System combination
From system  . . . . . . .  RAZLEE2            System, *ALL
Replicate to system  . . .  *ALL               System, *group, *ALL
Replicate (set all to blanks for "no replication")
Create user  . . . . . . .  Y                  Y=Yes, A=Yes/Change if exists
Change user  . . . . . .  .  Y                 Y=Yes, A=Yes/Create if missing
Delete user  . . . . . . .  Y                  Y=Yes
If Change, replicate also                      (See more on next screen)
  User disabled  . . . . .  Y                  Y=Yes
  User enabled . . . . . .  Y                  Y=Yes
  Password changes . . . .  Y                  Y=Yes

At run time, the best fit (most specific) rule for user names, regardless of
systems, is selected. Rules with this user notation are then processed.
Entries which FROM SYSTEM correspond or is *ALL, are scanned and a
single replication request is sent for each TO SYSTEM.

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

Parameters	Description
User	Enter the name of the User Profile to replicate. **Name** = Enter the name of a specific profile to replicate **Generic*** = Use a generic name to copy a group of profiles ***ALL** = Replicate all profiles
System combination	From system = Type the source system name or select ***ALL** systems Replicate to system= Type the target system name, a group of systems or select *ALL systems
Operations to Replicate	Define how to replicate common operations. Set to blanks for no replication. Create user: **Y** = Yes – On the target computer, create all users that meet the rule definition and exist on the source computer, and do not exist on the target computer. **A**= Yes / Change if the User profile already exists On the target computer, create all users that meet the rule definition and exist on the source computer, and do not exist on the target computer. Users that meet the rule definition on the source computer and already exist on the target computer are changed on the target computer to be identical to the user on the source computer. Change user: **Y** = Yes – All users that meet the rule definition on the source computer and also exist on the target computer are changed on the target computer to be identical to the user on the source computer. **A**= Yes / Create if the User profile does not exist All users that meet the rule definition and also exist on the target computer are changed to be identical to the user on the source computer. Users that only exist on the source computer are created on the target computer. Delete user:

Parameters	Description
	Y = Yes – All users that meet the rule definition are deleted from the source computer. If they also exist on the target computer, they are deleted also from the target computer.
Common attributes to replicate	Select what common attributes to replicate. Set to blanks for no replication. User disabled: **Y** = Yes User enabled: **Y** = Yes Password changes: **Y** = Yes

3. Type the appropriate parameters and press **Enter**. The **Modify Replication Rules 2/2** screen appears.

```
Screen 2/2                  Modify Replication Rules

Type choices, press Enter.
Description  . .  ____________________________________________________
                  ____________________________________________________
                  ____________________________________________________
Parameters or Parameters with partial value to omit e.g. INLPGM or INLPGM(A/B
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________

F3=Exit                F12=Cancel
```

4. Type a description and enter exception parameters that are not to be replicated and press **Enter**.

Replicate Users

Use this feature to replicate one or more user profiles to another system.

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

```
System type: AS400        Work with Network Systems           System: S520
                                                Position to . . . _________
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Check DDM  9=Verify communication

Opt   System    Group
 _    RAZLEE1   *RL      RAZLEE1 machine
 _    RAZLEE2   *G1      RAZLEE2 machine
 _    RAZLEE3   *G1      RAZLEE3 machine

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

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

```
System type: AS400            Add Network System              System: S520

System  . . . . . . . . . .  __________
Description . . . . . . . .  ______________________________________________
Group where included  . . .  *NONE___                 *Name

Communication Details
IP or remote name . . . . .  ______________________________________________
                             ______________________________________________
                             ______________________________
Type  . . . . . . . . . . .  *IP                      *SNA, *IP
Entry of *LOCAL on System .  ___________________       Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed .  *SYSTEM                   Name, *SYSTEM
Extension Id on remote  . .  ___



Note: After adding a system, run again "Network Authentication".

F3=Exit   F12=Cancel
Modify data, or press Enter to confirm.
```

3. Select **72. Network Authentication** in the **BASE Support** screen (*STRAUD* **> 89 > 72**). 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 of 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
```

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

5. Select **5. Auto start activities in ZAUDIT** in the **iSecurity/Base System Configuration** menu (*STRAUD* **> 81 > 5**). The **Auto Start Activities in ZAUDIT Subsystem** screen appears.

```
                    Auto Start Activities in ZAUDIT Subsystem  22/07/19 17:30:46

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) . . . . . . . . . .  Y          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
```

Parameter	Description
Real-Time Auditing (All systems)	**Y** = Yes **N** = No If you set the Change Tracker parameters Enable Change Tracker and Enable Real Time Tracking to **Y**, then even if this parameter is set to **N**, activating the ZAUDIT subsystem activates the Audit job. You access the Change Tracker parameters in the Activation Mode option in the System Configuration menu in Change Tracker (*STRCT* **> 81 > 1**).
Status & Active jobs	**Y** = Yes **N** = No
Firewall & Screen (Action)	**Y** = Yes **A** = Always **N** = No Selecting A=Always will perform Action activities even if Firewall is running in *FYI. Action must be running in real mode (not in FYI).
Message Queues (set to start at *IPL)	**Y** = Yes **N** = No If this parameter is set to Y, then when adding new Message Queues, you can set them to start automatically at *IPL time. For more details, see "Create Message Queue Audit Rules" on page 127.
Replication of User, Pwd, SysVal	**Y** = Yes **N** = No

6. Enter the required parameters and press **Enter**.
7. In the Source system only, run **71. Enable User/Password Replication** in the **Replication** menu (*STRAUD* **> 69 > 25 > 71**). The **Call Program (CALL)** screen appears.

```
                              Call Program (CALL)

 Type choices, press Enter.

 Program  . . . . . . . . . . . . > AURPUEP      Name
   Library  . . . . . . . . . . . >   SMZ4        Name, *LIBL, *CURLIB
 Parameters . . . . . . . . . . . > *ADD
_______
                + for more values
_______

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

8. Display active jobs in the Target Machine.
9. Select **51. Work with Replication Rules** from the **Replication** menu (*STRAUD* **> 69 > 25 > 51**).

```
                         Work with Replication Rules

Type options, press Enter.                Position to . . . __________
  1=Select   4=Remove    5=Display        Subset  . . . . . ______________
                --Systems--        --Replicate--
Opt  User*      From     To        CRT  CHG  DLT
 _   *ALL       *ALL     *ALL       Y    Y    Y
 _   AB*        RAZLEE2  *ALL       Y    Y    Y

                                                                      Bottom
 If CRT, CHG and DLT are blanks, no replication occurs.

 F3=Exit    F6=Add New                        F8=Print    F12=Cancel
```

10. Press **F6** to add a new rule or type 1 to modify an existing rule. The **Modify Replication Rules 1/2** screen appears.

```
Screen 1/2                Modify Replication Rules

Type choices, press Enter.

User . . . . . . . . . . . .  *ALL              Name, generic*, *ALL
System combination
From system  . . . . . . . .  *ALL              System, *ALL
Replicate to system  . . .  *ALL              System, *group, *ALL
Replicate (set all to blanks for "no replication")
Create user  . . . . . . . .  Y                 Y=Yes, A=Yes/Change if exists
Change user  . . . . . .  .   Y                 Y=Yes, A=Yes/Create if missing
Delete user  . . . . . . . .  Y                 Y=Yes
If Change, replicate also                       (See more on next screen)
  User disabled  . . . . . .  Y                 Y=Yes
  User enabled . . . . . . .  Y                 Y=Yes
  Password changes . . . .  Y                   Y=Yes

At run time, the best fit (most specific) rule for user names, regardless of
systems, is selected. Rules with this user notation are then processed.
Entries which FROM SYSTEM correspond or is *ALL, are scanned and a
single replication request is sent for each TO SYSTEM.

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

Parameters	Description
User	Enter the name of the User Profile to replicate. **Name** = Enter the name of a specific profile to replicate **Generic*** = Use a generic name to copy a group of profiles ***ALL** = Replicate all profiles
System combination	From system = Type the source system name or select ***ALL** systems Replicate to system= Type the target system name, a group of systems or select ***ALL** systems
Operations to Replicate	Define how to replicate common operations. Set to blanks for no replication. Create user: **Y** = Yes – On the target computer, create all users that meet the rule definition and exist on the source computer, and do not exist on the target computer. **A**= Yes / Change if the User profile already exists On the target computer, create all users that meet the rule definition and exist on the source computer, and do not exist on the target computer. Users that meet the rule definition on the source computer and already exist on the target computer are changed on the target computer to be identical to the user on the source computer. Change user: **Y** = Yes – All users that meet the rule definition on the source computer and also exist on the target computer are changed on the target computer to be identical to the user on the source computer. **A**= Yes / Create if the User profile does not exist All users that meet the rule definition and also exist on the target computer are changed to be identical to the user on the source computer. Users that only exist on the source computer are created on the target computer. Delete user:

Parameters	Description
	Y = Yes – All users that meet the rule definition are deleted from the source computer. If they also exist on the target computer, they are deleted also from the target computer.
Common attributes to replicate	Select what common attributes to replicate. Set to blanks for no replication. User disabled: **Y** = Yes User enabled: **Y** = Yes Password changes: **Y** = Yes

11. Type the appropriate parameters and press **Enter**. The **Modify Replication Rules 2/2** screen appears.

```
Screen 2/2                  Modify Replication Rules

Type choices, press Enter.
Description  . .  ____________________________________________________
                  ____________________________________________________
                  ____________________________________________________
Parameters or Parameters with partial value to omit e.g. INLPGM or INLPGM(A/B
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ___________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________
                  ____________________________________

F3=Exit                F12=Cancel
```

12. Type a description and enter exception parameters that are not to be replicated and press **Enter**.
13. Select ***STRAUD* > 69 > 26 > 52. Replicate Users** in the **Replication** menu (***STRAUD*** > 69 > 25 > 52). The **Replicate (Audit) User Profile** screen appears.

```
                    Replicate (Audit) user Profile (RPCAUUSR)

Type choices, press Enter.

User profile . . . . . .  .          __________     Name, generic*, *ALL
System to replicate to . . . . .     ________       Name
Replicate GRPPRF/SUPPRF first  .     *YES           *NO, *YES
Mark rightmost TEXT char with  .     A              Character value, *NONE

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

Parameters	Description
User profile	Enter the name of the User Profile to replicate. **Name** = Enter the name of a specific profile to replicate **Generic*** = Use a generic name to copy a group of profiles ***ALL** = Replicate all profiles
System to replicate to	**Name** = Enter the name of the target system
Replicate GRPPRF/SUPPRF first	***Yes** = Replicate these profiles first ***No** = Do not replicate these profiles first
Mark rightmost TEXT char with	Character value ***NONE** = do not mark the text.

14. Enter the appropriate parameters and press **Enter**. The profiles are replicated.

Program Exceptions for Replication

You can specify that operations, such as create, delete or change user profile, generated by programs in the Replication Exception list, are not replicated.

1. Select **`55. Program Exceptions for Replication`** in the **Replication** menu (*STRAUD* **`> 69 > 25 > 55`**). The **User Replication – Work with Program Exceptions** screen appears.

```
                User Replication - Work with Program Exceptions

Operations such as create, delete or change user profile, generated by
programs in exception list, will not be replicated.
Type options, press Enter.
 4=Delete
                                          Position to  . . . . . _________
Opt Program
 _   PGM1
 _   PGM2
                                                                    Bottom
F3=Exit   F6=Add new            F12=Cancel
```

2. Press **F6** to add a new program to the list. The **Add Program Exception** screen appears.

```
                              Add Program Exception

Type choices, press Enter.

   Program
   PGM1       
   PGM2       
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________
   __________

F3=Exit   F12=Cancel
```

3. Enter the required programs and press **Enter**.

Revive Deleted Users

Deleted users can be restored to the system and then be available again for replication.

1. Select **57. Revive deleted users** in the **Replication** menu (*STRAUD* **> 69> 25 > 57**). The **Revive Deleted Users** screen appears.

```
                              Revive Deleted Users

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

Opt User       Description                                        Delete date
 _  ALEX5      Alex - Supporteam strong user                      2019-07-21
 _  AODTMP001  Temp. user of job 559777/LOWUSR/QPADEV000W         2019-07-21
 _  DB2        DB-Gate                                            2019-07-23

                                                                        Bottom
F3=Exit   F5=Refresh
```

2. Type **1** to select a user profile to recreate.

Replication Log

Access the log to display a list of replications that were requested and completed. Filter according to time, replicated item type or item name.

1. Select **`1. Display Replication Log`** in the Replication menu (*STRAUD* **`> 69 > 25 > 1`**). The **Display Replication Log** screen appears.

```
                        Display Replication Log (DSPRPLOG)

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
Item type  . . . . . . . . . . .   *ALL         *ALL, *SYSVAL, *USER
Item name  . . . . . . . . . . .   *ALL         Name, generic*, *ALL





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

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 start and end times specified below
Starting date and time Ending date and time	Selects only those events occurring within the range specified by the start and end 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**/ ***PRVMONTHS** = Current month/Previous month ***YEARSTR**/ ***PRVYEARS** = Current year/ Previous year ***SUN** -***SAT** = Day of week
Item Type	You can filter the log by Item Type. ***ALL** ***SYSVAL** ***USER**
Item Name	Enter the name of the Item to display. **Name** = Enter the name of a specific item to display **Generic*** = Use a generic name to display a group of items ***ALL** = Display all items

2. Enter the required parameters and press **Enter**. The **Display Replication Log** screen appears.

```
                          Display Replication Log

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

Opt Date-time           Type    Item       Target     Sent   Done  Errors  Wait
 _  2019-07-23-11.33.53 *USER   VV2        RAZLEE2      1      0      0      1

                                                                        Bottom
                           Total:     1 requests.      1      0      0      1
 F3=Exit   F5=Refresh   F17=Top   F18=Bottom
```

Parameter	Description
Date-time	Date and time of the replication request
Type	Type of object to replicate (*USER or *SYSVAL)
Item	The item that was replicated
Target	The target system of the replicated objects
Status	Sent = How many items were sent for replication Done = How many items replication requests are done Errors = How many replication errors Wait = How many items are waiting to be replicated

3. Type `1` to select a transaction to view the individual items. The **Display Replication Details** screen appears.

```
                        Display Replication Details        2019-07-23-11.33.53
 Item . . . . . *USER      VV2                               Request ID.       8

 Use F6 to toggle additional detailed information.

 From system To        To system Result
 S520        RAZLEE2   RAZLEE2   No answer

                                                                        Bottom

 F3=Exit    F6=Display/Undisplay Request Information
```

4. You can press **F6** to unfold and view the full information of the replication request.

```
                        Display Replication Details        2019-07-23-11.33.53
 Item . . . . . *USER      VV2                               Request ID.       8

 Use F6 to toggle additional detailed information.

 From system To        To system Result
 S520        RAZLEE2   RAZLEE2   No answer
    Request: CRTUSRPRF USRPRF(VV2) PWDEXP(*NO) STATUS(*DISABLED) USRCLS(*PGMR) A
STLVL(*SYSVAL) CURLIB(*CRTDFT) INLPGM(*N/*NONE) INLMNU(*LIBL/MAIN) LMTCPB(*NO) T
EXT('Victor weak user test CP.A') SPCAUT(*NONE) SPCENV(*SYSVAL) DSPSGNINF(*SY...

                                                                        Bottom

 F3=Exit    F6=Display/Undisplay Request Information
```

Configuration and Maintenance

The purpose of this Chapter is to provide information on configuration and maintenance settings and properties.

System Configuration

This section shows you how to set general configuration for Audit. To access configuration features, select **81. System Configuration** in the Main menu (*STRAUD* > **81**). The **iSecurity/Base System Configuration** menu appears.

```
                    iSecurity/Base System Configuration     20/08/19 10:51:18

Audit  *SIEM Only* Mode Active           SIEM Support
 1. General Definitions                  30. Main Control-----> Active
 3. Log QSH, PASE activity               31. SIEM 1: Kiwi         Y
 5. Auto start activities in ZAUDIT      32. SIEM 2: VictorPC     N
 9. Log & Journal Retention              33. SIEM 3: QRADAR       N
                                         34. JSON Definitions (for DAM)
Action *FYI* Mode Active                 35. SNMP Definitions
11. General Definitions                  36. Twitter Definitions
12. SMS/Special Definitions
13. E-Mail Definitions                   39. Syslog test

SIEM Event Classification                General
21. QSYSOPR, QHST, MsgQ & User msgs      91. Language Support
22. QAUDJRN Type/Sub Severity Setting    99. Copyright Notice

Selection ===>  _

Release ID . . . . . . . . . . . . . .  14.06 19-08-14    44DE466  520 7459   1
Authorization code A (starts with 4) .  401910757307  1            1   S520
Authorization code B (starts with N) .  N01910748657
F3=Exit    F22=Enter Authorization Code
```

[[[Undefined variable Audit.ProductName]]] Configuration

General Definitions

1. Select **`1. General Definitions`** in the **iSecurity/Base System Configuration** menu (*STRAUD* **`> 81 > 1`**). The **Audit General Definitions** screen appears.

```
                          Audit General Definitions          23/07/19 11:35:52

Type options, press Enter.

  Enable Audit Scheduling . . . . . .  Y              Y=Yes, N=No
  Audit can automatically replace the OS/400 audit setting with pre-defined
  settings according to the time and day of the week. Y enables this feature.

  "Field changed" symbol (print). . .  #
  This symbol is printed before each user profile attribute that has been
  changed.

  Use *N to represent empty fields  .  Y              Y=Yes, N=No
  Empty fields can be displayed as *N when the log is displayed. If you select
  N=No, the system will use less disk space.

  Start log display . . . . . . . .  N              N=New, O=Old
  Start query display . . . . . . .  N              N=New, O=Old



 F3=Exit   F12=Cancel
```

Parameter	Description
Enable Audit Scheduling	**Y** = Yes **N** = No Audit can automatically replace the global audit setting with pre-defined settings according to the time and day of the week. Enter **Y** to enable this feature.
"Field changed" symbol (print)	Audit can compare "before" and "after" images of records. When you print the Audit log, this symbol entered will appear before each changed field.
Use *N to represent empty fields	**Y** = Yes **N** = No Empty fields can be displayed as `*N` when the log appears. If you select **N**, the system will use less disk space.

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

Log QSH, PASE activity

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

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

```
                        Log QSHELL (QSH, PASE) Commands       23/07/19 11:38:19

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
```

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.

2. 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.

Auto start activities in ZAUDIT

Define the activities that will start automatically when the ZAUDIT subsystem starts.

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

```
                  Auto Start Activities in ZAUDIT Subsystem  22/07/19 17:30:46

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) . . . . . . . . . .  Y          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
```

Parameter	Description
Real-Time Auditing (All systems)	**Y** = Yes **N** = No If you set the Change Tracker parameters **Enable Change Tracker** and **Enable Real Time Tracking** to **Y**, then even if this parameter is set to **N**, activating the ZAUDIT subsystem activates the Audit job. You access the Change Tracker parameters in the Activation Mode option in the System Configuration menu in Change Tracker (*STRCT* **> 81 > 1**).
Status & Active jobs	**Y** = Yes **N** = No
Firewall & Screen (Action)	**Y** = Yes **A** = Always **N** = No Selecting **A**=Always will perform Action activities even if Firewall is running in ***FYI**. Action must be running in real mode (not in FYI).
Message Queues (set to start at *IPL)	**Y** = Yes **N** = No If this parameter is set to **Y**, then when adding new Message Queues, you can set them to start automatically at ***IPL** time. For more details, see "Create Message Queue Audit Rules" on page 127.
Replication of User, Pwd, SysVal	**Y** = Yes **N** = No

2. Enter the required parameters and press Enter.

Log and Journal Retention

Define the parameters for log and journal retention. A specified backup program may run before deleting old logs and journals. It will backup all data deleted after the retention period expires. The ***STD** (default) backup program for logs is ***SMZ4/AUSOURCE AULOGBKP***.

A specified backup program may run before deleting old journal receivers. It will backup data deleted after the retention period expires. The ***STD** backup program for journals is ***SMZ4/AUSOURCE AUJRNBKP***. You should always backup the journal receiver because it may contain data not logged in [[[Undefined variable Audit.ProductName]]].

1. Select **81 > 9. Log & Journal Retention** in the **iSecurity/Base System Configuration** menu (*STRAUD* **> 81 > 9**). The **Log & Journal Retention** screen appears.

```
                          Log & Journal Retention          23/07/19 11:39:11

Log retention period (days) . . . . . . .   7          Days, 9999=*NOMAX
Backup program for logs . . . . . . . . .  *NONE       Name, *STD, *NONE
Backup program library  . . . . . . . . .  __________
A specified backup program may run before deleting old logs. It will backup
all data deleted after the retention period expires.  The *STD backup
program source is in SMZ4/AUSOURCE AULOGBKP.

Keep deleted users for revival (days) . .  10          Days, 999=*NOMAX

The following parameters apply to the audit journal receivers.  This is
the primary data source for Audit. You should always backup the journal
receiver because it may contain data not logged in Audit.
QAUDJRN receivers retention period (days)   5          Days, 9999=*NOMAX
Backup program for journal  . . . . . . .  *NONE       Name, *STD, *NONE
Backup program library  . . . . . . . . .  __________
A specified backup program may run before deleting old journal receivers.
It will backup data deleted after the retention period expires. The *STD
program is SMZ4/AUSOURCE AUJRNBKP.

F3=Exit   F12=Cancel
```

Parameter	Description
Log Retention Period	Transactions are retained for the specified number of days. At the end of this period, transactions are purged from the log. Enter **9999** to retain all data indefinitely.
Backup Program for Logs	Enter the name of the backup program to use to back up logs. Type ***STD** to use the [[[Undefined variable Audit.ProductName]]]standard backup program or ***NONE** for no backup. You must ensure the appropriate backup media is loaded before the automatic backup program runs.
Library	Enter the name of the library where the Backup program is stored.
Keep users for revival for (days)	Enter the number of days for which deleted users are kept on the system. Enter **999** to keep all users indefinitely.
Journal Retention Period	Transactions are retained for the specified number of days. At the end of this period, transactions are purged from the journal. Enter **9999** to retain all data indefinitely.
Backup Program for journal	Enter the name of the backup program to use to back up journals. Type ***STD** to use the Audit standard backup program or ***NONE** for no backup. You must ensure the appropriate backup media is loaded before the automatic backup program runs.
Library	Enter the name of the library where the Backup program is stored.

2. Enter the required parameters and press Enter.

Action Definitions

General Definitions

1. Select **`11. General Definitions`** in the **iSecurity/Base System Configuration** menu (*STRAUD* **`> 81 > 11`**). The **Action General Definitions** screen appears.

```
                          Action General Definitions         23/07/19 14:17:48

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 . . . . . . . . . 1200    Seconds
  Prevent action for same rule (default).    20     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
```

Parameter	Description
Work in *FYI* (Simulation) mode	***FYI*** is an acronym for "For Your Information". In this mode, security rules are fully operational, but no action is actually taken. This enables you to review your History Log for analysis, and thereby later create valid security rules. **Y**= Enable FYI **N** = Do not enable FYI
Log CL Script commands	This option enables you to save a log of CL commands that run in a particular action in the joblog of the real-time processor. **1**= Do not save to the log **2** = Save only failed commands **3** = Save all commands
Status & Active jobs detection	Actions are not repeated for the same rule until the specified period has elapsed. This prevents unnecessary repetition of actions.
Interval between checks	The amount of time (in seconds) to wait between checks
Prevent action for same rule for	The amount of time (in seconds) to wait before performing this action again
Prevent actions for "old" events	Do not perform actions for events if the time passed since they occurred passed the specified limits.
Send message only if within	If this amount of time or more (in minutes) has passed since the triggering event occurred, do not send a message.
Run scripts only if within	If this amount of time or more (in minutes) has passed since the triggering event occurred, do not run any scripts.

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

SMS Definitions

If you have an agreement with your company's mobile phone provider to be able to send text messages from software, the action triggered by an event can be a text message to the person who must be informed. You define here the parameters for the text sender, all of which you should have received from your mobile phone provider.

Before you add/change these definitions, you should contact Raz-Lee support staff.

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

```
                        Action SMS/Special Definitions       23/07/19 11:40:31

When SMS or Special (usually used for Beeper) options are selected, Action
calls a standard program. See below another option.
In the USA and some other countries, it is possible to use a free SMS or
Beeper service. It is done by sending the message via email. The email addres
is made of the phone number and a cellular provider specific extension.
i.e. number@vtext.com will send SMS to a Verizon number.

To use, enter the full email address, instead of the phone number.
Action will send an email to the Destination with the Message text.

You may override this method. To do so, create a program AUALR6R for SMS,
or AUALR7R for Special in library SMZ4DTA.
When called, these programs receives the parameters:
- Destination (A   64)
- Message     (A 1000)

Example programs are in SMZ4/AUSOURCE AUALR6R and AUALR7R.


F3=Exit   F12=Cancel
```

Parameter	Description
Sender	The telephone number from which the text messages will be sent.
User	Your User name with your mobile phone provider.
Password	Your password with your mobile phone provider.
Supplier Id	An ID that identifies your mobile phone provider.

2. Enter the required parameters and press Enter.

Email Definitions

If you have an agreement with your company's mobile phone provider to be able to send text messages from software, the action triggered by an event can be a text message to the person who must be informed.

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

```
                              E-mail Definitions            23/07/19 11:41:22

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.land.com
                                        Mail server, *LOCALHOST
Port  . . . . . . . . . . .    25               SSL Secured    N   Y=Yes, N=No
Use the Mail Server as defined for outgoing mail in MS Outlook.
Reply to mail address . . .  VICTOR@RAZLEE.COM
If Secured, E-mail user . .  ALEXM@RAZLEE.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
```

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.
Advanced/Secured E-mail Support:	
Mail (SMTP) server name	The name of the STMP server or **`*LOCALHOST`**
Reply to mail address	The e-mail address to receive tests.
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
Native E-mail:	
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**.

Security Event Manager

QSYSOPR and other message queues

You can monitor QSYSOPR and other message queues:

1. Select the **`Message Queue (SysCtl)`**.
2. Select the Message Queues to control.
3. Add all the Message Queues, joining each of them to group @1, with input every 10 seconds.
4. Select Message Queue rules.
5. Add a rule for group @1 specifying the preferred method of sending the information. You might wish to specify filters.
6. Select Activate at IPL (or add SMZ4/ACTAUMSGQ to the startup program).

You can also choose other methods of monitoring message queues:

- Create and monitor message queue QSYSMSG. See IBM documentation for more information.
- Create a group with message IDs you wish to monitor, and specify in the filter the test ITEM to compare against the items in the group.

To monitor message queues, you must install Action. To use Syslog, SNMP, and so on, you must install Central Admin.

QAUDJRN Type/Sub Severity Setting

You can set the range of severities for each Audit type to control when to send entries to SIEM reporting.

1. Select **22. QAUDJRN Type/Sub Severity Setting** from the iSecurity/Base System Configuration screen (*STRAUD* **> 81 > 22**). The **QAUDJRN Type/Sub Severity Setting** screen appears.

```
                              SIEM Severity Setting
                                                Subset by type. .  _________
                                                       by entry .  __
 Type options, press Enter.                            by text. .  _______________
   blank=Do not send   0=Emergency   1=Alert   2=Critical   3=Error
   4=Warning   5=Notice   6=Info   7=Debug   I=Use IBM standard
 SIEM   IBM  Audit            Pink represents additions
 1 2 3  STD  Type  Type       to types not covered by IBM
 6 6 6   6   @1 A  *ACTIVE    Message queue (Group Id 1)
 6 6 6   6   @2 A             Message queue (Group Id 2)
 6 6 6   6   @3 A             Message queue (Group Id 3)
 6 6 6   6   @4 A             Message queue (Group Id 4)
 6 6 6   6   @5 A             Message queue (Group Id 5)
 6 6 6   6   @6 A             Message queue (Group Id 6)
 6 6 6   6   @7 A             Message queue (Group Id 7)
 6 6 6   6   @8 A             Message queue (Group Id 8)
 I I I   I   @9 A             QHST messages. Set I for IBM standard severety.
 5 5 5   5   AD D  *SECURITY  Auditing of a DLO was changed with CHGDLOAUD
                              command.
 5 5 5   5   AD G             Get user from identity token successful
                                                                      More...
 F3=Exit  F19=Info  F21=Set 1 as IBM  F22=Set 2 as IBM  F23=Set 3 as IBM
```

Parameter	Description
Opt	Enter the required severity level. All events of this Audit Type/ Subtype that have this severity level or higher are sent to SIEM. The higher the level, the fewer events that are sent. ▪ Blank = Do not send ▪ 0 = Emergency ▪ 1 = Alert ▪ 2 = Critical ▪ 3 = Error ▪ 4 = Warning ▪ 5 = Notice ▪ 6 = Info ▪ 7 = Debug

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

SIEM Support

Numerous iSecurity products integrate with SEM/SIEM systems by sending security alerts instantaneously to these systems. 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 Series 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 **`30. Main Control`** from the **iSecurity/Base System Configuration** screen (*STRAUD* **`> 81 > 30`**). The **`Main Control for SIEM & DAM`** screen appears.

```
                         Main Control for SIEM & DAM         23/07/19 11:48:50

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

Send SYSLOG Messages to SIEM
SIEM 1: kiwi        . . . . . .     N          Y=Yes, N=No, A=Action only
SIEM 2: VictorPC    . . . . . .     Y          Y=Yes, N=No, A=Action only
SIEM 3: QRADAR      . . . . . .     N          Y=Yes, N=No, A=Action only
Use Action-Only to send syslog messages from Action, without QAUDJRN info.
To increase performance, add SIEM Processors by ADDAJE JOB(AU..n) n=SIEM ID.
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.

Skip info if SIEM is inactive .     Y          Y=Yes, N=No
Y is recommended, unless it is the only operation.




Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel
```

Parameter	Description
Run rules before sending	**Y** = Yes **N** = No
Send SYSLOG messages to SIEM	**Y** = Yes **N** = No **A** = Action only; Use Action-Only to send syslog messages from Action, without QAUDJRN info.
Send JSON messages (for DAM)	**Y** = Yes; Y is recommended, unless it is the only operation. **N** = No
As only operation	**Y** = Yes; If Y, information is not collected, and no other functionality is performed. **N** = No
Skip info if SIEM is inactive	**Y** = Yes; Y is recommended, unless it is the only operation. **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 a range of severities such as Emergency, Alert, Critical, Error, and Warning. 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 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 in overcoming 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:

1. Select the SIEM system from the iSecurity/Base System Configuration menu (*STRAUD*> **81**).
    - For SIEM 1, Select **31. SIEM 1** (*STRAUD*> **81 > 31**).
    - For SIEM 2, Select **32. SIEM 2** (*STRAUD*> **81 > 32**).
    - For SIEM 3, Select **33. SIEM 3** (*STRAUD*> **81 > 33**).
2. The selected SIEM Definitions screen appears.

```
                              SIEM 1 Definitions            23/07/19 11:52:10

SIEM 1 name . . . . . . . . . .   Kiwi                          Port:   514
SYSLOG type . . . . . . . . . .   1           1=UDP, 2=TCP, 3=TLS
Destination address . . . . . .   1.1.1.129
____________________________________________________________________________

"Severity" range to auto send .   0 - 5       Emergency - Notice (significant)
"Facility" to use . . . . . . .   22          Local use 6 (Local6)

Msg structure or *LEEF, *CEF  .   *CEF
____________________________________________________________________________
*LEEF, *CEF, *CEF-SPLUNK, 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

Note: Re-activate subsystem after changes.
F3=Exit   F12=Cancel            F22=Set SYSLOG handling per audit sub-type
```

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 at 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

Parameter	Description
	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)
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 "Original Input Formats" on page 95).
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.
&t	Tab character.

Variable	Description
&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

2. Enter the required parameters and press Enter.
   - **&0** or **&2** can 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:

- These fields are not converted to ASCII.
- SYSLOG manager must set maximum message length from default (1024) to expected size (10000).
- SYSLOG manager must take care of non-printable characters option.

Syslog Simulation Software

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

1. Download Kiwi Syslog Server from http://www.kiwisyslog.com
2. 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.

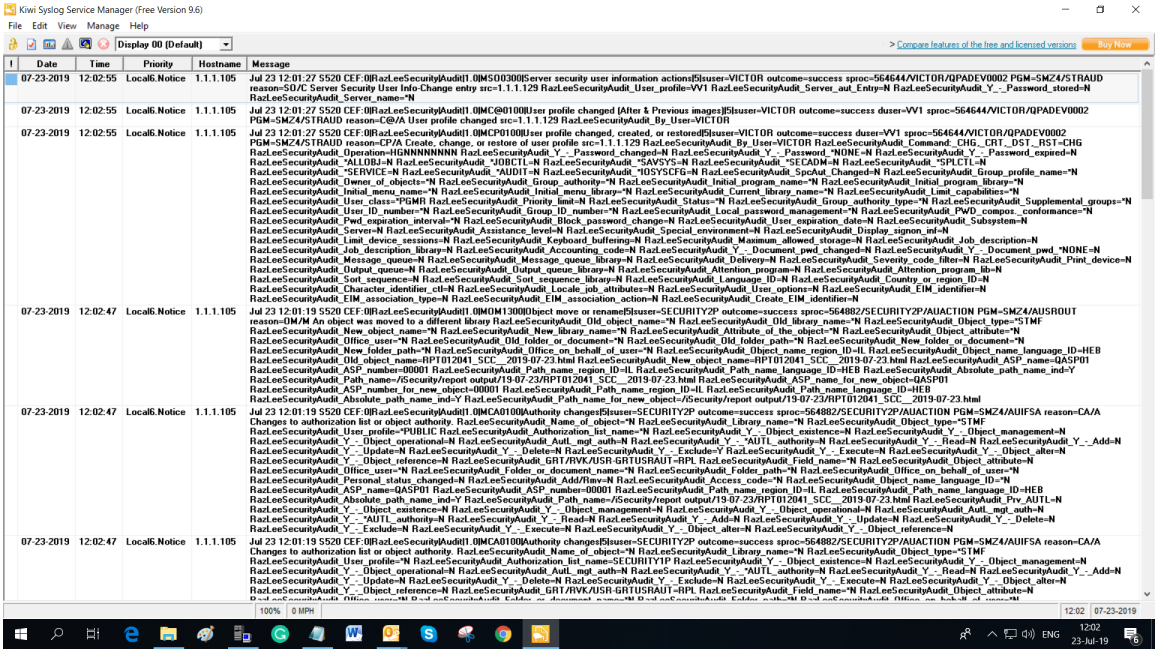
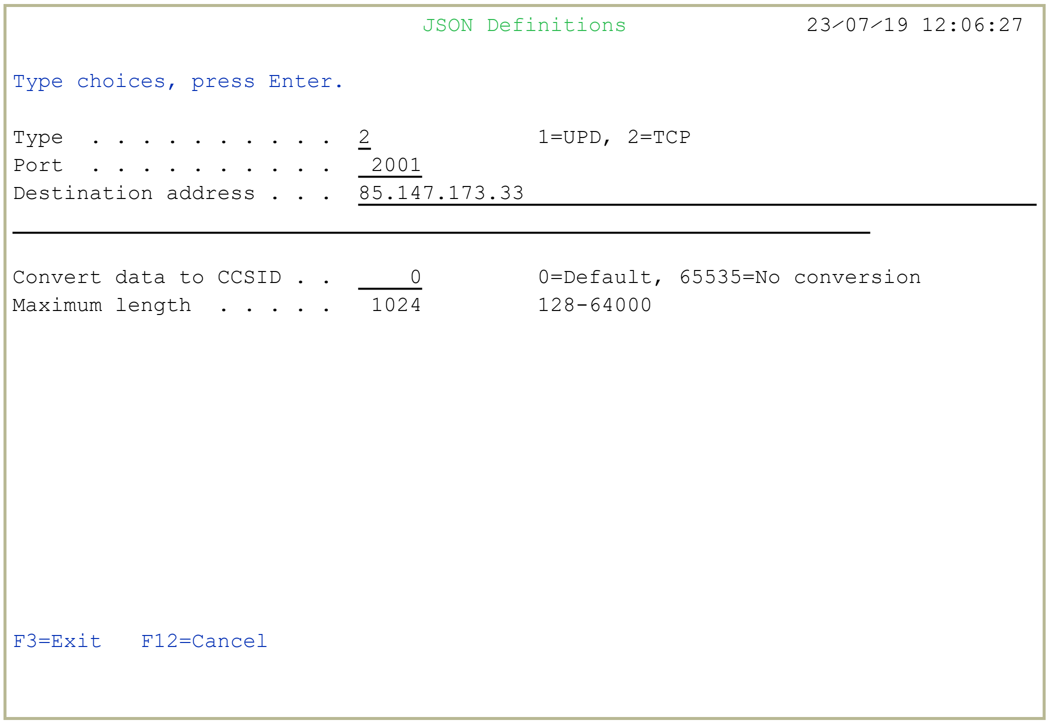


Figure 4: Kiwi Syslog Server

JSON Definitions

1. Select **`34. JSON Definitions`** (for DAM) in the **iSecurity/Base System Configuration** menu (*STRAUD*> **`81 > 34`**). The **JSON Definitions** screen appears.



```
                                JSON Definitions              23/07/19 12:06:27

Type choices, press Enter.

Type  . . . . . . . . . . .   2             1=UPD, 2=TCP
Port  . . . . . . . . . . .    2001
Destination address . . . .   85.147.173.33


Convert data to CCSID . . .       0         0=Default, 65535=No conversion
Maximum length  . . . . . .    1024         128-64000









F3=Exit   F12=Cancel
```

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 **35. SNMP Definitions** in the **iSecurity/Base System Configuration** menu (*STRAUD* **> 81 > 35**). The **SNMP Definitions** screen appears.

```
                              SNMP Definitions              23/07/19 12:07:53

 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
```

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 (seen in "Triple Syslog Definitions (#1-#3)" on page 299).

3. To prompt and receive alerts, define an Alert Message in Action (Use **31.Work with Actions** in the Action main menu (*STRAUD*> **61 > 31**)).

Maintenance Menu

The Maintenance Menu enables you to set and display global definitions for Security Part 2.To access the Maintenance Menu, select **82. Maintenance Menu** in the Audit main menu (*STRAUD* **> 82**).

```
AUMINTM                          Maintenance Menu                iSecurity/Base
                                                            System:   S520
iSecurity/Base Global                  Trace Definition Modifications
 1. Export Definitions                 71. Add Journal
 2. Import Definitions                 72. Remove Journal
 5. Display Definitions                79. Display Journal

Audit
21. Start a New QAUDJRN Receiver
22. Change QAUDJRN Receiver Library
23. Work with QAUDJRN Attributes
24. Use Local Field Description
25. Use English Field Description      Other
29. Delete Statistic Data              98. Uninstall iSecurity/Base



Selection or command
===> ____________________________________________________________________________

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

Transfer Log Copy

Export Product Log

You can export a product log to another library. You can filter by date the portion of the log to send.

1. Select **33. Export Log** in the **Maintenance** menu (*STRAUD* **> 82 > 33**). The **Export iSecurity/BASE Log (EXPS2LOG)** screen appears.

```
                    Export iSecurity/BASE Log (EXPS2LOG)

Type choices, press Enter.

To library . . . . . . . . . . .   __________   Name
Starting date  . . . . . . . . .   *YESTERDAY   Date, *CURRENT, *YESTERDAY...
Ending date  . . . . . . . . . .   *YESTERDAY   Date, *CURRENT, *YESTERDAY...

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

Parameter	Description
To library	Type the name of the library to receive the log.
Starting date	Type the starting date of the range to extract from, or choose one of the following: ***CURRENT** ***YESTERDAY** ***WEEKSTR** ***PRVWEEKS** ***MONTHSTR** ***PRVMONTHS** ***YEARSTR** ***PRVYEARS** ***MON** ***TUE** ***WED** ***THU** ***FRI** ***SAT** ***SUN**
Ending date	Type the ending date of the range to extract from, or choose one of the following: ***CURRENT** ***YESTERDAY** ***WEEKSTR** ***PRVWEEKS** ***MONTHSTR** ***PRVMONTHS** ***YEARSTR** ***PRVYEARS** ***MON** ***TUE** ***WED** ***THU** ***FRI** ***SAT** ***SUN**

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

Import Product Log

You can import a product log from another library. You can filter by date the portion of the log to receive.

1. Select **`34. Import Product Log, Collect from Rmt`** in the **Maintenance** menu (*STRAUD* **`> 82 > 34`**). The **Import iSecurity/BASE Log (IMMPS2LOG)** screen appears.

```
                    Import iSecurity/BASE Log (IMPS2LOG)

Type choices, press Enter.

From input type  . . . . . . . . > *NET          *LIB, *SAVF, *NET
System to import from  . . . . .   ________       Name, *group, *ALL
To data library extension  . . .   *SYSTEM       for *NET & *group use *SYSTEM
Starting date  . . . . . . . . .   *YESTERDAY    Date, *CURRENT, *YESTERDAY...
Ending date  . . . . . . . . . .   *YESTERDAY    Date, *CURRENT, *YESTERDAY...

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

Parameter	Description
From input type	***LIB** ***SAVF** ***NET**
System to import from	Only if the input type is *NET Type the name of the system to import from ***ALL**
Work library	Only if the input type is *LIB Type the name of the Library to import from
From save file	Only if the input type is *SAVF Type the name of the SAVF to import from
From library	Only if the input type is * SAVF Type the name of the library that contains the SAVF *LIBL
To data library extension	***SYSTEM**
Starting date	Type the starting date of the range to receive from, or choose one of the following: ***CURRENT** ***YESTERDAY** ***WEEKSTR** ***PRVWEEKS** ***MONTHSTR** ***PRVMONTHS** ***YEARSTR** ***PRVYEARS** ***MON** ***TUE** ***WED** ***THU** ***FRI** ***SAT** ***SUN**
Ending date	Type the ending date of the range to receive from, or choose one of the following: ***CURRENT**

Parameter	Description
	***YESTERDAY** ***WEEKSTR** ***PRVWEEKS** ***MONTHSTR** ***PRVMONTHS** ***YEARSTR** ***PRVYEARS** ***MON** ***TUE** ***WED** ***THU** ***FRI** ***SAT** ***SUN**

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

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 [[[Undefined variable Audit.ProductName]]]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 **`1. Export Definitions`** in the **Maintenance** Menu (*STRAUD*> **`82 > 1`**). 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, *SAME
System Configuration (opt. 81)     *NO           *REPLACE, *CLEAR, *NO
Job Schedule Entries . . . . . .   *NO           *ALL, *RPT, *NO

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

	Description
Collection type	***ADD** – Add subjects to an existing library ***NEW** – Clear and restart ***OLD** – Use this option only with the guidance of support; this option is kept for computability purposes only.
Work library and SAVF in QGPL	Destination of export library. Name= name of target library ***AUTO** (S2 + System) default security setting
Operation type	Definitions pertaining to these two applications ***REPLACE** = replace a previously imported/exported rule ***BYMODULE**= import/export rules by module ***SAME** = no change
System Configuration (opt. 81)	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 ***REPLACE** = replace the definition file and copy the new ***CLEAR** = replace the definition file and copy the new ***NO** = no update to files can be exported as is

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

```
                    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, *SAME
System Configuration (opt. 81)     *NO           *REPLACE, *CLEAR, *NO
Job Schedule Entries . . . . . .   *NO           *ALL, *RPT, *NO
Update remote systems:
  Systems to update  . . . . . .   *NONE         Name, *group, *ALL, *NONE
  Update type  . . . . . . . . .   *UPD          *UPD, *REPLACE

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

	Description
Update remote systems	
Systems to update	**Name** = Name of the system ***group** = Name of the group ***ALL** = All systems ***NONE** = No systems
Update type	***UPD** = Update using UPD ***REPLACE** = Replace current

Import Definitions

You can import the SAVF file containing the exported definitions and settings to another computer or LPAR.

To import the SAVF definitions file:

1. Select **`2. Import Definitions`** in the **Maintenance** menu (*STRAUD*> **`82 > 2`**). The **Import iSecurity/BASE Defns.** screen appears.

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

 Type choices, press Enter.

 Input type . . . . . . . . . . .   *SAVF         *LIB, *SAVF



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

	Description
Input type	**`*LIB`** = Input from a library **`*SAVF`**= Input from a saved file

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** in the **Maintenance** menu (*STRAUD* **> 82 > 5**). The **Display Security 2 Definitions** screen appears.
2. Select the desired Report type. 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...
 From item  . . . . . . . . . . .   *ALL
_____
 To item  . . . . . . . . . . . .   *SAME
_____
 From item  . . . . . . . . . . .   *ALL        Character value, *ALL, *START
 To item  . . . . . . . . . . . .   *SAME       Character value, *ONLY, *LAST
 From item  . . . . . . . . . . .   *ALL        Character value, *ALL, *START
 To item  . . . . . . . . . . . .   *SAME       Character value, *ONLY, *LAST
 From item  . . . . . . . . . . .   *ALL        Character value, *ALL, *START
 To item  . . . . . . . . . . . .   *SAME       Character value, *ONLY, *LAST
 Format . . . . . . . . . . . . .   *DETAILS    *LIST, *DETAILS
 Output . . . . . . . . . . . . .   *          *, *PRINT, *PRINT1-*PRINT9



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

	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 "Setting up the *PRINT1-*PRINT9 Printers and *PDF Output" on page 356 for details.

Transfer Definitions

Export Definitions

You can export your Audit definitions to another computer.

To export Audit definitions to another computer:

1. Select **`1. Export Definitions`** in the **Maintenance** menu (*STRAUD* **`> 82 > 31`**). The **Export iSecurity/BASE Defns. (EXPS2DFN)** 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, *SAME
System Configuration (opt. 81)     *NO           *REPLACE, *CLEAR, *NO
Job Schedule Entries . . . . . .   *NO           *ALL, *RPT, *NO
Update remote systems:
  Systems to update  . . . . . .   *NONE         Name, *group, *ALL, *NONE
  Update type  . . . . . . . . .   *UPD          *UPD, *REPLACE

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

2. Type **`*NEW`**, **`*ADD`**, or **`*OLD`** as the Collection type and press **Enter**. The appropriate continuation screen appears.

Field	
Collection type	***NEW** - the information exported is completely new ***ADD** - the information exported will be added to previous information ***OLD** – the information exported will be old
Work library and SAVF in QGPL	**Name** - provide name of library ***AUTO** - library will be automatically retrieved
Operation type	***REPLACE** - replace data originally in the database ***BYMODULE** - replaces per module according to specifications ***SAME** – stays the same as previous
System Configuration (opt. 81)	***REPLACE** – replace data ***CLEAR** - clear data ***NO** - no operation required

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

Import Definitions

You can import [[[Undefined variable Audit.ProductName]]] definitions to your computer that were exported from another computer.

1. Select **`2. Import Definitions`** in the **Maintenance** menu (*STRAUD* **`> 82 > 2`**). The **Import iSecurity/BASE Defns. (IMPS2DFN)** screen appears.
2. Type `*SAVF` or `*LIB` in the Input type field and press **Enter**. The appropriate continuation screen appears.

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

 Type choices, press Enter.

 Input type . . . . . . . . . . .   *SAVF         *LIB, *SAVF



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

Parameter	Description
Input type	***SAVF** ***LIB**
Save file	If Input type = *SAVF, name of the SAVF to which the exported definitions were saved
Library	If Input type = *SAVF, name of the library that contains the SAVF If Input type = *LIB, name of the library to which the exported definitions were saved
Audit options	***UPD** ***REPLACE** ***BYSUBJECT** ***SAME**
Action options	
Compliance options	
Replication options	
General options	
General Groups options	
Keep backup in library	Keep the exported definitions in this library.

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

[[[Undefined variable Audit.ProductName]]] Maintenance

Start a New Journal Receiver

[[[Undefined variable Audit.ProductName]]]periodically maintains its Journal Receivers according to your configuration (with no intervention). This, and the following features, gives you the option of manually handling all Journal Receiver maintenance.

1. Select **`21. Start a New Journal Receiver`** in the Maintenance menu (*STRAUD* **`> 82 > 21`**). The Change Audit Journal Attr. (CHGAUJRNA)screen appears.
2. Select **`*YES`** or **`*NO`** and press Enter.

Change Journal Receiver Library

1. Select **22. Change Journal Receiver Library** in the **Maintenance** Menu (*STRAUD*> **82 > 22**). 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
```

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**.

Work with Journal Attributes

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

1. Select **`23. Work with Journal Attributes`** in the **Maintenance** Menu (*STRAUD* **`> 82 > 33`**). The **Work with Journal Attributes** screen appears.

```
                          Work with Journal Attributes

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

Attached receiver  . :   AUDITR0027      Library  . . . . . . :   QGPL

Text . . . . . . . . :

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
```

Options	Description
F13 Display journaled files	The Display Journaled Files Attributes screen appears.
F14 Display journaled access paths	The Display Journaled Access Paths screen appears.
F15 Work with receiver directory	The Work with Receiver Directory screen appears. You can display a selected receiver (option 8) or delete a selected receiver (option 4)
F16 Work with remote journal information	The Work with Remote Journal Information screen appears.
F17 Display attached receiver attributes	The Display Journal Receiver Attributes screen appears. From this screen you can go to secondary screens to display associated receivers (**F6**) or to work with journal attributes (**F10**)
F19 Display journaled objects	The Display Journaled Objects screen appears. Choose the type of object to display: ■ **1** = Files: Displays the physical database files being journaled. ■ **2** = Access Paths: Displays the access paths being journaled ■ **3** = Data Areas: Displays the data areas being journaled ■ **4** = Data Queues: Displays the data queues being journaled ■ **5** = Integrated File System objects: Displays the integrated file system objects being journaled. This includes *STMF, *DIR and *SYMLNK objects that are in the Root ('/'), QOpensys, and User-defined file systems. ■ **6** = Commitment Definitions: Displays the commitment definitions being journaled

2. Select options you want to work with.

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 **24. Auto-Translate Field Descriptions** in the **Maintenance** Menu (*STRAUD* > **82** > **24**). The translation is generated automatically.

Use English File Descriptions

- Select **`25. Use English File Descriptions`** in the **Maintenance** Menu (*STRAUD* **`> 82 > 25`**).

Delete Statistic Data

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

1. Select **`29. Delete Statistic Data`** in the **Maintenance** Menu (*STRAUD* **`> 82 > 29`**). 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
```

Journal Product Definitions

You can record the system physical files changes in the data library.

To start recording physical file changes:

1. Select **`71. Add Journal`** from the **Maintenance** Menu (*STRAUD* **`> 82 > 71`**). The **Create Journal – Confirmation** screen appears.
2. Press **Enter** to confirm.

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

To stop recording physical file changes:

1. Select **`72. Remove Journal`** from the **Maintenance** menu (*STRAUD* **`> 82 > 72`**). The **End Journal - Confirmation** screen appears.
2. Press **Enter** to confirm.

Display Journal

1. Select **`79. Display Journal`** from the **Maintenance** menu (*STRAUD* **`> 82 > 79`**) to view journaled files. The **Display Journal Entries** screen appears.

```
                          Display Journal Entries

Journal  . . . . . . :   SMZ4            Library  . . . . . . :   SMZ4DTA
Largest sequence number on this screen  . . . . . . : 00000000000000000013
Type options, press Enter.
  5=Display entire entry


Opt    Sequence  Code  Type  Object      Library     Job         Time
 _            1   J     PR                          SCPF        22:06:52
 _            3   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:10:04
 _            4   R     UP   AUSELCP     SMZ4DTA     AUACTJOBOP  22:10:04
 _            5   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:10:04
 _            6   R     UP   AUSELCP     SMZ4DTA     AUACTJOBOP  22:10:04
 _            7   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:30:08
 _            8   R     UP   AUSELCP     SMZ4DTA     AUACTJOBOP  22:30:08
 _            9   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:30:08
 _           10   R     UP   AUSELCP     SMZ4DTA     AUACTJOBOP  22:30:08
 _           11   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:50:08
 _           12   R     UP   AUSELCP     SMZ4DTA     AUACTJOBOP  22:50:08
 _           13   R     UB   AUSELCP     SMZ4DTA     AUACTJOBOP  22:50:08
                                                                   More...
F3=Exit   F12=Cancel
```

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

Copy Queries from Backup

The option to copy queries to and from the SMZ4DTA file exists. By selecting the file to backup the user can save queries or recover queries in the event of data loss.

NOTE: This activity requires backups of files AUSELQP and AUSELCP to be on both the From and To libraries.

To **move or recover** selected reports from SMZ4DTA library:

1. Select **`93. Copy Queries from Backup`** in the **Maintenance** menu (*STRAUD* **`> 82 > 93`**).
2. In the **`From Library`** field, type the name of the 'Backup' file.
3. In the **`To Library`** field, type the name of the file to backup (SMZ4DTA is default).
4. Press **Enter**. The list of reports in the **`From`** library appears.

Uninstall

To uninstall Security Part 2:

1. Select **`98. Uninstall Security Part 2`** in the Maintenance Menu (*STRAUD* **`> 82 > 98`**).
2. Follow the directions on the **`Uninstall SECURITY2P`** screen.

Central Administration

The iSecurity Central Administration – Audit menu enables you to work with various administration settings for Security Part 2.

To access the iSecurity Central Administration – Audit menu

- Select **83. Central Administration** in the [[[Undefined variable Audit.ProductName]]]main menu (STRAUD > **83**).

```
AUCNTMN              iSecurity Central Administration - Audit   iSecurity/CntAdm
                                                                System:  S520
Select one of the following:

Definitions                                  Network Support
 1. Work with network definitions            51. Run CL Scripts
 2. Network Authentication                   52. Send PTF
Use SYSTEM() in the reporting menu
                                             Log Copy
Transfer Log Copy                            11. Run Reports on a Copy of Rmt Log
21. Export Log
22. Import Log, Collect from Rmt

Transfer Definitions                         Communication Log
31. Export Definitions, Update Rmt Sys       71. Current Job CntAdm Messages
32. Import Definitions                       72. All Jobs CntAdm Messages


Selection or command
===> ____________________________________________________________________________

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

BASE Support

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

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

```
AUBASE                          BASE Support                    iSecurity/Base
                                                          System:   RLDEV
Email                                     General
 1. Address Book                          51. Work with Collected Data
 2. Email Definitions                     52. Check Locks
 9. Target Restrictions                   53. Security Assessment
                                          55. Raz-Lee Support Menu
Operators                                 56. Re-create Damaged Data Queues
11. Work with Operators                   58. *PRINT1-*PRINT9, *PDF Setup
12. Work with AOD, P-R Operators          59. Global Installation Defaults

Authority Codes                           Network Support
21. Set Authorization Codes               71. Work with Network Definitions
22. Display Authorization Status          72. Network Authentication
23. Add Daily Check of Auth Codes         74. Send PTF
24. Remove Daily Check of Auth Codes      75. Run CL Scripts
25. Display CPU/Lpar Information          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=System main menu
```

Network Definitions

When you connect to a remote database (RDB), the RDB name in the connection request must match a valid entry on the target machine to get current information from existing reports or queries. Adjust the system parameters only to collect information from all the groups in the system to output files that can be sent via email.

NOTE: Update of this parameter is recommended in all cases, and is required based on the PTF level of the system

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

```
System type: AS400        Work with Network Systems           System: RLDEV
                                                Position to . . . __________
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Test DDM  9=Ping

Opt   System    Group
 _    RLDEMO    *TT      Demo system Audit release 14.16
 _    RLDEV     *NONE    Razlee Develop
 _    RLG       *TT      RL Germany
 _    RLMED     *TT      RLEMD
 _    RLPRV     *TT      Razlee Production
 _    RL74A     *VVVV    Demo system
 _    RL74B     *NONE    Test Yoel
 _    VERDE     *NONE    verde





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

2. Press **F6** to define a new network system to use.

```
System type: AS400            Add Network System              System: S520

System  . . . . . . . . . .  __________
Description . . . . . . . .  ______________________________________________
Group where included  . . .  *NONE___                 *Name

Communication Details
IP or remote name . . . . .  ______________________________________________
                             ______________________________________________
                             ______________________________
Type  . . . . . . . . . . .  *IP                      *SNA, *IP
Entry of *LOCAL on System .  ___________________       Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed .  *SYSTEM                   Name, *SYSTEM
Extension Id on remote  . .  ___



Note: After adding a system, run again "Network Authentication".

F3=Exit   F12=Cancel
Modify data, or press Enter to confirm.
```

3. Press **Enter** to confirm the settings.

Network Authentication

DDM Data Queues are rebuilt automatically. This program also handles the TCP/IP Host Table Entry and performs ***ADDTCPHTE*** or ***CHGTCPHTE*** to apply the definition automatically.

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

1. Select **`72. Network Authentication`** in the **BASE Support** menu (*STRAUD*> **`89 > 72`**). 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 of 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
```

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

Email

Email Address Book

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

1. Select **`1. Address Book`** in the **BASE Support** menu (*STRAUD*> **`89 > 1`**). 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                                                Pwd.
 _   AAA@BBB         1  test chkisa                                     *NO
 _   ABRAHAM         1  Abraham Notik                                   *NO
 _   ALEX            2  ALEX                                            *NO
 _   JHJHJH          1  Yuri's Email                                    *NO
 _   NOREPLY         1  Do Not Reply                                    *NO
 _   SUPPORT         1  Support mail box                                *NO
 _   TZION           1  Tzion's email                                   *NO
 _   VV              1  Victor                                          *NO
 _   YOEL            1  Yoel's email                                    *NO
 _   YURIW           1  Yuri work email                                 *NO
 _   ZAILER          1  Shmuel's email                                  *NO


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

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 . . . . . . .  ____________________________________________________
ZIP password exists . . .  N                   Use F8 to work with password

Email address(s) (blank, comma, new-line separated)
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
                                                                       More...
F3=Exit   F4=Prompt   F8=ZIP password   F12=Cancel
```

The screen contains the following fields:

Name

The name to identify the email addresses. Use this name when requesting reports that you send by email.

Description

A meaningful description

ZIP Password exists

You can specify a password to attach to any zip file sent to the addresses in this group. Without the password, the recipients will not be able to open the zip file. To add a password, press **F8**.

Email addresses

The email addresses of the group. Separate the addresses by a comma, or start each email address on a new line.

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

Email Definitions

iSecurity products can send out automatic emails according to settings in **Global Installation Defaults** (*STRAUD*> **89 > 59**).

Select **2. Email Definitions** in the **BASE Support** menu (*STRAUD*> **89 > 2**). The **E-mail Definitions** screen appears.

```
                              E-mail Definitions            23/07/19 11:41:22

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.land.com                                    
                                     Mail server, *LOCALHOST
Port  . . . . . . . . . . .    25              SSL Secured    N   Y=Yes, N=No
Use the Mail Server as defined for outgoing mail in MS Outlook.
Reply to mail address . . .  VICTOR@RAZLEE.COM                                
If Secured, E-mail user . .  ALEXM@RAZLEE.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
```

The screen contains these fields:

E-mail Method

Advanced or Secured mode is recommended for simplicity and performance. Possible values are:

- **1**=Advanced
- **2**=Native
- **3**=Secured
- **0**=None

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 SMTP server or ***LOCALHOST.** You can find or enter this information at your system's Work with TCP/IP Host Table Entries screen (*CGFTCP* **> 10**).

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.

To confirm the change to email definitions and send a confirmation email to the Reply-to mail address, press the F10 key. A dialog opens in which you can confirm these settings. Check that you have received the confirmation email. If it is not received, there is a problem with your email definitions.

Operators and Authority Codes

Work with Operators

For a detailed explanation of this feature, see Working with Operators' Authorities.

Work with Operators for Authority on Demand and Password Reset

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 tasks such as starting, stopping subsystems, jobs, and import/export. iSecurity automatically adds all users listed in Work with Operators to the appropriate product authorization list.

1. Select **12. Work with AOD, P-R Operators** in the **BASE Support** menu (*STRAUD*> **89 > 12**). 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
 _  AVI            S520       9   9   9    9
 _  JAVA2          S520       9   9   9    9
 _  NISSIMM        S520       1   1   1    1
 _  NIV            S520       9   9   9    9
 _  OD             S520       9   9   9    9
 _  OS             *ALL
 _  TEST           S520       9   9   9    9
 _  TZION          S520       9   9   9    9
 _  VICTOR         S520       9   9   9    9
                                                                        More...
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
```

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

Type choices, press Enter.

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

Authorities by subject:
Authority on Demand . . . .    9                 1=*USE, 4=Limited *EMERGENCY
                                                 5=*EMERGENCY, 8=Limited *FULL
                                                 9=*FULL
Password Reset  . . . . . .    9                 1=*USE, 9=*FULL
User Provisioning . . . . .    9                 1=*USE, 5=*ENTRY, 9=*FULL
Product Administrator . . .    9                 1=*USE, 9=*FULL

Note: Emergency operator can enable or modify emergency rules. This allows
      solving of critical problems without the intervention of the security
      administrator.
      The term Limited denotes that the user cannot change PIN codes.

F3=Exit    F12=Cancel
```

Work with Authorization

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

1. Select **`21. Add Authorization Codes`** from the **BASE Support** screen (*STRAUD*> **`89 > 31`**). The **Add iSecurity Authorization (ADDISAUT)** screen appears.

```
                    Add iSecurity Authorization (ADDISAUT)

Type choices, press Enter.

CPU number . . . . . . . . . . .   ___         Character value
Any iSecurity product:
  Part 1 . . . . . . . . . . . .   _________   Character value
  Part 2 . . . . . . . . . . . .   _________
Any iSecurity product:
  Part 1 . . . . . . . . . . . .   _________   Character value
  Part 2 . . . . . . . . . . . .   _________
Any iSecurity product:
  Part 1 . . . . . . . . . . . .   _________   Character value
  Part 2 . . . . . . . . . . . .   _________
Any iSecurity product:
  Part 1 . . . . . . . . . . . .   _________   Character value
  Part 2 . . . . . . . . . . . .   _________
Any iSecurity product:
  Part 1 . . . . . . . . . . . .   _________   Character value
  Part 2 . . . . . . . . . . . .   _________
                                                                  More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

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

   Set the **`Password`** field to a valid password, to **`*SAME`** to keep it the same as the previous password when edited, or to **`*BLANK`** to have no password.

   The **`AuthLevel`** field for each item can have the values:

   - **`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 or 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.

Display Authorization Status

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

1. Select **`22. Display Authorization Status`** from the **BASE Support** menu (*STRAUD* **`> 89 > 22`**). The **Status of iSecurity Authorization** screen appears.

```
 44DE466  520 7459    Status of iSecurity Authorization      LPAR Id 1 S520
Type choices, press Enter.                Subset by . . . . . _______________
 1=Select                                 Warning days before expiration . 14

Opt Lib.   Status      Release ID      Product
 _  SMZ4-A Demo 19-08  14.04 19-06-27  *BASE, Audit, Action, SIEM, MSys, CmpEvl
     Auth code: 499999999999 1            Valid until 2019-08-31
 _  SMZ4-B Demo 19-08  14.04 19-06-27  Compliance (User,Native,IFS), Replicate
     Auth code: 499999999999 1            Valid until 2019-08-31
 _  SMZ8   Demo 19-08  18.06 19-07-14  Firewall, Screen, Command, Password
     Auth code: 899999999999 1            Valid until 2019-08-31
 _  SMZJ   Demo 19-08  09.05 19-07-16  AP-Journal, Update-Control
     Auth code: J99999999999              Valid until 2019-08-31
 _  SMZO   Demo 19-08  05.09 19-05-21  Authority on Demand,Pwd-Reset
     Auth code: O99999999999              Valid until 2019-08-31
 _  SMZC   Demo 19-08  05.00 18-10-08  Capture, w/BI
     Auth code: C99999999999 123          Valid until 2019-08-31
 _  SMZT   Demo 19-08  01.35 19-07-10  Change Tracker
     Auth code: T99999999999 *ALL         Valid until 2019-08-31
 _  SMZV   Demo 19-08  06.98 18-03-20  Antivirus, Anti-Ransomware, ICAP
     Auth code: V99999999999 1            Valid until 2019-08-31
                                                                      More...
F3=Exit   F10=Authority Code
```

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.

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 **`51. Work with Collected Data`** from the **BASE Support** screen (*STRAUD*> **`89 > 51`**). 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
```

2. Enter **`2 (Audit)`** and press Enter. The **Work with Collected Data –**

Audit screen appears.

```
                 Work with Collected Data - Audit                      S520

Type options, press Enter.                          Total Size (MB):       502.8
  4=Delete

Opt Collected Date    Records  Size (MB)  Save Date  Save Time
 _   16/07/19          19,907      90.2   22/07/19   23:51:37
 _   17/07/19          28,430     111.2   22/07/19   23:51:37
 _   18/07/19          10,619      45.1   22/07/19   23:51:37
 _   19/07/19           7,412      27.6   22/07/19   23:51:37
 _   20/07/19          11,225      54.1   22/07/19   23:51:37
 _   21/07/19          14,066      69.3   22/07/19   23:51:37
 _   22/07/19          15,479      78.2   22/07/19   23:51:37
 _   23/07/19           5,950      27.1

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

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

Purging all AUDIT data

You can purse all AUDIT data.

WARNING: Before you run these commands, back up the Audit data to offline storage.

To purge all Audit data, run these commands:

- *RMVM SMZ4DTA/AUXX *ALL*
- *CLRPFM SMZ4DTA/AUSTTSP*

Purging all AUDIT data

You can purse all AUDIT data.

WARNING: Before you run these commands, back up the Audit data to offline storage

To purge all Audit data, run these commands:

- *RMVM SMZ4DTA/AUXX *ALL*
- *CLRPFM SMZ4DTA/AUSTTSP*

Check Locks

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

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

```
GSLCKMNU                          Check Locks                          iSecurity
                                                                System:   S520
Select one of the following:

Check Locks
   1. Data Base Files

   -. Display Files
      End this session. From a new session, enter: CHKSECLCK TYPE(*DSPF)

   -. All File Types
      End this session. From a new session, enter: CHKSECLCK TYPE(*ALL)





Selection or command
===> ____________________________________________________________________________
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

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

Setting up the *PRINT1-*PRINT9 Printers and *PDF Output

You can 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 that you can enter in the OUTPUT parameter of any commands or options that support printed output.

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

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

- **`*PRINT3`** creates an excel file.
- **`*PRINT3-9`** are user modifiable

To define remote printers:

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

```
                              Printer Files Setup

Select one of the following:

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





Selection ===>     _





F3=Exit
```

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

```
                            *PRINT1-*PRINT9 Setup

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    __________ __________   _  _   ____________________________________
   4    __________ __________   _  _   ____________________________________
   5    __________ __________   _  _   ____________________________________
   6    __________ __________   _  _   ____________________________________
   7    __________ __________   _  _   ____________________________________
   8    __________ __________   _  _   ____________________________________
   9    __________ __________   _  _   ____________________________________
                                                                     Bottom

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

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

- **OUTQ()** : 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, for ***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:

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

```
                              Printer Files Setup

Select one of the following:

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









Selection ===>     _









F3=Exit
```

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...
```

3. Follow the instructions on the screen.

NOTE: You must repeat this task after every upgrade of the Base System.

*PDF Setup

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

To define PDF printers:

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

```
                              Printer Files Setup

Select one of the following:

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









Selection ===>     _









F3=Exit
```

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...
```

3. Follow the instructions on the screen.

NOTE: You must re-perform this task after every upgrade of the Base System.

Global Installation Defaults

Global installation configuration now includes access to the Raz-Lee Support Menu. Customers should not use it without guidance. It includes:

- Adding a system to enter field help and possible values for all fields in Query Generator and Logs in all products
- Setting of Default Report Summaries

You can set the parameters that iSecurity uses to control the Installation and upgrade processes. The option includes a Product-Admin Email and SYSTEM was added to the query mail subject line.

NOTE: Consult Raz-Lee support staff at support@razlee.com before changing any of the values on this form.

Select **`59. Global Installation Defaults`** from the **BASE Support** menu (*STRAUD* **`> 89 > 59`**). The **Global Site Defaults - Menu** screen appears.

```
                         Global Site Defaults - Menu                iSecurity

 1. Installation
 2. Run Time Attributes
 3. Output and Logo
 4. Syslog (SIEM) Support
 5. Product Behavior
 6. E-Mail definitions and Java Path
 7. Character Set for Person Names

 9. Post Installation Changes









 Select option ===> _

                                                                     More...
 F3=Exit   F12=Cancel
```

The items in the menu lead to seven further screens. You can also use the **PgUp** and **PgDn** keys to move among them:

Installation

```
                    Global Site Defaults - Installation              iSecurity

General purpose cmd library . . .  QGPL      

ASP for data libraries  . . . . .  01

Wait for STROBJCVN to end . . . .  Y           Y=Yes

Auto journal definition files . .  N           Y=Yes

SBS to start iSec after IPL . . .  QSYSWRK    *LIBL     

Allow group access to IFS . . . .  Y           Y=Yes

Refresh Z* report definitions . .  N           Y=Yes, A=Add new
Z* reports are provided with the products. User should use other names.

First day of work week  . . . . .  _           1=Monday, 2=Sunday, 3=Saturday
For backward compatibility, blank is considered Sunday.


                                                                      More...
F3=Exit   F12=Cancel
```

The **Installation** page includes these fields:

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 which are 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.

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 in parallel to the installation. If you want the conversion to run inline, (wait until it ends), this field should be set to **Y**.

The default value, which Raz-Lee recommends, is **N**.

Auto journal definition files

Y: Yes

N: No

SBS to start iSec after IPL

The Subsystem name and library to use for the Autostart Job.

Allow group access to IFS

Allow access to IFS from group profiles.

Y: Yes

N: No

Refresh Z* report definitions

Y: Yes

A: Replace all

First day of work week

The day on which the work week begins. If left blank, this defaults to Sunday.

Run Time Attributes

```
                  Global Site Defaults - Run Time Attributes         iSecurity

Product-Admin Email . . . . . . .  victor@razlee.com

Days before to warn Code-Expires.  15

Special Customer Id.  . . . . . .  __       Raz-Lee Support Restricted Usage

                                                                       More...
F3=Exit   F12=Cancel
```

The **Run Time Attributes** page includes these fields:

Product-Admin Email

The email of the product admin to send automated messages to.

Days before to warn Code-Expires

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.

Special Customer ID

To be used only by Raz-Lee Support.

Output and Logo

```
                        Global Site Defaults - Output                iSecurity

Append date to report gen files .  _           Y=Yes, S=Subject, B=Both

Add SYSTEM to query mail subject.  Y           Y=Yes. D=For AOD, B=Body

Use old PDF generation  . . . . .  N           Y=Yes

Excel extension . . . . . . . . .  .xml        .xls, .xml

Set SPLF attribute to query name.  U           U=USRDTA, N=No

Attach empty reports  . . . . . .  Y           Y=Yes

Use group text as ZIP file name .  N           Y=Yes, N=Use group name

Setting your Logo for PDF reports
Rename /iSecurity/LOGO/LOGO.JPG to LOGO-RAZLEE.JPG and place yours instead.
File should be no more than 110 x 50 pixels, 120 DPI.


                                                                      More...
F3=Exit   F12=Cancel
```

The **Output** page includes these fields:

Append date to report gen files

Y: Yes

N: No

B:Both

Add SYSTEM to query mail subject

Y: Yes

D: For Authority on Demand

B: Body

Use old PDF generation

Whether to use the older method of generating PDFs, rather than the current method.

Y: Yes

N: No

Excel extension

The extension to be used when creating Excel files

Set SPLF attribute to query name

Whether to set the SPLF attribute in a query to USRDTA

Placing Your Organization's Logo on Reports

The screen also describes how to place your own logo on reports. In the product, as shipped, the file **/iSecurity/LOGO/LOGO.JPG** contains the Raz-Lee logo. Rename this file to **LOGO-RAZLEE.JPG**. Place your own logo in the **LOGO.JPG** file. It must be no more than 110 pixels wide by 60 pixels tall, at 120 DPI.

Syslog (SIEM) Support

```
                 Global Site Defaults - Syslog (SIEM) Support        iSecurity

                            Leave blank for defaults
Syslog source Port/IP 1 .   _____  ________________________________________
              Port/IP 2 .   _____  ________________________________________
              Port/IP 3 .   _____  ________________________________________

TLS DCM Applic. ID SIEM 1   SUMO________________________________________________
                   SIEM 2   SUMO________________________________________________
                   SIEM 3   1.1.1.192____________________________________________


Std CEF Ext. fld. names .   Y           Y=Yes

Include QAUDJRN Seq. Num.   N           Y=Yes
Helps identify the original message.

*AUTO Level of message  .   1           1=1st-*AUTO1, 2=2nd-*AUTO2
The meaning of *AUTO when specified: 1st/2nd level of message.


                                                                      More...
F3=Exit   F12=Cancel
```

The Syslog (SIEM) Support page includes these fields:

Syslog source Port/IP 1, 2, 3

Syslog port source IP for each of the three Syslog sources

TLS DCM Applic. ID SIEM 1, 2, 3

TLS ID for SIEM application for each of the three Syslog sources

Std CEF Ext. fld. names

Whether to use standard external Common Event Field names, which include the company and product names.

Y: Yes

N: No

Include QAUDJRN Seq. Num.

Whether to include QUADJRN sequence numbers. These might be useful in tracking back to the source of Syslog messages.

Y: Yes

N: No

***AUTO Level of message**

Whether *AUTO, when specified, means the first or second level of message.

1=1st-*AUTO1

2=2nd-*AUTO2

Product Behavior

```
                    Global Site Defaults - Product Behavior           iSecurity

GUI must run in SSL . . .  N           Y=Yes

Use IBM std auto disable.  Y           Y=Yes (IBM), E=Extended (iSec, generic*)
On change, set ANZPRFACT accordingly.

Mask User name & text . .  ?--%-%----  ?=Display, %=Display, random if blank
Masks sensitive info in the report of user profiles that have default passwords

AP-Journal shares Groups.  _           Y=Yes, share Audit groups
Reference to General Groups in AP-Journal is to the groups in Audit.

Firewall shares Groups  .  I           Y=Yes, share Audit groups, I=Items only
Reference to General Groups in Firewall is to the groups in Audit.
As soon as you change this, use STRFW, 82, 99, 5. to merge the values.





                                                                      More...
F3=Exit   F12=Cancel
```

The Product Behavior page includes these fields:

GUI must run in SSL

Whether the GUI must run in SSL mode.

Y: Yes

N: No

Use IBM std auto disable

How ANZPRFACT is set on changes.

Y=Yes (IBM)

E=Extended (iSec, generic*)

Mask User name & text

How to mask sensitive info in the report of user profiles that have default passwords.

?: Display

%: Display

Blank: Random character

AP-Journal shares Groups

Whether references to General Groups in AP-Journal are to the groups in Audit.

Y: Yes, share Audit groups

Firewall shares Groups

Whether references to General Groups in AP-Journal are to the groups in Audit.

Y: Yes, share Audit groups

I: Items only

As soon as you change this, use **STRFW > 82 > 99 > 5** to merge the values.

E-Mail Definitions and Java Path

```
            Global Site Defaults - E-Mail definitions and Java Path    iSecurity

Email type  .  J                A=Auto, J=Java, I=IBM-API


When setting I=IBM-API, a directory entry is created in the system directory,
where USRID is RLSNDM, the address is system name and the user is SECURITY2P.
SECURITY2P is also defined as a SMTP user.
For other requirements, see
  https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/cl/sndsmtpemm.htm


Java path . .  /qopensys/QIBM/ProdData/JavaVM/jdk80/64bit/bin/java
Leave empty if the Java system default corresponds the email needs. Otherwise,
use the format /qopensys/QIBM/ProdData/JavaVM/jdk80/64bit/bin/java





                                                                        More...
F3=Exit   F12=Cancel
```

The **E-Mail Definitions and Java Path** page includes the following fields:

Email type

A: Auto

J: Java

I: IBM-API

When setting I=IBM-API, a directory entry is created in the system directory, where USRID is RLSNDM, the address is system name and the user is SECURITY2P. SECURITY2P is also defined as a SMTP user. For other requirements, see https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/cl/sndsmtpemm.htm

Java path

The path to the Java executable on your system. In many cases, the default value is accurate. If it is not, change it to refer to the actual location on your system.

Character Set for Person Names

```
             Global Site Defaults - Character Set for Person Names     iSecurity

Character set for names . . . . .  2     1=No check
                                         2=Is compatible with CCSID  273
                                         5=CCSID 640 + #@
                                         6=CCSID 640 + #@$^~[\]{|}!`
CCSID 640 represents all English alphanumeric in upper and lower case. These
characters have the same hex code in all single byte CCSID, except CCSID 290.
i.e. ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz-%&()*,./:;?_'"+<=>
We recommend using options 5 or 6 in a multi-language environment.

                                                                        More...
F3=Exit   F12=Cancel
```

To define the character set for Person names, enter the value corresponding to the set in the Character set for name field:

- **1**: Do not check the character set
- **2**: CCSID 273 (used in Austria and Germany)
- **5**: CCSID 640, which incorporates all uppercase and lowercase English letters, plus the characters **#** and **@**.
- **6**: CCSID 640, plus the following characters: **#@$^~[\]{|}!`**

Post Installation Changes

```
                Global Site Defaults - Post Installation Changes

Place Site modifications in program datalib/xxUPGRADE e.g. SMZ4DTA/AUUPGRADE
When such a program exists, it is called automatically after products upgrades.

                                                                        Bottom
F3=Exit   F12=Cancel
```

To make changes after installation, follow the instructions on the **Post-Installation Changes** page.

Network Support

Work with network definitions

To get current information from existing report or query, adjust system parameters, or to collect information from all the groups in the system into output files that can be sent via email, open the **Work with Network Systems** screen by selecting **`71. Work with network definitions`** from the **BASE Support** menu (*STRAUD*> **`89 > 71`**).

NOTE: Whenever you create or modify a network definition. you must re-enter the password in the **Network Authentication** screen, as shown in "Network Authentication" on page 377.

```
System type: AS400        Work with Network Systems           System: RLDEV
                                                Position to . . . __________
Type options, press Enter.
  1=Select  4=Remove  7=Export dfn.  8=Test DDM  9=Ping

Opt   System    Group
 _    RLDEMO    *TT      Demo system Audit release 14.16
 _    RLDEV     *NONE    Razlee Develop
 _    RLG       *TT      RL Germany
 _    RLMED     *TT      RLEMD
 _    RLPRV     *TT      Razlee Production
 _    RL74A     *VVVV    Demo system
 _    RL74B     *NONE    Test Yoel
 _    VERDE     *NONE    verde





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

To **define a new netwok system**, press the **F6** key. The **Add Network Systems** screen appears:

```
System type: AS400            Add Network System              System: S520

System  . . . . . . . . . .  __________
Description . . . . . . . .  ______________________________________________
Group where included  . . .  *NONE___                 *Name

Communication Details
IP or remote name . . . . .  ______________________________________________
                             ______________________________________________
                             ______________________________
Type  . . . . . . . . . . .  *IP                      *SNA, *IP
Entry of *LOCAL on System .  __________________        Use WRKRDBDIRE to verify
Auto filled for this system. Required for Multi-LPAR of AOD, P-R, Replication.

Copy of QAUDJRN on a different system
Where is QAUDJRN analyzed .  *SYSTEM                   Name, *SYSTEM
Extension Id on remote  . .  ___


Note: After adding a system, run again "Network Authentication".

F3=Exit   F12=Cancel
Modify data, or press Enter to confirm.
```

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 IBM is assigned

Where is QAUDJRN analyzed

Give the name of the System where QAUDJRN is analyzed. Enter **`*IBM`** if it is analyzed locally.

Default extension Id

Enter the extension ID for local copy details

Type

The type of communication this system uses, Valid values are **`*SNA`** and **`*IP.`**

IP or Remote Name

Enter the IP address or SNA Name, depending on the Type of communication you defined.

Enter your required definitions and press **Enter** to confirm.

To **modify a network definition**, enter **1** in the **Opt** field for the definition that you want to modify in the **Work with Network Systems** screen. The **Modify Network System** screen appears, which contains the same fields as the **Add Network System** screen.

Network Authentication

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

1. Select **`72. Network Authentication`** from the **BASE Support** menu (*STRAUD*> **`89 > 72`**). 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 of 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
```

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

Send PTF

This option allows you to run 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, you must

- define the entire network, as described in "Network Definitions" on page 251, and
- define user SECURITY2P on all nodes, using the same password, as described in "Network Authentication" on the previous page.

Select **`74. Send PTF`** from the **BASE Support** Menu (*STRAUD*> **`89 > 74`**). 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, ISECSETUP
Object types . . . . . . . . . .   *ALL     __   *ALL, *ALRTBL, *BNDDIR...
               + for more values   ________
Save file  . . . . . . . . . . .   *LIB     ____  Name, *LIB
  In library . . . . . . . . . .     QGPL    ____ Name
Send SAVF to remote library  . .   *AUTO    ____  Name, *AUTO (RL+job number)
On remote, backup LIB to SAVF  .   *NONE    ____  Name, *NONE, *LIB
  In library . . . . . . . . . .     __________   Name
Restore the objects  . . . . . .   *NONE    ____  Name, generic*, *NONE, *ALL
  Into library . . . . . . . . .     __________   Name, *LIB, *SAVF, ISECSETUP
Call the installation pgm  . . .   *NONE    ____  Name, *NONE
  Library  . . . . . . . . . . .     __________   Name, *LIBL, *RSTLIB

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

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

- **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.

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

Run CL Scripts

WIth the iSecurity Remote Command screen, you can run 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)

Before you can use this option, you must

- define the entire network, as described in "Network Definitions" on page 339, and
- define user SECURITY2P on all nodes, using the same password, as described in "Network Authentication" on page 341.

Select **75. Run CL Scripts** from the **BASE Support** menu (*STRAUD* **> 89 > 75**). 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
 Run on *CURRENT if in *group . .   *NO      __     *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
```

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 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 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**: The library list

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: A save file

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

Displaying Communication Logs

To display the current job log, select **`76. Current Job CntAdm Messages`** from the BASE Support menu (*STRAUD*> **`89 > 76`**).

To display the job log for all jobs, select **`77. All Jobs CntAdm Messages`** from the BASE Support menu (*STRAUD*> **`89 > 77`**)

Appendix A: Raz-Lee Information Sources

The Report Generator and its associated Report Scheduler service all iSecurity products. They are implemented with its full capacity in both Green and GUI environments.

This appendix contains the list of types of information that are included for each products.

Each of these types is an information source. Their names are two characters long.

All products come with example reports. The example report names that are sent with the product start with **Z_xx**…., where **xx** is the information source.

Some types refer to static information such as attributes of User profiles, Object descriptions or values of System values. Usually such start with $ or #.

Other represent Audit Types that appear in QAUDJRN. Such are usually alphabetical.

Firewall servers are denoted by 2 digits.

Summary of Raz-Lee Entry Types

iSecurity uses several unique additional information types:

$9	Enables any command or call to a program that produces one or more spool files to become a part of the report generator capabilities. $9 can include the Display xx Definition (DSPxxDFN) Command, enabling incorporation of all definition information.
00	All information types for Firewall and Screen
A#	All types of QAUDJRN
A$	All types of QAUDJRN containing Library & Object
$@	History Log (QHST)
$8	Query log report. Information of any run of a report and its output

- **$@**- History Log
- **A$**- All types of QAUDJRN containing Library and Object

- **A#**- All types of QAUDJRN
- **C@**- User Profile Changed (After and Previous Images)

Report Generator Capabilities

Output

Screen, GUI, *PRINT, *PRINT1-9 (special user settings for print), PDF, HTML, CSV, OUTFILE (output file by fields)

Select (Filter)

The following TEST operations are supported:

- **EQ**, **NE**, **LE**, **GE**, **LT**, **GT**
- **LIST**, **NLIST** (Not LIST), **LIKE**, **NLIKE** (Not LIKE), **START**, **NSTART** (Not START),
- **ITEM**, **NITEM** (Not ITEM), where a value is checked to see if it is in a group. Supported groups include:
  - ***GRPPRF** User is included in Group/Supplemental profile
  - ***LMTCPB** User Limit Capabilities
  - ***SPCAUT** User has a specified or any Special Authority
  - ***TIMEGRP** Time group – a weekly time table (e.g. after hours and weekends)
  - ***USRGRP** User is included in iSecurity/Firewall Group
  - **General group** Multiple groups ordered in classes such as Users, IPs, Libraries, and Objects. To simplify the setting of a rule, enter **ITEM** or **NITEM** as the TEST and press F4
- **PGM**, **NPGM** (Not Program), a provided or user written program that return True or False. For example, whether the command in CD audit type was entered during elevated authority by Authority On Demand

To simplify the setting of rules, enter **PGM**, **NPGM**, **ITEM**, or **NITEM** as the test and press F4.

General groups can include generic names. ***GENERIC** should follow the named group.

You can combine test with And or Or. And is the default. You can include the same field multiple times.

Sort

The following characteristics are available:

- Multiple Fields
- Ascending or Descending order
- Break after change of a number of sort fields. A title is created containing the specified sort fields. All lines exclude these fields.
- Report can include either all records or one record per key

Summary Sub Reports

While running the main report, data can be grouped in addition sub-reports. For example, when running on objects in a group of libraries, you can create counts of objects by owner or counts of objects by type, or sum objects sizes per library).

Up to 3 Summary Sub Reports can be processed simultaneously.

Data is Counted or a value of a field is Summarized.

Each such report classifies the data based on 1 to 3 fields.

Condition to print lines in a Summary Sub Reports.

The total number of records is always printed.

Explanation

Each report may carry a free format text that explains its contents. This reduces the effort of explaining the intention of the report and saves as its documentation.

Print of Filter

The filter used for the report can be printed.

Print of Header

A place for signing the report after inspecting it can be printed.

Information Types

Information code ID		Where used (products)
$@	History Log	Audit
$A	User profile information	Audit,UserProfile
$B	Objects that are owned by a user	Audit
$C	Objects that a user is their primary group	Audit
$D	Objects for which a user has specific authority	Audit
$E	Job schedule entries	Audit
$F	Command attributes	Audit
$G	Group profile and their users	Audit,UserProfile
$H	File members	Audit
$I	Object description	Audit
$J	Object authority	Audit
$K	Job descriptions with user profile & *PUBLIC=*USE	Audit
$L	Libraries description	Audit
$M	User profile activation schedule	Audit,UserProfile
$N	User profile expiration schedule	Audit,UserProfile
$O	Program/Service-Program information	Audit
$P	Users with default password (Repair by ANZDFTPWD)	Audit,UserProfile
$Q	Programs that adopt authorities	Audit
$R	IFS Objects	Audit
$S	System values	Audit
$T	Network attributes	Audit
$U	Authorization Lists	Audit
$V	Native objects secured by authorization list	Audit
$W	DLO objects secured by authorization list	Audit
$X	Library information [run RTVDSKINF first]	Audit

$Y	Modules of Program/Service-Program	Audit
$0	Audit Statistics processing	Audit
$1	Firewall Statistics processing	Audit
$3	Compliance report	Audit
$8	Query log report	Audit
$9	Interface to any spool file query	All products
#A	System limits trending	Audit,KPI
#C	PTF Groups Installed vs. Available	Audit,ChgTracker,KPI
#G	Group PTF Info	Audit,ChgTracker,KPI
#H	PTF Info	Audit,ChgTracker,KPI
#K	Netstat information	Audit,KPI
#L	NETSTAT interface information	Audit,KPI
#M	NETSTAT routing information	Audit,KPI
#N	NetStat job info	Audit,KPI
#Q	AU TCP/IP information	Audit
#R	Current server information	Audit,KPI
#S	List of Servers-Share info	Audit
#U	System status	Audit,KPI
#V	System memory pool information	Audit,KPI
#W	AU Active jobs	Audit
#X	Disk status	Audit,KPI
#Y	Output queue information (summary)	Audit,KPI
#Z	License Information	Audit
@J	Active job information	Audit
@K	Job NOT active	Audit
@P	Pool NOT active	Audit
@Q	Active JobQ/OutQ information	Audit
@S	System status and pool information	Audit
@0	Message queue (Group Id 0)	Audit
@1	Message queue (Group Id 1)	Audit
@2	Message queue (Group Id 2)	Audit
@3	Message queue (Group Id 3)	Audit

@4	Message queue (Group Id 4)	Audit
@5	Message queue (Group Id 5)	Audit
@6	Message queue (Group Id 6)	Audit
@7	Message queue (Group Id 7)	Audit
@8	Message queue (Group Id 8)	Audit
@9	QHST messages	Audit
A$	All types of QAUDJRN containing Library & Object	Audit
A#	All types of QAUDJRN	Audit
AD	Auditing changes	Audit
AF	Authority failure	Audit
AP	Obtaining adopted authority	Audit
AU	Attribute change	Audit
AX	Row and Column Access Control (RCAC)	Audit
C@	User profile changed (After & Previous images)	Audit,UserProfile
CA	Authority changes	Audit
CD	Command string audit	Audit,AOD
CF	Mail configuration info (QZMF)	Audit
CO	Create object	Audit
CP	User profile changed, created, or restored	Audit,UserProfile
CQ	Change of *CRQD object	Audit
CU	Cluster operations	Audit
CV	Connection verification	Audit
CY	Cryptographic configuration	Audit
D@	Command checked	Command
DI	Directory services	Audit
DO	Delete object	Audit
DP	Direct print info (QACGJRN)	Audit
DS	DST security password reset	Audit
ER	Mail error info (QZMF)	Audit

EV	System environment variables	Audit
GR	Generic record	Audit
GS	Socket description was given to another job	Audit
IM	Intrusion monitor	Audit
IP	Interprocess communication	Audit
IR	IP rules actions	Audit
IS	Internet security management	Audit
JB	Job resource info (QACGJRN)	Audit
JD	Change to user parameter of a job description	Audit
JS	Actions that affect jobs	Audit
KF	Key ring file	Audit
LD	Link, unlink, or look up directory entry	Audit
LG	Mail logging table info (QZMF)	Audit
ML	Office services mail actions	Audit
MP	QoS policies Modification (QQOS)	Audit
NA	Network attribute changed	Audit
ND	APPN directory search filter violation	Audit
NE	APPN end point filter violation	Audit
OM	Object move or rename	Audit
OR	Object restore	Audit
OW	Object ownership changed	Audit
O1	Optical access: Single file or directory	Audit
O2	Optical access: Dual file or directory	Audit
O3	Optical access: Volume	Audit
P@	Password Reset	P-R
PA	Program changed to adopt authority	Audit
PF	PTF Operations	Audit
PG	Change of an object's primary group	Audit
PO	Printed output	Audit
PS	Profile swap	Audit
PU	PTF Object Change	Audit

PW	Invalid password	Audit
RA	Authority change during restore	Audit
RJ	Restoring job description with profile specific	Audit
RO	Change of object owner during restore	Audit
RP	Restoring adopted authority program	Audit
RQ	Restoring a *CRQD object	Audit
RU	Restoring user profile authority	Audit
RZ	Changing a primary group during restore	Audit
SD	Changes to system distribution directory	Audit
SE	Subsystem routing entry changed	Audit
SF	Actions to spooled files	Audit
SG	Asynchronous Signals	Audit
SK	Sockets Connections (IP/Port)	Audit
SM	System management changes	Audit
SN	Simple Network Management Protocol (SNMP) informat	Audit
SO	Server security user information actions	Audit
SP	Spooled print info (QACGJRN)	Audit
ST	Use of service tools	Audit
SV	System value changed	Audit
SY	Mail system info (QZMF)	Audit
TF	IP filter rules actions (QIPFILTER)	Audit
TN	IP NAT rules actions (QIPNAT)	Audit
TS	VPN information (QVPN)	Audit
VA	*REMOVED BY IBM* Changing an access control list	Audit
VC	*REMOVED BY IBM* Starting or ending a connection	Audit
VF	*REMOVED BY IBM* Closing server files	Audit

-

VL	*REMOVED BY IBM* Account limit exceeded	Audit
VN	*REMOVED BY IBM* Logging on and off the network	Audit
VO	Validation list actions	Audit
VP	Network password error	Audit
VR	*REMOVED BY IBM* Network resource access	Audit
VS	*REMOVED BY IBM* Starting/ending a server session	Audit
VU	*REMOVED BY IBM* Changing a network profile	Audit
VV	*REMOVED BY IBM* Changing service status	Audit
XD	Directory server extension	Audit
XE	DSNX error entry (QDSNX)	Audit
XL	DSNX logging entry (QDSNX)	Audit
X0	Network Authentication	Audit
X1	Identity token	Audit
X2	Query Manager profile values.	Audit
YC	DLO object accessed (change)	Audit
YR	DLO object accessed (read)	Audit
ZC	Object accessed (change)	Audit
ZM	SOM method access (no longer used by IBM)	Audit
ZR	Object accessed (read)	Audit
00	Generic entry type (00-99 for reporting only)	Firewall
01	*FILTFR Original File Transfer Function	Firewall
02	*FTPLOG FTP Server Logon	Firewall
03	*FTPSRV FTP Server-Incoming Rqst Validation	Firewall
04	*SQL Database Server - SQL access	Firewall
05	*RMTSRV Remote Command/Program	Firewall

	Call	
06	*FILSRV File Server	Firewall
07	*DDM DDM request access	Firewall
08	*TELNET Telnet Device Initialization	Firewall
09	*TFTP TFTP Server Request Validation	Firewall
1K	*FW-DFN Native Object Security	Firewall (dfn)
1L	*FW-DFN IFS object security	Firewall (dfn)
1M	*FW-DFN Command Exceptions	Firewall (dfn)
1N	*FW-DFN Users & Groups	Firewall (dfn)
1Y	iSecurity groups members	Audit
10	*REXLOG REXEC Server Logon	Firewall
11	*REXEC REXEC Server Request Validation	Firewall
12	*RMTSQL Original Remote SQL Server	Firewall
13	*NDB Database Server - data base access	Firewall
14	*WSG WSG Server Sign-On Validation	Firewall
15	*ORDTAQ Original Data Queue Server	Firewall
16	*DTAQ Data Queue Server	Firewall
17	*MSGSRV Original Message Server	Firewall
18	*SQLENT Database Server - entry	Firewall
19	*OBJINF Database Server - object information	Firewall
20	*VPRT Original Virtual Print Server	Firewall
21	*NPRENT Network Print Server - entry	Firewall
22	*NPRSPL Network Print Server - spool file	Firewall
23	*CHGUP Change User Profile	Firewall
24	*CRTUP Create User Profile	Firewall
25	*DLTUPA Delete User Profile - after delete	Firewall
26	*DLTUPB Delete User Profile	Firewall
27	*RSTUP Restore User Profile	Firewall

-

28	*ORLICM Original License Mgmt Server	Firewall
29	*CSLICM Central Server - license mgmt	Firewall
30	*CSCNVM Central Server - conversion map	Firewall
31	*CSCLNM Central Server - client mgmt	Firewall
32	*TCPSGN TCP Signon Server	Firewall
33	*PWRDWN Prepower Down System	Firewall
34	*RMTSGN Remote sign-on (Passthrough)	Firewall
35	*PWDVLD Password Dictionary Check / Validation	Firewall
36	*DRDA DRDA Distributed Relational DB access	Firewall
37	*FTPCLN FTP Client-Outgoing Rqst Validation	Firewall
38	*TELOFF Telnet Device Termination	Firewall
39	*DHCPAB DHCP Address Binding Notify	Firewall
40	*DHCPAR DHCP Address Release Notify	Firewall
41	*DHCPRP DHCP Request Packet Validation	Firewall
42	*SIGNON Sign-On completed	Firewall
43	*PWDCHK Password Dictionary Check / Check	Firewall
44	*SSHD SSH Daemon	Firewall
45	*DBOPEN Open Database	Firewall
46	*PWDVL2 Password Dictionary Check /Validation fmt2	Firewall
47	*SKTACP Socket Accept	Firewall
48	*SKTCNT Socket Connect	Firewall
49	*SKTLSN Socket Listen	Firewall
5A	Tracking Data (Native/IFS/PTF/Source)	ChgTracker
5B	ILE Modules Inventory	ChgTracker

5D	Definition of IFS Directories	ChgTracker
5F	PTF Status	ChgTracker
5G	PTF Advanced status (Rel 7.2)	ChgTracker
5I	Definition of Activity to Disregard	ChgTracker
5J	Definition of Environments	ChgTracker
5L	Definition of Libraries to Trace	ChgTracker
5M	Definition of Projects	ChgTracker
5N	Definition of Tasks	ChgTracker
5R	Definition of IFS Directories to Disregard	ChgTracker
5W	Tracking Data (Native Objects)	ChgTracker
5X	Tracking Data (Source Members)	ChgTracker
5Y	Tracking Data (IFS Objects)	ChgTracker
5Z	Tracking Data (PTF Objects)	ChgTracker
50	*DBSTT Database statistics	Firewall
6A	Object Journaling Plan	AP-Journal
6B	Object check Journaling Plan	AP-Journal
6C	Confirmation tickets	AP-Journal
6I	AOD History	AOD
6V	Virus, Worm, Trojan, Ransomware detected	Antivirus
6X	Person - Attributes	P-R
6Y	Users of a Person	P-R
6Z	Log of who changed questions	P-R
7E	User Compliance Check	Action
7F	User Compliance Plan	Action
7I	Native Object Compliance Check	Action
7J	Native Object Compliance Plan	Action
7M	IFS Object Compliance Check	Action
7N	IFS Object Compliance Plan	Action
97	*SCRLCK Screen locked due to timeout	Firewall
98	*SCRRLS Screen released	Firewall
99	*SCREND Screen jobs ended as	Firewall

timeout passed

Appendix B: configuring CEF format for Apache and WebSphere login records

Disclaimer

This guide refers to products and services that are not under Raz-Lee product's umbrella. Use the information in this Appendix under your own risk and discretion. Raz-Lee is not responsible for any damages whatsoever that may happen using this procedure.

Appendix objective

This Appendix demonstrates how to successfully configure Apache or IBM Websphere webservers to send login records (or messages) in the format of Common Event Format (CEF).

Configuring CEF output for Apache web server

To configure CEF output for Apache web server:

1. Find the relevant Apache configuration file which contains the logs settings.
2. Open it using an editor.
3. Select the desired log you wish to configure CEF output. There are three types of directives:
    - Errorlog.
    - CustomLog.
    - GlobalLog.
4. Once the desired directive is found, look for the directive LogFormat.
5. Right after the "LogFormat" directive, enter a space and type a quotation mark (") before and after the desired value parameters mentioned below section 8.
6. Right after the closing quotes, add the desired nickname. Normally it would be "cef".
7. The content of the configuration varies, depending whoever the protocol is HTTP or HTTPS.

It is up to the user's discretion to decide which kind of parameters (marked as %X) they would like to use.

NOTE: In Apache the division of fields is through the pipe "|" symbol.

Below is an example of such parameters:

HTTP protocol:

LogFormat "CEF:0|Apache|apache||%>s|%m %U%q|Unknown|end=%{%b %d %Y %H:%M:%S}t app=HTTP cs2=%H suser=%u shost=%h src=%a dhost=%V dpt=%p dproc=apache request=%U requestMethod=%m fname=%f cs1Label=Virtual Host cs1=%v cn1Label=Responce Time cn1=%T out=%B cs4Label=Referer cs4= %{Referer}i dvchost=%v dvc=%A deviceProcessName=apache_access_log

requestClientApplication=%{User- Agent}i cs3Label=X-Forwarded-For cs3=% {X-Forwarded-For}I" cef

HTTPS:

LogFormat "CEF:0|Apache|apache||%>s|%m %U%q|%>s|end=%{%b %d %Y %H:%M:%S}t app=%H proto=TCP cs2=%H suser=%u shost=%h src=%a dhost=%V dpt=%p dproc=apache request=https://%{HOST}i:%p%U%q requestMethod=%m fname=%f cs1Label=Virtual Host cs1=%v cn1Label=Response Time cn1=%T in=%I out=%B cs4Label=Referer cs4=%{Referer}i cs5Label=SSL Protocol cs5=%{SSL_PROTOCOL}x cs6Label=SSL CIPHER cs6=%{SSL_CIPHER}x dvchost=%v dvc=%A deviceProcessName=apache_access_log

requestClientApplication=%{User-Agent}i cs3Label=X-Forwarded-For cs3=%{X-Forwarded-For}I" cef

For example:

- **%a** = Client IP address of the request (see the mod_remote ip module)
- **%A** = Local IP-address
- **%m** = The request method

NOTE: A legend of %X parameters can be found at http://httpd.apache.org/docs/current/mod/mod_log_config.html

Configuring CEF output for IBM Websphere web server

Use the `IS_install_path/wlp/usr/servers/iis/server.xml` configuration file to configure logging messages for WebSphere® Application Server Liberty Core. The log files are produced in the `IS_install_path/wlp/usr/servers/iis/logs` folder.

The user must configure the logging messages in two sections: Network deployment and Application Server Liberty Profile:

To configure WebSphere Application Server Network Deployment:

1. Log in to the WebSphere Application Server administrative console.
2. Go to **`Troubleshooting > Logs and trace > <servername>`**.
3. Configure the logging options that you desire. For more information, see Configuring Java™ logging using the administrative console.
4. Save your changes to the master configuration.

To configure the WebSphere Application Server Liberty Profile:

1. Open the `IS_install_path/wlp/usr/servers/iis/server.xml` configuration file.
2. Configure logging related information. Use the comments in the server.xml file to add or change what types of messages are logged.
3. Save your changes.

The configuration is the same for HTTP or HTTPS.

It is up to the user's discretion to decide which kind of parameters (marked as %X) they would like to use.

Below is an example of such values:

HTTP, HTTPS protocols:

CEF:0|WebSphere|websphere||%>s|%m %U%q|%>s|end=%{%b %d %Y %H:%M:%S}t app=%H proto=TCP cs2=%H shost=%h src=%a dhost=%v dpt=%p dproc=websphere request=https://%{HOST}i:%p%U%q requestMethod=%m cs1Label=Virtual Host cs1=%v cn1Label=Response Time cn1=%T in=%I out=%B cs4Label=Referer cs4=%{Referer}i dvchost=%v dvc=%A deviceProcessName=websphere_access_log requestClientApplication=%{User-Agent}i cs3Label=X-Forwarded-For cs3=%{X-Forwarded-For}i

NOTE: A legend of %X parameters can be found at the following link:

`https://www.ibm.com/support/knowledgecenter/en/SSAW578.5.5/com.ibm.websphere.nd.doc/ae/cwve_xdcustomlog.html`

Restart WebSphere Application Server for the configuration changes to take effect.

Appendix C: Analyzing QAUDJRN on Other Systems

Preparing the Systems for Remote Auditing

[[[Undefined variable Audit.ProductName]]]allows you to audit other systems in your network. Before you can do this, you must prepare both the system where you want to run the audit (your local system) and the system that you want to audit (the remote system).

On the remote system:

1. Use the *WRKRDBDIRE* command to get the RDB-name of the *LOCAL entry.
2. Make a note of the RDB name. You will need it when configuring the local system.
3. In the [[[Undefined variable Audit.ProductName]]]main menu, select **`89. Base Support`** (*STRAUD* **`> 89`**). The BASE Support menu appears.
4. Select **`71. Work with network definitions`**. The Work with Network Systems screen appears.
5. Type **`1`** for each system and define it to the network in the Modify Network System screen.
6. Set **`Where is QAUDJRN analyzed`** to the proper system name of the local system.
7. Enter a unique ID in **`Default Extension Id`**.

On the local system:

1. Use the *WRKRDBDIRE* command to verify that you defined the remote system. If not, enter the following command: *ADDRDBDIRE RDB(<RDB_NAME>) RMTLOCNAME('<IP_ADDRESS>' *IP)*
   - <RDB_NAME> - Enter the RDB name you noted above.
   - <IP_ADDRESS> - Enter the IP Address of the remote system.
2. Enter the following command:
   ADDRMTJRN RDB(<RDB_NAME>) SRCJRN(QSYS/QAUDJRN) +
   TGTJRN(SMZ4DTA???/QAUDJRN) / ???="Default Extension Id." */*
3. Enter the following command:
   *SBMJOB AUCATCHUP CMD(CALL SMZ4/AURMQAUD *ACTIVE)*

4. Add the *SBMJOB* command from the previous step to the IBM i startup program.
5. In the [[[Undefined variable Audit.ProductName]]] main menu, select **`89. Base Support`** (*STRAUD* **`> 89`**). The BASE Support menu appears.
6. Select **`71. Work with network definitions`**. The Work with Network Systems screen appears.
7. Type **`1`** for each system and define it to the network in the Modify Network System screen.

To see a brief version of these instructions online:

1. Select **`1. Setup Instructions`** in the **`Analyzing QUADRJN on another system`** menu (*STRAUD* **`> 2 > 41 > 1`**).

Activation of Remote Auditing

For the Remote System (The System being Analyzed):

When you have finished preparing both systems, you can activate the collection of data either on the remote system or on the local system.

To **start data collection directly on the remote system**:

1. Select **`2.`** in the main [[[Undefined variable Audit.ProductName]]]menu. The Activation menu appears.
2. Select **`41. Setup Analyzing QAUDRN`**. The **`Analyzing QAUDRJN`** on another system menu appears.
3. Select **`51. Activate in the Analyzing QAUDRJN on another system`** . The system sends a command to the remote system to activate audit real-time detection.

To **stop data collection directly on the remote system**:

1. Select **`2. Activation`** in the main [[[Undefined variable Audit.ProductName]]]menu. The **`Activation`** menu appears.
2. Select **`41. Setup`**. The **`Analyzing QAUDRJN on another system`** menu appears.
3. Select **`52. Deactivate`**. The local system sends a command to the remote system to stop audit real-time detection.

To **work with journal attributes**:

1. Select **`2. Activation`** in the main [[[Undefined variable Audit.ProductName]]]menu. The **`Activation`** menu appears.
2. Select **`41. Setup`**. The **`Analyzing QAUDRJN on another system`** menu appears.
3. Select **`55. Work with journal status`**. The **`Work with Journal Attributes`** screen appears.

```
                          Work with Journal Attributes

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

Attached receiver  . :   AUDITR0027      Library  . . . . . . :   QGPL

Text . . . . . . . . :

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
```

For the Local System (The System Where the Analysis is Done)

To start data collection directly on the remote system:

1. Select **2. Activation** in the main [[[Undefined variable Audit.ProductName]]]menu. The **Activation** menu appears.
2. Select **41. Setup**. The **Analyzing QAUDRJN on another system** menu appears.
3. Select **61. Activate**. The **Submit Audit Remote Command** screen appears.

```
                    Submit Audit Remote Command (AURMTCMD)

Type choices, press Enter.

System to run on . . . . . .   ________      Name, *group, *ALL..
Run only on source of QAUDJRN  . > *YES         *ALL, *YES, *NO
Command to run . . . . . . . . > CALL PGM(SMZ4/AURMQAUD) PARM(*ACTIVE)

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

To stop data collection directly on the remote system:

1. Select **2. Activation** in the main [[[Undefined variable Audit.ProductName]]]menu. The **Activation** menu appears.
2. Select **41. Setup**. The **Analyzing QAUDRJN on another system** menu appears.
3. Select **62. Deactivate**. The Submit Audit Remote Command screen appears.
4. Enter the name of the remote system and press **Enter**. The command is sent to the remote system.

Appendix D Audit Command Reference

The following pages document commands within Audit.

Check Raz-Lee Authorization (CHKISA)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Check Raz-Lee Authorization (CHKISA) command checks the authorization status of iSecurity products on one or more LPARs.

Top

Parameters

Keyword	Description	Choices	Notes
PRD	Product ID or *ALL	***ALL**, AU, NS, GS, GR, CA, JR, OD, AV, CT, DB, VW, EN, SA, FS, CS	Optional, Positional 1
SYSTEM	System to run for	*Character value*, ***CURRENT**, *ALL	Optional, Positional 2
SYSOPR	Inform *SYSOPR about problems	*YES, ***NO**	Optional, Positional 3
WRNDAYS	Days to warn before expir-ation	*Decimal number*, ***DFT**	Optional, Positional 4
CHKDBG	Check if in FYI/Debug mode	*YES, ***NO**	Optional, Positional 5
CHKSIZE	Check Data Size	*YES, ***NO**	Optional, Positional 6
OUTPUT	Output (in BCH *=*ERREMAIL)	*****, *ERREMAIL, *EMAIL, *OUTFILE, *SYSOPR	Optional, Positional 7
OUTFILE	File to receive output	*Qualified object name*	Optional, Positional 8
	Qualifier 1: File to receive out-put	*Name*, ***FILE**	
	Qualifier 2: Library	*Name*, *LIBL, *CURLIB, ***FILE**	
MAILTO	Mail to (list, *SELECT)	*Character value*, *SELECT, ***ADMIN**, *NONE	Optional, Positional 11

MAILTEXT	Mail text	*Character value*	Optional, Positional 12
ZIP	Zip	***NO**, *YES	Optional, Positional 13
ZIPPWD	ZIP password	*Character value*	Optional, Positional 14
ORGSYS	Internal use - Sent from	*Character value*, ***NO**	Optional, Positional 9
JOBNBR	Internal use - By job number	*Character value*, ***NO**	Optional, Positional 10

Top

Product or *ALL (PRD)

Specifies the product to check.

<u>*ALL</u>
Check all products.

AU
Audit (including Action, Compliance, Native Object Security, and Replication)

NS
Object Security and Replication

GR
Firewall

CA
Capture

JR
AP Journal (including Safe Update and SIEM)

OD
Authority on Demand (including Password Reset)

AV
Antivirus (including Anti-Ransomware)

CT
Change Tracker

DB
DB-Gate

VW
View

EN
Encryption

SA
iSecurity Agent - SecureSphere Agent for DB2/400

FS
FileScope Platinum / SIEM

CS
CodeScope

Top

System to run for (SYSTEM)

Specifies the system for which you are checking authorizations.

<u>*CURRENT</u>
The system on which the query is running.
***ALL**
All systems.
character-value
The name of the system to check.

Top

Inform *SYSOPR about problems (SYSOPR)

Specifies whether to inform SYSOPR about problems encountered when checking.

***YES**
Inform SYSOPR about problems.

***NO**
Do not inform SYSOPR about problems.

Top

Days to warn before expiration (WRNDAYS)

Specifies whether to report that the product authorization is due to expire within a given number of days.

***DFT**

The default number of days.

decimal-number

Specify the number of days.

Top

Check if in FYI/Debug mode (CHKDBG)

Specifies whether to check if the product is in FYI/Debug mode.

***YES**

Check whether the product is in FYI/Debug mode.

***NO**

Do not check whether the product is in FYI/Debug mode.

Top

Check Data Size (CHKSIZE)

Check the average size of the data that was provided with the product over the past thirty days, if the product has been run during that time.

***YES**

Check data size.

***NO**

Do not check data size.

Top

Output (in BCH *=*ERREMAIL) (OUTPUT)

Specifies the destination for output.

*****

If run interactively, output goes to the screen. If run in batch mode, acts like *ERREMAIL.

***ERREMAIL**

Send email only if problems are found. Additional fields appear to specify the email recipients.

***EMAIL**

Send email. Additional fields appear to specify the email recipients.

***OUTFILE**

Send output to a file.

***SYSOPR**

If problems are found, send messages to SYSOPR.

Top

File to receive output (OUTFILE)

Specifies the file to receive output if OUTFILE has been selected.

Qualifier 1: File to receive output

***FILE**

The name of the file is formed from the string "ISA" and the job number.

name

Specify the name of the file to receive output.

Qualifier 2: Library

***LIBL**

Search a set of libraries for that file.

***CURLIB**

The current library.

***FILE**

The SMZ4DTA library.

name

The name of the library.

Top

Mail to (list, *SELECT) (MAILTO)

Specifies whether and to whom output should be emailed.

***SELECT**
If running interactively, presents a list of possible addressees.
***ADMIN**
Email to the system administrator.
***NONE**
Do not email output.
character-value
Email output to a user with a specific name.

Top

Mail text (MAILTEXT)

Specifies text to be included in email.

character-value

Text to be included in email.

Top

Zip (ZIP)

Specifies whether an attachment should be packaged in a ZIP file.

***NO**
Do not package the attachment in a ZIP file.

***YES**
Package the attachment in a ZIP file.

Top

ZIP password (ZIPPWD)

If the attachment is packaged in a ZIP file, whether to encrypt the ZIP file with a password.

character-value

Specify the password with which to encrypt the ZIP file.

Top

Internal use - Sent from (ORGSYS)

For internal use only. Leave it at the default value. Specifies the system from which the original command was sent.

***NO**

The default value. Do not change it.

character-value

Specify the system name. Do not use this.

Top

Internal use - By job number (JOBNBR)

For internal use only. Leave it at the default value. Specifies the job number of running this program.

***NO**
The default value. Do not change it.
character-value
The job number.

Top

Examples

None

Top

Error messages

Unknown

Top

Define AU Report Group Details (DFNAUGRPD)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Define AU Report Group Details (DFNAUGRPD) command serves as a template for creating report definitions. It contains parameters for many fields that are used frequently in definitions.

Top

Parameters

Keyword	Description	Choices	Notes
FROMTIME	Starting date and time	*Element list*	Optional, Positional 1
	Element 1: Starting date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Starting time	*Time*, **000000**	
TOTIME	Ending date and time	*Element list*	Optional, Positional 2
	Element 1: Ending date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Ending time	*Time*, **235959**	
USRPRF	User profile	*Generic name, name*, ***ALL**	Optional, Positional 3
SYSTEM	System to run for F4=Names	Single values: *ALL Other values (up to 30 repetitions): *Character value*, ***CURRENT**	Optional, Positional 4
OUTPUT	Output	*, ***PDF**, *HTML, *CSV, *OUTFILE, *PRINT,	Optional, Positional 5

		*PRINT1, *PRINT2, *PRINT3, *PRINT4, *PRINT5, *PRINT6, *PRINT7, *PRINT8, *PRINT9	
MRGDTA	Merge data to a single output	***YES**, *NO	Optional, Positional 6
OUTON	Place output on	*Name*, ***CURRENT**, *SYSTEM	Optional, Positional 7
PRTFMT	Print format	***SHORT**, *FULL	Optional, Positional 8
COLHDG	Add column headings	*NO, ***YES**	Optional, Positional 9
CTLFLD	Add control fields	*NO, ***YES**	Optional, Positional 10
OUTFILE	File to receive output	*Qualified object name*	Optional, Positional 11
	Qualifier 1: File to receive output	*Name*, ***AUTO**, *QRY	
	Qualifier 2: Library	*Name*, *LIBL, ***DATE**	
MAILTO	Mail to (mail1,-mail2,mail3..)	*Character value*, ***USER**	Optional, Positional 14
MAILTEXT	Mail text	Values (up to 20 repetitions): *Character value*	Optional, Positional 15
FOOTNOTE	Footnote Message	*Character value*, *DFT,	Optional,

		*ATTACHMENT, ***GRP**, *NONE	Positional 16
ZIP	Zip	***NO**, *YES	Optional, Positional 17
ZIPPWD	ZIP password	*Character value*	Optional, Positional 18
ATCOBJ	Object size to allow attach	*Decimal number*, **20**, *NO, *NOMAX	Optional, Positional 19
ATCDLT	Delete if attached	*NO, ***YES**	Optional, Positional 20
OBJ	Object (*TEMP for attach only)	*Character value*, *TEMP, *QRY, ***AUTO**, *DESC	Optional, Positional 12
DIR	Directory ('/dir/')	*Character value*, '/iSecurity/report output/', ***DATE**	Optional, Positional 13
JOBD	Job description.	Single values: *NONE Other values: *Qualified object name*	Optional, Positional 21
	Qualifier 1: Job description.	*Name*, **QBATCH**	
	Qualifier 2: Library	*Name*, ***PRODUCT**, *LIBL, *CURLIB	
USRDFNDTA	User defined data	*Character value*	Optional, Positional 22

Top

-

Starting date and time (FROMTIME)

Specifies the date and time at which the information to be included begins.

Element 1: Starting date

<u>*CURRENT</u>
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. The starting day is specified in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

date

Specify the date on which the information to be included begins. The day must be in YYMMDD format, with or without separators.

Element 2: Starting time

000000

The start of the day.

time

The time to begin on the date specifed in the previous parameter, in 24-hour HHMMSS format, with or without separators.

Top

Ending date and time (TOTIME)

Specifies the date and time of the last information to be included.

Element 1: Ending date

<u>*CURRENT</u>
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. By default, this is Sunday.

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

date
Specify the date on which the information to be included ends, in YYMMDD format, with or without separators.

Element 2: Ending time

235959

The end of the specifed date.

time

The time to end on the specifed date, in 24-hour HHMMSS format, with or without separators.

Top

-

User profile (USRPRF)

Specifies the name or generic* name of users to include.

<u>*ALL</u>
Include data for all users.

generic-name
Specify the generic name of users or groups to include.

name
Specify the name of the single user or group to include.

Top

-

System to run for F4=Names (SYSTEM)

If the local repository contains information from multiple systems, specifies the subset of systems whose information is to be included.

Single values

***ALL**

Include information from all systems.

Other values (up to 30 repetitions)

***CURRENT**

The current system.

character-value

Specify the name of the subset of systems to be included.

Top

-

Output (OUTPUT)

Specifies the destination for output.

*****

For interactive jobs, the report is displayed. For non-interactive jobs, the report is printed with the job's spooled output.

***PDF**

Print report to PDF outfile.

***HTML**

Print report to HTML outfile.

***CSV**

Print report to CSV outfile.

***OUTFILE**

Print report as text to an outfile.

***PRINT**

Print to default printer.

***PRINT1-9**

User-defined options.

Top

-

Merge data to a single output (MRGDTA)

Specifies whether to merge all data to a single output.

<u>*YES</u>
Merge all data to a single output.

***NO**
Do not merge all data to a single output.

Top

-

Place output on (OUTON)

Specifies where output is produced. For internal use only. Do not change this parameter.

***CURRENT**

Place output in the current folder.

***SYSTEM**

Place output in a folder determined by the system.

name

Specify the name of the folder.

Top

-

Print format (PRTFMT)

Specifies the format if output is created as a message.

<u>*SHORT</u>
Output must only be one line.
***FULL**
Output may be more than one line.

Top

-

Add column headings (COLHDG)

Specifies whether to output column headings for CSV (Excel) format.

***NO**

Do not output column headings.

***YES**

Output column headings.

Top

-

Add control fields (CTLFLD)

Specifies whether to output control fields for CSV (Excel) format or outfile.

***NO**
Do not output control fields.

***YES**
Output control fields.

Top

-

File to receive output (OUTFILE)

Specifies the file to receive output if OUTFILE has been selected.

Qualifier 1: File to receive output

***AUTO**

The report name plus a six-digit number (automatically incremented).

***QRY**

The name of the query.

name

Another specified name for the file.

Qualifier 2: Library

***LIBL**

Search the Library List for an appropriate library.

***DATE**

A library name derived from the date on which the query is run.

name

Specify a defined name for the library.

Top

-

Mail to (mail1,mail2,mail3..) (MAILTO)

Specifies users or lists to receive email that the query sends. The field can contain multiple values.

***USER**

Send email to the user running the query.

character-value

A particular defined user or list.

Top

-

Mail text (MAILTEXT)

Specifies the text that the query sends as email. You can specify up to 20 values for this parameter.

Other values (up to 20 repetitions)

character-value

A character string to be sent.

Top

-

Footnote Message (FOOTNOTE)

Specifies what to place as a footnote at the end of the output.

***DFT**
Include the default message: "This e-mail is produced by Raz-Lee."

***ATTACHMENT**
Include the message: "This e-mail and its attachments may contain confidential information. It is advisable to delete suspicious e-mails and to contact the corporate Security Administrator promptly."

***GRP**
Include a standard footnote showing the names of the product and the report group.

***NONE**
Do not include a footnote.

character-value
A text string to be included in the footnote.

Top

-

Zip (ZIP)

Specifies whether to include a ZIP file containing the output.

***NO**
Do not include a ZIP file.

***YES**
Include a ZIP file.

Top

-

ZIP password (ZIPPWD)

Specifies a password used to encrypt the ZIP file.

character-value

The password as a character string.

Top

-

Object size to allow attach (ATCOBJ)

Specifies whether to allow an attached object, and its maximum size.

20
: Include attachments up to 20 MB in size.

***NO**
: Do not allow attachments.

***NOMAX**
: Attachments of any size are allowed.

decimal-number
: Specify a maximum size in MB.

Top

-

Delete if attached (ATCDLT)

Whether to automatically delete the output file after the email to which it is attached has been sent successfully.

***NO**
Do not delete the file.

***YES**
Delete the file.

Top

-

Object (*TEMP for attach only) (OBJ)

Specifies the name of the object in which output is collected. This information depends on the Global Site Defaults, entered via STRAUD > 81 > 59 > 3.

***TEMP**
: A temporary name, assigned by the system, used if the file is only used as an attachment.

***QRY**
: The name of the query.

***AUTO**
: The object is determined automatically.

***DESC**
: The description of the query

character-value
: A specific character string.

Top

-

Directory ('/dir/') (DIR)

Specifies the directory containing the object.

'/iSecurity/report output/'
The '/iSecurity/report output/' directory.

<u>*DATE</u>
A directory name determined by the date on which the query is run.

character-value
A character string to serve as the directory name.

Top

-

Job description. . . . . (JOBD)

Specifies the job within which the query will run.

Single values

***NONE**

Run within the job that is running the query.

Qualifier 1: Job description. . . . . .

QBATCH

Run within the job QBATCH.

name

Specify the name of the job within which it is to run.

Qualifier 2: Library

***PRODUCT**

The program is within the library for the product.

***LIBL**

Search the Library List for an appropriate library.

***CURLIB**

The program is within the current library.

name

The name of the library containing the program.

Top

-

User defined data (USRDFNDTA)

Specifies other information, defined by the user

character-value
A string of text or other information.

Top

Examples

None

Top

Error messages

Unknown

Top

Display Action Log Entries (DSPACLOG)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Display Action Log Entries (DSPACLOG) command displays the log of Actions taken.
Action is a set of activities that are usually taken as a response to situations detected by various iSecurity products. This command enables selecting logged actions based on parameters related to the products.

Top

Parameters

Keyword	Description	Choices	Notes
PRVMIN	Display last minutes	*Decimal number*, ***BYTIME**	Optional, Positional 1
FROMTIME	Starting date and time	*Element list*	Optional, Positional 2
	Element 1: Starting date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Starting time	*Time*, **000000**	
TOTIME	Ending date and time	*Element list*	Optional, Positional 3
	Element 1: Ending date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Ending time	*Time*, **235959**	
ACTION	Action	*Generic name, name*, ***ALL**	Optional, Positional 4
APP	Application	*AUDIT, *FIREWALL, *SCREEN, *ACTIVE, *STATUS, ***ALL**	Optional, Positional 5
USRPRF	User profile	*Generic name, name*, ***ALL**	Optional, Positional

			6
JOB	Job name	*Qualified job name*	Optional, Positional 7
	Qualifier 1: Job name	*Generic name, name*, ***ALL**	
	Qualifier 2: User	*Generic name, name*, ***ALL**	
	Qualifier 3: Number	000000-999999, ***ALL**	
NBRRCDS	Number of records to process	*Decimal number*, ***NOMAX**	Optional, Positional 8
OUTPUT	Output	*****, *PRINT, *PRINT1, *PRINT2, *PRINT3, *PRINT4, *PRINT5, *PRINT6, *PRINT7, *PRINT8, *PRINT9, *OUTFILE	Optional, Positional 9
OUTFILE	File to receive output	*Qualified object name*	Optional, Positional 10
	Qualifier 1: File to receive output	*Name*	
	Qualifier 2: Library	*Name*, ***LIBL**	
OUTMBR	Output member options	*Element list*	Optional, Positional 11
	Element 1: Member to receive output	*Name*, ***FIRST**	
	Element 2: Replace or add records	***REPLACE**, *ADD	
AUDTYP	Audit type	***ALL**, *BYENTTYP, *SELECT,	Optional,

		*AUTFAIL, *CMD, *CREATE, *DELETE, *JOBDTA, *NETCMN, *OBJMGT, *OFCSRV, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDTA, *SAVRST, *SECURITY, *SERVICE, *SPLFDTA, *SYSMGT, *CHANGE, *CHGALL	Positional 12
FWTYP	Type	*NATIVE, *IFS, *IPIN, *IPOUT, *FILTFR, *FTP, *FTPLOG, *FTPSRV, *FTPCLN, *TFTP, *REXLOG, *REXEC, *RMTSQL, *SQL, *NDB, *RMTSRV, *FILSRV, *TELNET, *WSG, *ORDTAQ, *DTAQ, *VPRT, *LICMGT, *ORLICM, *CSLICM, *SNA, *DDM, *DRDA, *RMTSGN, *USRSEC, *CSCNVM, *CSCLNM, *NPRENT, *NPRSPL, *MSGSRV, *SQLENT, *OBJINF, *SIGNON, *PWDVLD, ***ALL**	Optional, Positional 13
SCTYP	Type	*SCRLCK, *SCRRLS, *SCREND, ***ALL**	Optional, Positional 14
PGM	Program name	*Generic name, name*, ***ALL**	Optional, Positional 15
FWOBJ	Object	*Qualified object name*	Optional, Positional 18
	Qualifier 1: Object	*Generic name, name*, ***ALL**	
	Qualifier 2: Library	*Generic name, name*, ***ALL**	
FWOBJT	Object type	***ALL**, *FILE, *LIB, *DTAQ, *PRTF, *PGM, *CMD	Optional, Positional 19

FWFSYS	File System	*Name*, ***ALL**	Optional, Positional 20
FWDOCN	Directory/File name contains	*Character value*, ***ALL**	Optional, Positional 21
FWIPA	IP generic address	*Character value*, ***ALL**	Optional, Positional 22
FWSRC	Source location	*Name*, ***ALL**	Optional, Positional 23
FWPROD	Product ID	*Character value*, ***ALL**	Optional, Positional 24
FWFEAT	Feature ID	*Character value*, ***ALL**	Optional, Positional 25
SCIPA	IP generic address	*Character value*, ***ALL**	Optional, Positional 26
SCRSNL	Reason locked	***ALL**, *GRLOCK, *GRMONITOR	Optional, Positional 27
SCRSNR	Reason released	***ALL**, *USRPWD, *GRPPWD, *QSECOFPWD, *SYSPWD, *LCLPWD	Optional, Positional 28
SCRSNE	Reason ended	***ALL**, *USRRQST, *ENDDELAY, *PWDRETRY, *VARYOFF, *SIGNOFF, *HELD, *BREAK	Optional, Positional 29
ENTTYP	Journal entry types	Single values: ***ALL**, *SELECT Other values (up to 50 repe-	Optional, Positional

		titions): AD, AF, AP, CA, CD, CO, CP, CQ, CU, CV, CY, DI, DO, DS, EV, GR, GS, IP, IR, IS, JD, JS, KF, LD, ML, NA, ND, NE, OM, OR, OW, O1, O2, O3, PA, PG, PO, PS, PW, RA, RJ, RO, RP, RQ, RU, RZ, SD, SE, SF, SG, SK, SM, SO, ST, SV, VA, VC, VF, VL, VN, VO, VP, VR, VS, VU, VV, X0, YC, YR, ZC, ZM, ZR, *J, *S	30
SUBTYP	Subtype	Single values: ***ALL** Other values (up to 10 repetitions): A-9	Optional, Positional 31
PRTFMT	Print format	***SHORT**, *FULL	Optional, Positional 32
OBJ	Object Qualifier 1: Object Qualifier 2: Library	*Qualified object name* *Generic name, name*, ***ALL** *Generic name, name*, ***ALL**	Optional, Positional 33
OBJTYPE	Object type	***ALL**, ***ALL**, *ALRTBL, *AUTL, *BNDDIR, *CFGL, *CHTFMT, *CLD, *CLS, *CMD, *CNL, *COSD, *CSI, *CSPMAP, *CSPTBL, *CSPTBL, *CTLD, *CRQD, *DEVD, *DOC, *DTAARA, *DTADCT, *DTAQ, *EDTD, *EXITRG, *FCT, *FILE, *FLR, *FNTTBL, *FNTRSC, *FORMDF, *FTR, *GSS, *IPXD, *JOBD, *JOBQ, *JOBSCD, *JRN, *JRNRCV, *LIB, *LIND, *LOCALE, *MENU, *MODD, *MODULE, *MSGF, *MSGQ, *M36,	Optional, Positional 34

		*M36CFG, *NODL, *NODGRP, *NWID, *OUTQ, *NWSD, *NTBD, *OVL, *PAGDFN, *PAGSEG, *PDG, *PGM, *PNLGRP, *PRDDFN, *PRDLOD, *PSFCFG, *QMFORM, *QMQRY, *QRYDFN, *RCT, *SBSD, *SCHIDX, *SPADCT, *SQLPKG, *SRVPGM, *SVRSTG, *SSND, *SOCKET, *S36, *TBL, *USRIDX, *USRPRF, *USRQ, *USRSPC, *SYMLNK, *STMF, *VLDL, *WSCST	
SYSVAL	System value	*Generic name, name*, ***ALL**	Optional, Positional 35
TIMEGRP	Filter by time group	*Element list*	Optional, Positional 16
	Element 1: Relationship	*IN, *OUT, ***NONE**	
	Element 2: Time group	*Name*, ***SELECT**	
QRY	Filter per query rules	*Name*, ***NONE**	Optional, Positional 17
START	Start log display	*OLD, *NEW, ***DFT**	Optional, Positional 36

Top

-

Display last minutes (PRVMIN)

To view activity in a period of time up to when the report is run, set this parameter to the number of minutes that you would like to check. To see information for the previous five minutes, set this value to "5".

***BYTIME**

Use the values set in the FROMTIME and TOTIME parameters.

decimal-number

The number of minutes before the current time.

Top

-

Starting date and time (FROMTIME)

Specifies the date and time at which the information to be queried begins.

Element 1: Starting date

***CURRENT**
The current date.

***YESTERDAY**
Yesterday's date.

***WEEKSTR**
The first day of the current week. NOTE: The starting day of the week is based on the specification made in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week.

***MONTHSTR**
The first day of the current month.

***PRVMONTHS**
The first day of the previous month.

***YEARSTR**
The first day of the current year.

***PRVYEARS**
The first day of the previous year.

***MON**
Monday.

***TUE**
Tuesday.

***WED**
Wednesday.

***THU**
Thursday.

***FRI**
Friday.

***SAT**
Saturday.

***SUN**
Sunday.

date

Specify the date on which the information to be queried begins. The date is in the date format that this job uses, with or without date separators.

Element 2: Starting time

time

The time to begin. The time is in 24-hour HHMMSS format, with or without separators.

Top

Ending date and time (TOTIME)

Specifies the date and time of the last information to be queried.

Element 1: Ending date

***CURRENT**
The current date.

***YESTERDAY**
Yesterday's date.

***WEEKSTR**
The first day of the current week. The starting day is based on the specification made in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week.

***MONTHSTR**
The first day of the current month.

***PRVMONTHS**
The first day of the previous month.

***YEARSTR**
The first day of the current year.

***PRVYEARS**
The first day of the previous year.

***MON**
Monday.

***TUE**
Tuesday.

***WED**
Wednesday.

***THU**
Thursday.

***FRI**
Friday.

***SAT**
Saturday.

***SUN**
Sunday.

date

Specify the date on which the information to be queried ends. The date is in the date format that this job uses, with or without separators.

Element 2: Ending time

time

The time to end. The time is in 24-hour HHMMSS format, with or without separators.

Top

-

Action (ACTION)

Specifies the action taken.

***ALL**
Include all actions.

generic-name
Specify the generic name of actions to be included.

name
Specify the name of the action to be included.

Top

-

Application (APP)

Specifies that logs that come from the specified application or product are to be included.

***AUDIT**
Include logs from iSecurity Audit.
***FIREWALL**
Include logs from iSecurity Firewall.
***SCREEN**
Include logs from iSecurity Screen.
***ACTIVE**
Include logs from checking system activity.
***STATUS**
Include logs from checking system status.
***ALL**
Include logs from all applications.

Top

-

User profile (USRPRF)

Specifies the name or generic* name of users to include.

<u>*ALL</u>
Include data for all users.

generic-name
Specify the generic name of users or groups to include.

name
Specify the name of the single user or group to include.

Top

-

Job name (JOB)

Specifies the jobs to be included.

Qualifier 1: Job name

***ALL**
All job names.

generic-name
Specify the generic user name of the jobs.

name
Specify the user name of the job.

Qualifier 2: User

***ALL**
All users.

generic-name
Users with the specified generic name.

name
Users with the specific name.

Qualifier 3: Number

***ALL**
All jobs.

000000-999999
Jobs with the specific number.

Top

-

Number of records to process (NBRRCDS)

Specifies the maximum number of records to process.

<u>*NOMAX</u>
Process all records.
decimal-number
The maximum number of records to process.

Top

-

Output (OUTPUT)

Specifies the destination for output.

*****

The default output. If running interactively, this is the current screen.

***PRINT**

Print report to PDF outfile.

***PRINT1-9**

User-defined option.

***OUTFILE**

Print report as text to an outfile.

Top

-

File to receive output (OUTFILE)

Specifies the database file to which the output of the command is directed. If the file does not exist, this command creates a database file in the specified library.

Qualifier 1: File to receive output

name

Specify the name of the database file to which the command output is directed.

Qualifier 2: Library

***LIBL**

The library list is used to locate the file. If the file is not found, one is created in the current library. If no current library exists, the file will be created in the QGPL library.

name

Specify the name of the library to be searched.

Top

-

Output member options (OUTMBR)

Specifies the name of the database file member that receives the output of the command.

Element 1: Member to receive output

***FIRST**

The first member in the file receives the output. If OUTMBR(*FIRST) is specified and the member does not exist, the system creates a member with the name of the file specified for the "File to receive output (OUTFILE)" parameter. If the member already exists, you have the option to add new records to the end of the existing member or clear the member and then add the new records.

name

Specify the name of the file member that receives the output. If it does not exist, the system creates it.

Element 2: Replace or add records

***REPLACE**

The system clears the existing member and adds the new records.

***ADD**

The system adds the new records to the end of the existing records.

Top

-

Audit type (AUDTYP)

Specifies the audit Type for the query. Most of the values are documented in the IBM i Security Reference Manual, in either

- Table 115 (Possible values for AUDLVL) online at www.ib-m.com/docs/en/i/7.4?topic=profiles-action-auditing
- Table 133 (Security auditing journal entries) online at www.ib-m.com/docs/en/i/7.4?topic=actions-security-auditing-journal-entries

***ALL**

Examine all Audit Types.

***BYENTTYP**

Use the ENTTYP (entry type) parameter to determine the audit type.

***SELECT**

If running interactively, a list of Audit Types appears from which you can select items.

Top

-

Type (FWTYP)

For logs from iSecurity Firewall, specifies the type of Firewall-enabled server and object rules to include. Most of the options correspond to those shown on the Firewall "Work with Server Security" screen (STRFW > 1 > 1).

***NATIVE**
Include rules for Native objects,

***IFS**
Include rules for IFS objects.

***IPIN**
Include rules based on incoming IP addresses.

***IPOUT**
Include rules based on outgoing IP addresses.

***ALL**
Include rules for all servers and objects.

Top

-

Type (SCTYP)

For logs from iSecurity Screen, describes the activity to include.

***SCRLCK**
Include locking screens.
***SCRRLS**
Include unlocking screens.
***SCREND**
Include ending Screen sessions.
***ALL**
Include all types of logs.

Top

-

Program name (PGM)

Specifies the program running when the message was produced.

***ALL**
Messages from all programs.

generic-name
Messages produced by programs with this generic name.

name
Messages produced by programs with this specific name.

Top

-

Object (FWOBJ)

If including logs from iSecurity Firewall, the names of objects to include.

Qualifier 1: Object

***ALL**

Include all objects.

generic-name

Include objects with the specified generic* name. Specify the generic name of objects to include.

name

Include objects with the specified name.

Qualifier 2: Library

***ALL**

Include objects from all libraries.

generic-name

Include objects from libraries with the specified generic* name.

name

Include objects from libraries with the specified name.

Top

-

Object type (FWOBJT)

For logs from iSecurity Firewall, include logs for specified types of objects.

***ALL**
All objects.
***FILE**
Files.
***LIB**
Libraries.
***DTAQ**
Data queues,
***PRTF**
Print files.
***PGM**
Programs.
***CMD**
Commands.

Top

-

File System (FWFSYS)

For logs from iSecurity Firewall, specifies the filesystems for which logs are included.

***ALL**

Include logs for all filesystems.

name

Include logs for a specified filesystem.

Top

-

Directory/File name contains (FWDOCN)

For logs from iSecurity Firewall, include logs for files whose directory or file names contain a specified string.

***ALL**

Include files with all names.

character-value

Specify the string which must appear in directory or file names for them to be included.

Top

-

IP generic address (FWIPA)

Specifies IP address ranges to include.

***ALL**
Include all IP address ranges.

generic-name
Specify the IP address range as a generic name.

character-value
Specify the IP address range.

Top

-

Source location (FWSRC)

Specifies the system name of systems to include.

<u>*ALL</u>
Include all system names.

name
Include a specific system name.

Top

-

Product ID (FWPROD)

If including logs from iSecurity Firewall, include logs coming from a specific Product ID.

***ALL**

Include logs coming from any Product ID.

character-value

Include logs coming from a specific Product ID.

Top

-

Feature ID (FWFEAT)

If including logs from iSecurity Firewall, whether to consider those referring to features with a specified name.

***ALL**

Include all logs.

character-value

Include logs that include a specified feature name.

Top

-

IP generic address (SCIPA)

If including logs from iSecurity Screen, whether to include those referring to a specified IP address range.

***ALL**

Include logs from all IP addresses.

character-value

Include logs from a specified IP address range.

Top

-

Reason locked (SCRSNL)

If including logs from iSecurity Screen, include those referring to screens that were locked for a specified reason.

***ALL**

Do not consider the reasons that screens were locked.

***GRLOCK**

The screen was locked via the Self-Lock feature (the GRLOCK command).

***GRMONITOR**

Job required a lock but was not enabled to be locked.

Top

-

Reason released (SCRSNR)

If including logs from iSecurity Screen, include logs about screen locks that were released for a specified reason.

***ALL**
Do not consider the reason that a screen lock was released.

***USRPWD**
A user password was entered.

***GRPPWD**
A group password was entered.

***QSECOFPWD**
A QSECOFR password was entered.

***SYSPWD**
A system password was entered.

***LCLPWD**
A local password was entered.

Top

-

Reason ended (SCRSNE)

If including logs from iSecurity Screen, include logs that show a Screen session ending for specified reasons.

***ALL**
Include Screen sessions that ended for any reason.
***USRRQST**
Session ended when user pressed the relevant function key.
***ENDDELAY**
Session expired while waiting for password.
***PWDRETRY**
Permitted number of password retries exceeded.
***VARYOFF**
Terminal varied off (disconnected from system).
***SIGNOFF**
User signed off.
***HELD**
Job was set to HOLD state.
***BREAK**
Break message sent.

Top

-

Journal entry types (ENTTYP)

Specifies the type of update made, by entry type. Entry types are documented at www.ibm.com/docs/en/i/7.4?topic=information-all-journal-entries-by-code-type

Single values

***ALL**

Accept all entry types.

***SELECT**

If running interactively, a dialog window opens from which you can select entry types.

Other values (up to 50 repetitions)

Top

-

Subtype (SUBTYP)

Specifies the subtypes of the entry type to include.

Single values

***ALL**

Include all subtypes.

Other values

A-9

Subtypes to be included.

Top

-

Print format (PRTFMT)

Specifies the format if output is created.

<u>*SHORT</u>
Output must only be one line.
***FULL**
Output may be more than one line.

Top

-

Object (OBJ)

If the Audit type involves specific objects, the objects to be included.

Qualifier 1: Object

***ALL**
Include all objects.

generic-name
Include objects with a specified generic name.

name
Include objects with a specified name.

Qualifier 2: Library

***ALL**
Include objects from all libraries.

generic-name
Include objects within libraries with a specified generic name.

name
Include objects in libraries with a specified name.

Top

-

Object type (OBJTYPE)

Specifies external object types, as specified in https://www.ibm.com/docs/en/i/7.2?topic=objects-external-object-types

***ALL**

Include all object types.

Top

-

System value (SYSVAL)

If the activity involves particular system values.

***ALL**
Include all values.

generic-name
Specify the generic name of values to include.

name
Specify the name of the system values to include.

Top

-

Filter by time group (TIMEGRP)

Specifies a defined set of times to be included or excluded.

Element 1: Relationship

***IN**
Include the timegroup.

***OUT**
Exclude the timegroup.

***NONE**
Do not consider timegroups.

Element 2: Time group

***SELECT**
If running interactively, present a set of timegroups to consider.

name
The name of a specific timegroup.

Top

-

Filter per query rules (QRY)

Specifies a named query to run.

<u>*NONE</u>
Do not run a query.

name
Specify the name of the query to run.

Top

-

Start log display (START)

Specifies whether to display information starting with the oldest or newest records.

***OLD**
Start with the oldest records.
***NEW**
Start with the newest records.
***DFT**
Start with whichever is specified in the default values.

Top

Examples

None

Top

Error messages

Unknown

Top

Display Audit Log Entries (DSPAULOG)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Display Audit Log Entries (DSPAULOG) command displays selected entries from an audit log.

Top

Parameters

Keyword	Description	Choices	Notes
PRVMIN	Display last minutes	*Decimal number*, ***BYTIME**	Optional, Positional 1
FROMTIME	Starting date and time	*Element list*	Optional, Positional 2
	Element 1: Starting date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN, *START	
	Element 2: Starting time	*Time*, **000000**	
TOTIME	Ending date and time	*Element list*	Optional, Positional 3
	Element 1: Ending date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Ending time	*Time*, **235959**	
AUDTYP	Audit type	*SELECT, ***ALL**, *BYENTTYP, *AUTFAIL, *CMD, *CMDENT, *CMDAODINT, *CMDCHK, *CMDUNIX, *CREATE, *DELETE, *JOBDTA, *NETCMN, *OBJMGT, *OFCSRV, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDTA, *SAVRST, *SECURITY, *SERVICE, *SPLFDTA, *SYSMGT, *CHANGE, *CHGALL,	Optional, Positional 4

		*PTFOBJ, *PTFOPR, *VIRUS, *AGENT	
SYSSBST	System (from local repos-itory)	*Name*, ***CURRENT**, *ALL	Optional, Positional 5
USRPRF	User profile	*Generic name, name*, ***ALL**	Optional, Positional 6
PGM	Program name	*Qualified object name*	Optional, Positional 7
	Qualifier 1: Program name	*Generic name, name*, ***ALL**	
	Qualifier 2: Library	*Generic name, name*, ***ALL**	
IPADR	IPv4 (gen-eric*) or IPv6	*Character value*, ***ALL**	Optional, Positional 8
ADRPFXLEN	Prefix length for IPv6	1-128, ***ALL**	Optional, Positional 9
JOB	Job name	*Qualified job name*	Optional, Positional 10
	Qualifier 1: Job name	*Generic name, name*, ***ALL**	
	Qualifier 2: User	*Generic name, name*, ***ALL**	
	Qualifier 3: Number	000000-999999, ***ALL**	
TIMEGRP	Filter by time group	*Element list*	Optional, Positional 11
	Element 1:	*IN, *OUT, ***NONE**	

	Relationship		
	Element 2: Time group	*Name*, ***SELECT**	
QRY	Filter using query rules	*Name*, ***NONE**	Optional, Positional 12
NBRRCDS	Number of records to process	*Decimal number*, ***NOMAX**	Optional, Positional 13
OUTPUT	Output	*****, *PRINT, *PRINT1, *PRINT2, *PRINT3, *PRINT4, *PRINT5, *PRINT6, *PRINT7, *PRINT8, *PRINT9, *OUTFILE	Optional, Positional 14
ENTTYP	Journal entry types	Single values: ***ALL**, *SELECT Other values (up to 50 repetitions): *Character value*	Optional, Positional 15
SUBTYP	Subtype	Single values: ***ALL** Other values (up to 10 repetitions): A-9	Optional, Positional 16
PRTFMT	Print format	***SHORT**, *FULL	Optional, Positional 17
OBJ	Object	*Qualified object name*	Optional, Positional 18
	Qualifier 1: Object	*Generic name, name*, ***ALL**	
	Qualifier 2: Library	*Generic name, name*, ***ALL**	
OBJTYPE	Object type	***ALL**, *FILE, *STMF, *ALRTBL, *AUTL, *BNDDIR, *CFGL, *CHTFMT, *CLD, *CLS, *CMD, *CNL, *COSD, *CSI, *CSPMAP,	Optional, Positional 19

		*CSPTBL, *CSPTBL, *CTLD, *CRQD, *DEVD, *DOC, *DTAARA, *DTADCT, *DTAQ, *EDTD, *EXITRG, *FCT, *FLR, *FNTTBL, *FNTRSC, *FORMDF, *FTR, *GSS, *IPXD, *JOBD, *JOBQ, *JOBSCD, *JRN, *JRNRCV, *LIB, *LIND, *LOCALE, *MENU, *MODD, *MODULE, *MSGF, *MSGQ, *M36, *M36CFG, *NODL, *NODGRP, *NWID, *OUTQ, *NWSD, *NTBD, *OVL, *PAGDFN, *PAGSEG, *PDG, *PGM, *PNLGRP, *PRDDFN, *PRDLOD, *PSFCFG, *QMFORM, *QMQRY, *QRYDFN, *RCT, *SBSD, *SCHIDX, *SPADCT, *SQLPKG, *SRVPGM, *SVRSTG, *SSND, *SOCKET, *S36, *TBL, *USRIDX, *USRPRF, *USRQ, *USRSPC, *SYMLNK, *VLDL, *WSCST	
SYSVAL	System value	*Generic name, name*, ***ALL**	Optional, Positional 20
OUTFILFMT	Outfile format	***BYTYPE**, *ALL	Optional, Positional 21
OUTFILE	File to receive out-put	*Qualified object name*	Optional, Positional 22
	Qualifier 1: File to receive out-put	*Name*	

	Qualifier 2: Library	*Name*, ***LIBL**	
OUTMBR	Output member options	*Element list*	Optional, Positional 23
	Element 1: Member to receive output	*Name*, ***FIRST**	
	Element 2: Replace or add records	***REPLACE**, *ADD	
USRDFNDTA	User defined data	*Character value*	Optional, Positional 24
START	Start log display	*OLD, *NEW, ***DFT**	Optional, Positional 25

Top

Display last minutes (PRVMIN)

To view activity in a period of time up to when the report is run, set this parameter to the number of minutes that you would like to check. For example, to see information for the previous two hours, set this value to "120"; to see information for the previous five minutes, set this value to "5".

***BYTIME**

Use the values set in the FROMTIME and TOTIME parameters.

decimal-number

Specify the number of minutes before the time that the query is run to be checked.

Top

Starting date and time (FROMTIME)

Specifies the date and time at which the information to be queried begins.

Element 1: Starting date

***CURRENT**
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. The starting day is specified in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

***START**

The earliest information available.

date

Specify the date on which the information to be queried begins. The day must be in YYMMDD format, with or without separators.

Element 2: Starting time

000000

The start of the day.

time

The time to begin on the date specifed in the previous parameter, in 24-hour HHMMSS format, with or without separators.

Top

-

Ending date and time (TOTIME)

Specifies the date and time of the last information to be queried.

Element 1: Ending date

***CURRENT**
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. By default, this is Sunday.

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

date
Specify the date on which the information to be queried ends, in YYMMDD format, with or without separators.

Element 2: Ending time

235959

The end of the specifed date.

time

The time to end on the specifed date, in 24-hour HHMMSS format, with or without sparators.

Top

Audit type (AUDTYP)

Specifies the audit Type for the query. Most of the values are documented in the IBM i Security Reference Manual, in either

- Table 115 (Possible values for AUDLVL) online at www.ib-m.com/docs/en/i/7.4?topic=profiles-action-auditing
- Table 133 (Security auditing journal entries) online at www.ib-m.com/docs/en/i/7.4?topic=actions-security-auditing-journal-entries

***SELECT**
: If running interactively, a list of Audit Types appears from which you can select items.

***ALL**
: Examine all Audit Types.

***BYENTTYP**
: Use the ENTTYP (entry type) parameter to determine the audit type.

***CMDENT**
: Commands entered interactively.

***CMDAODINT**
: Commands entered during an AOD (Authority on Demand) session.

***CMDCHK**
: Information resulting from iSecurity/Command.

***CMDUNIX**
: Not used. Kept for compatibility use only.

***CHGALL**
: Included for compatibility only. Do not use this.

***VIRUS**
: Information resulting from iSecurity/Antivirus and iSecurity/Anti-ransomware.

***AGENT**
: Information related to the Imperva SecureSphere Agent.

Top

System (from local repository) (SYSSBST)

If the local repository contains information from multiple systems, specifies the subset of systems whose information is to be included.

***CURRENT**

The current system.

***ALL**

Include information from all systems.

name

Specify the name of the subset of systems to be included.

Top

User profile (USRPRF)

Specifies the name or generic* name of users to include.

***ALL**
Examine data for all users.

generic-name
Specify the generic name of users or groups to include.

name
Specify the name of the single user or group to include.

Top

Program name (PGM)

Specifies the program running when the message was produced.

Qualifier 1: Program name

***ALL**

Messages from all programs.

generic-name

Messages produced by programs with this generic name.

name

Messages produced by programs with this specific name

Qualifier 2: Library

***ALL**

All libraries that might contain the program.

generic-name

The generic name of the library containing the program.

name

The specific name of the kibrary containing the program.

Top

IPv4 (generic*) or IPv6 (IPADR)

Specifies the IP address from which the program was run.

<u>*ALL</u>
Examine entries from all IP addresses.
character-value
A specific IP address.

Top

Prefix length for IPv6 (ADRPFXLEN)

The Prefix Length of an IPv6 address, if one was specified in the IPADR parameter.

***ALL**

All prefix lengths.

1-128

The range of IP addresses to include..

Top

Job name (JOB)

Specifies the job to be examined.

Qualifier 1: Job name

***ALL**
All job names.

generic-name
Specify the generic name of the job to include.

name
Specify the job name.

Qualifier 2: User

***ALL**
All users.

generic-name
Specify the generic name of the user to include.

name
Specify the user name.

Qualifier 3: Number

***ALL**
All jobs.

000000-999999
Jobs with the specific number.

Top

Filter by time group (TIMEGRP)

Specifies a defined set of times to be included or excluded.

Element 1: Relationship

***IN**
Include the timegroup.

***OUT**
Exclude the timegroup.

***NONE**
Do not consider the timegroup.

Element 2: Time group

***SELECT**
If running interactively, present a set of timegroups to consider.

name
The name of a specific timegroup.

Top

Filter using query rules (QRY)

Specifies a named query to run.

<u>*NONE</u>
Do not run a query.

name
Specify the name of the query to run.

Top

Number of records to process (NBRRCDS)

Specifies the maximum number of records to process.

<u>*NOMAX</u>
Process all records.
decimal-number
The maximum number of records to process.

Top

Output (OUTPUT)

Specifies the destination for output.

*****

The output is displayed for interactive jobs or printed with the job's spooled output for non-interactive jobs.

***PRINT**

Print report to PDF outfile.

***PRINT1**

User-defined option.

***PRINT2**

User-defined option.

***PRINT3**

User-defined option.

***PRINT4**

User-defined option.

***PRINT5**

User-defined option.

***PRINT6**

User-defined option.

***PRINT7**

User-defined option.

***PRINT8**

User-defined option.

***PRINT9**

User-defined option.

***OUTFILE**

Print report as text to an outfile.

Top

Journal entry types (ENTTYP)

Specifies the type of update made, by entry type. Entry types are documented at www.ibm.com/docs/en/i/7.4?topic=information-all-journal-entries-by-code-type

Single values

***ALL**

All entry types.

***SELECT**

If running interactively, a dialog window opens from which you can select entry types.

Other values (up to 50 repetitions)

character-value

Specify up to fifty entry types.

Top

Subtype (SUBTYP)

Specifies the subtypes of the entry type to include.

Single values

***ALL**

Include all subtypes

Other values (up to 10 repetitions)

A-9

The names of up to ten subtypes to be included.

Top

Print format (PRTFMT)

Specifies the format if output is created as a message.

<u>*SHORT</u>
Output must only be one line.
***FULL**
Output may be more than one line.

Top

Object (OBJ)

If the Audit type involves specific objects, the objects to be considered. This information depends on the Global Site Defaults, entered via STRAUD > 81 > 59 > 3.

Qualifier 1: Object

***ALL**
Include all objects.

generic-name
The generic* name of objects to be included.

name
The specific names of objects to be included.

Qualifier 2: Library

***ALL**
Include objects in all libraries.

generic-name
Specify the generic name of libraries containing objects to be included.

name
Include specific names of libraries to be included.

Top

Object type (OBJTYPE)

Specifies extrnal object types, as specified in https://www.ibm.com/docs/en/i/7.2?topic=objects-external-object-types

***ALL**

Include all object types.

Top

System value (SYSVAL)

If the activity involves particular system values, the values it examines.

<u>*ALL</u>
All system values.

generic-name
The generic name of the system values.

name
The specific name of the system value.

Top

Outfile format (OUTFILFMT)

Specifies whether to build the output file based on the fields of the particular journal entry type or based on the generic structure.

<u>*BYTYPE</u>

Send output in fields related to the first specified journal entry type.

***ALL**

Send information reelated to all common fields.

Top

File to receive output (OUTFILE)

If output is sent to a file, the location of the file.

Qualifier 1: File to receive output

name

Specify the name of the file.

Qualifier 2: Library

<u>*LIBL</u>

Search the libraries in the library list, in order, until the object is found.

name

The name of the library containing the file.

Top

Output member options (OUTMBR)

Specifies which member of the object receives output, and whether the output replaces or adds to existing information in the member.

Element 1: Member to receive output

***FIRST**

Place output in the first member.

name

Specify the name of the member to receive output.

Element 2: Replace or add records

***REPLACE**

Replace existing records.

***ADD**

Add new records to existing ones.

Top

User defined data (USRDFNDTA)

Specifies other information, defined by the user

character-value

A string of text or other information.

Top

Start log display (START)

Specifies whether the records are processed starting with the oldest or with the newest.

***OLD**
Start with the oldest record.
***NEW**
Start with the newest record.
***DFT**
Use the system default to determine whether to start with the oldest or newest record.

Top

Examples

None

Top

Error messages

Unknown

Top

Display iSec Authorization (DSPISA)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Display iSecurity Authorization (DSPISA) command displays the authorization status of each of your iSecurity products. It shows the same information as the menu option STRAUD > 89 > 22.
The command has no parameters.
The command displays the "Status of iSecurity Authorization" screen with a line for each authorized product. Each line contains the name of the product, as well as its main Product Library, Release ID, and authorization

status. Pressing the F10 key shows the authorization code for each product. Entering "1" in the Opt field for a product shows expanded information.

Top

Parameters

None

Top

Examples

None

Top

Error messages

Unknown

Top

Send SMTP Mail (RLSNDM)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Send SMTP Mail (RLSNDM) command specifies parameters affecting the content and sending of email messages. It is intended for use only within Raz-Lee.

Top

Parameters

Keyword	Description	Choices	Notes
TO	To (mail1,-mail2,mail3..)	*Character value*, *SENDER, *SELECT, *REPLY, *USER	Required, Positional 1
SUBJECT	Subject	*Character value*, ***NONE**	Optional, Positional 2
TEXT	Mail text	*Character value*, ***SUBJECT**, *FILE, *NONE	Optional, Positional 3
ATTACH	Attachment	Values (up to 15 repetitions): *Path name*, *FILE, ***NONE**	Optional, Positional 4
SNDMODE	Mail Sending Mode	***DFT**, *JAVA, *IBM, *DEFINED, *SECURED, *UNSECURED, *NONE	Optional, Positional 5
FILE	Mail text file	Single values: ***NONE** Other values: *Qualified object name*	Optional, Positional 6
	Qualifier 1: Mail text file	*Name*	
	Qualifier 2: Library	*Name*, ***LIBL**, *CURLIB, *NONE	
MBR	Member	*Name*, ***NONE**	Optional, Positional 7
ATTFILE	Attached file	Single values: ***NONE** Other values: *Qualified object name*	Optional, Positional 8
	Qualifier 1: Attached file	*Name*	
	Qualifier 2: Library	*Name*, ***LIBL**, *CURLIB,	

-

		*NONE	
FILEMBR	File Member	*Name*, ***NONE**	Optional, Positional 9
SENDER	Sender	*Element list*	Optional, Positional 10
	Element 1: Address, *TO, *REPLY, *USER...	*Character value*, *TO, ***REPLY**, *USER, *DONOTREPLY, *SELECT	
	Element 2: Description	*Character value*	
REPLYTO	Reply-to	*Element list*	Optional, Positional 11
	Element 1: Reply to (mail1,mail2,mail3..)	*Character value*, *SENDER, *USER, ***REPLY**, *TO, *DONOTREPLY, *SELECT	
	Element 2: Description	*Character value*	
CC	CC (mail1,-mail2,mail3..)	*Character value*, ***NONE**, *SELECT, *USER	Optional, Positional 12
BCC	BCC (mail1,-mail2,mail3..)	*Character value*, ***NONE**, *SELECT, *USER	Optional, Positional 13
FOOTNOTE	Footnote Message	*Character value*, *DFT, *EMPTY, *ATTACHMENT, ***NONE**	Optional, Positional 14
SMTPPORT	Mail port number	*Character value*, ***DFT**, *LOCAL	Optional, Positional 15
SMTPSSL	SSL/TLS Secured Mail	***DFT**, *YES, *NO	Optional, Positional 16

ATCOBJ	Object size to allow attach	*Decimal number*, *NO, ***NOMAX**	Optional, Positional 17
ATCDLT	Delete attachment	*NO, ***YES**	Optional, Positional 18
CVTATT	Convert attachment to ASCII	***NO**, *YES	Optional, Positional 19
ZIP	Zip	***NO**, *YES	Optional, Positional 20
ZIPPWD	ZIP password	*Character value*, ***NO**	Optional, Positional 21
ENVLIB	Environment	***AUD**, *AV, *FS	Optional, Positional 22
BATCH	Send in BATCH mode	*YES, ***NO**	Optional, Positional 23
DUMP	Dump RLSNDM command into QGPL	***NO**, *FILE, *JOBLOG, *BOTH, *DUMP	Optional, Positional 24
HOST	Mail (SMTP) server name	*Character value*, *LOCALHOST, ***DFT**	Optional, Positional 25
ACCOUNT	Mail account	*Character value*, *SENDER, ***DFT**, *NONE	Optional, Positional 26
PWD	Account password	*Character value*, ***DFT**, *NONE	Optional, Positional

-

			27
CCSID	CCSID	37-65535, *JOB, *PROD, ***DFT**, *SYSVAL, *SMS	Optional, Positional 28
INSCR	Insert CR in text body	*Decimal number*, ***NONE**, *DFT	Optional, Positional 29
USRDFNDTA	User defined data	*Character value*, ***NONE**	Optional, Positional 30

Top

-

To (mail1,mail2,mail3..) (TO)

Specifies the addresses to which email is sent. There can be multiple recipients, separated by commas.
This is a required parameter.

***SENDER**
Use the value of the SENDER parameter.

***SELECT**
If running interactively, opens the "Work with Email Address Book" screen to select email addresses.

***REPLY**
Use the value of the "Reply to mail address" parameter specified through STRAUD > 89 > 2.

***USER**
The user running the query.

character-value
Specify one or more addresses.

Top

-

Subject (SUBJECT)

Specifies the subject line for the email message.

<u>*NONE</u>
The email will have no subject line.
character-value
Specify the text for the Subject line.

Top

-

Mail text (TEXT)

Specifies the text of the email message.

<u>*SUBJECT</u>
The message text is the same as the Subject line.
***FILE**
If run interactively, displays a dialog to select the file and member.
***NONE**
The message has no text.
character-value
Specify the text of the message.

Top

-

Attachment (ATTACH)

Specifies one or more files to be attached to the message.
You can specify 15 values for this parameter.

***FILE**
If running interactively, the user is prompted for a file name.

***NONE**
Nothing is attached.

path-name
The pathname to the file to be attached.

Top

-

Mail Sending Mode (SNDMODE)

Specifies the mail sending mode.

***DFT**
Use the default mode.

***JAVA**
Send email using Java.

***IBM**
Use the IBM standard mode to send email.

***DEFINED**
Follow the system definition to determine whether to send email *SECURED or *UNSECURED.

***SECURED**
Send a username and password to the server when you send email.

***UNSECURED**
Send mail without sending a username and password to the server.

***NONE**
Do not send mail.

Top

-

Mail text file (FILE)

Specifies the file containing mail text.

Single values

***NONE**

No file is specified.

Qualifier 1: Mail text file

name

The name of the file containing mail text.

Qualifier 2: Library

***LIBL**

All libraries on the library list are searched until a match is found.

***CURLIB**

The current library.

***NONE**

No library is specified.

name

. Specify the name of the library.

Top

-

Member (MBR)

Specifies whether to use a specified member of a file as the email text.

***NONE**

Do not use a member.

name

Specify the name of the member to send.

Top

-

Attached file (ATTFILE)

Specifies the file to be attached to the email.

Single values

***NONE**

No file is attached.

Qualifier 1: Attached file

name

Specify the name of the file.

Qualifier 2: Library

***LIBL**

All libraries on the library list are searched until a match is found.

***CURLIB**

The current library.

***NONE**

No library is specified.

name

Specify the name of the library.

Top

-

File Member (FILEMBR)

Specifies the member of the file specified as the *ATTFILE parameter to attach.

<u>*NONE</u>
Do not specify a member.

name
Specify the name of the member.

Top

-

Sender (SENDER)

Specifies the username shown as the sender of the email.

Element 1: Address, *TO, *REPLY, *USER...

***TO**

The value of the TO parameter.

***REPLY**

Use the value of the "Reply to mail address" parameter specified through STRAUD > 89 > 2.

***USER**

The user running the query.

***DONOTREPLY**

Specifies an address that does not accept replies.

***SELECT**

If running interactively, opens the "Work with Email Address Book" screen.

character-value

Specify one or more addresses.

Element 2: Description

character-value

Specify a username.

Top

-

Reply-to (REPLYTO)

Specifies the address to which replies to the email are directed.

Element 1: Reply to (mail1,mail2,mail3..)

***SENDER**
Use the value of the SENDER parameter.

***USER**
The user running the query.

***REPLY**
Use the value of the "Reply to mail address" parameter specified through STRAUD > 89 > 2.

***TO**
The value of the To parameter.

***DONOTREPLY**
An address that discards replies.

***SELECT**
If running interactively, opens the "Work with Email Address Book" screen,

character-value
Specify one or more addresses.

Element 2: Description

character-value
A text description of the address.

Top

-

CC (mail1,mail2,mail3..) (CC)

Specifies who is specified on the CC: (Carbon Copy) line of the email header.

***NONE**
No CC: is specified.

***SELECT**
If running interactively, opens the "Work with Email Address Book" screen.

***USER**
The user running the query.

character-value
Specify one or more addresses.

Top

-

BCC (mail1,mail2,mail3..) (BCC)

Specifies BCC: (Blind Carbon Copy) recipients for the email.

***NONE**

The are no BCC: recipients.

***SELECT**

If running interactively, opens the "Work with Email Address Book" screen.

***USER**

The user running the query.

character-value

Specify one or more addresses.

Top

-

Footnote Message (FOOTNOTE)

Specifies a footnote to be appended to the email.

***DFT**
A default message.
***EMPTY**
An empty message is appended.
***ATTACHMENT**
The text of the file specified in the ATTACH parameter.
***NONE**
No text is appended.
character-value
Specify the character string to be appended.

Top

-

Mail port number (SMTPPORT)

Specifies the SMTP port for the email.

***DFT**
The default port specified in STRAUD > 89 > 2.
***LOCAL**
The default local port.
character-value
Specify a particular value.

Top

-

SSL/TLS Secured Mail (SMTPSSL)

Specifies whether mail is sent via secured or unsecured SMTP.

***DFT**

The defualt value specified in STRAUD > 89 >2.

***YES**

Mail is sent secured.

***NO**

Mail is sent unsecured.

Top

-

Object size to allow attach (ATCOBJ)

Specifies the maximum size of an attachment.

***NO**
No objects can be attached.

***NOMAX**
Objects of any size can be attached.

decimal-number
Specify a maximum size, in MB.

Top

-

Delete attachment (ATCDLT)

Specifies whether to delete the attached file once the email is successfully sent.

***NO**
Do not delete the file.

***YES**
Delete the file.

Top

-

Convert attachment to ASCII (CVTATT)

Specifies whether to convert the attachment to ASCII.

***NO**
Do not convert the document.

***YES**
Convert the document.

Top

-

Zip (ZIP)

Specifies whether to attach the document in ZIP format.

***NO**
Do not zip the document.

***YES**
Zip the document.

Top

-

ZIP password (ZIPPWD)

Specifies whether to use a password for an attached ZIP file, and what the password should be.

***NO**

Do not use a password for the ZIP file.

character-value

The password to use for the ZIP file.

Top

-

Environment (ENVLIB)

Specifies the environment library to use.

***AUD**
The environment library for iSecurity Audit.

***AV**
The environment library for iSecurity Antivirus.

***FS**
The environment library for FileScope.

Top

-

Send in BATCH mode (BATCH)

Specifies whether to send the email in batch mode.

***YES**
Send the email in batch mode.

***NO**
Do not send the email in batch mode.

Top

-

Dump RLSNDM command into QGPL (DUMP)

Specifies whether and how to send dump data if needed.

***NO**
Do not send dump data.
***FILE**
Write the dump data to a file.
***JOBLOG**
Write the dump data to the joblog.
***BOTH**
Write the dump data to both a file and the job log.
***DUMP**
Write the dump data to the default destination defined for it.

Top

-

Mail (SMTP) server name (HOST)

Specifies the SMTP server for sending mail.

***LOCALHOST**
The local server.

***DFT**
The default server.

character-value
Specify the name of a server.

Top

-

Mail account (ACCOUNT)

Specifies the account used for sending email.

***SENDER**
Use the value of the SENDER parameter.

***DFT**
The default account.

***NONE**
Do not specify an account.

character-value
Specify the name of the account.

Top

-

Account password (PWD)

Specifies the account password used in sending email.

***DFT**
The default password.
***NONE**
Do not specify a password.
character-value
Specify the password.

Top

-

CCSID (CCSID)

Specifies the CCSID for sending mail.

***JOB**
The CCSID of the job.

***PROD**
The CCSID specified as the "CCSID to use as origin of data" in BASE System Configuration Language Support (STRAUD > 81 > 91).

***DFT**
The default CCSID.

***SYSVAL**
The value of the system value "CCSID".

***SMS**
819, the value for standard ASCII.

37-65535
The literal value "37-65535".

Top

-

Insert CR in text body (INSCR)

Specifies whether to insert carriage returns at line endings in the email.

***NONE**
Do not insert carriage returns.

***DFT**
Follow the system default.

decimal-number
Specify the number of carriage returns to be inserted.

Top

-

User defined data (USRDFNDTA)

Specifies user-defined data concerning the email/

***NONE**
Do not use user-defined data.
character-value
Specify the user-defined data.

Top

Examples

None

Top

Error messages

Unknown

Top

Run Audit Query (RUNAUQRY)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Run Audit Query (RUNAUQRY) command runs queries within audit. Depending on how and from where within Audit you are running the query, some fields may already be filled in with read-only values.

Top

Parameters

Keyword	Description	Choices	Notes
QRY	Query F4=Names	*Name*, ***SELECT**	Optional, Positional 1
PRVMIN	Display last minutes	*Decimal number*, ***BYTIME**	Optional, Positional 2
FROMTIME	Starting date and time	*Element list*	Optional, Positional 3
	Element 1: Starting date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN, *START	
	Element 2: Starting time	*Time*, **000000**	
TOTIME	Ending date and time	*Element list*	Optional, Positional 4
	Element 1: Ending date	*Date*, ***CURRENT**, *YESTERDAY, *WEEKSTR, *PRVWEEKS, *MONTHSTR, *PRVMONTHS, *YEARSTR, *PRVYEARS, *MON, *TUE, *WED, *THU, *FRI, *SAT, *SUN	
	Element 2: Ending time	*Time*, **235959**	
USRPRF	User profile	*Generic name, name*, ***ALL**	Optional, Positional 6
RUNACT	Run Action on each row	*Name*, *YES, ***NO**	Optional, Positional

			10
RUNACTEND	Run Action after end of query	*Name*, ***NO**	Optional, Positional 11
SYSTEM	System to run for F4=Names	Single values: *ALL Other values (up to 30 repetitions): *Character value*, ***CURRENT**	Optional, Positional 12
NBRRCDS	Number of records to process	*Decimal number*, ***NOMAX**	Optional, Positional 13
OUTPUT	Output	*****, *PDF, *HTML, *CSV, *OUTFILE, *PRINT, *PRINT1, *PRINT2, *PRINT3, *PRINT4, *PRINT5, *PRINT6, *PRINT7, *PRINT8, *PRINT9	Optional, Positional 14
MRGDTA	Merge data to a single output	***YES**, *NO	Optional, Positional 15
OUTON	Place output on	*Name*, ***CURRENT**, *SYSTEM	Optional, Positional 16
PRTFMT	Print format	***SHORT**, *FULL	Optional, Positional 18
COLHDG	Add column headings	*NO, ***YES**	Optional, Positional 19
CTLFLD	Add control fields	***NO**, *YES	Optional, Positional 20
OUTFILE	File to	*Qualified object name*	Optional,

	receive output		Positional 21
	Qualifier 1: File to receive output	*Name*, ***AUTO**, *QRY	
	Qualifier 2: Library	*Name*, *LIBL, *CURLIB, ***DATE**	
MAILTO	Mail to (list, *USER, *SELECT)	*Character value*, *SELECT, *USER, ***NONE**	Optional, Positional 24
MAILTEXT	Mail text	Values (up to 20 repetitions): *Character value*	Optional, Positional 25
FOOTNOTE	Footnote Message	*Character value*, *DFT, ***ATTACHMENT**, *NONE	Optional, Positional 26
ZIP	Zip	***NO**, *YES	Optional, Positional 27
ZIPPWD	ZIP password	*Character value*	Optional, Positional 28
ATCOBJ	Object size to allow attach	*Decimal number*, **20**, *NO, *NOMAX	Optional, Positional 29
ATCDLT	Delete if attached	*NO, ***YES**	Optional, Positional 30
JOBD	Job description.	Single values: ***NONE** Other values: *Qualified object name*	Optional, Positional 32

	Qualifier 1: Job description.	*Name*, **QBATCH**	
	Qualifier 2: Library	*Name*, ***PRODUCT**, *LIBL, *CURLIB	
AUDTYP	Audit type	*ALL, ***QRY**, *AUTFAIL, *CMD, *CMDENT, *CMDAODINT, *CMDCHK, *CMDUNIX, *CREATE, *DELETE, *DFN, *JOBDTA, *NETCMN, *OBJMGT, *OFCSRV, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDTA, *SAVRST, *SECURITY, *SERVICE, *SPLFDTA, *SYSMGT, *CHANGE, *CHGALL, *PTFOBJ, *PTFOPR, *VIRUS	Optional, Positional 5
PGM	Program name	*Generic name, name*, ***ALL**	Optional, Positional 7
JOB	Job name	*Qualified job name*	Optional, Positional 8
	Qualifier 1: Job name	*Generic name, name*, ***ALL**	
	Qualifier 2: User	*Generic name, name*, ***ALL**	
	Qualifier 3: Number	000000-999999, ***ALL**	
TIMEGRP	Filter by time group	*Element list*	Optional, Positional 9
	Element 1: Relationship	*IN, *OUT, *NONE, ***QRY**	
	Element 2: Time group	*Name*, ***SELECT**	
ORGSYS	Original com-	*Name*, ***CURRENT**	Optional,

	mand sent from		Positional 17
OBJ	Object (*TEMP for attach only)	*Character value*, *TEMP, *QRY, ***AUTO**, *DESC	Optional, Positional 22
DIR	Directory ('/dir/')	*Character value*, '/iSecurity/report output/', ***DATE**	Optional, Positional 23
USRDFNDTA	User defined data	*Character value*	Optional, Positional 31
START	Start query display	*OLD, *NEW, ***DFT**	Optional, Positional 33

Top

Query F4=Names (QRY)

Specifies the name of the query to run.

<u>*SELECT</u>

If the command is running interactively, opens a dialog with a list of existing queries.

name

Specify the name of the query to run.

Top

Display last minutes (PRVMIN)

To view activity in a period of time up to when the report is run, set this parameter to the number of minutes that you would like to check. For example, to see information for the previous two hours, set this value to "120". This parameter overrides the FROMTIME and TOTIME parameters.

***BYTIME**

Use the values set in the FROMTIME and TOTIME parameters.

decimal-number

Specify the number of minutes before the time that the query is run to be checked.

Top

Starting date and time (FROMTIME)

Specifies the date and time at which the information to be queried begins.

Element 1: Starting date

***CURRENT**
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. The starting day is specified in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

***START**

The earliest information available.

date

Specify the date on which the information to be queried begins. The day must be in YYMMDD format, with or without separators.

Element 2: Starting time

000000

The start of the day.

time

The time to begin on the date specifed in the previous parameter, in 24-hour HHMMSS format, with or without separators. Specify the time in HHMMSS format.

Top

-

Ending date and time (TOTIME)

Specifies the date and time of the last information to be queried

Element 1: Ending date

<u>*CURRENT</u>
The current date

***YESTERDAY**
Yesterday's date

***WEEKSTR**
The first day of the current week. The starting day is specified in Base Support > Global Installation Defaults > Installation (STRAUD > 89 > 51 > 1).

***PRVWEEKS**
The first day of the previous week

***MONTHSTR**
The first day of the current month

***PRVMONTHS**
The first day of the previous month

***YEARSTR**
The first day of the current year

***PRVYEARS**
The first day of the previous year

***MON**
Monday

***TUE**
Tuesday

***WED**
Wednesday

***THU**
Thursday

***FRI**
Friday

***SAT**
Saturday

***SUN**
Sunday

date

Specify the date on which the information to be queried ends, in YYMMDD format with or without separators.

Element 2: Ending time

000000

The start of the date specifed in the previous parameter, at midnight.

time

The time to end on the pecifed date, in 24-hour HHMMSS format, with or without separators.

Top

User profile (USRPRF)

Specifies name of a user, or the generic* name or %GROUP name of a group of users, whose data the query examines.

<u>*ALL</u>
Include data for all users.

generic-name
Specify the generic name of users or groups to include.

name
Specify the name of the single user or group to include.

Top

Run Action on each row (RUNACT)

Specifies whether an action will be run as each row is examined.

***YES**

Run the action with the name previously specfied in the query definition on each row.

***NO**

Do not run an action on each row.

name

Specify the name of an action to be run on each row.

Top

Run Action after end of query (RUNACTEND)

Specify whether to run immediately, at the end of the query, the action defined for query type $8.

***NO**

Do not run an action at the end of the query.

name

Specify the name of an action to run immediately when the query ends.

Top

System to run for F4=Names (SYSTEM)

If the local repository contains information from multiple systems, specifies the subset of systems whose information is to be included.

Single values

***ALL**

Include information for all systems.

Other values (up to 30 repetitions)

***CURRENT**

The current system.

character-value

Specify the name of the subset of systems to be included.

Top

Number of records to process (NBRRCDS)

Specifies the maximum number of records to process.

<u>*NOMAX</u>
Process all records.
decimal-number
The maximum number of records to process.

Top

Output (OUTPUT)

Specifies the destination for output.

*****

For interactive jobs, the report is displayed. For non-interactive jobs, report is printed with the job's spooled output.

***PDF**

Print report to PDF outfile.

***HTML**

Print report to HTML outfile.

***CSV**

Print report to CSV outfile.

***OUTFILE**

Print report as text to an outfile.

***PRINT**

Print to default printer.

***PRINT1-9**

User-defined options.

Top

Merge data to a single output (MRGDTA)

Specifies whether to merge all data to a single output.

<u>*YES</u>
Merge all data to a single output.
***NO**
Do not merge all data to a single output.

Top

Place output on (OUTON)

Specifies where output is produced. For internal use only. Do not change this parameter.

<u>*CURRENT</u>
Place output in the current folder.

***SYSTEM**
Place output in a folder determined by the system.

name
Specify the name of the folder.

Top

Print format (PRTFMT)

Specifies the format if output is created as a message.

<u>*SHORT</u>
Output must only be one line.
***FULL**
Output may be more than one line.

Top

Add column headings (COLHDG)

Specifies whether to output comlumn headings for CSV (Excel) format.

***NO**

Do not output column headings.

***YES**

Output column headings.

Top

Add control fields (CTLFLD)

Specifies whether to output control fields for CSV (Excel) format or outfile.

<u>*NO</u>
Do not output control fields.

***YES**
Output control fields.

Top

File to receive output (OUTFILE)

Specifies the file to receive output if OUTFILE has been selected.

Qualifier 1: File to receive output

***AUTO**

The report name plus a six-digit number (automatically incremented).

***QRY**

The name of the query.

name

Another speficied name.for the file.

Qualifier 2: Library

***LIBL**

Search the Library List for an appropriate library.

***CURLIB**

The current library.

***DATE**

A library name derived from the date on which the query is run.

name

Specify a defined name for the library.

Top

Mail to (list, *USER, *SELECT) (MAILTO)

Specifies users or lists to receive email that the query sends. The field can contain multiple values.

***SELECT**
If running interactively, opens a dialog to specify the recipient.
***USER**
Send email to the user running the query.
***NONE**
Do not send email.
character-value
A particular defined user or list.

Top

Mail text (MAILTEXT)

Specifies the text that the query sends as email.
You can specify 20 values for this parameter.

character-value

A character string to be sent.

Top

Footnote Message (FOOTNOTE)

Specifies what to place as a footnote at the end of the output.

***DFT**

Include the default message: "This e-mail is produced by Raz-Lee."

***ATTACHMENT**

Include the message: "This e-mail and its attachments may contain confidential information. It is advisable to delete suspicious e-mails and to contact the corporate Security Administrator promptly."

***NONE**

Do not include a footnote.

character-value

A text string to be included in the footnote.

Top

Zip (ZIP)

Specifies whether to include a ZIP file containing the output.

<u>*NO</u>
Do not include a ZIP file.
***YES**
Include a ZIP file.

Top

ZIP password (ZIPPWD)

Specifies a password used to encrypt the ZIP file.

character-value

The password as a character string.

Top

Object size to allow attach (ATCOBJ)

Specifies whether to allow an attached object, and its maximum size.

20
: Include attachments up to 20 MB in size.

***NO**
: Do not allow attachments.

***NOMAX**
: Attachments of any size are allowed.

decimal-number
: Specify a maximum size in MB.

Top

Delete if attached (ATCDLT)

Whether to automatically delete the output file after the email to which it is attached has been sent successfully.

***NO**
Do not delete the file.

***YES**
Delete the file.

Top

Job description. (JOBD)

Specifies the job within which the query will run.

Single values

***NONE**

Run within the job that is running the query.

Qualifier 1: Job description.

QBATCH

Run within the job QBATCH.

name

Specify the name of the job within which it is to run.

Qualifier 2: Library

***PRODUCT**

The program is within the library for the product.

***LIBL**

Search the Library List for an appropriate library.

***CURLIB**

The program is within the current library.

name

The name of the library containing the program.

Top

Audit type (AUDTYP)

Specifies the audit Type for the query. Most of the values are documented in the IBM i Security Reference Manual, in either

- Table 115 (Possible values for AUDLVL) online at www.ib-m.com/docs/en/i/7.4?topic=profiles-action-auditing
- Table 133 (Security auditing journal entries) online at www.ib-m.com/docs/en/i/7.4?topic=actions-security-auditing-journal-entries

Those that are not in those tables are documented below.

***QRY**
The audit type previously specified for the query.

***CMDENT**
Commands entered interactively.

***CMDAODINT**
Commands entered during an AOD (Authority on Demand) session.

***CMDCHK**
Information resulting from iSecurity/Command.

***CMDUNIX**
Not used. Kept for compatibility use only.

***DFN**
Specifies the definition of the firewall.

***CHGALL**
Included for compatibility only. Do not use this.

***VIRUS**
Information resulting from iSecurity/Antivirus and iSecurity/Anti-ransomware.

Top

Program name (PGM)

Specifies the message running when the message was produced.

***ALL**
Messages from all programs.

generic-name
Messages produced by programs with this generic name.

name
Messages produced by programs with this specific name.

Top

Job name (JOB)

Specifies the jobs to be examined.

Qualifier 1: Job name

***ALL**
All jobs.

generic-name
Jobs with the specified generic name.

name
Jobs wih the specified name.

Qualifier 2: User

***ALL**
All users.

generic-name
Users with the specified generic name.

name
Users with the specific name.

Qualifier 3: Number

***ALL**
All jobs.

000000-999999
Jobs with a specific number.

Top

Filter by time group (TIMEGRP)

Specifies a defined set of times to be included or excluded.

Element 1: Relationship

***IN**
Include the timegroup.

***OUT**
Exclude the timegroup.

***NONE**
Do not consider the timegroup.

***QRY**
If running interactively, ask whether to include or exclude the timegroup.

Element 2: Time group

***SELECT**
If running interactively, present a set of timegroups to consider.

name
The name of a specific timegroup.

Top

Original command sent from (ORGSYS)

Specifies the system from which the original command was sent.

***CURRENT**

The current system.

name

The name of a specific other system.

Top

Object (*TEMP for attach only) (OBJ)

Specifies the name of the object in which output is collected. This information depends on the Global Site Defaults, entered via STRAUD > 81 > 59 > 3.

***TEMP**

A temporary name, assigned by the system, used if he file is only used as an attachment.

***QRY**

The name of the query.

***AUTO**

The object is determined automatically.

***DESC**

The description of the query

character-value

A specific character string.

Top

Directory ('/dir/') (DIR)

Specifies the directory containing the onject.

'/iSecurity/report output/'
The '/iSecurity/report output/' directory.

<u>*DATE</u>
A directory name determined by the date on which the query is run.

character-value
A character string to serve as the directory name.

Top

User defined data (USRDFNDTA)

Specifies other information, defined by the user

character-value

A string of text or other information.

Top

Start query display (START)

Specifies whether the records are processed starting with the oldest or with the newest.

***OLD**
Sart with the oldest record.

***NEW**
Start with the newest record.

***DFT**
Use the system default to determine whether to start with the oldest or newest record.

Top

Examples for RUNAUQRY

Example 1: Simple Command Example

```
RUNAUQRY QRY(Z$A_ALLOBJ)          SYSTEM(*ALL)
  OUTPUT(*)
```

This command runs the query Z$A_ALLOBJ (User Profiles with *ALLOBJ authority) collecting information from all systems and showing it on the screen.

Example 2: More Complex Command Example

```
RUNAUQRY QRY(ZCD_ALL)          FROMTIME(*MON 000000)
           TOTIME(*CURRENT)    OUTPUT(*PDF)
           MAILTO(ADMIN@COMPANY.COM)
```

This command runs the query ZCD_ALL (Auditing Command Strings) for information collected since last Monday, creates a PDF and emails it.

Top

Error messages

Unknown

Top

Set iSecurity Authorization (SETISAUT)

Where allowed to run: All environments (*ALL)
Threadsafe: No

Parameters
Examples
Error messages

The Set iSecurity Authorization (SETISAUT) command sets the authorization codes for iSecurity products.
Codes can be set for multiple products on a single CPU. The codes do not have to be in any particular order. The command recognizes the product for each code and applies the code to it.
The screen is frequently used to generate a command string that can be run later.

Top

Parameters

Keyword	Description	Choices	Notes
CPU	CPU serial number	*Character value*, *CURRENT	Optional, Positional 1
A	Any iSecurity product	*Element list*	Optional, Positional 2
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
B	Any iSecurity product	*Element list*	Optional, Positional 3
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
C	Any iSecurity product	*Element list*	Optional, Positional 4
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
D	Any iSecurity product	*Element list*	Optional, Positional 5
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
E	Any iSecurity product	*Element list*	Optional, Positional 6
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
F	Any iSecurity product	*Element list*	Optional, Positional 7
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
G	Any iSecurity product	*Element list*	Optional, Positional 8

	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
H	Any iSecurity product	*Element list*	Optional, Positional 9
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
I	Any iSecurity product	*Element list*	Optional, Positional 10
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
J	Any iSecurity product	*Element list*	Optional, Positional 11
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
K	Any iSecurity product	*Element list*	Optional, Positional 12
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
L	Any iSecurity product	*Element list*	Optional, Positional 13
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
M	Any iSecurity product	*Element list*	Optional, Positional 14
	Element 1: Part 1	*Character value*	
	Element 2: Part 2	*Character value*	
N	Any iSecurity product	*Element list*	Optional, Positional 15
	Element 1: Part 1	*Character value*	

Element 2: Part 2 *Character value*

Top

CPU serial number (CPU)

Specifies the serial number of the CPU for which the authorization codes are to be set.

***CURRENT**

The CPU on which the command is running.

character-value

Specify the serial number of a CPU.

Top

Any iSecurity product (A)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (B)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (C)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (D)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (E)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (F)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (G)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (H)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (I)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (J)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (K)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (L)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (M)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Any iSecurity product (N)

Specifies a security code valid for that CPU.

Element 1: Part 1

character-value

Specify the first part of an authorization code or, if the code is not divided into two parts, the entire code.

Element 2: Part 2

character-value

If the authorization code is in two parts, the second part of the code.

Top

Examples

None

Top

Error messages

Unknown

Top