

# Softlight Auditor

## for the IBM iSeries and AS/400

Version 3.3  
System Reference Manual

Softlight Corporation  
[www.softlightcorp.com](http://www.softlightcorp.com)

*Convention:*

Throughout this manual **[ENTER]** means to press the key marked as Enter, **[F3]** means to press the key marked F3 or Cmd3, etc.

This manual describes Version 3.3 of Softlight Auditor for the IBM AS/400 and iSeries midrange systems running OS/400. Softlight, and Softlight Auditor, are trademarks of Softlight Corporation. Trademarks of other companies belong to their respective owners.

**What was changed/enhanced in this release?**

The primary change to this release was the addition of reports for use of Service Tools and changes logged for \*SYSMGT (actions on the QAUDLVL system value). While both of these actions should be rare, it is important to have a report that identifies them.

In addition, the stop list for filtering reports was updated to be able to filter by security journal record type (instead of report) making it more flexible.

Copyright © 1992, 2009 by Softlight Corporation  
All Rights Reserved



## Softlight Auditor Reference Guide

Getting Started .....	3
Before you begin.....	3
System requirements.....	4
Displaying hardware configuration and OS/400 level.....	4
For additional information .....	4
Data Flow.....	5
Notices .....	5
How this manual is organized.....	6
On-line information .....	7
Installing Softlight Auditor.....	9
Getting the software loaded onto your AS/400 or iSeries .....	9
Installation procedure .....	12
Changing the Auditing Level After Setup .....	16
Turn off auditing during major software installation.....	16
Troubleshooting Installation Issues .....	16
Removing Softlight Auditor from your system .....	18
Running Your First Audit.....	19
What to look for on a first audit.....	20
Configuring Softlight Auditor .....	23
Normal business hours.....	25
Business holidays.....	27
Normal locations.....	28
User profile controls .....	28
Report defaults.....	30
Library/object stop list.....	31
Changing where reports print .....	32
Auditing all commands by a user.....	33
Auditing individual objects and commands.....	34
Status Auditing .....	36
Event Auditing.....	37
Audit new events .....	38
Display security-related messages.....	39
Display audit start date .....	39
Change audit start date.....	39
Common Tasks .....	41
Managing security journal size.....	41
System-managed security journal receivers .....	42

Scheduling SLA to run at night .....	43
Troubleshooting .....	45
Symptom: Audit ends abnormally, no reports printed.....	45
Symptom: Audit runs, reports cannot be found.....	48
Report Samples .....	51
General comments about reports .....	52
Authority Failures .....	53
Program Failures .....	54
Authority Changes .....	55
Audited Commands .....	56
Objects Created.....	57
Programs Created.....	58
Objects Deleted.....	59
Reset DST Security Password .....	60
User Profile Changes .....	61
User ID changed on Job Description .....	62
Objects Moved or Renamed.....	63
Changes in Object Ownership .....	64
Programs Changed to Adopt Authority .....	65
Invalid Password or User ID.....	66
Programs Restored that Adopt Authority .....	67
System Value Changes .....	68
Audited Object Accesses .....	69
Audited Object Changes .....	70
Service Tool Actions Report.....	70
System Management Report.....	70
Interactive Job Exceptions .....	71
Random Sample of Jobs by User .....	72
System History Log Messages.....	73
Functions retained from prior releases.....	74
Job logs .....	74
Sample of messages in QHST.....	75
Message control file.....	76
Default percentage of messages by severity .....	78
Capturing job logs.....	78
How the CHGSIGNOFF command works .....	79
SETUP Worksheet.....	81
Reader comment form.....	83
License agreement .....	84
Index .....	85

---

## Getting Started

### Before you begin

Thank you for this chance to earn your business!

We, at Softlight Corporation, are delighted that you are interested in our software, and we want it to perform up to your expectations. Please read this section carefully before you install Softlight Auditor.

If you must review activity on your AS/400 or iSeries, you are faced with a daunting task. Many security events are logged to the system history log, QHST. Many more are logged to the security journal, QAUDJRN.

Unfortunately, these records are arranged chronologically, not logically. Our program selects, sorts, sifts and randomly samples to help you review activity with less effort. With one command, Softlight Auditor will select every security-related event that has occurred since your last audit, and prepare a series of short, well-organized reports for your review.

Softlight Auditor™ is designed to help you perform normal DP audit functions on your IBM AS/400 or iSeries. The programs of Softlight Auditor are *tools* to aid you, not substitutes for your judgment. This is a key point: we do not warrant that the use of these programs will catch all events that you might want to review, nor do we claim that Softlight Auditor will give you a risk-free system. Seems obvious, doesn't it, but we must emphasize that *you, not we*, are responsible for the security of your system.

The programs and documentation are copyrighted. We make them available to you only by license agreement. *A copy of our license agreement is included at the end of this manual. If you do not wish to accept our terms, do not install the software and return the media and other materials we sent you before the end of your trial period.*

We do believe that the use of our software will make your job easier, less tedious, and shorter. Your trial period gives you the opportunity to decide for yourself.

## System requirements

- **Your AS/400 or iSeries must be running Version 4, Release 1, Modification level 0 (or higher) of OS/400.**
- You should not have a user profile named SLAUDIT.
- You should not have a library named SLAINSTALL, SLAUDIT or SLAUDIT2.
- Your system should have at least 40 megabytes of free disk space.

Although not required, we strongly recommend that your system be running at security level 30 or above, and that you use the security journal, QAUDJRN. While Softlight Auditor will run at level 10 or 20, and without QAUDJRN, *much information needed for a good security audit is not available.*

Moving from a lower security level can be a time-consuming task. We are not able to assist sites with a security implementation. If you do not have an in-house DP staff, you will probably need assistance from IBM or a third party.

## Displaying hardware configuration and OS/400 level

If you need to check which version of OS/400 your system has installed, sign on as the security officer and use the IBM command DSPSFWRSC (Display Software Resources). This command can take a minute to run. Use [F11] to display the version numbers for any of the following

5769999	*BASE	5050	AS/400 Licensed Internal Code
5769SS1	*BASE	5050	Operating System/400
5769SS1	*BASE	2924	Operating System/400

If you need the processor number of your AS/400 or iSeries, use the command DSPHDWRSC TYPE(\*PRC) (Display Hardware Resources). Take option 7 on the line CEC01 9402-40S Operational Main Card Enclosure to get the processor, model number and serial number, should you need them.

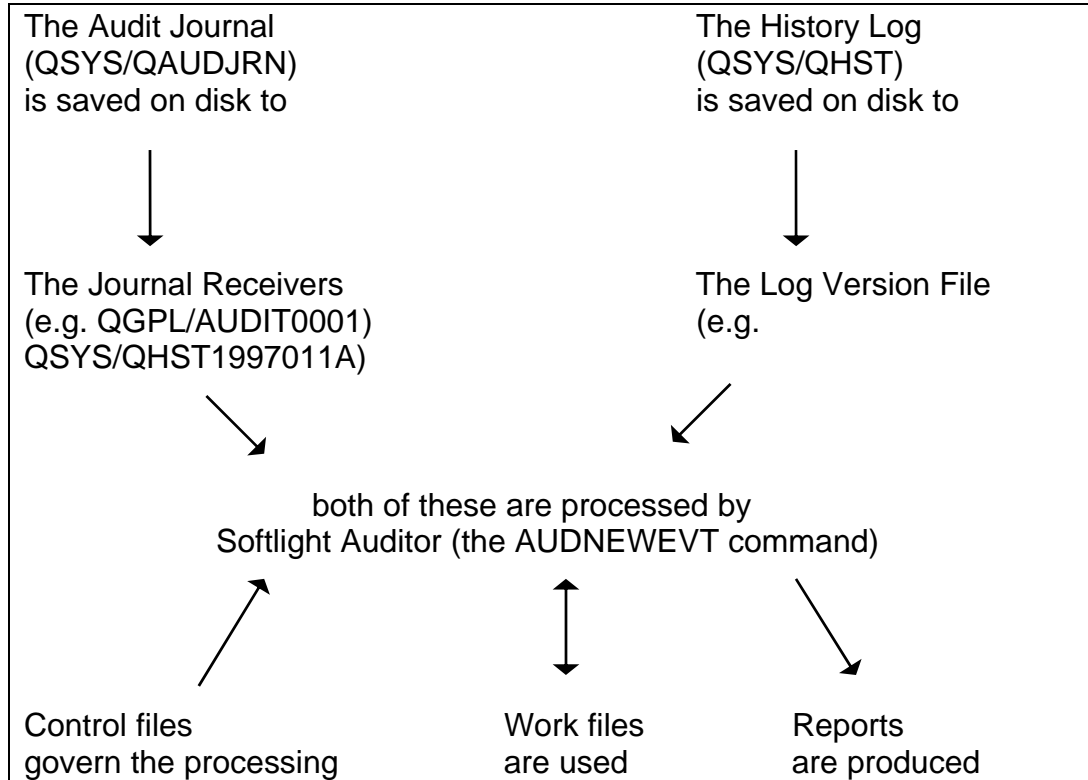
## For additional information

We provide online information, accessible from our menus.. We also recommend the following resources.

- iSeries Security  
<http://publib.boulder.ibm.com/series/v5r2/ic2924/books/c4153026.pdf>
- IBM Redbooks  
<http://www.redbooks.ibm.com/Redbooks.nsf/portals/systemi>

## Data Flow

Here is a schematic representation of how Softlight Auditor relates to the OS/400 security journal and history log.



## Notices

Softlight, the Softlight logo, and Softlight Auditor are trademarks of Softlight Corporation. IBM, AS/400, iSeries, OS/400 and Application System/400 are trademarks of IBM. This manual may contain typographical errors.

There is a reader comment form at the back of this manual. We welcome your comments and suggestions for improvement. If the form is missing, please write to us.

Softlight Corporation  
PO Box 923 Clinton, SC 29325 USA [www.softlightcorp.com](http://www.softlightcorp.com)  
Phone (voice and fax): 1-864-833-6559 E-mail: [info@softlightcorp.com](mailto:info@softlightcorp.com)

Copyright © 1992, 2009 by Softlight Corporation. All rights reserved.

---

## How this manual is organized

The major section headings of this manual are

*Installing Softlight Auditor*, which tells how to load the product on your system, enter the authorization code to allow its use, and grant the authorities needed to those who will run the audits.

Complete the *Installing* section before you proceed to any of the others.

*Running Your First Audit*, which gives our recommendations for how to get started with the program.

*Configuring Softlight Auditor*, which explains the ways you can tailor the program.

*Event auditing*, which shows how you will use Softlight Auditor on a regular basis to save you time and work.

Sections on *Common tasks* and *Troubleshooting* are included.

Then manual also contains samples of reports produced by the programs.

You will find a reader comment form at the back, just before the index. We welcome suggestions for making this manual more useful to you.



## On-line information

On-line information (help text) is available after you install Softlight Auditor. Take option 88 from any Softlight Auditor menu to search the help index. For example, if you want to know how to run an event audit at night, you could search for "how night" or "unattended."

Here are some of the topics contained in the on-line information.

```
Softlight Auditor Online Information

Type options, press Enter.
 5=Display topic  6=Print topic

Option  Topic
  _      Tutorial, getting started
  _      How to use online information.
  _      Quick Start.
  _      Defining what is "normal."
  _      How to run an audit automatically (unattended).
  _      How to remove old entries from QAUDJRN.
  _      How to change the starting date for an audit.
  _      How to change which reports print automatically.
  _      How to change report characteristics
  _      How to change which messages from QHST to report.
  _      How to capture and view job logs.
  _      How to order or renew your annual license.

More...
Or to search again, type new words and press Enter.
night_____
```

This information is provided as an OS/400 search index. Thus, it works just like any other OS/400 search index. You may view or print topics.

A tutorial is part of the on-line information. Search for "intro" to locate it.

To locate "how to" topics, search for the word "how." To locate "what is" topics, search for the word "what." Other common key words include "change" and "error."

When viewing on-line information, you will see some words and phrases that are **highlighted** and preceded by an underscore ( ). Use the tab key to position the cursor on any of these underscores, then press Enter to go directly to the related topic. After reading the related topic, [F12] will take you back.

A sample screen from a topic in the on-line help is reproduced below.

Help

Running an unattended audit.

You may run an event audit automatically, for example, as a part of a nightly procedure. The values you would normally supply on the prompt screen may be passed as arguments when you invoke the command from another procedure.

The command which runs an event audit is SLAUDIT/AUDNEW EVT

You should adjust the library list of the submitting job to add libraries SLAUDIT and SLAUDIT2 before running the AUDNEW EVT command, and to remove them after the audit is finished.

To invoke the command from another procedure, or from a job scheduler, the correct syntax is

```
SLAUDIT/AUDNEW EVT +  
SOURCE(*BOTH) REPORTS(*ALL) CLEAR(*YES) BATCH(*YES) +  
NEWRCVR(*NO)
```

More...

F3=Exit help    F10=Move to top    F12=Cancel    F13=User support  
F14=Print help

Most commands used by Softlight Auditor have on-line help. Key the command name and press [F4] to view the command's parameters. Then press the Help key to view the on-line information for the command.

The on-line information may have been updated since this manual was printed.

We are very interested in your comments about this on-line help facility. We want you to be able to find the answers to most of your questions by consulting it. If you think new topics should be added, or current topics need to be rewritten or indexed differently, please drop us a note.

---

## Installing Softlight Auditor

*Note: Softlight Auditor is delivered as a compressed, Windows-based file. You must first load and uncompress the file on a desktop PC, and then transfer the software to your AS/400 or iSeries computer over your network.*

### ***You will need 4 things:***

- The IP address of your iSeries or AS/400
- The QSECOFR password  
(The system operator or manager in your data center will normally have these two.)
- The Windows-based file slaudit.zip (which we ship to you on a CD or which you may download from our web site.)
- A Windows-based PC connected to your iSeries or AS/400 via a network.

If you are curious about security during installation, please note the following general information. Specific instructions, including setting these conditions, are provided further below, in the step by step instructions.

- The *installation* must be run by the security officer, QSECOFR.
- The system value ALWOBJRST must be set to \*ALL before beginning this installation. Use WRKSYSVAL ALWOBJRST to display this system value. Note the current value so that you can change it back after installation.
- After installation, all programs may be run by user profile SLAUDIT. We recommend using profile SLAUDIT, since we have configured it with the minimum authority adequate to run the programs. Profile SLAUDIT *does not* have ALLOBJ authority. If you wish to use another profile, it is your responsibility to configure that profile with adequate authority.

## Getting the software loaded onto your AS/400 or iSeries

☞ The first two steps are performed on a desktop computer attached to the same network as your iSeries or AS/400. This example assumes a Windows PC. If you use a Mac, your IT department can supply equivalent commands.

1. **Get the file “slaudit.zip” loaded onto your Windows-based PC.**  
(Use either of the following options.)

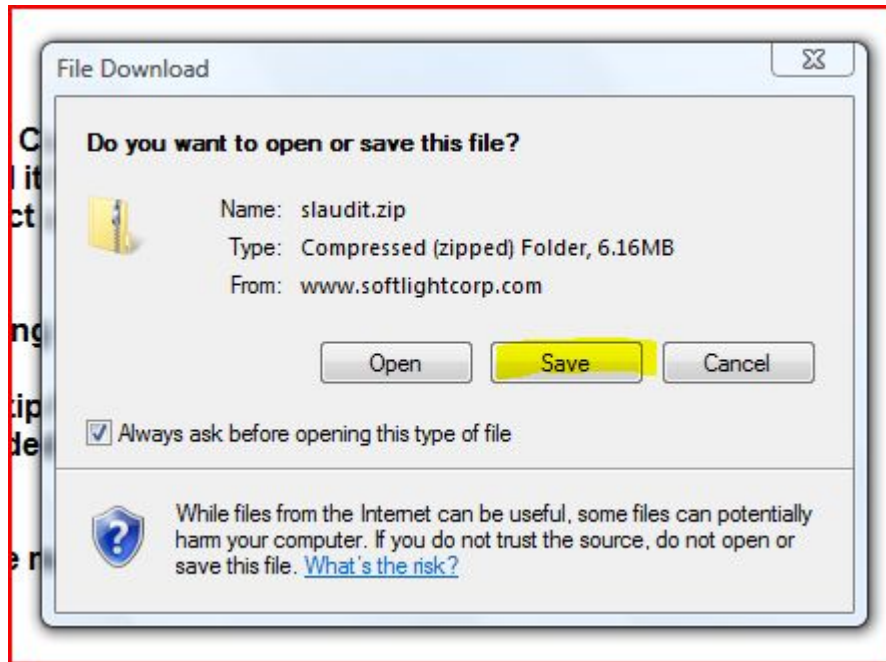
- Copy the file to your PC from the CD we shipped to you, or
- Download the file from <http://www.softlightcorp.com/download2> (“Step 2” on the web page. If you are reading this, you have “Step 1.” If you have not received a manual in the mail, you should download a copy while you are visiting our web site – “Step 3.”.)

Step 1: Click [here](#) to download instructions for installing from a personal computer.

Step 2: Click [here](#) and choose "save" to download a zip file containing the software to your personal computer.

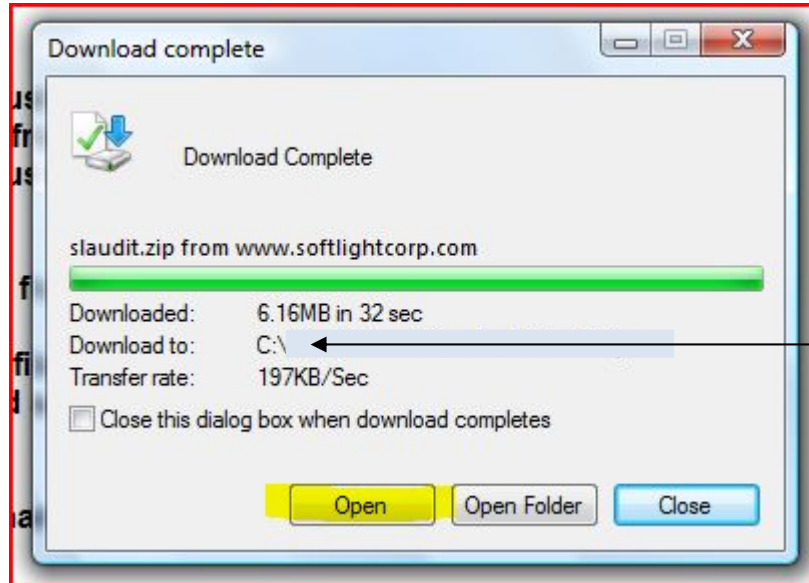
Step 3: Click [here](#) and choose "save" to download the manual.

The example screens assume you are using Vista. Check with your IT support group if you need help downloading from the web or uploading to your iSeries/AS400.



2. Open the downloaded file, slaudit.zip, and follow the instructions to extract/unzip the iSeries/AS400 file SLAUDIT.

**Make a note of the location on your PC to which the software is extracted. This example assumes you extract to the top level of the C: drive, "C:\".**



Now you have a compressed file named slaudit.zip on your PC. Double click to unzip it (we suggest into the c:\ root directory), producing a second file named "slaudit" (no suffix, just "slaudit") on your PC. This file is in iSeries (AS/400) format, and ready to upload.

☞ The next two steps are performed on the iSeries or AS/400 and will create a file there to hold the installation program.

3. *On the iSeries/AS/400:* Sign-on as QSECOFR.
4. *On the iSeries/AS/400:* Type CRTSAVF QGPL/SLAUDIT [ENTER]

*Note: If you are upgrading, the prior command will likely fail because you already have a save file named QGPL/SLAUDIT. In that case, delete it and recreate it:*

```
DLTF QGPL/SLAUDIT [ENTER]
CRTSAVF QGPL/SLAUDIT [ENTER]
```

☞ Switching back to the Windows desktop, the next step copies the installation program to the iSeries.

5. *On the Windows PC:* Transfer the file "slaudit" from your PC to the iSeries or AS/400.

**There are different programs available to do this, and your system manager may be able to recommend an option.**

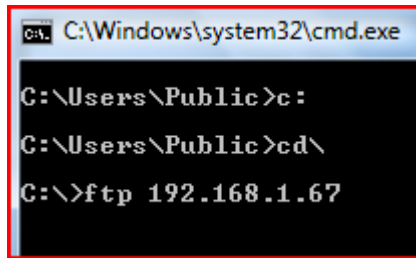
The following example assumes that you will use the Windows command line ftp program.

On XP, from the start menu, choose Run and enter “cmd” or on Vista, from the Start Menu, type “cmd” in the Start Search box.

You should see a command line prompt. Type the following commands.

<b>cd\</b>	(to get to root directory) <i>Change, if you extracted the file to another location on your PC.</i>
<b>ftp x.x.x.x</b>	(for x.x.x.x, use the IP address of iSeries or AS/400)
<b>qsecofr</b>	(in response to user prompt in ftp)
<b>password</b>	(enter actual password for qsecofr, when prompted)
<b>binary</b>	(ftp command to initiate binary transfer to AS/400)
<b>cd qqpl</b>	(ftp command to use the QGPL library on AS/400)
<b>put slaudit</b>	(ftp command to transfer library in saved format)
<b>bye</b>	(end ftp)
<b>exit</b>	(exit command line session on Windows)

In the following, 192.168.1.67 is assumed to be the IP address of the iSeries. Substitute the correct address for your system.



```
C:\Windows\system32\cmd.exe
C:\Users\Public>c :
C:\Users\Public>cd\
C:\>ftp 192.168.1.67
```

etc.

All of the remaining steps are to be done on your AS/400 or iSeries.

## Installation procedure

(Check boxes as completed.)

- Be sure you are signed on QSECOFR
- Enter WRKSYSVAL QALWOBJRST [ENTER]  
*write down the current value, and, if it is not set to \*ALL, change it to \*ALL*

Current value(s): \_\_\_\_\_

**If upgrading from a prior release of SLAUDIT, skip the next section.**

***☞ If installing for the first time:***

- RSTLIB SAVLIB(SLAINSTALL) DEV(\*SAVF)  
SAVF(QGPL/SLAUDIT) [ENTER]
- ADDLIBLE SLAINSTALL [ENTER]
- SLAINSTALL/INSTALL (Press [F4])

Key authorization code and date (values shown below are just illustrations; use those provided with your order), then [ENTER]

If you make a mistake in the expiration date or authorization code, but do not notice it until after you press Enter, don't worry. The installation should run to completion, and you may correct the code or date by using the SLAUDIT/AUTHSLA command.

```
Expiration date YYYYMMDD . . . . 20120615      Character value
      (Example only: 20030615 is June 15, 2003 in YYYYMMDD format)
Authorization code . . . . . 8457325461      Character value
      (Example only. Use code provided with your order.)
Your organization name . . . . . Universal_Widgets,_Inc
Place job on batch queue . . . . *YES          *YES, *NO
      (*YES runs job at lower priority. *NO lets you watch on your terminal. Either is fine.)
```

- Agree to our license terms

After you press [ENTER] on the installation screen, above, the welcome screen shown below will appear. We ask you to read the license agreement found near the end of the manual carefully, and indicate that you accept it by typing the word "YES" in the space provided.

```
Welcome to Softlight Auditor (tm). We are delighted to have this opportunity
to earn your business. PLEASE READ THIS SCREEN CAREFULLY before proceeding.

This program will install everything you need to run Softlight Auditor. It
will create one user profile, SLAUDIT, and two libraries, SLAUDIT and SLAUDIT2.


The program code, screen panels and related documentation are copyrighted, by
Softlight Corporation, Clinton, SC, USA. All rights are reserved except for those
specifically granted by license. Kindly inform any of your employees who may have
access to these programs of our copyright.
***** IMPORTANT *****

By proceeding, you acknowledge that you have read and understand this notice,
and have a copy of our evaluation license agreement. (A copy is in your manual).

Do you understand and agree? (Type YES or NO)  YES
```

When the INSTALL command is finished, you will go back to the OS/400 menu and command line. Our software is now loaded on your system, but it needs initial setup or configuration. Continue with the following steps to complete the installation of Softlight Auditor.

- ADDLIB SLAUDIT [ENTER]
- SLAUDIT/SETUP (Press [F4])

**IMPORTANT:** The values shown in the following example are suggestions for new installations which have not used the OS/400 audit journal before. If you are upgrading, see the  next section.

```

Auditing system values . . . . . *BASIC          *BASIC, *SAME
  *BASIC uses Softlight Corporation's recommendations for new sites
  *SAME leaves the values as they are on your system
  You can always change these later with the WRKSYSVAL command

Receiver name . . . . . AUDIT0001      *GEN, *SAME, name
  Example only. By ending with a 4-digit number, the system can automatically
  name the next receiver AUDIT0002, etc.

Receiver library . . . . . QGPL          *GEN, *SAME, library
  Typical location..

Receiver threshold (KB) . . . . . 7000      5000 to 192000 in KB
  Larger values will lengthen the time of an audit; smaller values will increase the number
  of journal receivers on your system. 7000 - 10000 is a good compromise.

Journal sequence numbering . . . *RESET      *CONT, *RESET
  For new installations, *RESET is recommended. *CONTinue or *RESET may be used
  for upgrades.
  
```

Press [ENTER] to run the SETUP command.

- WRKUSRPRF SLAUDIT (Press [F4])  
Assign a password to user SLAUDIT, then press [ENTER]
- (Skip upgrading steps that follow.)

 **Or, if upgrading from an earlier release of Softlight Auditor:**

- DLTLIB SLAINSTALL [ENTER]
- RSTLIB SAVLIB(SLAINSTALL) DEV(\*SAVF)  
SAVF(QGPL/SLAUDIT) [ENTER]
- ADDLIB SLAINSTALL [ENTER]
- SLAINSTALL/INSTALLUPG (Press [F4])



ADDLIBLE SLAUDIT [ENTER]

SLAUDIT/SETUP (Press [F4])

***IMPORTANT: The values shown in the following example, while typical for upgrading, are for purposes of illustration only.***

Auditing system values . . . . .	*SAME	*BASIC, *SAME
Receiver name . . . . .	*SAME	*GEN, *SAME, name
Receiver library . . . . .	*SAME	*GEN, *SAME, library
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . . .	*CONT	*CONT, *RESET

Press [ENTER] to run the SETUP command.

***☞ In either case (first time or upgrade)***

WRKSYSVAL QALWOBJRST [ENTER]

(Set QALWOBJRST back to the value noted on page 2, above.)

The installation is now complete. If you have trouble, please contact us by phone or fax, (864-833-6559) or by email ([info@softlightcorp.com](mailto:info@softlightcorp.com)).

## Changing the Auditing Level After Setup

You may change the auditing level after you have set up the security journal. Use the WRKSYSVAL QAUDLVL command to enter a new auditing level. On-line help is available for these IBM commands.

To stop logging events to the security journal, change QAUDCTL (not QAUDLVL) to \*NONE. You must stop logging in this way before you can delete the QAUDJRN journal or grant authority to it.

### Turn off auditing during major software installation

We **highly recommend** turning off auditing during major software upgrades, including upgrades of OS/400 and upgrades of any major application software. Why? So many objects are changed during major upgrades that the audit journal receiver can grow to an unwieldy size. To turn off auditing, use WRKSYSVAL QAUDCTL and change it to “\*NONE”. After the upgrade, use the WRKSYSVAL command to change the value of QAUDCLT back to what it was before the upgrade (normally \*AUDLVL and \*OBJAUD).

See the section entitled *Report Samples* in this manual to see what auditing levels are required to collect the data used by the various reports.

## Troubleshooting Installation Issues

**I downloaded the .zip file and unzipping it gives the message: “Cannot open file: it does not appear to be a valid archive. If you downloaded this file, try downloading the file again.” I did re-download and got the same results.**

If you are using WinZip, try right clicking on the files and then select “Extract All” to let Windows do the unzipping.

### **What was changed/enhanced in this release?**

The primary change to this release (which was a maintenance release) was to add reports for use of Service Tools and changes logged for \*SYSMGT (actions on the QAUDLVL system value). While both of these actions should be rare, it is good to have a report that identifies them.

In addition, the stop list for filtering reports was updated to be able to filter by security journal record type (instead of report) making it more flexible.

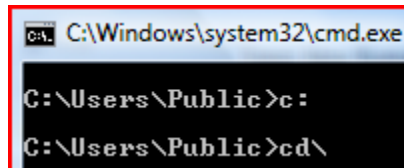
**Will we lose our current Softlight settings when we upgrade (Deleting Lib SLAINSTALL or rerunning setup)?**

Generally, on upgrades all prior settings are retained. However, if there are any issues, we can work with you with you remotely and correct any issues in a matter of a few minutes.

**Error message occurred during FTP: error opening local file SLAUDIT**

When you run ftp you need to be in the same directory as the SLAUDIT file that was unzipped.

Typically, the easiest way to do this is to move the unzipped file to C:\ (root directory of C: drive – not in any folders such as Desktop or My Documents). Then run (CMD) from your PC and follow the example FTP commands above. Note the example assumes the unzipped file “slaudit” is in the C:\ directory.



```
C:\Windows\system32\cmd.exe
C:\Users\Public>c:
C:\Users\Public>cd\
```

## Removing Softlight Auditor from your system

We hope you will decide to license Softlight Auditor. If you have questions please call us.

If you decide that Softlight Auditor is not right for you, you may use the SLAINSTALL/RMVSLA command to remove it from your system.

Make sure that no one is using Softlight Auditor, and that the libraries SLAUDIT and SLAUDIT2 are not in *anyone's* library list. Then key the command SLAINSTALL/RMVSLA and press [F4].

```
Remove Softlight Auditor (RMVSLA)

Type choices, press Enter.

Delete security journal . . . . DLTJRN          *YES
Delete SLAUDIT2 data library . . DLTDTA        *YES
Delete user profile SLAUDIT . . DLTUSR         *YES
```

*Delete security journal* means to change QAUDLVL to \*NONE, stopping security auditing, then to delete the QAUDJRN journal its receiver. You may get a message stating that the receiver has not been fully saved. Take the I option, to ignore this message.

*Delete SLAUDIT2* means to remove the library that contains the data collected by Softlight Auditor on your system. The program library, SLAUDIT, is deleted regardless of your answer here.

*Delete user profile* means to remove the special profile SLAUDIT that was created on your system by the installation procedure. Any objects owned by profile SLAUDIT will also be deleted. Note that you cannot specify \*NO to the prior option and \*YES to this one, since library SLAUDIT2 is owned by profile SLAUDIT.

You may wish to use the WRKOBJOWN (work with objects by owner) command to see what objects are owned by profile SLAUDIT before you run the RMVSLA command.

Use the following commands to remove the installation library.

```
RMVLIBLE SLAINSTALL
DLTLIB SLAINSTALL
```

Softlight Auditor should now be completely removed from your system.

---

## Running Your First Audit

The commands that operate Softlight Auditor may be keyed directly from the command line. We also supply menus for those who prefer them, or who must use menus because their user profile limits access to the command line.

We will assume you want to use menus at first. The command names are usually listed next to each menu line, so you can become familiar with them.

To get to the main menu, sign on as user SLAUDIT.

Although we do not support it, if you prefer to run the audit as some other user, you may bring up the menu by typing, SLAUDIT/STRSLA

```
SLA                               Softlight Auditor Main Menu
                                     System:   S1015241
Select one of the following:

    1. Event auditing                GO SLAEVT
    2. Status auditing              GO SLASTS
    3. Define or change Softlight Auditor  GO SLACFG

    10. Common tasks
    20. Ordering and reauthorization    GO SLAORD

    88. Search Softlight Auditor help index

    90. Signoff
```

Each menu is discussed in a subsequent section.

To run an audit, take option 1, “Event auditing.” From that menu, take option 1 again, “Audit new events.”

You may accept the defaults shown below, or, if you want to watch the program run, you may change “Submit job to batch queue” to “\*NO.” (If you elect not to submit the job, do not run it during a period of peak activity if your system is heavily loaded.) You should also press [F10] on this screen to see how you can change the security journal receiver as a part of the audit.

```

                                Audit New Events (AUDNEW EVT)

Type choices, press Enter.

Source of events to audit . . . *BOTH____      *BOTH, *QHST, *QAUDJRN
Reports to run . . . . . *DEFAULT          *DEFAULT, *ALL, *NONE
Clear work files after run . . *NO_      *YES, *NO
Submit job to batch queue . . *YES      *YES, *NO

(By pressing F10, the following option is shown.)
                                Additional Parameters

Generate new security receiver   *NO          *YES, *NO

```

The audit may take up to ten minutes, depending on the speed of your AS/400 or iSeries and the number of other jobs running. The reports should go to the same printer that your other jobs use. If you need to change where the reports print, see option 9 on the configuration menu “Change where reports print,” (also provided as option 13 on the “Common Tasks” menu).

You may use the WRKSBMJOB (work with submitted jobs) command to monitor the job while it runs. This command is option 34 on the “Common Tasks” menu in Softlight Auditor.

## What to look for on a first audit

Each site is different, and your needs will determine your security policies and priorities. Knowing that, we can still offer a few suggestions for reviewing your first set of audit reports. Samples of these reports are included toward the back of this manual.

You should become familiar with your users’ sign on IDs and with the names of the libraries used on your AS/400. The IBM commands WRKUSRPRF and DSPOBJD can help you find the descriptions for users and libraries, respectively.

1. Look at the invalid user ID and password report (RPJPW1). One or two bad passwords in a short period of time probably indicates someone is “all thumbs.” Many attempts in a row probably indicate an attempt to guess someone’s password.

*Note: a common error is to type one’s password in the place of the user name. Since this report lists user names that failed to log in, you may wish to shred it.*

2. Scan the authority failure report (RAJAF). Repeated, failed attempts to access a payroll library, for instance, should be investigated.
3. Look at the user profile changes (RPJCP1) report to see what new users have been created, and to learn of any changes made to existing user profiles.

4. Review the programs created report (RAJCOP) to see what programs have been compiled on your system. If you have significant development activity, it is good practice to limit compiles to a development library (or set of libraries). Only tested programs are then moved to the production libraries. If your shop operates in this way, you can use the *stop list* feature of Softlight Auditor to keep all compiles in a named set of (development) libraries off this report. Any compiles into production libraries would then stand out.
5. Refer to the objects moved or renamed report (RPJOM1) to see any objects (including programs) moved into or out of significant libraries on your system. The *stop list* allows you to eliminate any routine, nightly object movement.
6. Look at the programs changed to adopt authority (RPJPA1). In particular, programs that adopt the authority of QSECOFR or other “powerful” users should be scrutinized. Also check report RPJRP1 to see if any programs created on other systems to adopt authority have been *restored* to your system.

*What is adopted authority?* OS/400 provides a mechanism to allow a program to run with all of the authorities of the *owner* of the program

Here is an example. User TOM may not have authority to library PAYROLL. Thus, TOM cannot run Query/400 to view data in the PAYROLL library. If management wants employees to be able to check their own sick and vacation leave balances, a program can be written to access just that information for the user who is logged in to OS/400.

If the program owner has access to the PAYROLL library, and if the program is changed to adopt the authority of its owner, and if TOM has authority to run the program, then TOM can check his leave balances, but he can do nothing else in the PAYROLL library.

This is a reasonable way to control access, and does not necessarily indicate a problem. Softlight Auditor, for instance, uses several programs that adopt authority to allow an auditor, who normally would not need access to system objects, to read and manage the audit journal and history log.

7. See what system values have been changed by referring to report RPJSV1. Note that some changes in performance-related values are made automatically by IBM’s Operational Assistant program, so you may see entries on this report that you did not make via the WRKSYSVAL or CHGSYSVAL commands.
8. Look at the system management report (RAJOR). Activity on this report will be rare in most shops, and indicates an action was taken to change such items as the System Reply List, Operational Assistant functions, or Network File Operations.

9. See if users with \*SERVICE special authority used the STRSST (service tools) function to change anything on the system by looking at the RAJST report. This should be a rare occurrence and should correspond to known service activity.

For those new to the system there is a lot to learn about the AS/400 in order to do a thorough audit. However, Softlight Auditor can help you, not only by summarizing the information, but also by organizing your approach to auditing. For example, you can use the library/object stop list (discussed in the chapter on configuring Softlight Auditor) to “check off” events that you determine to be normal. Over a few months, your Softlight Auditor reports – already much smaller than the raw audit journal – will be further trimmed down to a very manageable size.

After you are comfortable with the basic reports, you may expand your auditing activities a bit. Two common requests – to monitor the actions of the security officer or another key user, and to note every time a key program such as DFU is run – are discussed in the sections of this manual entitled “Auditing Users” and “Auditing Objects.”



## Configuring Softlight Auditor

Softlight Auditor will run "out of the box," but time you spend tailoring it to your situation will be rewarded by shorter and more relevant reports. We make extensive use of exception reporting (management by exception), which means that you must define what is normal before we can report what is *not* normal.

Here is a copy of the configuration menu, which is reached by taking option 3 on the main menu.

```
SLACFG                Softlight Auditor Configuration Menu
                                System:      S1015241
Select one of the following:

    1. Normal business hours      WRKNBH
    2. Holidays                   WRKHLDY
    3. Locations                  WRKLOC
    4. User profile controls      WRKUSRCF
    5. Message ID controls       WRKMSGCF
    6. Defaults for random sample of messages  CHGRNDDFT
    7. Default reports set to print WRKSLARPT
    8. Stop list                  WRKLOS
    9. Change where reports print CHGPRTF SLAPRINT

    21. Proofing reports menu     GO SLARP1

    88. Search help index
    90. Signoff

Selection or command
===>
```

In this section, we discuss the ways in which you can tailor the product to your needs. We will present examples of several commands discussed in subsequent sections. The later sections include sample screens. Read this section for concepts, and the following sections to learn "how to."



***One piece of advice:*** change one thing (or just a few things) at a time, and see the impact on your next set of reports before making more changes. It will probably take you a few weeks to get the hang of customizing Softlight Auditor to your needs, but the payback comes every time you review a shorter set of reports.

### *User profile controls*

Each user on your system *may* have a user profile control record in Softlight Auditor, in addition to his or her user profile record in the operating system. The operating system record contains such information as password and starting menu or program. The Softlight Auditor record contains additional controls, such as normal business or working hours, normal workstations used, and percentage of jobs to select at random for review.

You do *not* have to define a separate user profile control record for each of your users. A special profile, \*DEFAULT, is included. If a user's ID is not separately defined, the values in the \*DEFAULT profile are used.

The WRKUSRCF (Work with user control file) command is described in the section "User profile controls."

### *Time of Day*

As shipped, Softlight Auditor will report as an exception any interactive job that starts before 8 am or ends after 5:30 pm, Monday through Friday. It will also report all interactive jobs run on weekends, Christmas day or the Fourth of July.

These times are considered outside normal business hours. You may change this definition, and add other definitions to accommodate shifts or remote sites in other time zones.

For example, if you have a night operator, you could use the WRKNBH (Work with normal business hours) command to create a schedule named NITEOP. On this schedule, you could specify that the hours 1930 (7:30 pm) to 0300 (3:00 am) are "normal" on Monday through Friday. You would then use the WRKUSRCF (Work with user control file) command to create a record for the night operator's user profile, and specify NITEOP as his or her normal business hours schedule.

By the way, it is better to name business hour schedules for their function or purpose, rather than for the user, even if a schedule applies to a single user ID. If your night operator is MARY, and you name the normal business hours schedule MARY, what will you do when Mary moves to the first shift, or when you hire a second night operator? We recommend that you create schedule NITEOP, then specify that schedule for Mary's user control record.

Hint: if your users tend to come in a few minutes early or stay a few minutes late, expand your normal business hours schedule 15 or 20 minutes each way to cut down on the number of exceptions you must review. You can change the schedule at any time if you want to see who is staying a few minutes late, but for routine operations, unless it is critical that your people start and stop work "on the dot," we suggest you expand the schedule slightly.

For a sample screen, see the section "Normal business hours."

### Workstation locations

As shipped, Softlight Auditor does not consider the location from which a user signs on to be important. You may want to be notified if a user signs on from anywhere other than his or her normal location.

If a user normally signs on from only one device, enter that device name (e.g., DSP14) in the user profile control record. See the section, "User profile controls."

If a user normally signs on at one of a group of workstations, assign a name to that group (1-10 characters, e.g., ACCOUNTING), enter that group name in the user profile control record, then define the group by adding individual device names to it. See the section "Normal locations."

## Normal business hours

To define one or more schedules of normal business hours, use the SLAUDIT/WRKNBH command. This command is option 1 of the configuration menu.

The following screen will appear.

```
Work with Normal Business Hours                               WRKNBH 1
Enter schedule ID . . . . . _____ Enter=Position list
                                                F6=Create new schedule
Normal business hours are defined by a pair of
start-end times for each day of the week and one pair for holidays.

Type options, press Enter.
  2=Change      4=Delete      5=Display
  Schedule
Opt ID      Description      SUN  SUN  SUN
  2  *DEFAULT  Mon-Fri, 8am - 5:30 pm    9999 0000  0
F3=Exit      F6=Add new record
```

All "work with" commands in Softlight Auditor look and feel the same as this command. When the command starts, it presents a scrolling list of defined schedules. You may:

- scroll the list by using the Roll or Page keys

- reposition the list by keying all or part of a schedule ID on the line provided, then pressing [ENTER]
- create a new schedule by keying the new schedule ID on the same line, then pressing [F6]
- change an existing schedule by positioning the cursor next to it in the list, keying "2", and pressing [ENTER]
- delete an existing schedule by keying a "4" next to it (you will have a chance to confirm your choice)
- display a schedule (prevents accidental changes) by keying a "5" next to it
- exit the program by pressing [F3].

On-line help is not yet available from the work-with screens. Please refer to this manual if the use of a field is not clear.

The \*DEFAULT schedule is used for all user profiles that do not specify some other schedule. To change it, key a "2" next to it, and press [ENTER]. The following screen will appear.

UPDATE	Work with Normal Business Hours	WRKNBH 2
Normal business hours schedule. . .	*DEFAULT	
Description . . . . .	Mon-Fri,_8am_-_5:30_pm_____	
	SPANS	
	FROM	DAYS TO
Sunday hours. . . . .	9999	000 0000
Monday hours. . . . .	0800	000 1730
Tuesday hours . . . . .	0800	000 1730
Wednesday hours . . . . .	0800	000 1730
Thursday hours. . . . .	0800	000 1730
Friday hours. . . . .	0800	000 1730
Saturday hours. . . . .	9999	000 0000
Holiday hours . . . . .	9999	000 0000
Schedule status . . . .	___	Blank=active, I=inactive
F3=Exit	F12=Cancel	F4=Delete Roll=Next/Prev rcd

*Description* is any text you desire to identify the schedule.

*Sunday hours* is a pair of times in 24-hour format. Business hours start with the first time and end with the second time. For all user profiles governed by this schedule, interactive jobs that start before or end after these times will be reported as exceptions .

*Monday - Saturday hours* are similar. *Holiday hours* are used for dates that are defined as business holidays. See the section "Business holidays" or the SLAUDIT/WRKHLDY command.

To allow jobs all day, enter a *from* time of 0000 and a *to* time of 2359. To prevent any jobs on a day, enter a *from* time of 9999 and a *to* time of 0000.

To accommodate a schedule that crosses midnight (a night shift), enter a value of 001 in the "*Spans Days*" column. For instance, 7 p.m. to 2:30 a.m. would be entered as

	FROM	SPANS	TO
Monday	1900	001	0230

To accept changes, press [ENTER] or [F3].

To cancel any changes made on the screen, press [F12].

To delete the schedule, press [F4]. You will have a chance to confirm.

To move to the next/prior schedule, use the Page or Roll keys.

## **Business holidays**

The preceding section, "Normal business hours," allows you to define different hours on holidays. The SLAUDIT/WRKHLDY command allows you to specify which dates are holidays. This command is option 2 of the configuration menu.

All holidays are entered in the format YYYYMMDD, regardless of the job date format. For example, Christmas 1997 would be 19971225.

## Normal locations

To group a number of devices in to a location name of your own choosing, use the SLAUDIT/WRKLOC command, option 3 on the configuration menu.

In the example shown here, devices DSP01 and DSP02 are already in location SAMPLE. By pressing [F6], device DSP09 would be added to that location.

The default location is \*ALL devices. You may delete that item, and create your own \*DEFAULT location by adding devices one at a time.

```
Work with Location Definitions                                WRKLOC 1

Location name . . . . . SAMPLE_____ Enter to position list
Device name . . . . . DSP09_____ F6 to add a record

Type options, press Enter.
  2=Change      4=Delete      5=Display

Opt LOCATION  DEVICE  DESCRIPTION
_  *DEFAULT    *ALL    Default is all devices until you change it
_  SAMPLE     DSP01    Sample location - entry 1 of 2
_  SAMPLE     DSP02    Sample location - entry 2 of 2

F3=Exit          F6=Add new record          Bottom
```

## User profile controls

You do *not* have to define user profile control records for all your users before you can use Softlight Auditor.

If a user profile control record does not exist, the \*DEFAULT business hours schedule and \*DEFAULT location list will be used for reporting "unusual" interactive jobs.

To define a user profile control for a particular user, use the SLAUDIT/WRKUSRCF command, option 4 on the configuration menu.

*Note:* These controls are separate from the user profile controls in OS/400. They supplement those controls, but *do not* replace them. They report exceptions after the fact. IBM's controls can block some exceptions. To examine the system's user profile controls, use the WRKUSRPRF command.

```

                                Work with User Profile Controls                                WRKUSR 1

User ID . . . . . _____      Enter = Position list
                                      F6 = Add user

Type options, press Enter.
  2=Change      4=Delete      5=Display

NORMAL
Opt USERID      USER TEXT      HOURS
  2 QSECOFR      Security Officer      *ALL
  _ SLAUDIT      Softlight Auditor      *DEFAULT

F3=Exit          F6=Add new record

```

The control record for user profile QSECOFR is shown on the next page. Fields on that screen include:

*Normal business hours* refers to a defined schedule. \*DEFAULT must be defined. It is shipped to you as 8 am to 5:30 pm, Monday through Friday. You may change it, and define other schedules. See the section "Normal business hours." \*ALL and \*NONE are valid special values; they are pre-defined and mean what they say.

*Normal locations* is the name of a device or of a defined location list. See the section "Normal locations." \*ALL and \*NONE are valid here, too.

```

UPDATE                                Work with User Profile Controls                                WRKUSR 2

Type information for user QSECOFR      Press Enter.
Text. . . . . Security_Officer_____

Normal business hours . . . . .      *ALL_____      *ALL, *NONE, Name
Normal locations. . . . .      DSP02_____      *ALL, *NONE, Name

The following items are retained for compatibility with prior releases. See the section entitled "Functions Retained from Prior Releases, near the end of this manual, to learn more about the values that may still be used in this version of Softlight Auditor.

Pct normal job logs . . . . .      _10 %      0-100
Pct abnormal job logs . . . . .      100 %      0-100
Pct jobs to report. . . . .      _25 %      0-100
Allow sign on . . . . .      Y      Y, N
Termination date YYYYMMDD . . . . .      *NONE____      *NONE, YYYYMMDD
...etc.

F3=Exit          F12=Cancel          F4=Delete          Roll=Next/Prev rcd

```

## Report defaults

Softlight Auditor prints a number of reports each time it runs. If you do not need some of these reports, you may turn them off. Samples of the reports are included in appendix A.

Use the SLAUDIT/WRKSLARPT command, configuration menu option 7.

```

                                Work with Report Defaults                                WRKRPT 1
Report Name . . . . . _____ Enter=Position list

Type options, press Enter.
  2=Change      4=Delete      5=Display
  REPORT
Opt NAME       DESCRIPTION                                           TYPE
- RPIJB1CL     Interactive Job Exceptions      *QHST
- RAJAFACL     Authority failures                *QAUDJRN
- RPJCP1CL     User profile changes              *QAUDJRN
- RPJDS1CL     Security officer password reset via DST *QAUDJRN
- RPQH2ACL     Random sample of messages from history log *QHST

F3=Exit          F6=Add new record
  
```

```

UPDATE                                Work with Report Defaults                                WRKRPT 2
Type information for report RPIJB1CL

Description . . . . .
Interactive_Job_Exceptions_____

Type of report. . . . . *QHST_____ *QHST, *QAUDJRN, *STATUS
Include in default set. . . . . Y          Y, N
Include in alternate set. . . . . Y          Y, N

F3=Exit          F12=Cancel          F4=Delete          Roll=Next/Prev rcd
  
```

*Type* refers to the type of audit which contains the reports. \*STATUS is not yet implemented. For \*QHST and \*QAUDJRN, see the section "Audit new events."

Each time you run an audit, you are given the choice of printing all reports, no reports, the default set or the alternate set.



## Library/object stop list

Softlight Auditor reports on a number of security related events which are logged in the system security journal, QAUDJRN. On a busy AS/400 or iSeries, hundreds or thousands of events may occur between event audits. The library and object stop list allows you to "filter out" events that occur regularly, and which do not require review.

For example, in many shops programmers do their work in their own libraries, and move the finished product to production. You may not want to see object creations, deletions, or authority changes in these libraries.

Although this paragraph applies to a minority of AS/400 shops, it may be helpful if you have a lot of System/36 code which has never been converted to AS/400 native mode.. Work files are commonly deleted and recreated by programs created on the System/36. When such a program is moved to an AS/400, it can clutter the object creation report, the object deletion report, the object ownership change report, and the object authority change report. The stop list has help you filter out those events.

Such normal events make it less likely you will spot the abnormal events. Softlight Auditor lets you stop the reporting of several types of events

- on a single object, or
- on all objects in a given library.

Library/Object Stop List		WRKLOS 2
For library QRPLOBJ      object *ALL      type *ALL		
type the following information, then press Enter.		
Description . . . . .		
Object_replacement_holding_library_____		
Report object deletions . . . . .	N	
Report object creations . . . . .	Y	Answer Y or N to each
Report object ownership changes . .	Y	
Report object authority changes . .	Y	
Report objects restored . . . . .	Y	
Report pgm running unsupported API.	Y	
Report objects moved/renamed . . .	Y	

Note: deletions of objects in the job's temporary library, QTEMP, are not written to QAUDJRN, and thus are never reported.

We recommend you run the reports as they come for a few days to see all the activity on your system. Once you know what is normal, start adding entries to the Library/Object stop list until your reports are short enough that unusual activity will stand out to you.

## Changing where reports print

All Softlight Auditor reports are printed using printer file SLAUDIT/SLAPRINT.

By changing the characteristics of this file, you may change

- the output queue or printer used
- whether or not the reports are saved in the queue after printing is finished (useful, for instance, if you want to save copies to optical disk)
- the forms ID
- the number of copies
- the page size, rotation and other attributes.

Use IBM's CHGPRTF command (change printer file), or the configuration menu option provided by us, to make your changes. Press [F10] for additional parameters, and scroll down until you find the options you need to change.

Spool the data . . . . .	*YES	*SAME, *YES, *NO
<b>Spooled output queue</b> . . . . .	<b>*JOB</b>	Name, *SAME,
<b>Library</b> . . . . .		Name, *LIBL,
Form type . . . . .	*STD	Character val
Copies . . . . .	1	1-255, *SAME
Page range to print:		
Starting page . . . . .	1	Number, 1, *SAME
Ending page . . . . .	*END	Number, *SAME, *END
Max spooled output records . . .	100000	1-999999, *SAME,
File separators . . . . .	0	0-9, *SAME
Spooled output schedule . . . .	*FILEEND	*SAME, *FILEEND,
<b>Hold spooled file</b> . . . . .	<b>*NO</b>	*SAME, *NO, *YES
<b>Save spooled file</b> . . . . .	<b>*NO</b>	*SAME, *NO, *YES
Output priority (on OUTQ) . . .	*JOB	*SAME, *JOB, 1, 2,
User data . . . . .	*SOURCE	Character value,
Spool file owner . . . . .	*CURUSRPRF	*SAME, *CURUSRPRF,

If you change "Hold spool file" to "\*YES", the spooled output file is held until it is released by the Release Spooled File (RLSSPLF) command. In other words, no reports will print until you explicitly release them.

If you change "Save spool file" to "\*YES", the spooled file data is kept on the output queue until the file is deleted. In other words, after the requested copies have printed, the spool file is *not* deleted from the output queue. This option allows you to copy reports to an optical storage system, then delete them.

You may also find it helpful to change the output queue name and library for all Softlight Auditor reports.

## Auditing all commands by a user

OS/400 provides a way to audit all actions of one or more users. This feature is commonly used to track the actions of a few key users, such as QSECOFR, or when a particular user is suspected of abuse. It is *not* intended to log every command by every user.

To audit users (or to audit certain objects, as described in the next section), the OS/400 system value QAUDCTL must include \*OBJAUD. The appropriate values for V3R6 are shown below. Some earlier versions may not support \*NOQTEMP, which prevents audit records from being written for objects in the session work library QTEMP. Check the on-line help to see if \*NOQTEMP is an option available on your version.

Change System Value	
System value . . . . . :	QAUDCTL
Description . . . . . :	Auditing control
Auditing control	
*OBJAUD	
*AUDLVL	
*NOQTEMP	

Once object auditing has been enabled by adding \*OBJAUD to the QAUDCTL system value, you may request auditing of one or more users or objects.



**Note:** Softlight Corporation recommends you proceed with caution, requesting auditing on one user at a time. Auditing users can generate thousands of auditing records, depending on how active the user is. Your audited commands report could be so long it is too hard to review and your computer can slow down if asked to log too many events..

User auditing works best in situations where powerful profiles, such as QSECOFR, are not used for ordinary jobs. (It is never a good idea to run production jobs as QSECOFR, not just because of the potential size of the resulting audit log!)

To turn user auditing for a user profile on or off, use the Change User Auditing command, CHGUSRAUD, found on the SLA common tasks menu as option 3. The following example shows how to request auditing of all commands issued by the security officer, QSECOFR.

To turn off command auditing for QSECOFR, use the same command, changing the “User action auditing” value to \*NONE.

Keep a paper log of what you have requested, since there is no easy way to have the system list all users for whom auditing has been requested.

```
Change User Auditing (CHGUSRAUD)

Type choices, press Enter.

User profile . . . . . QSECOFR      Name
      + for more values
Object auditing value . . . . . *SAME      *SAME, *NONE, *CHANGE, *ALL
User action auditing . . . . . *CMD       *SAME, *NONE, *CMD...
```

The RAJCDACL report shows the commands run by audited users.

## Auditing individual objects and commands

OS/400 also provides a way to audit every access to certain objects. You might use this feature to see who has accessed a particularly sensitive file or library. Another common use is to make a record every time a key command, such as STRDFU – start data file utility – is run. (Since commands, files, libraries, programs, and devices are all objects under OS/400, you may request object auditing on any of them with this one method.)

To audit objects, the OS/400 system value QAUDCTL must include \*OBJAUD. See the prior section on user auditing for details.



**Note:** Softlight Corporation recommends you proceed with caution, requesting auditing on *one or a few objects at a time*. Requesting object auditing for \*ALL objects in \*LIBL is a very quick way to bring your system to a crawl or even cause a crash, as the system writes tens or hundreds of thousands of audit records to the security journal!

Use the CHGOBJAUD command (available on the SLA common tasks menu as option 2) to control object auditing. The following example shows how to request a log record every time someone runs the Start DFU (STRDFU) command. To turn off the request, run the CHGOBJAUD command again, with “Object auditing value” set to \*NONE.

Keep a paper log of what you have requested, since there is no easy way to have the system list all objects for which auditing has been requested.

```

Change Object Auditing (CHGOBJAUD)

Type choices, press Enter.

Object . . . . . STRDFU      Name, generic*, *ALL
Library . . . . . *LIBL      Name, *LIBL, *USRLIBL...
Object type . . . . . *CMD      *ALL, *ALRTBL, *AUTHLR...
Object auditing value . . . . . *ALL      *NONE, *USRPRF, *CHANGE, *ALL

```

Note that this feature will only record that a command (or other object) was read or changed. *It will **not** log which records in a file were read or changed, nor what the before and after values were.*

The RAJCDACL report shows audited commands run. The RAJZRA and RAJZCA reports show read and change access, respectively, to other types of audited objects.

## Status Auditing

The status auditing menu of Softlight Auditor groups a number of OS/400 commands which are useful for reviewing the current configuration of your system.

The features grouped are shown below.

```
SLASTS                               Status Auditing Menu                               System:  S1015241
Select one of the following:
    1. Print system values related to security           WRKSYSVAL
    2. Display programs that adopt authority             DSPPGMADP
    3. Display object authority                          DSPOBJAUT
    4. Display user profile                              DSPUSRPRF
    5. Display authorized users                         DSPAUTUSR
    90. Signoff
Selection or command
===> _____
```

IBM's on-line help is available for each of these commands. There are commercial programs available which help with status auditing, beyond the basics provided here. For further information on what we recommend, please contact Softlight Corporation.

## Event Auditing

(This section elaborates on the earlier section, entitled "Running Your First Audit.")

Event auditing refers to periodic monitoring of security-related events on your AS/400 or iSeries. "Periodic" will mean different things to different shops, but many sites perform event auditing daily or weekly.

IBM designed these systems with security in mind, and focused on *blocking* unauthorized access to workstations, programs and files. However, event auditing is still vital to note *changes* which might weaken security or *attempts* to breach security.

Here is a list of some events you might need to monitor.

- Bad passwords or User IDs
- Ownership changes
- New or restored programs that adopt authority
- Authorizations granted or revoked
- Authorization failures
- Object deletions
- Jobs run after normal business hours, on weekends or holidays
- System value changes
- Actions of key user profiles, such as QSECOFR
- Use of sensitive objects, such as the STRDFU command

You might attempt to sign on with a bogus user ID, for example, just to verify that Softlight Auditor is working correctly.

Softlight Auditor processes the system history log, QHST, and the system security journal, QAUDJRN, to locate and filter events for your review.

The event auditing menu, option 1 from the main menu, is shown below.

```
SLAEVT                               Event Auditing Menu                               System:  S1015241
Select one of the following:
    1. Audit new events                               AUDNEWEVT
    2. Display security-related messages from QHST
    4. Display start dates for next event audit       DSPADTSTR
    5. Change start dates for next event audit       CHGADTSTR
    6. Display QAUDJRN audit journal entries         DSPAUDLOG
Selection or command
===> _
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

## Audit new events

Since you might run an event audit daily or weekly, we spent most of our development time trying to save you time here. Our goal is to make the reports useful even if you do not tailor the system to your site. If you do spend time over the first dozen or so audits configuring Softlight Auditor - as discussed earlier in the manual - we want to repay that with interest as time saved when you review the event audit reports. These reports will then be more sharply focused on what you consider important.

The SLAUDIT/AUDNEW EVT command, menu option 1, is the principal command used in periodic event auditing.

It recalls the ending date and time of the its last run, selects events from that date to the present, filters them, sorts and summarizes, selects random samples, and produces reports.

This command may be included as a part of a standard, nightly procedure, or run by a job scheduling package, such as the WRKJOBSCDE command included in OS/400..

The command defaults are shown on the prompt screen, below.

```

                                Audit New Events (AUDNEW EVT)

Type choices, press Enter.

Source of events to audit . . . *BOTH___      *BOTH, *QHST, *QAUDJRN
Reports to run . . . . . *DEFAULT      *DEFAULT, *ALL, *NONE
Clear work files after run . . *NO_      *YES, *NO
Submit job to batch queue . . *YES      *YES, *NO

(By pressing F10, the following option is shown.)
                                Additional Parameters

Generate new security receiver *NO          *YES, *NO
```

On-line help is available for this command.

*Source of events* specifies whether to take events from the system history log \*QHST, the system security journal \*QAUDJRN, or \*BOTH. The history log is present on all AS/400s. Someone at your site must set up the security journal. See the "Setup command" or "Manual setup" sections in this manual for more details.

*Reports to run* governs which reports are produced automatically. Your choices are \*ALL, \*NONE, \*DEFAULT, or \*ALT. The first two are self-explanatory. As shipped, \*DEFAULT and \*ALT are the same as \*ALL. See the section "Report defaults" to learn how to change the default and alternate sets.



*Clear work files* should be \*NO if you plan to run additional reports after the audit has finished. If you are printing all the reports you need as a part of the audit (most clients do), you may specify \*YES to save space on disk. Note that *only the work files created by this command* are cleared. Softlight Auditor does not clear your QHST history log, nor your QAUDJRN security journal.

Note: Softlight Auditor can create and attach a new journal receiver to the security journal as a part of the event audit. Press [F10] to show the additional parameter to control this feature when you prompt the AUDNEW EVT command.

Very busy sites may want to attach a new receiver every time they run an event audit. Other sites may find that attaching a new receiver once a week or once a month is adequate. To conserve disk space on your system, do not let the QAUDJRN receiver grow without bounds. Rather, attach a new receiver, then save and delete the old one.

We recommend that you use the option on the AUDNEW EVT command to create a new receiver, rather than doing it yourself via IBM's commands. However, if you choose to do it yourself, be sure you do not delete the old receiver until after the *next* event audit. (The next audit will look for information in the old and new receivers.)

Another option is to let the system manage creation and attaching of new journal receivers. This is described in a subsequent section of the manual.

## Display security-related messages

Menu option 2 runs the IBM command `DSPLOG MSGID(CPF2200)`. Most, but not all, security-related messages are in this range. This option is a quick way to review security-related events between event audits. IBM provides on-line help for the DSPLOG command.

## Display audit start date

To see where the last event audit ended (where the next audit will start), use menu option 4 on the audit new events menu.

## Change audit start date

Softlight Auditor records the ending date and time of each event audit so that it can start the next audit at that point automatically.

On occasion, you may need to reset the start date. To do so, use the SLAUDIT/CHGADTSTR command (menu option 5 on the audit new events menu).

Change Audit Start Date (CHGADTSTR)

Type choices, press Enter.

Starting date for QHST . . . . .	*SAME_____	Date, *SAME
Starting time for QHST . . . . .	*SAME_____	Time, *SAME
Starting date for QAUDJRN . . . . .	*SAME_____	Date, *SAME
Starting time for QAUDJRN . . . . .	*SAME_____	Time, *SAME
QAUDJRN receiver name . . . . .	*SAME_____	Name, *SAME, *CURRENT
QAUDJRN receiver library . . . . .	*SAME_____	Name, *SAME, *CURRENT

On-line help is available.

Enter *dates* in the **job date format**; separators are optional. For example, if your job date format is \*MDY and the date separator is "/", July 4, 1992 could be entered as 070492 or 07/04/92.

Enter *times* in 24 hour format, including seconds (e.g. 4:30 pm entered as 163000); separators are optional (e.g. 16:30:00).

The *receiver name* and *library* will not normally need to be changed. However, if you have manually changed the QAUDJRN receiver and deleted the old one, the event audit will fail, since Softlight Auditor is looking for the old receiver. The quickest way to fix the problem is to set the receiver name and library to \*CURRENT on this screen.

The recommended way of changing receivers is via the AUDNEW EVT command itself. See the section on auditing new events, above.

## Common Tasks

You will likely perform a few tasks with Softlight Auditor on a routine basis. Event auditing is a daily task in many installations. Since the audit journal receiver grows without bound, you will need to change receivers and delete older ones, according to some records retention policy. You may need to turn auditing on or off for a user or a command. You may also need to look up the description of an object, view the status of an audit, or see the spooled reports from your jobs.

These tasks, and others, are grouped for your convenience on the SLA common tasks menu, shown here.

```
SLATASK                Softlight Auditor - Common Tasks                System:  S101160G
Select one of the following:

EVENT AUDITING
  1. Audit new events
  2. Request object auditing *
  3. Request user auditing *
  4. Request office (DLO) auditing
  5. Event auditing menu
    * please read help

REPORTS
  11. Enable/disable entire reports
  12. Suppress an item on a report
  13. Control where SLA reports print
  14. Work with spooled files

SECURITY JOURNAL (QAUDJRN) MANAGEMENT
  21. Display SLA system information
  22. Backup QAUDJRN receivers
  23. Manage QAUDJRN receivers
  24. Display QAUDJRN entries
    (specify FROMTIME/TOTIME to
    cut down the number of entries)

OTHER CONTROLS
  31. SLA configuration menu
  32. Work with system values
  33. Display object descriptions
  34. Work with submitted job
  35. Work with spooled files
```

## Managing security journal size

The security journal, QAUDJRN, is saved on disk to a series of journal receivers. If you used the Softlight Auditor setup defaults, these receivers are named AUDIT0001, AUDIT0002, etc., and are in library QGPL. The current receivers grows without bound until someone changes it.

The easiest way to change a receiver is via the AUDNEW EVT (audit new events) command. When the prompt screen is displayed for an event audit, press [F10] for additional parameters. Set “Generate new security receiver” to “\*YES”.

To backup receivers, use common tasks menu option 22. Even if you save SLA reports, you may want to keep the actual security journals, since they are the “contemporaneous record.”

To delete old receivers, use common tasks menu option 23. Press [F15] on the first screen to work with the receiver list (directory). On that screen [F11] will toggle the display between save date and size.

## System-managed security journal receivers

As noted, Softlight Auditor provides a way to create and attach a new security journal receiver. The AUDNEW EVT command has a special parameter to generate a new receiver as a part of the audit. By using that method, you are assured that all entries from the old receiver are audited *on the current audit*. Thus, you are free to archive and delete the old receiver as soon as the audit is through. You can also control when the changes are made, perhaps aligning them with some natural schedule such as a week or a month.

However, you may prefer to let OS/400 create and attach a new receiver whenever the *size* of the existing one exceeds a threshold you set. This frees you from having to remember to change the receiver as a part of an audit.

*Note: If you use system-management, do not delete the immediate past QUADJRN receiver until an audit is run which contains events from the new receiver. Softlight Auditor leaves a “bookmark” in the receiver at the end of each audit. If the bookmark points to the old receiver, and if you have deleted that receiver, the audit will fail. You may use option 4 on the Event Auditing Menu to see the location of the bookmark.*

To use the automatic system change journal management, two conditions must be met.

- The current journal receiver must have a storage threshold of at least 5000 KB. (Softlight Auditor's default is 7000 KB, but some systems may have had a smaller threshold manually set before Softlight Auditor was installed.)
- The journal itself must have “manage receivers” set to \*SYSTEM. (This is done via the CHGJRN command.)

To see what the current setting is, use option 23 on the common tasks menu.

To change from \*USER to \*SYSTEM management, you must also change the journal receiver. Sign on as QSECOFR and key

CHGJRN QAUDJRN (press [F4])

```

Change Journal (CHGJRN)

Type choices, press Enter.

Journal . . . . . > QAUDJRN      Name
Library . . . . . > *LIBL      Name, *LIBL, *CURLIB
Journal receiver:
  Journal receiver . . . . . > *GEN      Name, *SAME, *GEN
  Library . . . . . >          Name, *LIBL, *CURLIB
  Journal receiver . . . . .      Name, *GEN
  Library . . . . .      Name, *LIBL, *CURLIB
Sequence option . . . . . *CONT      *RESET, *CONT
Journal message queue . . . . . QSYSOPR      Name, *SAME
  Library . . . . .      *LIBL      Name, *LIBL, *CURLIB
Manage receivers . . . . . > *SYSTEM *SAME, *USER, *SYSTEM
Delete receivers . . . . . *NO      *SAME, *NO, *YES
Receiver size options . . . . . *NONE      *SAME, *NONE, *RMVINTENT
Text 'description' . . . . . 'Security journal'

```

Specify \*GEN for the first journal receiver (generate a new one), leave the second receiver blank, and specify either \*USER or \*SYSTEM for "Manage receivers."

**Important:** Leave "Delete receivers" as \*NO to prevent the system from deleting an old receiver before Softlight Auditor has finished auditing it. You should delete receivers manually, as noted in the section above, regardless of whether you allow the system to change (manage) them.

### Scheduling SLA to run at night

OS/400 includes a basic job scheduling facility. You may use it to schedule the AUDNEW EVT command to run, unattended, overnight (or on any regular schedule).

Use the WRKJOBSCDE (work with job schedule entry) command to view, add, or change scheduled jobs. The following examples show how to schedule an audit each morning at 4:00 AM, and change to a new receiver on Friday. (Note that you must add two job scheduler entries, since the command is different on Friday.)

```

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . > AUDNEW EVT      Name, *JOB
Command to run . . . . . > SLAUDIT/AUDNEW EVT SOURCE(*BOTH) REPORTS(*DEF
AULT) CLEAR(*YES) BATCH(*YES) NEWRCVR(*NO)

Frequency . . . . . > *WEEKLY      *ONCE, *WEEKLY, *MONTHLY
Schedule date, or . . . . . *NONE      Date, *CURRENT, *MONTHSTR...
Schedule day . . . . . > *MON      *NONE, *ALL, *MON, *TUE...
> *TUE
> *WED
> *THU
+ for more values
Schedule time . . . . . > '04:00:00'      Time, *CURRENT

... F10=Additional parameters

```

```

                                Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . > AUDNEW EVT      Name, *JOB D
Command to run . . . . . > SLAUDIT/AUDNEW EVT SOURCE(*BOTH) REPORTS(*DEF
AULT) CLEAR(*YES) BATCH(*YES) NEWRCVR(*YES)

Frequency . . . . . > *WEEKLY      *ONCE, *WEEKLY, *MONTHLY
Schedule date, or . . . . . *NONE      Date, *CURRENT, *MONTHSTR...
Schedule day . . . . . > *FRI      *NONE, *ALL, *MON, *TUE...
      + for more values
Schedule time . . . . . > '04:00:00'  Time, *CURRENT

... F10=Additional parameters

```

You may schedule the job while signed on as user SLAUDIT if you have authority to the command line. Otherwise, have QSECOFR schedule the job. If QSECOFR schedules the job, we recommend having the job run as SLAUDIT. To change the user of a scheduled job, press [F10] while adding or viewing the job, and page down to the next screen of additional parameters, where the user may be set to \*CURRENT or to a user name – SLAUDIT, in this case.

*This information is provided as a model, but since the scheduler is an IBM product, consult the on-line help for definitive guidance.*

---

## Troubleshooting

### **Symptom: Audit ends abnormally, no reports printed.**

There are several reasons why an audit can fail. Consult the job log for the audit, if you can still access it, go to the very end, then back up until you find an error message that does not say something like "see previous message/error for details." That is likely the error that caused the audit to fail.

If you cannot find the job log for an audit submitted to the batch queue, try options 34 and 35 on the Common Tasks menu, or the equivalent IBM commands, WRKSBMJOB and WRKSPLF. (You may also choose to run an audit with "Submit job to batch queue" set to \*NO, then use the DSPJOBLOG command to see the job log for your interactive session. With any of these methods, go to the very end of the job log, then back up until you see an error message that does not refer you to a prior message for details.

Softlight Auditor provides a command, SLADEBUG, to increase the level of detail in the job log for the Audit New Events command (AUDNEW EVT). This can be helpful in isolating a problem. From the command line of any Softlight menu..

- SLADEBUG ON            *turns on increased detail in job logs*
- SLADEBUG OFF        *turns off increased detail*
- SLADEBUG             *shows the current setting, ON or OFF*

Note that this command does not affect any other job logs, only the log for the event audit.

*Note* Messages like "Object USERnnnn in library SLAUDIT not found" are normal, and are *not* the cause of the failure. If you see that message in the log of a failed audit, the real culprit is further along in the log. .

Any of the following may cause a failure of an audit. You may try any of these corrections, based on what you find in the job log.

***Four out of five times, failing audits can be fixed by running the SLAUDIT/SETUP command, option 10 on the System Management Menu (reachable from Softlight Auditor main menu option 4). Leave all the default values on the SETUP command alone.***

Following is a list of other troubleshooting tips.

- **Error message occurred after upgrading: CPF4131 error appeared during open**

Here are the steps to correct the CPF4131 error.  
 The stop file was not properly restored and is still using the old version.  
 Enter the following commands on a command line (probably will need QSECOFR privilege).

```
DLTF FILE(SLAUDIT2/PFSTP3)
RSTOBJ OBJ(PFSTP3) SAVLIB(SLAUDIT2) DEV(*SAVF)
SAVF(SLAINSTALL/SLA##2)
```

This should correct the error.

- **Error message occurred after upgrading when running AUDNEW EVT: Level check on file PFSTP3.**

The stop file was not properly restored and is still using the old version.  
 Enter the following commands on a command line (probably will need QSECOFR privilege).

```
DLTF FILE(SLAUDIT2/PFSTP3)
RSTOBJ OBJ(PFSTP3) SAVLIB(SLAUDIT2) DEV(*SAVF)
SAVF(SLAINSTALL/SLA##2)
```

This should correct the error.

- **Has your copy of SLA expired?**

Use the SLAUDIT/SYSINFO command (option 21 on the SLA common tasks menu) and check the expiration date on line 3 of the screen. Call us if you need a temporary code to get you through until we receive your license payment.

- **Did anyone change the journal receiver manually and delete the old one?**

If so, SLA's bookmark from the last audit will point to a non-existent journal receiver. Check the current receiver using the WRKJRNA QAUDJRN command (option 23 on the SLA common tasks menu). Compare the receiver name to the one in SLA's bookmark from the DSPADTSTR command (SLA event auditing menu, option 4). If they differ, use the SLAUDIT/SETUP command, System Management Menu option 10, and leave the parameters at their default values..

Auditing system values . . . . .	*SAME	*BASIC, *SAME
Receiver name . . . . .	*SAME	*GEN, *SAME, name
Receiver library . . . . .	*SAME	*GEN, *SAME, library
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . . .	*CONT	*CONT, *RESET



- **Was a new version of OS/400 installed since the last successful audit?**

You should turn auditing off before any major software upgrade. So many objects are replaced that the audit journal becomes huge and unwieldy. Use the WRKSYSVAL command to change system value QAUDCLT to \*NONE when you want to turn off auditing. After the upgrade, change QAUDCTL back to what it was before.

If you did not do this, it is likely that OS/400 itself changed journal receivers and SLA does not have authority to the new one. The new receiver also probably has an unintelligible name. The quickest way to get back on track is to use the SETUP command, System Management Menu option 10, and enter the following parameters

Auditing system values . . . . .	*SAME	*BASIC, *SAME
<b>Receiver name</b> . . . . .	<b>*GEN</b>	*GEN, *SAME, name
<b>Receiver library</b> . . . . .	<b>*SAME</b>	*GEN, *SAME, library
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . .	*CONT	*CONT, *RESET

If you have a preferred receiver naming strategy and if you are comfortable resolving OS/400 naming conflicts, you can substitute an available name and library (we recommend QGPL) for the \*GEN and \*SAME values shown in the example.

- **Did the work file, PFQHST2, run out of space?**

Change physical file PFQHST2 in library SLAUDIT2 to a larger size. Use the command

CHGPF FILE(SLAUDIT2/PFQHST2)

Press [F10], if needed, to see more parameters, like the example below.

Change Physical File (CHGPF)		
Type choices, press Enter.		
Physical file . . . . .	> PFQHST2	Name
Library . . . . .	> SLAUDIT2	Name, *LIBL, *CURLIB
System . . . . .	*LCL	*LCL, *RMT, *FILETYPE
Source file . . . . .	*NONE	Name, *NONE
Library . . . . .		Name, *LIBL, *CURLIB
Expiration date for member . . . .	*NONE	Date, *SAME, *NONE
Maximum members . . . . .	1	Number, *SAME, *NOMAX
Access path size . . . . .	*SAME	*SAME, *MAX4GB, *MAX1TB
Access path maintenance . . . . .	*SAME	*SAME, *IMMED, *REBLD,
Access path recovery . . . . .	*SAME	*SAME, *NO, *AFDIPL, *IPL
Force keyed access path . . . . .	*SAME	*SAME, *NO, *YES
<b>Member size:</b>		
Initial number of records . . . . .	10000	1-2147483646, *NOMAX,
Increment number of records . . . .	5000	0-32767, *SAME

<i>Maximum increments</i> . . . . .	3	0-32767, *SAME
Allocate storage . . . . .	*NO	*NO, *YES, *SAME

Change the initial number of records, increment number of records and/or the maximum increments values to allow more rows. The values shown above are usually adequate, but you may need to use slightly larger ones if you run audits infrequently on a very busy system.

- **Are you signed on as user SLAUDIT?**

The audit needs access to the audit journal QAUDLOG and its receivers, the system history file QHST and all history log versions, libraries SLAUDIT and SLAUDIT2, and certain specific authorities to run successfully. Errors which state that you are not authorized to an object can usually be corrected by signing on as user SLAUDIT to run the audit.

If you have scheduled the audit via IBM's WRKJOBSCDE command, make sure the job is running under user profile SLAUDIT. (QSECOFR should work, as well, but should not be necessary).

If you are running the audit as user SLAUDIT and still have authority problems, run the SLAUDIT/SETUP command, System Management Menu option 10, and leave the parameters at their default values..

Auditing system values . . . . .	*SAME	*BASIC, *SAME
Receiver name . . . . .	*SAME	*GEN, *SAME, name
Receiver library . . . . .	*SAME	*GEN, *SAME, library
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . . .	*CONT	*CONT, *RESET

**Symptom: Audit runs, reports cannot be found.**

- **Did they go to a different queue?**

Use the WRKSPLF (work with spooled files) command, found on SLA common tasks menu, option 35.

To change where future audits send their reports, use option 13 on the Common Tasks menu.

- **Has the audit finished?**

Use the WRKSBMJOB (work with submitted jobs) command, found on SLA common tasks menu, option 34, to see if the AUDNEW EVT job is still running. You can examine the job log of that job, or any running job to which you have authority, from the WRKSBMJOB screen.

- **Were they printed and deleted from the queue?**

If you want to archive reports (for example, if you use an optical storage system), and you also let copies print, you need to instruct OS/400 to leave the copies in the print queue after they have finished printing.

All SLA reports refer to a defined printer file, SLAUDIT/SLAPRINT. Use the CHGPRTF command on that printer file (Common Tasks menu 13).

When the first page of the command is displayed, press [F10] for additional parameters, and scroll down until you see a panel like this.

```

Change Printer File (CHGPRTF)

Type choices, press Enter.

Spool the data . . . . . *YES          *SAME, *YES, *NO
Spooled output queue . . . . . *JOB      Name, *SAME,
  Library . . . . .          Name, *LIBL,
Form type . . . . . *STD          Character val
Copies . . . . . 1          1-255, *SAME
Page range to print:
  Starting page . . . . . 1          Number, 1, *SAME
  Ending page . . . . . *END        Number, *SAME, *END
Max spooled output records . . . 100000 1-999999, *SAME,
File separators . . . . . 0          0-9, *SAME
Spooled output schedule . . . . *FILEEND *SAME, *FILEEND,
Hold spooled file . . . . . *NO      *SAME, *NO, *YES
Save spooled file . . . . . *NO      *SAME, *NO, *YES
Output priority (on OUTQ) . . . *JOB      *SAME, *JOB, 1, 2,
User data . . . . . *SOURCE        Character value,
Spool file owner . . . . . *CURUSRPRF *SAME, *CURUSRPRF,

```

If you change "Hold spool file" to "\*YES", the spooled output file is held until it is released by the Release Spooled File (RLSSPLF) command. In other words, no reports will print until you explicitly release them.

If you change "Save spool file" to "\*YES", the spooled file data is kept on the output queue until the file is deleted. In other words, after the requested copies have printed, the spool file is *not* deleted from the output queue. This option allows you to copy reports to an optical storage system, then delete them.

Softlight Corporation does not provide an automatic way to copy reports to optical archives and then delete them, but most providers of optical storage do provide such a means.

If you need Softlight reports to go to a certain printer queue for archiving, you may change the "Spooled output queue" on the same page, above.

---

## Report Samples

Samples of many of the reports delivered with Softlight Auditor follow.

Brief descriptions are included here, but you may also want to refer to the *IBM System i Security Guide for IBM i5/OS Version 5 Release 4* manual, <http://www.redbooks.ibm.com/abstracts/SG246668.html>, for more information.

For a complete list of reports, and to control which ones print automatically when you run an audit, consult the configuration menu option "Default report set to print" (WRKSLARPT command). We add reports from time to time. The on-line list is always the most current.

Here is the list as of the printing date of this manual.

Type	Report	Description
*QAUDJRN	RAJAFACL	Authority Failures
*QAUDJRN	RAJAFBCL	Program Failures
*QAUDJRN	RAJCACL	Authority Changes
*QAUDJRN	RAJCDACL	Audited Users and Commands
*QAUDJRN	RAJCOCL	Objects Created
*QAUDJRN	RAJCOPL	Programs Created (Subset of RAJCOCL)
*QAUDJRN	RAJDOCL	Objects Deleted
*QAUDJRN	RAJDSCL	Reset of DST Security Password
*QAUDJRN	RPJCP1CL	User Profile Changes
*QAUDJRN	RPJJD1CL	Job descriptions that specify a user profile name
*QAUDJRN	RPJOM1CL	Objects Moved or Renamed
*QAUDJRN	RAJORCL	System Management Actions
*QAUDJRN	RPJOW1CL	Object Ownership Changed
*QAUDJRN	RPJPA1CL	Programs Changed to Adopt Authority
*QAUDJRN	RPJPW1CL	Invalid User ID or Password Sign On Attempts
*QAUDJRN	RPJRP1CL	Programs Restored that Adopt Authority
*QAUDJRT	RAJSTCL	Use of Service Tools
*QAUDJRN	RPJSV1CL	System Value Changes
*QAUDJRN	RAJZRA	Audited Object Accesses
*QAUDJRN	RAJZCA	Audited Object Changes
*QHST	RPIJB1CL	Interactive Job Exceptions
*QHST	RPJBR2CL	Random Sample of Jobs by User ID
*QHST	RPQH2ACL	Random Sample of Messages from History Log

*Note:* The "CL" appended to the report name indicates the name of the control language program which sets up and runs the report. For instance, on the report header you will see "RAJAFACL" not "RAJAFACL".

## General comments about reports

You may omit any report. See the section *Report defaults* in this manual.

You may change where the reports print, the number of copies, and similar attributes of the print file. See *Changing where reports print*.

Any report listed in the prior section as type \*QHST can run on any AS/400 or iSeries, since all maintain the system history log, QHST, automatically. Reports listed as type \*QAUDJRN will contain data only if

1. the security journal, QAUDJRN, has been set up on your AS/400, and
2. the proper auditing level has been set in system value QAUDLVL.

See the sections in this manual entitled *The SETUP Command* and *Changing the Auditing Level After Setup* for more information about the security journal.

Many of the QAUDJRN reports allow you to selectively filter out events that you consider normal or uninteresting. This is done via a "stop list" feature on the Softlight Auditor configuration menu. The comments about each report indicate whether the stop list may be used. See the section entitled *The Library/Object Stop List* to learn how to edit the stop list.

The required auditing level is noted after each report sample in the pages that follow.

For a full discussion, refer to the IBM manual *AS/400 Security Concepts and Planning, SC41-8083* (renamed *Security Reference* for OS/400 V2R3).

Most reports of type \*QAUDJRN list the *journal sequence number*. With this number, you can use the DSPJRN command to locate the entry. You might need to do so, for instance, to see what other events occurred at or near the same time.

## Authority Failures

```

*.....1.....2.....3.....4.....5.....6.....7.....8.....9
.....0.....1.....2.....3
1/01/94 15:30:24 RAJafa 2.0
User SLAUDIT Page Authority Failures
- - JOB INFORMATION - -
JOURNA
1 LIBRARY OBJECT TYPE USER DATE TIME NUMBER NAME USER
SEQ NU
A A
A QSYS QHST94001A *FILE SLAUDIT 010194 152654 13652 QSYSARB QSYS
2433
A QSYS QMHLDISP *PGM SLAUDIT 010194 145947 13815 DSP01 SLAUDIT
2433
A QSYS QMHLDISP *PGM SLAUDIT 010194 151917 13652 QSYSARB QSYS
2433
A QSYS QMHLDISP *PGM SLAUDIT 010194 151936 13837 DSP01 SLAUDIT
2433
Legend: 1=Violation subtype.
Attempts to access objects or perform functions which were blocked because the user did
not have proper authority appear on this
report. Section headings describe the coded (1) violation subtypes.
Count 4 System S1015241 QAUDJRN type AF, subtypes A J P S U QAUDLVL
value *AUTFAIL

```

If your OS/400 system value QAUDLVL includes \*AUTFAIL, authorization failures will appear on this report.

The first field gives the type of authority failure. (message issued at time of failure)

A = unauthorized object access attempt	CPI2226
J = submit job profile error	CPI2248
P = profile swap error	CPI2270
S = default sign on attempted	CPI2249
U = User permission request not valid	CPI2296

The next five fields identify the object involved and the date and time of the incident.

The ID of the job being run by the user when access was denied is also listed. For interactive jobs, the job name is the display station ID.

Finally, the journal sequence number in QAUDJRN is noted. You may use this number with IBM's DSPJRN command to retrieve the security journal entry, or to examine other entries made before or after this one.

Stop list: You may not omit authority failures from this report via the WRKLOS command.

# Program Failures

```

*.....1.....2.....3.....4.....5.....6.....7.....8.....9
.....0.....1.....2.....3
1/01/94 15:30:52 RAJAFB 2.0 Program Failures
User SLAUDIT Page
PROGRAM PROGRAM INSTRUC - - JOB INFORMATION - -
JOURNA
1 LIBRARY NAME NUMBER 2 USER DATE TIME NUMBER NAME USER
LIBRARY OBJECT TYPE SEQ NU
D D
D GN#LIB GN#040A 10 SLAUDIT 123093 101453 13652 QSYSARB QSYS
SLAUDIT2 AUDJAFJE *FILE 206
D GN#LIB GN#040A 11 SLAUDIT 123093 101453 13652 QSYSARB QSYS
SLAUDIT2 AUDJAFJE *FILE 206
D GN#LIB GN#040A 13 SLAUDIT 123093 101453 13652 QSYSARB QSYS
SLAUDIT2 AUDJAFJE *FILE 206
D GN#LIB GN#040A 13 SLAUDIT 123093 101453 13652 QSYSARB QSYS
SLAUDIT2 AUDJAFJE *FILE 206
D GN#LIB GN#040A 17 SLAUDIT 123093 101453 13652 QSYSARB QSYS
SLAUDIT2 AUDJAFJE *FILE 206

```

Some programs may attempt to use OS/400 features in a way which could breach security. If your AS/400 audit level (QAUDLVL) includes \*PGMFAIL, those events will be logged and will appear on this report. *This report does not track programs that end abnormally because of program or data errors, unless the error caused one of the following security events.*

The type of failure is noted in the first column (1) (message issued at time of failure)

B = Program ran a restricted machine interface instruction CPI2268  
 C = Restored program failed program validation checks CPI2250

See column (2) for details

A = changed object was restored which may violate security  
 B = object restored and all authority revoked  
 C = validation value failure; copy of program that was translated

was restored

D = a changed object was restored as requested by the security

officer

E = system install-time error detected

D = Program accessed an object through unsupported interface CPI2247  
 R = Attempt made to update object defined as read only CPI2274

Stop list: You may omit events of type "D" (use of unsupported API) from this report via the stop list. Enter the *program* name and *program* library on the stop list (WRKLOS command).



## Authority Changes

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:31:43 RAJCA 2.0 Authority Changes
User SLAUDIT Page
LIBRARY OBJECT OBJECT AUTHORITY AUTH LIST --OBJECT-- AUTH PUBLIC -----
DATA ----- GRANTED
NAME NAME TYPE TO USER NAME G/R EXS.MGT. OPR. MGT. *AUTL.
READ.ADD.UPD.DEL.EXCL DATE TIME BY USER
QGPL CAUTHNEW *PGM *PUBLIC GRT . . Y . . . Y .
Y . Y . Y . 123093 212708 QSECOFR
QGPL EXAMPLES *OUTQ *PUBLIC GRT . . Y . . . Y .
Y . Y . Y . 123193 153848 QSECOFR
QGPL LOADSVD *PGM *PUBLIC GRT . . Y . . . Y .
Y . Y . Y . 123193 174054 SLAUDIT
QGPL LOADSVD *PGM QPGMR GRT . . . . . . .
. . . Y 123193 174055 SLAUDIT
QSYS QHST *MSGQ SLAUDIT RVK Y . Y . Y . . . Y .
Y . Y . Y . 010194 151705 QSECOFR
QSYS QHST93364A *FILE QSRV GRT . . Y . . . Y .
. . . 123093 204818 QSYS
QSYS QHST93364A *FILE QSYSOPR GRT . . Y . . . Y .
. . . 123093 204819 QSYS
QSYS QHST93364A *FILE QPGMR GRT . . Y . . . Y .
. . . 123093 204820 QSYS
QTEMP GN#CFG *DTAARA *PUBLIC GRT . . Y . . . Y .
Y . Y . Y . 123093 101338 SLAUDIT
QTEMP GN#CFG *DTAARA QPGMR GRT . . . . . . .
. . . Y 123093 101338 SLAUDIT
QTEMP GN#CFG *DTAARA *PUBLIC GRT . . Y . . . Y .
Y . Y . Y . 123093 171218 SLAUDIT

```

If your OS/400 system value QAUDLVL includes \*SECURITY, changes to authorization list of object authority will appear here.

Some authorities to an object are granted when the object is created. Others are granted or revoked later.

The first three fields identify the object that was changed.

The user who received or lost authority to the object is listed next, followed by the authorization list used, if any.

Authority was granted (GRT) or revoked (RVK).

The specific object and data authorities are listed next. See the on-line help for the GRTOBJAUT command for a full description.

Finally, the date and time of the change, and the user who issued the command are noted.

Stop list: Individual objects or all objects in a given library may be excluded from this report via the library and object stop list. See the configuration menu option "Library stop list," or use the WRKLOS command.

## Audited Commands

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  2/13/96 11:40:38          RAJCDA          Audited Users and Commands Journal
SLAUDIT          Page
USER ID    DATE    TIME    JOB      1 OBJ NAME    OBJ LIBR    TYPE    2      COMMAND
STRING
  ** COMMANDS FOR JOB DSP01          USER QSECOFR          JOB NUMBER    018512
STARTING QAUDJRN RRN    0000000410
QSECOFR    121195 111719 DSP01      C SIGNOFF    QSYS          *CMD    N    SIGNOFF
  ** COMMANDS FOR JOB DSP01          USER QSECOFR          JOB NUMBER    018641
STARTING QAUDJRN RRN    0000000430
QSECOFR    010196 181012 DSP01      C CHGJOB     QSYS          *CMD    Y    CHGJOB
OUTQ(PGMRS) LOG(4 0 *NOLIST)
QSECOFR    010196 181037 DSP01      C SLAPGMR    QGPL          *CMD    N    SLAPGMR
QSECOFR    010196 181037 DSP01      C CHGLIBL    QSYS          *CMD    Y    CHGLIBL
LIBL(SLAUDIT2 SLAUDIT GN#LIB QGPL QTEMP) CURLIB(SL
DIT)
QSECOFR    010196 181038 DSP01      C CHGJOB     QSYS          *CMD    Y    CHGJOB
OUTQ(PGMRS)
QSECOFR    010196 181040 DSP01      C STRPDM     QSYS          *CMD    Y    STRPDM
QSECOFR    010196 181335 DSP01      C STRSEU     QSYS          *CMD    N    STRSEU
SRCFILE(SLAUDITSRC/QRPGSRC) SRCMBR(CKJOB1) OPTION(5
QSECOFR    010196 181341 DSP01      C ALCOBJ     QSYS          *CMD    N    ALCOBJ
OBJ((QSYS/SLAUDITSRC *LIB *SHRRD))
QSECOFR    010196 181430 DSP01      C DLCOBJ     QSYS          *CMD    N    DLCOBJ
OBJ((QSYS/SLAUDITSRC *LIB *SHRRD))
QSECOFR    010196 181456 DSP01      C SBMJOB     QSYS          *CMD    N    SBMJOB
JOB(CKJOB1) JOBD(*LIBL/QBATCH) RQSDTA('CRTRPGPGM
M(SLAUDIT/CKJOB1) SRCFILE(SLAUDITSRC/QRPGSRC)
SRCMBR(CKJOB1) REPLACE(*YES)')
QSECOFR    010196 181847 DSP01      C DSPMSG     QSYS          *CMD    N    DSPMSG
QSECOFR    010196 181924 DSP01      C WRKOUTQ    QSYS          *CMD    N    WRKOUTQ
OUTQ(PGMRS)
QSECOFR    010196 182032 DSP01      C CHGSPLFA   QSYS          *CMD    N    CHGSPLFA
FILE(CKJOB1) JOB(018642/QSECOFR/CKJOB1) SPLNBR(1)

```

If your OS/400 system value QAUDCTL includes \*OBJAUD, you may request object and command auditing. You have the choice of requesting auditing of particular commands (such as every time the STRDFU command is run to start the Data File Utility), or of requesting auditing of particular users (such as all commands run by the security officer, QSECOFR), or a combination of both.

See the sections on object auditing and user auditing in the manual for further details on how to request auditing.

## Objects Created

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:32:02 RAJCO 2.0                      Objects Created
User SLAUDIT                                     Page
LIBRARY  OBJECT  OBJECT                                     PROGRAM
JOURNAL
NAME     NAME     TYPE     STATUS  USER     JOB NAME  DATE    TIME    NAME
SEQ NUM
QGPL    CAUTHNEW  *PGM     N       QSECOFR  CAUTHNEW  123093  212709  QCMD
2247
QGPL    EXAMPLES  *OUTQ    N       QSECOFR  DSP02     123193  153848  Q
2406
QGPL    LOADSVD   *PGM     N       SLAUDIT  LOADSVD   123193  174055  QCMD
2411
QGPL    LOADSVD   *PGM     R       SLAUDIT  LOADSVD   123193  175324  QCMD
2413
QSYS    QHST93364A *FILE    N       QSYS     SCPF      123093  204812  QWCISCFR
2246
QSYS    QHST94001A *FILE    N       QSYS     SCPF      010194  13058   QWCISCFR
2425
SLAUDIT AUDNEW EVT *PGM     R       SLAUDIT  AUDNEW EVT 123093  215308  QCMD
2247
SLAUDIT DSPAUDLOG *CMD     N       QSECOFR  DSP02     010194  141209  TAATOLAC5
2431
SLAUDIT EXTLST    *CMD     N       QSECOFR  DSP02     010194  140923  TAATOLAC3
2431
SLAUDIT RAJAJFA  *PGM     N       SLAUDIT  RAJAJFA   123093  114250  ZCRTOBJ
2146
SLAUDIT RAJAJFA  *PGM     N       SLAUDIT  RAJAJFA   123093  121240  ZCRTOBJ
2188

```

---

If your OS/400 system value QAUDLVL includes \*CREATE, objects created or recreated on your AS/400 will appear here.

The first three fields on this report identify the object that was created.

Status is "N" for a new object or "R" for a replaced or recreated object.

The user, job ID, date and time are shown, For interactive jobs, the job name is the display station ID.

The program which created the object is also listed. QCMD is the command line.

Stop list: Individual objects or all objects in a given library may be excluded from this report via the library and object stop list. See the configuration menu option "Library stop list," or use the WRKLOS command.

## Programs Created

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:32:17 RAJCOP 2.0
User SLAUDIT Page
OBJECT CREATED IN OBJECT NEW OR - - JOB INFORMATION - -
JOURNAL
TYPE LIBRARY CREATED REPLACED NUMBER NAME USER DATE
TIME SEQ NUM
*CMD SLAUDIT DSPAUDLOG N 13816 DSP02 QSECOFR 010194
141209 24316
*CMD SLAUDIT EXTLST N 13816 DSP02 QSECOFR 010194
140923 24311
*CMD TAATOOL CRTTAATOOL N 13816 DSP02 QSECOFR 010194
133159 24274
*PGM QGPL CAUTHNEW N 13713 CAUTHNEW QSECOFR 123093
212709 22471
*PGM QGPL LOADSVD N 13768 LOADSVD SLAUDIT 123193
174055 24116
*PGM QGPL LOADSVD R 13770 LOADSVD SLAUDIT 123193
175324 24131
*PGM SLAUDIT AUDNEWEVT R 13714 AUDNEWEVT SLAUDIT 123093
215308 22473
*PGM SLAUDIT RAJAJFA N 13688 RAJAJFA SLAUDIT 123093
114250 21466
*PGM SLAUDIT RAJAJFA N 13691 RAJAJFA SLAUDIT 123093
121240 21889
*PGM SLAUDIT RAJAJFA N 13696 RAJAJFA SLAUDIT 123093
125937 21901

```

---

This report is a subset of the Objects Created report.

It lists only programs, commands, and SQL packages created or recreated on your system.

It is intended to help you spot program compile jobs.

Stop list: No provision is made for omitting programs from this report.

## Objects Deleted

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:32:33 RAJDO 2.0                      Objects Deleted
User SLAUDIT                                     Page
LIBRARY  OBJECT  OBJECT  DELETED                                     PROGRAM
JOURNAL
NAME     NAME     TYPE     BY USER   JOB NAME  DATE   TIME   NAME
SEQ NUM
SLAUDIT  RAJAF A  *PGM    SLAUDIT   RAJAF A   123093 114146 ZCRTOBJ
21463
SLAUDIT  RAJAF A  *PGM    SLAUDIT   RAJAF A   123093 121135 ZCRTOBJ
21886
SLAUDIT  RAJAF A  *PGM    SLAUDIT   RAJAF A   123093 125307 ZCRTOBJ
21894
SLAUDIT  RAJAF A  *PGM    SLAUDIT   RAJAF A   123093 132634 ZCRTOBJ
22321
SLAUDIT  RAJAF A  *PGM    SLAUDIT   RAJAF A   010194  4143  ZCRTOBJ
24228
SLAUDIT  RAJAF B  *PGM    SLAUDIT   RAJAF B   010194 10511  ZCRTOBJ
24237
SLAUDIT  RAJCA   *PGM    SLAUDIT   RAJCA     123193 130108 ZCRTOBJ
23369
SLAUDIT  RAJDS   *PGM    SLAUDIT   RAJDS     123193 131249 ZCRTOBJ
23588
SLAUDIT  RAJDS   *PGM    SLAUDIT   RAJDS     123193 132422 ZCRTOBJ
23807
SLAUDIT  WRKSTOPL *PGM    SLAUDIT   DSP01     123093 101302 SLAPGMRCL
20631

```

---

If your OS/400 system value QAUDLVL includes \*DELETE, objects deleted from your AS/400 will appear here.

The first three fields on this report identify the object that was deleted.

The user, job ID, date and time are shown, For interactive jobs, the job name is the display station ID.

Stop list: Individual objects or all objects in a given library may be excluded from this report via the library and object stop list. See the configuration menu option "Library stop list," or use the WRKLOS command.

## Reset DST Security Password

```
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  1/01/94 15:32:39  RAJDS    2.0          Reset DST Security Password to Default
User SLAUDIT          Page
```

JOURNAL	USER	DATE	TIME	JOB NAME	JOB USER	JOBNUM	PROGRAM
SEQ NBR							
24025	QSECOFR	123193	133605	DSP02	QSECOFR	13731	Q

Users appear on this report if they have used the CHGDSTPWD command to reset the dedicated service tools (DST) security password.

If this report shows any activity, investigate the reason. Someone who can IPL the system, and who has the DST security password, can access all objects on the system. You must use DST to set the DST security password to something other than the default

Count	1	System S1015241	QAUDJRN type DS
-------	---	-----------------	-----------------

---

If your OS/400 system value QAUDLVL includes \*SECURITY, a request to reset the dedicated service tools (DST) security password will appear on this report.

DST is a set of tools for performing tests and services on an AS/400 *outside of the normal operating system*. Anyone wishing to use DST must be able to IPL your system. However, IBM still recommends that you change the default DST password, since the default is the same on all AS/400s.

Keep the DST security password safe. If you forget the password for QSECOFR, you can reset it only if you know the DST security password.

In other words, you may reset the DST security password only if you know the QSECOFR password. You may reset the QSECOFR password (to its default value), only if you know the DST security password and can perform an attended IPL.

DP auditors may not be familiar with all of the steps involved, but they should investigate why the DST security password was reset, if such an event is logged on this report.

Stop list: No provision.

## User Profile Changes

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  1/01/94 15:32:51 RPJCP1 2.0                                User Profile Changes
User SLAUDIT Page
USER      CMD  USER      PROFILE  GROUP  OBJECT  GROUP  INITIAL
INITIAL   PASSWORD CHANGE MADE
PROFILE   USED  CLASS  STATUS  PROFILE  OWNER  AUTHORITY  PGM/LIBR
MENU/LIBR STATUS  ON    BY USER
SLAUDIT   CHG
010194 QSECOFR

151553 DSP02
User profiles that are changed appear on this report.
** LEGEND FOR CMD USED: CRT=Create User Profile (U.P.), CHG=Change U.P., RST=Restore
U.P., DST=Chg. Ded. Service Tools Passwd.
Count      1 System S1015241 QAUDJRN type CP

```

---

If your OS/400 system value QAUDLVL includes \*SECURITY, user profiles that are created, changed or restored will appear on this report.

The user profile that was changed appears first, followed by the command that was used.

CRT = CRTUSRPRF            create a new user profile  
 CHG = CHGUSRPRF change an existing user  
 RST = RSTUSRPRF           restore a profile from tape/diskette/etc.  
 DST (V2R3 and higher)    QSECOFR password was reset using dedicated  
 service tools

Only elements of the profile which were changed are listed.

Stop list: There is no provision for excluding events from this report.

## User ID changed on Job Description

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  2/11/94 12:08:52 RPJJD1 2.0 User ID Changed on Job Description
User SLAUDIT Page
JOB DESC OLD NEW
CRT JOURNAL
NAME LIBRARY USER NAME USER NAME DATE TIME JOB NAME USER
JOBNBR CHG USER ID SEQ NBR
Job descriptions on this report have been changed to include a user profile name. Anyone
who has access to this job description
and to the user profile may submit jobs as if signed on as the new user name.
Count 0 System QAUDJRN type JD QAUDLVL *SECURITY

```

---

If your OS/400 system value QAUDLVL includes \*SECURITY, job descriptions that are created or changed to specify a user profile will appear on this report.

Most job descriptions specify that the user profile of the person submitting the job be used. Thus, users cannot gain extra authorities when submitting a job. There are situations when a program must run under a job description that specifies a user profile. This report will tell you when any job descriptions are created or changed to specify a user profile name.

Stop list: No provision.



## Objects Moved or Renamed

```

*.....1.....2.....3.....4.....5.....6.....7.....8.....9
.....0.....1.....2.....3
  2/11/94 12:09:00 RPJOM1 2.0 Object Move/Rename Journal
User SLAUDIT Page
OLD OLD OBJECT MOVE / NEW NEW OBJECT CHANGED -
- JOB INFORMATION - - JOURNAL
LIBRARY NAME TYPE RENAME LIBRARY NAME MADE BY DATE TIME
NUMBER NAME USER SEQ NUM
QSYS QEIS87ZW *CMD R QSYS SIGNOFF QSECOFR 020894 210054
14211 DSP02 QSECOFR 25020
QSYS SIGNOFF *CMD R QSYS QEIS87ZW QSECOFR 020894 205950
14211 DSP02 QSECOFR 25012
QSYS SIGNOFF *CMD R QSYS SIGNOFFXX QSECOFR 020894 210054
14211 DSP02 QSECOFR 25019
QSYS SLAINSTALL *LIB R QSYS SLAINST200 QSECOFR 020894 213142
14226 DSP02 QSECOFR 25308
QTEMP SLAPRINT *FILE M SLAUDIT SLAPRINT QSECOFR 020894 220558
14226 DSP02 QSECOFR 26318
QTEMP SLAPRINT *FILE M SLAUDIT SLAPRINT QSECOFR 020994 180151
14257 INSTALLUPG QSECOFR 27860
SLAUDIT2 SLAPTF *FILE R SLAUDIT2 SLAPTFX SLAUDIT 021094 94924
14274 DSP01 SLAUDIT 27944
SLAUDIT2 SLAPTFX *FILE R SLAUDIT2 SLAPTF1 SLAUDIT 021094 94946
14274 DSP01 SLAUDIT 27946
SLAUDIT2 SLAPTF1 *FILE R SLAUDIT2 SLAPTF SLAUDIT 021094 94931
14274 DSP01 SLAUDIT 27945
Objects appear on this report when they are moved to another library or renamed. Routine
entries may be suppressed via the
stop list functions on the configuration menu.
Count 12 System S1015241 QAUDJRN type OM QAUDLVL value *OBJMGT

```

If your OS/400 system value QAUDLVL includes \*OBJMGT, objects that are moved or renamed appear on this report.

Stop list: Individual objects or all objects in a given library may be excluded from this report via the library and object stop list. See the configuration menu option "Library stop list," or use the WRKLOS command. **The "new" object name and library name are the ones checked by the stop list.**

## Changes in Object Ownership

```

*.....1.....2.....3.....4.....5.....6.....7.....8.....9
.....0.....1.....2.....3
  1/01/94    1:58  RPJOW1    2.0                      Changes in Object Ownership
User QSECOFR                               Page
LIBRARY  OBJECT      OBJECT              CHANGE
-  JOB INFORMATION - -  JOURNAL
NAME     NAME        TYPE      OLD OWNER  NEW OWNER  MADE BY   DATE    TIME
NUMBER NAME      USER          SEQ NBR
SLAUDIT2 PFQHSTOBJD *FILE     QSECOFR   SLAUDIT   QSECOFR   121193  122455
13553 DSP02      QSECOFR      20294
SLAUDIT2 PFSTP2      *FILE     QSECOFR   SLAUDIT   QSECOFR   123093  204940
13705 DSP02      QSECOFR      22469
Objects appear on this report when their ownership changes.
Count    2  System S1015241  QAUDJRN type OW  QAUDLVL value *SECURITY

```

If your OS/400 system value QAUDLVL includes \*SECURITY, changes in object ownership will appear on this report.

The first three fields identify the object that was changed. The next two tell which user *formerly* owned the object and which user *now* owns it.

The user ID who made the change and the job ID of the job that was running appear next. For interactive jobs, the job name is the display station ID.

The object was formerly owned by the Old Owner, but now is owned by the New Owner.

The user who made the change, the date and time of the change, and the job ID of the job that made the change come next on the report.

Finally, the journal sequence number in QAUDJRN is noted. You may use this number with IBM's DSPJRN command to retrieve the security journal entry, or to examine other entries made before or after this one.

Stop list: Individual objects or all objects in a given library may be excluded from this report via the library and object stop list. See the configuration menu option "Library stop list," or use the WRKLOS command.

## Programs Changed to Adopt Authority

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  2/11/94 12:09:12  RPJPA1                      Programs that Adopt Authority
User SLAUDIT      Page
      PROGRAM      LIBRARY      OBJECT
JOURNAL
OWNER            NAME            NAME            TYPE            DATE            TIME            JOB NAME      USER ID
JOBNBR
QPGMR            SELMSGs      SLAUDIT        *PGM            022594          201503          DSP02         QSECOFR
13402
                22432
  Programs appear on this report when someone changes them to adopt the authorities of the
  program owner, in addition to those
  of the user running the program.
Count           0      System                QAUDJRN type PA      QAUDLVL value *SECURITY

```

If your OS/400 system value QAUDLVL includes \*SECURITY, programs created or changed to adopt authority will appear on this report.

A user who has authority to such a program, *while he is running that program*, adopts or adds the authorities of the user profile that owns the program. Adopted authority is widely used in AS/400 and iSeries software.

The first field list the program owner -- the authorities of this user profile are adopted by anyone running the program. Programs that adopt the authority of the security officer, QSECOFR, should be reviewed with special care.

The USER ID identifies the user who changed the program to adopt its owner's authorities.

Stop list: You may not exclude events from this report via the library/object stop list.

See also: report RPJRP1 - programs *restored* to your system from tape or disk which adopt authority.

## Invalid Password or User ID

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  1/01/94 15:33:34 RPJPW1 2.0 Invalid Password or User ID Journal
User SLAUDIT Page

- - JOB INFORMATION - - JOURNAL
DESCRIPTION USER LOCATION DATE TIME
NUMBER NAME USER SEQ NBR
Bad PASSWORD for SLAUDIT at DSP03 123193 230853
13662 QBASE QSYS 24176
Bad PASSWORD for SLAUDIT at DSP03 123193 230859
13662 QBASE QSYS 24177
Bad USER ID for SLUADIT at DSP03 123193 230932
13662 QBASE QSYS 24178
Bad PASSWORD for QSECOFR at DSP02 010194 131746
13662 QBASE QSYS 24270
Records appear on this report when someone tries to sign on with an invalid password or
user ID.
Count 4 System S1015241 QAUDJRN type PW

```

If your OS/400 system value QAUDLVL includes \*AUTFAIL, invalid sign on attempts will appear on this report.

*Caution:* Suppose user BJONES has password T6HG3AA. By mistake, he keys his password in the User ID prompt on the sign on screen. This report will show, "Bad PASSWORD for T6HG3AA." Shred this report, rather than just throwing it away, if you see an entry that looks like it might be someone's password.

Some sites shred any security-related report.

Stop list: You cannot omit events from this report via the stop list.

## Programs Restored that Adopt Authority

More...

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  2/25/94 22:15:31 RPJRP1 2.0          Programs Restored that Adopt Authority
User SLAUDIT          Page
PROGRAM RESTORED          ADOPTS THE RESTORED ON  - - JOB
INFORMATION - -          JOURNAL
NAME TO LIBRARY BY USER AUTHORITY OF DATE TIME NUMBER NAME
USER SEQ NBR
BLDQHSTLST SLAUDIT QSECOFR QSECOFR 022594 204848 14460
INSTALLUPG QSECOFR 28154
GETJRCVRG SLAUDIT QSECOFR SLAUDIT 022594 204901 14460
INSTALLUPG QSECOFR 28172
NEEDLOG SLAUDIT QSECOFR SLAUDIT 022594 204905 14460
INSTALLUPG QSECOFR 28180
SELAUDJRNE SLAUDIT QSECOFR SLAUDIT 022594 204956 14460
INSTALLUPG QSECOFR 28256
SELMSGSLAUDIT QSECOFR QPGMR 022594 204957 14460
INSTALLUPG QSECOFR 28258
SIGNOFFCPP SLAUDIT QSECOFR SLAUDIT 022594 204958 14460
INSTALLUPG QSECOFR 28261
SOFFLOG SLAUDIT QSECOFR SLAUDIT 022594 205001 14460
INSTALLUPG QSECOFR 28266
Programs restored to this system which adopt authority are listed. Users who run these
programs have a combination of their own
authorities and the authorities of the user listed in the ADOPTS... column.

```

If your OS/400 system value QAUDLVL includes \*SECURITY, programs restored which adopt authority will appear on this report.

A user who has authority to such a program, *while he is running that program*, adopts or adds the authorities of the user profile that owns the program. Adopted authority is widely used in AS/400 and iSeries software.

The first field list the program owner -- the authorities of this user profile are adopted by anyone running the program. Programs that adopt the authority of the security officer, QSECOFR, should be reviewed with special care.

The USER identifies the user who restored the program. Note that the program could have been *created* on an entirely different system, then *restored* on your AS/400.

Stop list: You may not exclude events from this report via the library/object stop list.

See also: report RPJPA1 - programs changed to adopt authority.

# System Value Changes

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:34:02 RPJSV1 2.0 System Value Changes Journal
User SLAUDIT Page
INFORMATION - - JOURNAL - - JOB
USER NAME SEQ NBR NUMBER
System value QAUDLVL *** Security auditing level
As shipped: *NONE
Softlight: *SECURITY *SAVRST *AUTFAIL *DELETE *CREATE *OBJMGT
QAUDLVL was changed by QSECOFR on date 123193 at time 123907 13731
QSECOFR DSP02 24027
FROM: *SECURITY *SAVRST *AUTFAIL *DELETE *CREATE *OBJMGT *PGMFAIL
TO: *SECURITY *SAVRST *AUTFAIL *DELETE *CREATE *OBJMGT
System value QHOUR *** Hour of the day
As shipped: ' '
QHOUR was changed by QSECOFR on date 123193 at time 123848 13731
QSECOFR DSP02 24026
FROM: 13
TO: 12

```

---

If your OS/400 system value QAUDLVL includes \*SECURITY, changes to system values will appear on this report.

Changes to system values are made via the WRKSYSVAL and CHGSYSVAL commands.

For details of what each system value does, see the online help for the WRKSYSVAL command, or the *AS/400 Programming: Work Management Guide*, SC41-8078, from IBM.

This report lists the shipped value (for shipments in the United States, as of the time of the software release), the value before the change was made (from), and the value after the change (to).

Stop list: You cannot omit items from this report via the stop list.

# Audited Object Accesses

\*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9  
 .....0...+...1...+...2...+...3

2/13/96 11:46:00 RAJZRA 2.5 Audited Object Accesses

SLAUDIT Page

OBJECT NAME	LIBRARY	OBJECT TYPE	DATE	TIME	JOB NAME	USER	PROGRAM USED	ACCESS TYPE
DSP01	QSYS	*DEVD	021396	105122	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	105145	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	105638	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	110721	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	110817	DSP01	QSECOFR	WRKLOS	30
DSP01	QSYS	*DEVD	021396	111111	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	112604	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	112604	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	112620	DSP01	QSECOFR	STRSLA	30
DSP01	QSYS	*DEVD	021396	112634	DSP01	QSECOFR	WRKRPT	30

This report lists read accesses to objects that have been marked for auditing via the CHGOBJAUD command. See the IBM Security Reference manual for more details.

Count 64 System S1015241 QAUDJRN type ZR (See also report RAJZCA for changes to objects)

## Audited Object Changes

\*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9  
 .....0...+...1...+...2...+...3

2/13/96 11:45:23 RAJZCA 2.5 Audited Object Changes

SLAUDIT		Page		Audited Object Changes				
OBJECT		OBJECT					PROGRAM	ACCESS
NAME	LIBRARY	TYPE	DATE	TIME	USER	JOB	IN USE	CODE
DSP01	QSYS	*DEVD	010196	180953	QSECOFR	DSP01	QWTPIIPP	50
DSP01	QSYS	*DEVD	010196	182948	SLAUDIT	DSP01	QWTPIIPP	50
DSP01	QSYS	*DEVD	010296	161218	SLAUDIT	DSP01	QWTPIIPP	50
DSP01	QSYS	*DEVD	010396	120036	SLAUDIT	DSP01	QWTPIIPP	50
DSP01	QSYS	*DEVD	012396	205600	QSECOFR	DSP01	QWTPIIPP	50
PFNBH2	SLAUDIT2	*FILE	010396	120425	SLAUDIT	DSP01	WRKNBH	30
PFNBH2	SLAUDIT2	*FILE	012696	232022	QSECOFR	DSP01	WRKNBH	30

This report lists changes to objects which have object auditing set. The object must be flagged for auditing via the CHGOBJAUD command. See the Security Reference manual for further details.  
 Count 7 System S1015241 QAUDJRN type ZC

## Service Tool Actions Report

This report will identify those critical functions allowed by users with \*SERVICE special authority related to supporting the system by use of the service tool functions and command STRSST. This activity should normally be rare

## System Management Report

This report will identify system management activity such as changes to the System Reply List, changes to Operational Assistant functions, and Network File Operations. This activity should normally be rare. .



## Interactive Job Exceptions

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
1/01/94 15:36:10 RPIJB1CL Interactive Job Exceptions
System S1015241 Page

```

CLOCK	CPU	TRANS-	AVG. RESP.	NBR.	START	END	WALL	
USER	(DEVICE)	NUMBER	DATE	DAY	TIME	DATE	DAY	TIME
MINUTES	SECONDS	ACTIONS	(SECONDS)	AUX I				
QSECOFR	DSP02	013676				1993/12/30	THU	13:47:21
.00	638	1550	1.34193	241				
QSECOFR	DSP02	013705	1993/12/30	THU	15:55:09	1993/12/30	THU	22:49:39
415.00	180	625	.59520	80				
								CHECK
QSECOFR	DSP02	013751	1993/12/31	FRI	15:30:56	1993/12/31	FRI	18:37:18
186.00	108	256	.96484	54				
								CHECK
QSECOFR	DSP02	013777	1993/12/31	FRI	22:26:24	1994/01/01	SAT	01:34:50
188.00	78	156	1.64743	67				
					CHECK	HOLIDAY		CHECK
2+DAYS								
QSECOFR	DSP01	013814	1994/01/01	SAT	01:44:49	1994/01/01	SAT	01:45:13
.00	4	9	.44444	4				
					HOLIDAY	CHECK	HOLIDAY	CHECK
QSECOFR	DSP02	013816	1994/01/01	SAT	13:17:55	1994/01/01	SAT	15:29:10
131.00	1498	260	7.56153	122				
					HOLIDAY	CHECK	HOLIDAY	CHECK
ROOT	DSP03	013823	1994/01/01	SAT	13:51:53	1994/01/01	SAT	15:29:37
98.00	3	2	3.50000	3				
					HOLIDAY	CHECK	HOLIDAY	CHECK
SLAUDIT	DSP01	013672				1993/12/30	THU	13:46:07
.00	823	2340	.68504	292				
SLAUDIT	DSP01	013706	1993/12/30	THU	16:14:27	1993/12/30	THU	22:48:28
394.00	452	1249	.67974	150				
								CHECK

Interactive jobs are jobs run from a display station. "Abnormal" jobs appear on this report.

See the section *Configuring Softlight Auditor* in this manual to review how to define what the program will consider to be "normal" activity. In brief, you may specify business hours, holidays, and normal workstation locations for individual users. You may also specify defaults to apply to all other users.

Note that interactive jobs that last longer than 24 hours always appear. Batch jobs never appear.

## Random Sample of Jobs by User

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
  1/01/94 15:36:27      RPJBR2CL      Random Sample of Jobs by User
System S1015241      Page
      JOB  JOB      JOB      JOB      JOB      CPU      DURATION
NBR      AVERAGE      NBR
USER      TYPE  NUMBER  NAME      START      END      SECS      MINUTES
TRANS.  RSP.  TIME    AUX I/Os
SLAUDIT  -----
-----
      B - Batch jobs
SLAUDIT  B  013694  RAJafa  1993/12/30 THU  1993/12/30 THU      17      .6
.00000      812
      12:53:02      12:53:43
RPJBR2CL run by SLAUDIT on 1/01/94 at 15:36:27      Random Sample of Jobs by User
1 samples. System S1015241
* Note: A different percentage sample of jobs may be selected for each user ID via the
WRKUSRCF command.

```

This report lists a random sample of jobs run. It includes both batch and interactive jobs.

There may well be nothing wrong or abnormal about jobs listed on this report. Its purpose is to give you a good idea of the kinds of jobs run by and interactive sessions times used by each user on your AS/400.

You may specify a different sampling percentage for any user ID, as well as a default percentage. See the section in this manual entitled *User Profile Controls* to learn how to do so.

# System History Log Messages

```

*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9
...+...0...+...1...+...2...+...3
2/11/94 12:11:05  RPQH2ACL           Messages from System History Log
Page
Random Sample of Messages
MESSAGE ID                                DATE
DAY  USER      MESSAGE TYPE                               TIME
SEVERITY  MESSAGE TEXT
HOLIDAY  JOB NAME  MESSAGE LIBR/FILE
CPF2456 Log version QHST94036A in QSYS full and should be saved. 1994/02/09
WED  QSYS      Information
00
SCPF      *LIBL      /QCPFMSG
CPF2456 Log version QHST94010A in QSYS full and should be saved. 1994/02/02
WED  QSYS      Information
00
SCPF      *LIBL      /QCPFMSG
CPF2456 Log version QHST94033A in QSYS full and should be saved. 1994/02/05
SAT  QSYS      Information
00
SCPF      *LIBL      /QCPFMSG
CPF3848 1 security or data format changes occurred. 1994/02/08
TUE  QSECOFR   Diagnostic
20
DSP02      *LIBL      /QCPFMSG
CPF5140 messages. Targeting selection of 100 percent.
CPF5140 Session stopped by a request from device DSP02. 1994/02/09
WED  QSYS      Information
70
QBASE      *LIBL      /QCPFMSG
CPF5140 Session stopped by a request from device DSP01. 1994/02/02
WED  QSYS      Information
70
QBASE      *LIBL      /QCPFMSG

```

---

This report shows a random sample of messages from the system history log, QHST.

You may specify a different percentage to sample for each message ID -- anywhere from 0% to 100%. You may also specify a default percentage for all other messages by message severity.

See the sections in this manual entitled *Message control file* and *Default percentage of messages by severity*.

---

## Functions retained from prior releases

Some options, which are not in the strategic direction of the product, have nonetheless been retained for compatibility with prior releases of Softlight Auditor. We plan no enhancements to these functions, and may drop support from them in future releases, especially if changes in OS/400 render them obsolete or incompatible.

### Job logs

*This function is retained for compatibility; it may be absent from future versions.*

OS/400 is designed to *prevent* unauthorized access. It is not designed to record everything that a user does for later review. While it is certainly better to lock your doors before a burglar strikes, sometimes you need to check what is going on outside the house.

To review much of what your users are doing while they are signed on, you need to look at their job logs. Unfortunately, the job log is usually deleted if a job ends normally. (An interactive job consists of the entire period from sign on to sign off. Signing off a workstation is a normal job ending. Thus, interactive job logs are discarded at sign off.)

Softlight Auditor allows you to redefine the SIGNOFF command to print a random sample of interactive job logs to a special output queue, SLAUDIT2/JOBLOGS. You may use the WRKOUTQ command to review these copies later, at your leisure. The section "Capturing job logs" describes how to arrange for these copies to be made.

Hint: job logs can be long and detailed. Use the random sampling capability of Softlight Auditor to select a small percentage (2% - 3%) of job logs for most users. You may want a slightly greater percentage for programmers, and, perhaps, a very high percentage for the security officer. Run the WRKUSRCF command to set a low percentage for user \*DEFAULT, then raise that percentage only as needed. You may, of course, change the sample percentage for any user at any time.

The SLAUDIT/WRKUSRCF command, option 4 on the configuration menu, contains parameters you can define for each user profile.

Pct normal job logs . . . . .	_10 %	0-100
Pct abnormal job logs . . . . .	100 %	0-100
Pct jobs to report. . . . .	_25 %	0-100

*Pct normal job logs* specify the percentage (0 to 100) of interactive job logs for this user which are to be copied into the output queue SLAUDIT2/JOBLOGS for later review. Separate setup is required to have these copies made automatically. See the sections "Capturing job logs" and "Random sample of job logs." *Abnormal job logs* is not used in this release. All job logs are considered "normal" for reporting purposes.

The value 10% shown for normal logs is probably too high for "normal" users. Reviewing job logs is tedious! A sample of 2% is probably sufficient for users other than the security officer or programmers. Experiment until you get a reasonably small sample.

*Pct jobs to report* is the percentage (0 to 100) of batch and interactive jobs to select for a random sample. Only the date, time and job name are reported in this sample. It is intended to give you a feel for the normal activity on your system. Again, the 25% value shown is probably too high for normal users. (2% might be better.)

*Allow sign on, termination date, and the initial program and library* are not used.

## **Sample of messages in QHST**

*This function is retained for compatibility; it may be absent from future versions.*

OS/400 is a message-driven system. There are literally thousands of messages sent back and forth from various programs to each other and to the operating system.

Some of these messages are sent to the system history log, QHST. You will want to review many of these messages. Some, however, will be of no interest to you. For other messages, you might want to review a random sample of occurrences. You can tailor Softlight Auditor to report any percentage – from 0 to 100 – of occurrences of any message.

The messages are sorted by message ID and time, so you can review all occurrences of a given messages (or a random sample of, say 25%), grouped together for better understanding of what is happening. For instance, a string of "Bad password" messages from a variety of terminals between 9 and 10 pm should almost certainly be investigated.

You tailor which messages to report in full, which to sample, and which to suppress. As shipped, every security-related message (in the range CPF2200) will be reported. Every system alert or system integrity message (severity 80 or 90) will be reported. Between 2% and 5% of other messages (a random sample) will be reported.

You may select individual messages and report none (0%), all (100%), or a random sample (1% - 99%). See the section "Message control file."

You may also change the default random sample percentage for messages not individually selected. You might, for instance, want to see 20% of all severity 50 messages not elsewhere defined. See the section "Default percentage of messages by severity."

## Message control file

*Most information needed for an audit is contained in the system security journal, QAUDJRN. The system history file, QHST, normally has redundant information. We have no plans to stop supporting these features of Softlight Auditor, but all new features are based on QAUDJRN.*

The AS/400 sends a lot of messages to the history log, QHST. Many are not of interest to someone auditing system activity. Softlight Auditor will automatically sort messages by message ID. You may use the SLAUDIT/WRKMSGCF command, configuration menu option 5, to specify that you want to see all occurrences of a message, no occurrences, or a random sample -- from 1% to 99% of occurrences.

If you do not define a message control record via this command, the random sample size is determined by the severity of the message. To change those default sample sizes, use the SLAUDIT/CHGRNDDFT command, described in the next section.

```

Work with Message Control File                                WRKMSG 1

Message ID. . . . . _____ Enter=Position list to this ID
                                                F6=Create a new entry

Type options, press Enter.
  2=Change      4=Delete      5=Display

MESSAGE
Opt MSGID FILE TEXT ... PCT TO REPORT
- CPA0701 QCPFMSG MSGX received by Y at Z. (C D I R) 5
- CPA7025 QCPFMSG Receiver X in Y never fully saved. (I C) 100
- CPC1E1D QCPFMSG Cleanup has completed. 10
- CPC3701 QCPFMSG 999 objects saved from library X. 25
- CPF0901 QCPFMSG PWRDWN SYS command issued by user X and i 100
- CPF0965 QCPFMSG IPL options used. 100
- CPF1806 QCPFMSG System value X changed from Y to Z. 100
- CPF22AA QCPFMSG Only *AUTLMGT authority can be specified 100
- CPF22AB QCPFMSG Only *AUTLMGT can be specified with *CHA 100
- CPF22AC QCPFMSG Only *AUTLMGT authority can be specified 100

F3=Exit F6=Add new record More...
```

As shipped, security related messages (CPF2200 range) are pre-defined to print 100% of occurrences. If you wish to change those percentages, or to add new security messages as IBM adds them to OS/400, use this command.

UPDATE	Work with Message Control File		WRKMSG 2
Type choices, press Enter.			
Message ID. . . . .	CPF0965		
Message File. . . . .	QCPFMSG__	Optional	
Message File Library. . . .	*LIBL_____	Optional:	name or *LIBL
Message Text		Optional:	F11 to look up
IPL_options_used._____			
Percent to report (random sample)	100 %	0 to 100 %	of occurrences
Print message data fields on report	Y	Y or N	
F11=Lookup message			
F3=Exit	F12=Cancel	F4=Delete	Roll=Next/Prev rcd

*Message ID* should uniquely identify the message.

*Message file* and *library* are for information, but the file name is needed if you want Softlight Auditor to look up the text and insert it via the [F11] key.

If you have the same message ID in more than one message file, and if messages from both files may be sent to the history log, QHST, you will see both reported at the percentage you specify here. This is a very rare situation.

*Message text* may be keyed by you or looked up by the system. To look up the text, make sure the message file is specified and the library is either specified or is in your library list. Press [F11] to insert the message text.

*Percent to report* is none (0), all (100), or a random sample of from 1% to 99%.

*Print message data* is usually "N", since message data is merged with message text when the message is sent. For some messages, additional data is available only in the second-level text. Since only the first-level text is printed by Softlight Auditor, change this value to "Y" on those messages for which you need to see *all* message data. CPF0965, "IPL Options used," is an example of such a message.

## Default percentage of messages by severity

You do not need to define each message you want sampled on your reports. Use the SLAUDIT/CHGRNDDFT command, configuration menu option 6, to set defaults by message severity.

The screen is shown below.

```

                                Default Percentage of Messages to Print by Severity

Enter the default percentage for random sampling of each message
severity. You may override this percentage for specific messages via
WRKMSGCF.

Message severity      Percent to select      Customary usage
00 - 09 . . . . . : 002 %      Information
10 - 19 . . . . . : 002          Warning
20 - 29 . . . . . : 005          Error
30 - 39 . . . . . : 005          Severe error
40 - 49 . . . . . : 005          Abnormal end of pgm/function
50 - 59 . . . . . : 005          Abnormal end of job
60 - 69 . . . . . : 005          System status
70 - 79 . . . . . : 005          Device integrity
80 - 89 . . . . . : 100          System alert
90 - 98 . . . . . : 100          System integrity
99 . . . . . : 100          Action

Print message data separate from message text?  N  Y, N

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

Five percent of all messages of severity level 40, for example, will appear on the random sample report, *except* for any messages of severity level 40 which are specifically listed in the message control file.

## Capturing job logs

**Note:** *this feature is not supported. See the section entitled "Auditing all commands by a user" for a supported method of reviewing actions of a key user.*

The AS/400 is designed to *prevent* unauthorized access. It is not designed to record everything that a user does for later review. While it is certainly better to lock your doors before a burglar strikes, sometimes you need to check what is going on outside the house.



To review much of what your users are doing while they are signed on, you need to look at their job logs. Unfortunately, the job log is usually deleted if a job ends normally. (An interactive job consists of the entire period from sign on to sign off, so interactive job logs are usually lost at sign off.)

Softlight Auditor allows you to redefine the SIGNOFF command to print a random sample of interactive job logs to a special output queue, SLAUDIT2/JOBLOGS. Since this output queue is in library SLAUDIT2, only user SLAUDIT, others specifically authorized to that library, or users with \*ALLOBJ or \*SPLCTL authority will be able to view or delete these copies.

The SLAUDIT/CHGSIGNOFF command allows you to switch between IBM's normal SIGNOFF command, and Softlight's modified version, which randomly samples interactive job logs for you to review.

*CAUTION: changing the SIGNOFF command should be done during a period of low activity on your system, and it must be done by the security officer. Have him or her read this section before proceeding.*

## How the CHGSIGNOFF command works

For CHGSIGNOFF \*SLA:

1. The IBM command QSYS/SIGNOFF is renamed to QSYS/QEIS87ZW. (Why that name? It doesn't conflict with anything else, and isn't likely ever to do so.)
2. Softlight's SIGNOFF command is copied to library QSYS.
3. Softlight's command processing program, SIGNOFFCPP, is copied to library QSYS.

For CHGSIGNOFF \*IBM:

1. Softlight's SIGNOFF command and SIGNOFFCPP program are deleted from QSYS.
2. The original IBM signoff command is renamed from QEIS87ZW to SIGNOFF.

The SIGNOFFCPP command processing program computes a random number from 0 to 100 and compares it to the random sample threshold for the current user's ID. If the random number is less than the threshold, a copy of the job log is written to SLAUDIT2/JOBLOGS. (The SIGNOFFCPP command adopts authority so that it can access the output queue.)

Finally, the SIGNOFFCPP command runs the QEIS87ZW command to actually sign off. The normal job log is produced or not produced, based on the job end level and the parameters passed to the SIGNOFF command.

The process of capturing job logs is *not* foolproof. Users without limited capability restrictions may use the CHGJOB (change job) command to turn off their job logs. You will then see an empty job log, which may prompt you to investigate that user's actions in other ways.

Users with \*ALLOBJ or \*SPLCTL special authority will be able to delete the job log copies in SLAUDIT2/JOBLOGS. Monitoring the actions of someone with all object authority (such as the security officer) can be done via a journal. See "Monitoring the Security Officer's Actions," in the *AS/400 Security Concepts and Planning Guide*, for a sample program to journal all commands issued by the security officer.

As noted below, OS/400 V2R3 and higher provides a better way to monitor the actions of the security officer.

*Note: Before upgrading to a new release of OS/400, change the SIGNOFF command back to the IBM version. No damage will be done to OS/400 if you forget, but the CHGSIGNOFF command will not work properly.*

---

## SETUP Worksheet

Softlight Auditor comes with a versatile SETUP command, which can be used *both* for first-time setup and to reset values should problems occur. The SETUP command can fix most problems, but you must supply some information. Use this worksheet *before* running the SETUP command.

Determine the attached journal receiver name and library (if any) by running the command

**WRKJRNA QAUDJRN.** If you get a message to the effect that "Object QAUDJRN not found," note that, and skip to "Test 2," below.

Otherwise, if you get a screen showing the attached receiver name and library, note those values here in case they are needed for assistance later,

Library/Receiver: \_\_\_\_\_/\_\_\_\_\_

Press [F3] to exit the display, and use the following sets of values for SETUP. (This would normally be the case if you are *upgrading from a prior version of Softlight Auditor* or if you had auditing running for some other purpose.)

### SETUP VALUES - Choice 1

Setup Softlight Auditor (SETUP)

Auditing system values . . . . .	*SAME	*BASIC, *SAME (F1 for help)
Receiver name . . . . .	*SAME	*GEN, *SAME, name
Receiver library . . . . .	*SAME	*GEN, *SAME, library name
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . . .	*CONT	*CONT, *RESET

Stop at this point, mark these as the values to use, and resume setup.

---

## Test 2

If your get the error "Object QAUDJRN not found," you must perform one more test to check for a naming conflict.

Key **DSPOBJD OBJ(QGPL/AUDIT\*) OBJTYPE(\*JRNRCV)** and press [ENTER].

If you get the message "No objects of specified name or type exist in library QGPL.," use the following values for SETUP.

### SETUP VALUES - Choice 2

Auditing system values . . . . .	*BASIC	*BASIC, *SAME (F1 for help)
Receiver name . . . . .	AUDIT0001	*GEN, *SAME, name
Receiver library . . . . .	QGPL	*GEN, *SAME, library name
Receiver threshold (KB) . . . . .	7000	5000 to 192000 in KB
Journal sequence numbering . . . . .	*RESET	*CONT, *RESET

Stop at this point, mark these as the values to use, and resume setup.

---

If the previous command **DSPOBJD OBJ(QGPL/AUDIT\*) OBJTYPE(\*JRNRCV)** resulted in a list of journal receivers whose names begin with AUDIT, something like this

```
Display Object Description - Basic
```

Opt	Object	Type	Attribute	Size	Text
.	AUDIT0271	*JRNRCV		1183744	Security journal
.	AUDIT0272	*JRNRCV		593920	Security journal
.	AUDIT0273	*JRNRCV		528384	Security journal

Bottom

Already at bottom of area

then it is likely that Softlight Auditor or another audit package was installed on this system before.

If you know the history of auditing on your system, and are comfortable with starting over, you may simply choose a number one higher than the highest shown after paging down to the last screen (that would be AUDIT0274, in this example), and use the following values

### **SETUP VALUES - Choice 3**

```
Auditing system values . . . . . *BASIC          *BASIC, *SAME (F1 for help)
Receiver name . . . . . AUDIT0274      *GEN, *SAME, name
Receiver library . . . . . QGPL        *GEN, *SAME, library name
Receiver threshold (KB) . . . . . 7000    5000 to 192000 in KB
Journal sequence numbering . . . . *RESET      *CONT, *RESET
```

You could also change the naming scheme altogether, and use something like NEWJR0001 instead of AUDIT0274, in the example. The key is to pick a name not already in use, and to end the name with a string of digits, so OS/400 can generate a new name as the next in a sequence.

Stop at this point, mark these as the values to use, and resume setup.

---

If you are not sure, or would like help, run the following command, and fax it to us, including on the printout the fact that you need help with installation. Include your fax number, and any other information you think pertinent. Someone will get back to you with recommended values.

**DSPOBJD OBJ(QGPL/AUDIT\*) OBJTYPE(\*JRNRCV) OUTPUT(\*PRINT)**

---

## Reader comment form

Please photocopy and mail.

Product: Softlight Auditor

We welcome your comments and suggestions for improving this manual and the on-line information. Please use this form to send us your comments.

You agree that we may use anything you send us in any way we choose without incurring any obligation to you.

Name \_\_\_\_\_

Company \_\_\_\_\_

Phone \_\_\_\_\_ Fax \_\_\_\_\_

Mail to Softlight Corporation, PO Box 923 Clinton, SC 29325 USA

Our fax number is 864-833-6559. You may also call us at the same number.

---

## License agreement

Softlight Corporation ("we") and the company, individual or organization evaluating or using our product ("you") agree as follows.

We agree to supply to you one copy of our licensed computer program, Softlight Auditor, and its related documentation ("product"), for evaluation purposes only. This copy will function for a brief period, then cease to function. We warrant that we have the right to deliver the product to you, and that we are the copyright holder.

You agree that we hold the copyright to the product, and that the product represents considerable time, effort and expense on our behalf. You agree not to reverse engineer the product, nor to make copies available to any third party.

You agree not to use the product or any portion of it after the expiration date we supply to you without first paying our annual license fee.

If you elect not to license the product, you agree to remove the product from your system and not to reinstall it. You agree to continue to respect our copyright to the program and documentation.

Because modern computers (including the operating systems that support them) and computer programs (including this product) are complex and may be configured in many ways, we do not warrant that the product is free of all defects, nor that it will install or operate properly on every system. You agree that you will use this evaluation period to verify that the product operates on your system without interfering with other programs or operating procedures at your site.

During the evaluation period, the program is provided AS IS without warranty of any kind, including merchantability or fitness for any particular purpose. It is an *evaluation copy*, provided so that you may decide whether or not it meets your needs. We are happy to work with you to help you make your decision, but we are under no obligation to you, nor you to us, except as specified in this license agreement.

If you elect to keep the product beyond the trial period, you must pay our annual license fee. This license agreement remains in force, and is renewed each year, unless you send us notice that you plan to cancel the license and return the product. You agree to continue to respect our copyright. We agree to provide you with updates and bug fixes, as they become available, at no extra charge – as a part of your annual license fee.

If we cannot correct a material defect for a licensed customer, we will refund up to one year's license fee, pro-rated from the time the program defect was reported to us. We are not liable to you or to your customers or trading partners for incidental or consequential damages. By paying our license fee, you agree to the terms of this license.

This agreement is made in and shall be governed by the laws of the state of South Carolina.

###

# Index

- \*OBJAUD, value of QAUDCTL, 33
- abnormal end to audit, 45
- adopted authority, what is it, 21
- application screens, 25
- auditing key commands, e.g. DFU, 34
- auditing level, changing, 16
- auditing users, 33
- AUDNEW EVT command, 38
- AUDNEW EVT command, running overnight, 43
- authority, adopted, 65, 67
- authorization code, entry of, 13
- bibliography, 4
- break in, attempt to guess password or ID, 66
- business hours, 24, 25
- CHGUSRAUD command, 33
- commands, auditing, 34
- comment form, 83
- compiles, tracking, 58
- configuration, 23
- contacting Softlight Corporation, 5
- copyright notice, 5
- CPF4131 error, 46
- debugging, use of job log to help Softlight Corporation find an error, 45
- dedicated service tools (DST), 60
- de-installing, 18
- descriptions for users and objects, finding, 20
- DFU (and similar commands), auditing, 34
- disclaimer, you are responsible for security on your system, 3
- DSPLOG command, 39
- DST security password, 60
- error CPF4131 stop file, 46
- Error message occurred during FTP error opening local file SLAUDIT, 17
- event audit, command to run, 38
- event audit, re-running, 39
- event audit, starting date, 39
- event auditing, 37
- events, filtering out common, 31
- first audit, what to look for, 20
- flow of data to SLA, 5
- getting started, 20
- hardware configuration, displaying, 4
- help, on-line, 7
- history log, 76
- history log vs. log physical file version, 5
- holidays, 27
- index, on-line, 7
- installation, 9
- interactive job exceptions, 71
- job description, with user profile, 62
- job log, monitoring while active, 49
- job logs, 74, 78
- job scheduler, automatic, 43
- journal vs. journal receiver, 5
- level check error on PFSTP3, 46
- libraries used by SLA, 4
- license agreement, 84
- locations, normal, 25, 28
- long report, audited users, why, 33
- management by exception, 23
- manual, on-line, 7
- menu, main, 19
- message control file, 75
- message severity, 75, 78
- messages, random sample, 76
- night operator shift, 24, 27
- night run, unattended, 43
- nightly run, unattended, 38
- normal business hours, 24, 25
- normal business hours, exceptions to, 71
- normal events, filtering out, 31
- normal locations, 25, 28
- normal workstation locations, exceptions to, 71
- on-line help, 26
- optical storage of reports, 32, 49
- OS/400 release, finding which level you have, 4
- OS/400 upgrade, turn off auditing before, 16
- OS/400, upgrade causes audit to fail, 47
- OS/400, version upgrade, 80
- output queue for reports, changing permanently, 32
- overnight audit, scheduling, 43
- password guessing attacks, 66
- PFQHST2 file is full, abnormal end, 47
- PFSTP3 error CPF4131, 46
- printer file SLAPRINT, 32
- printer, changing which printer or page characteristics, 32
- processor number, hardware resources screen, 4
- program development libraries, 31
- programs compiled, tracking, 58
- QAUDCTL system value, 33
- QAUDCTL, stopping before OS/400 upgrade, 16
- QAUDJRN receiver, specifying name of, 40
- QAUDJRN receivers, managing size and number of, 41
- QAUDJRN, data flow from, 5
- QAUDJRN, deleting, 16
- QAUDJRN. attaching a new receiver, 39
- QAUDLVL, changing, 16
- qhst, 76
- QHST messages, random sample, 75
- QHST, data flow from, 5
- QSECOFR - resetting password for, 60, 61
- QSECOFR, adopting authority, 65, 67
- QSECOFR, auditing actions of, 33
- QTEMP, deletions from not reported, 31
- random sample of jobs run, 72
- random sample of messages, 75
- random sample of QHST messages, 73
- random sample, messages, 76
- references, further reading, 4
- removing the program, 18
- report RAJAJFA - authority failures, 53
- report RAJAFB - program failures, 54
- report RAJCA - authority changes, 55

report RAJCDA - audited commands, 56  
 report RAJCO - objects created, 57  
 report RAJCOP - programs created, 58  
 report RAJDO - object deletions, 59  
 report RAJDS - reset DST security password, 60  
 report RAJOR - system management, 70  
 report RAJST - use of service tools, 70  
 report RAJZCA – audited object changes, 70  
 report RAJZRA – audited object accesses, 69  
 report RPIJB1 - interactive job exceptions, 71  
 report RPIJBR2 - random sample of jobs run, 72  
 report RPJCP1 - user profile changes, 61  
 report RPJJD1 - user profile on job description, 62  
 report RPJOM1 - objects moved or renamed, 63  
 report RPJOW1 - object ownership changes, 64  
 report RPJPA1 - program changed to adopt authority,  
     65  
 report RPJPW1 - invalid password or ID, 66  
 report RPJRP1 - program restored that adopts  
     authority, 67  
 report RPJSV1 - system value changes, 68  
 report RPQH2A - random sample of messages from  
     QHST, 73  
 reports to print, 30, 38  
 reports, changing characteristics, 32  
 reports, changing where they print, 32  
 reports, holding in queue after printing, 32  
 reports, list of, 51  
 reports, what to look for on them, 20  
 RMVSLA command, 18  
 S/36 code, filling object deletion report, 31  
 security journal, changing audit level, 16  
 security journal, stopping and deleting, 16  
 security journal, stopping before OS/400 upgrade, 16  
 security level, QSECURITY, 4  
 security messages, displaying, 39  
 security officer, auditing actions of, 78  
 sequence number on reports, 52  
 service tools, use of, 70  
 sign off command, 79  
 sign on at abnormal time or location, 71  
 sign on attempt failed, 66  
 SLADEBUG command, 45  
 Softlight Corporation, address, phone, fax, 5  
 spans days, 27  
 start date for event audit, 39  
 status auditing, 36  
 stop list, 31  
 system value, change report, 68  
 times, normal, 24, 25  
 TREEV or similar optical storage system, 32, 49  
 troubleshooting, 45  
 troubleshooting installation, 16  
 upgrading to a new version, 9  
 user profile, 24  
 user profile changes, 61  
 USERnnnn, object in SLAUDIT not found - not an  
     error, 45  
 work files from System/36, suppress reporting of  
     creation and deletion, 31  
 work files, clearing, 39  
 workstation IDS, normal, 25, 28  
 work-with screens, 25  
 WRKJOBSCDE command, 43