www.SecureMyi.com

QAUDJRN Auditing: Configuration and Options

Dan Riehl
dan.riehl@SecureMyi.com

IT Security and Compliance Group, LLC

Cilasoft Security Solutions – US Operations

Security Auditing Defined

- Security Auditing is **NOT**!
  - Journaling database file record changes
  - Capturing before and after images of data records
  - Auditing financial records

- Security Auditing **IS**!
  - Recording and reporting security and other system events
    - Who changed that user profile?
    - Who deleted that logical file?
    - Who tried to access the Payroll file?
    - Who changed that system value?
    - Who deleted that spooled file?

- Security Auditing utilizes a special journal named QAUDJRN that you can create – **Auditing is not Automatic**

Do I really care…

- When a main production database just “disappears”?
- When someone tries to sign-on as “administrator” or “guest”?

- When my system just happened to power down today at 1:30 pm

  and yesterday at 1:30 pm,

  and the day before at 1:30 pm,

  and … (Power On/Off Schedule change)?

- When Bluto out on the loading dock views/prints the Payroll check register?

Do I really care…

- When someone in the Far East is scanning my IP Ports?
- When my contractor creates an adopting program as a back door into the system.
- When a bunch of new powerful user profiles appear on the system?
- When someone compiles a program directly into production?
- When someone views all your private personal health information.
- When my user profile has been deleted?

Security Auditing Principles

- Start auditing all important security/system events so that you have the needed data in the event of a security breach or other system failure.
- Record more information than you'll ever possibly need. You may actually need it.
- Retain the information forever, or as long as practical.
  - 12-24 Months can be a good starting point
- Your Security policy should include the specifics regarding retention of QAUDJRN audit journal receivers.

Real Life Examples

- The program ran correctly yesterday, but blew up today. Did someone change it?
- A user profile keeps becoming disabled, why?
- What commands were run by QSECOFR last week? And that new contractor?
- The QCRTAUT System Value is wrong. Who changed it, and when?
- How did that password get changed?
- How did that User’s Initial Program and Menu get changed?
- Who removed the FTP exit program from the exit point?
- Who added that entry to the Job Scheduler?

Security Auditing Constraints

- Disk Space for on-line retention of audit data
  - You can only report from what you have on-line

- Performance – If you turn on auditing of many things, there will be some performance impact. H/A solutions illustrate the extreme.

- Increased backup window to save potentially huge amounts of audit data.

- Most commercial HA software will force you to audit all object changes and events that you would not normally want to audit.

Data Collection Rationale

- Why collect GB or TB of audit data when you cannot tell WHO did WHAT?
  - There should be **No Shared Passwords**
  - There should be No Generic Profiles/Log-Ons!
    - QSYSOPR, QUSER, FTPUSER, ABCUSER
    - And yes, QSECOFR too (who knows the password?)
  - Users must be accountable for their own actions and trace-able

Security Auditing Check-Up

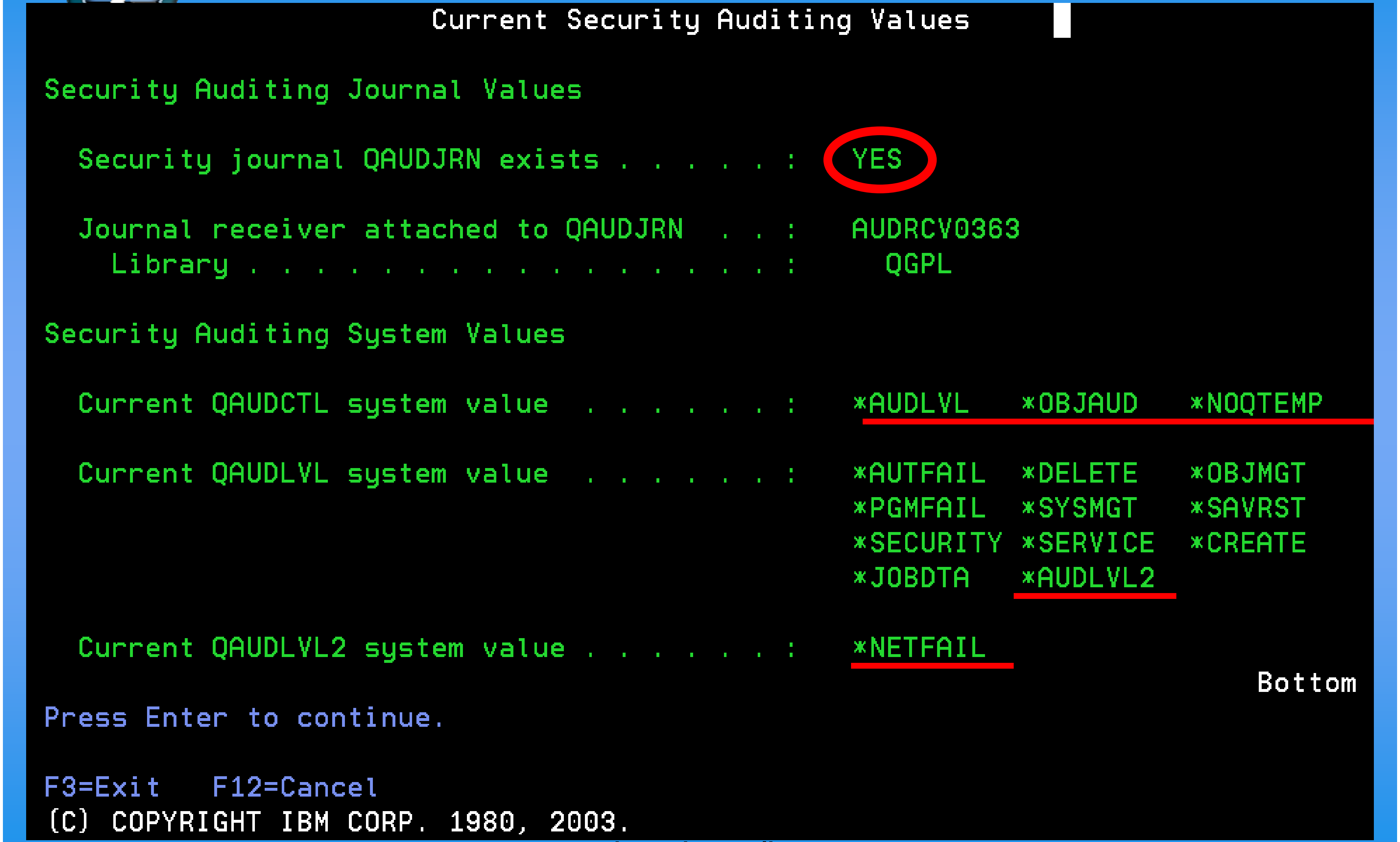
- If you want to inquire into your current security auditing setup, Use the command

DSPSECAUD (Display Security Auditing)

See the next page for details

- You must have *ALLOBJ and *AUDIT special authority to run the command.

DSPSECAUD Command Display



```
                        Current Security Auditing Values

Security Auditing Journal Values

  Security journal QAUDJRN exists . . . . . . :   YES

  Journal receiver attached to QAUDJRN  . . . :   AUDRCV0363
    Library . . . . . . . . . . . . . . . . . :     QGPL

Security Auditing System Values

  Current QAUDCTL system value  . . . . . . . :   *AUDLVL    *OBJAUD    *NOQTEMP

  Current QAUDLVL system value  . . . . . . . :   *AUTFAIL   *DELETE    *OBJMGT
                                                  *PGMFAIL   *SYSMGT    *SAVRST
                                                  *SECURITY  *SERVICE   *CREATE
                                                  *JOBDTA    *AUDLVL2

  Current QAUDLVL2 system value . . . . . . . :   *NETFAIL
                                                                      Bottom
Press Enter to continue.

F3=Exit   F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2003.
```

Security Auditing Three-Step

Step 1. Create a Journal Receiver

```
CRTJRNRCV JRNRCV(JOURNALS/AUDRCV0001)  +
                     THRESHOLD(100000) AUT(*EXCLUDE)
```

- Specify a threshold that is suitable for your case. It must be at least 100,000 kb as shown here
- End the name with numbers, so the CHGJRN *GEN function will increment the number starting from 0001
- Create the receiver in a library that is normally backed up. Do not create the receiver in QSYS.
- Create the receiver in a library whose name comes alphabetically before QSYS, for restore operations.

Security Auditing Three-Step

Step 2. Create the Journal QAUDJRN

```
CRTJRN  JRN(QSYS/QAUDJRN)                  +
         JRNRCV(JOURNALS/AUDRCV0001) +
        MNGRCV(*SYSTEM) DLTRCV(*NO)    +
        AUT(*EXCLUDE)
```

- The Journal must be created in library QSYS
- Let the *SYSTEM manage the receivers
- Do Not automatically delete the receivers

Step 3. Set the System Values

- Set QAUDCTL, QAUDLVL and QAUDLVL2 for the desired auditing options.

As with other journals, you must archive and remove old journal receivers.

Or use the Auditing One-Step!

NOTE: Do not use the **CHGSECAUD** command if Security Auditing is already configured on your system. It will almost certainly break your journal receiver chain, causing problems in reporting audit events occurring across the time period.

```
CHGSECAUD  QAUDCTL(*AUDLVL *OBJAUD  *NOQTEMP)    +
           QAUDLVL(*AUTFAIL *SECURITY  *SERVICE  +
                   *DELETE *OBJMGT *PGMFAIL)     +
           JRNRCV(Library-name/AUDRCV0001)
```

This creates the journal and the journal receiver and sets the system values.

You must have *ALLOBJ and *AUDIT special authority to run the command.

Setting the QAUDCTL System Value

- QAUDCTL(*AUDLVL *OBJAUD *NOQTEMP) Recommended

  QAUDCTL is the controller of what events you want to collect

- ***NONE*** – No Auditing will take place on this system

  NO Auditing

- ***AUDLVL*** – Enable Auditing for the events identified in the QAUDLVL and QAUDLVL2 System values

  Auditing

- ***OBJAUD*** – Enable Object Auditing, if you decide to audit any objects.

  Auditing

- ***NOQTEMP*** – Do not record events that occur within a job's QTEMP Library.

  Optional IF Auditing

Setting the QAUDLVL and QAUDLVL2 System Values

See Appendix for Details on all events based upon the QAUDLVL

QAUDLVL(*AUTFAIL *SECURITY *SERVICE *CREATE +
***DELETE *OBJMGT *SYSMGT *SAVRST *PGMFAIL)**

- For the QAUDLVL system value to be effective, QAUDCTL system value must contain the value *AUDLVL

- ***NONE** - means system-wide auditing isn't done, but auditing is performed for users who have a value other than *NONE specified in the AUDLVL parameter of their user profiles via CHGUSRAUD

- ***AUDLVL2** - means that you will specify additional audit level values in the QAUDLVL2 system value.

- ***AUTFAIL** - means unsuccessful log-on attempts and unauthorized attempts to use sensitive objects are audited. These include rejected connection attempts, invalid network sign-on attempts, and attempts to perform an operation or access an object to which the user isn't authorized.

Setting the QAUDLVL and QAUDLVL2 System Values

See Appendix for Details on all events based upon the QAUDLVL

- ***CREATE** - means the creation of new objects or objects that replace existing objects is audited. QTEMP library is exempted regardless of the *NOQTEMP setting in QAUDCTL.
- ***DELETE** means the deletion of objects is audited. QTEMP is excluded.
- ***JOBDTA** means start, change, hold, release, and end job operations are audited. This includes server sessions and remote connection jobs. Comprised of *JOBBAS and *JOBCHGUSR
- ***NETCMN** means violations detected by the APPN Filter support are audited. Comprised of *NETBAS, *NETCLU, *NETFAIL and *NETSCK.
- ***OBJMGT** means object rename and move operations are audited.

Setting the QAUDLVL and QAUDLVL2 System Values

See Appendix for Details on all events based upon the QAUDLVL

- ***OFCSRV** means changing the system distribution directory, opening a mail log and other mail activity is audited.
- ***OPTICAL** means that usage of optical volumes is logged
- ***PGMADP** means the starts and ends of programs that adopt authority will generate an audit entry.
- ***PGMFAIL** means programs that run a restricted machine interface instruction or access objects via an unsupported interface are audited.
- ***PRTDTA** means printing job output is audited whether the output is sent directly to a printer, sent to a remote system, or spooled and printed on a local machine.
- ***SAVRST** means save and restore operations are audited.

Setting the QAUDLVL and QAUDLVL2 System Values

See Appendix for Details on all events based upon the QAUDLVL

- ***SECURITY** means a wide range of security-related activities are audited. The events are comprised of: *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY and *SECVLDL
  - changing an object’s audit value or a user’s audit setting
  - changing an authorization list or an object’s authority
  - changing an object’s ownership
  - creating, restoring, or changing a user profile
  - requests to reset the DST QSECOFR password
  - generating a profile handle through the QSYGETPH API
  - changing a network attribute, system value, or service attribute
  - changing a program to adopt authority

Setting the QAUDLVL and QAUDLVL2 System Values

See Appendix for Details on all events based upon the QAUDLVL

- ***SERVICE** means using tools like DMPOBJ, STRCPYSCN and use of System Service Tools.

- ***SPLFDTA** means creating, changing, holding, and releasing spooled files is audited. An audit journal entry will also be written when someone other than the owner of a spooled file views it.

- ***SYSMGT** means changing backup options, automatic cleanup options, and power on/off schedules using Operational Assistant is audited. Changing the system reply list and access path recovery times is also audited.

- ***ATNEVT** New in V5R4 – Attention Events are monitored. IP Fragments, Malformed Packets, SYN Floods, Port scans, etc…

  (Setup required for V5R4 QOS Server(Not so in 6.1)

  See The Redbook - IBM i5/OS Intrusion Detection System

  http://www.redbooks.ibm.com/redpapers/pdfs/redp4226.pdf

Additional Auditing System Values

- **QAUDFRCLVL** – How many audit records are cached before being written to disk?
  - For most of us, we use the default for performance
    - ***SYS – Let the system decide**
  - For highly secure requirements
    - **1 – Write each audit record as created**

- **QAUDENDACN** – What happens if the system cannot write an audit record to the journal?
  - For most of us, we use the default
    - ***NOTIFY – Send a message**
  - For highly secure requirements
    - ***PWRDWNSYS – Ouch !!   PWRDWNSYS *IMMED**

Auditing Sensitive Objects

- **QAUDCTL system value must include the value *OBJAUD**

- Specify auditing of objects with the **CHGOBJAUD, CHGDLOAUD, CHGAUD** commands

- Entries are written to the system auditing journal **QAUDJRN**

```
CHGOBJAUD OBJ(libname/object) OBJTYPE(objtype) OBJAUD(*NONE)
```

- No auditing is done for this object under any circumstances

```
CHGOBJAUD OBJ(libname/object) OBJTYPE(objtype) OBJAUD(*ALL)
```

- Open for Read and Update operations to the object are audited.

```
CHGOBJAUD OBJ(libname/object) OBJTYPE(objtype) OBJAUD(*CHANGE)
```

- Open for Update operations to the object are audited

Auditing Sensitive Objects

- Object Auditing is associated with the user's OBJAUD value

```
CHGOBJAUD OBJ(libname/object) OBJTYPE(objtype) OBJAUD(*USRPRF)
```

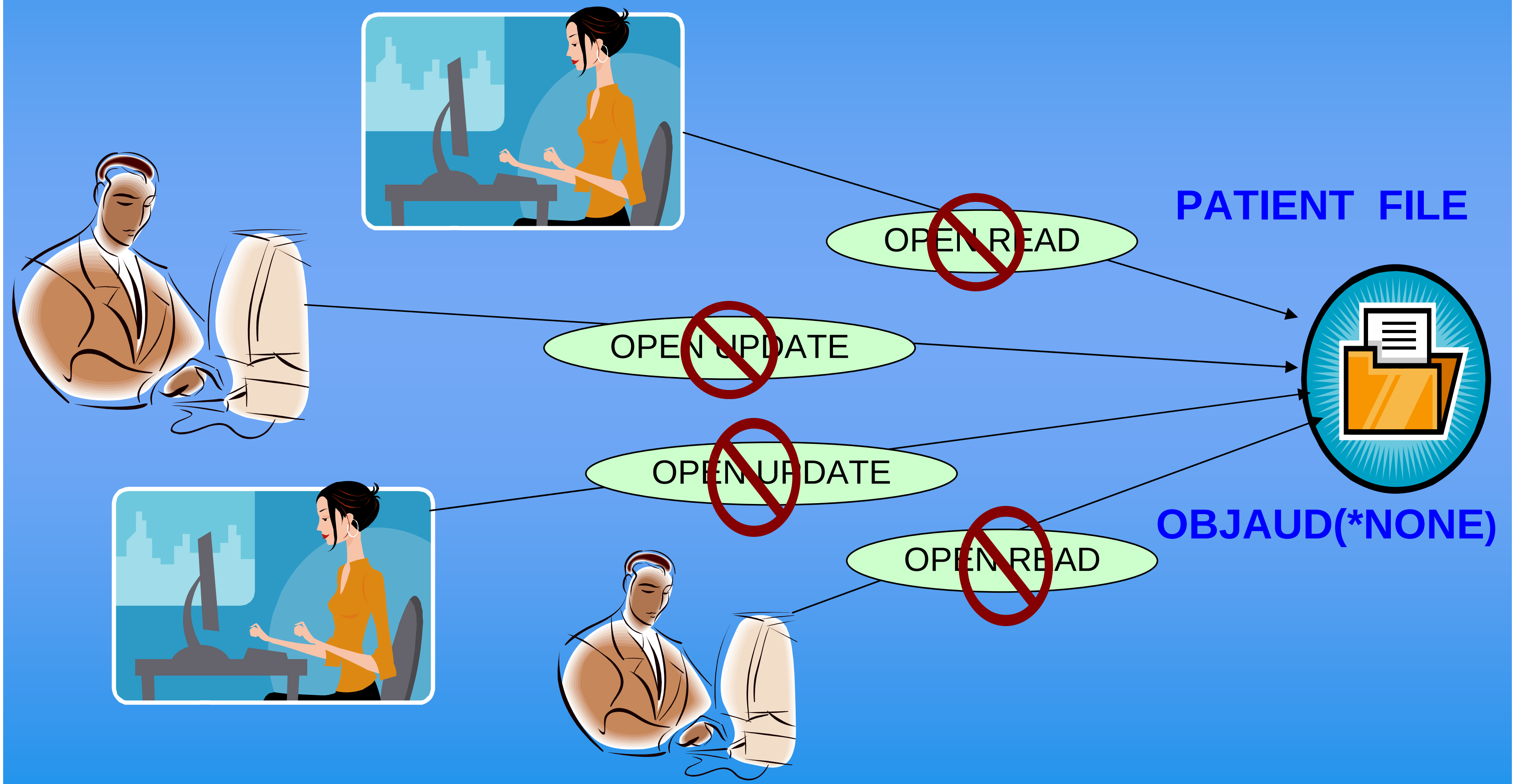
- Audit **<u>only</u>** if the user accessing the object has a value of *ALL or *CHANGE specified on their user profile's OBJAUD value.

```
CHGUSRAUD USRPRF(DAN) OBJAUD(*CHANGE)
```

- This will NOT cause the auditing of all of the objects that DAN opens for Update, Only the objects that specify an OBJAUD value of *USRPRF, *ALL or *CHANGE.

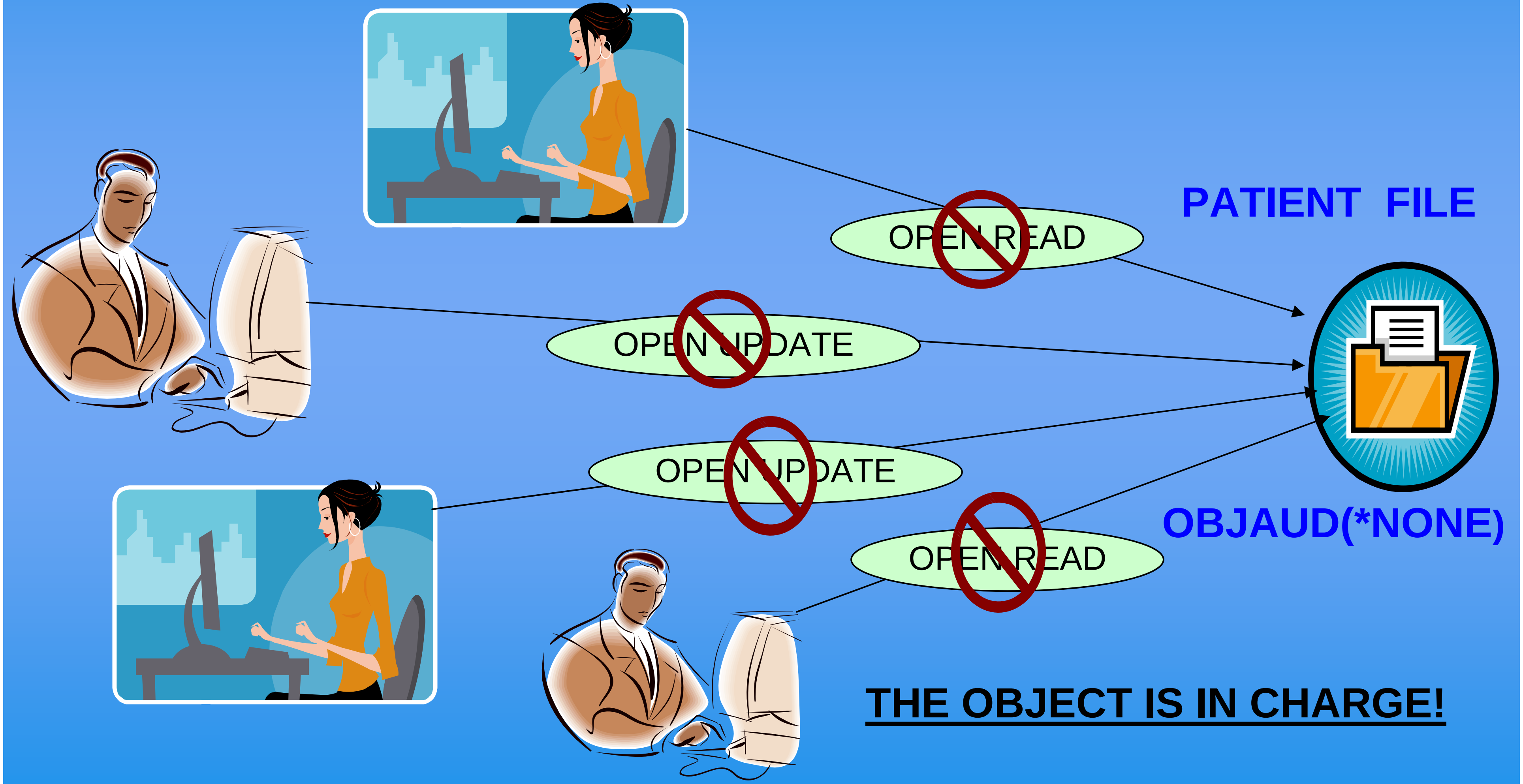
THE OBJECT'S OBJAUD VALUE IS IN CHARGE OF OBJECT AUDITING!

Using CHGOBJAUD … OBJAUD(*NONE)



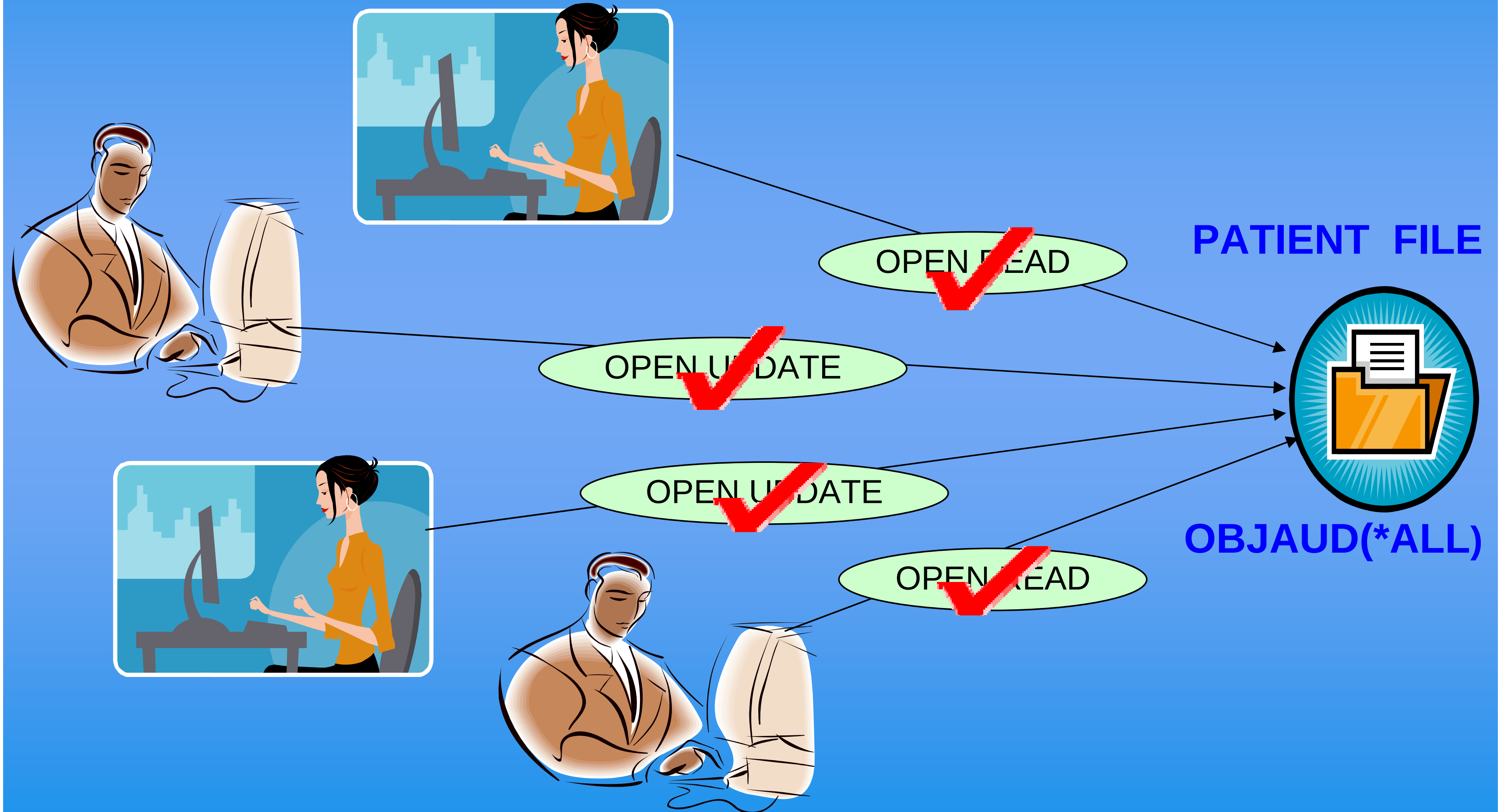
Using CHGOBJAUD … OBJAUD(*NONE)

But what if each user’s OBJAUD Value is OBJAUD(*ALL)?

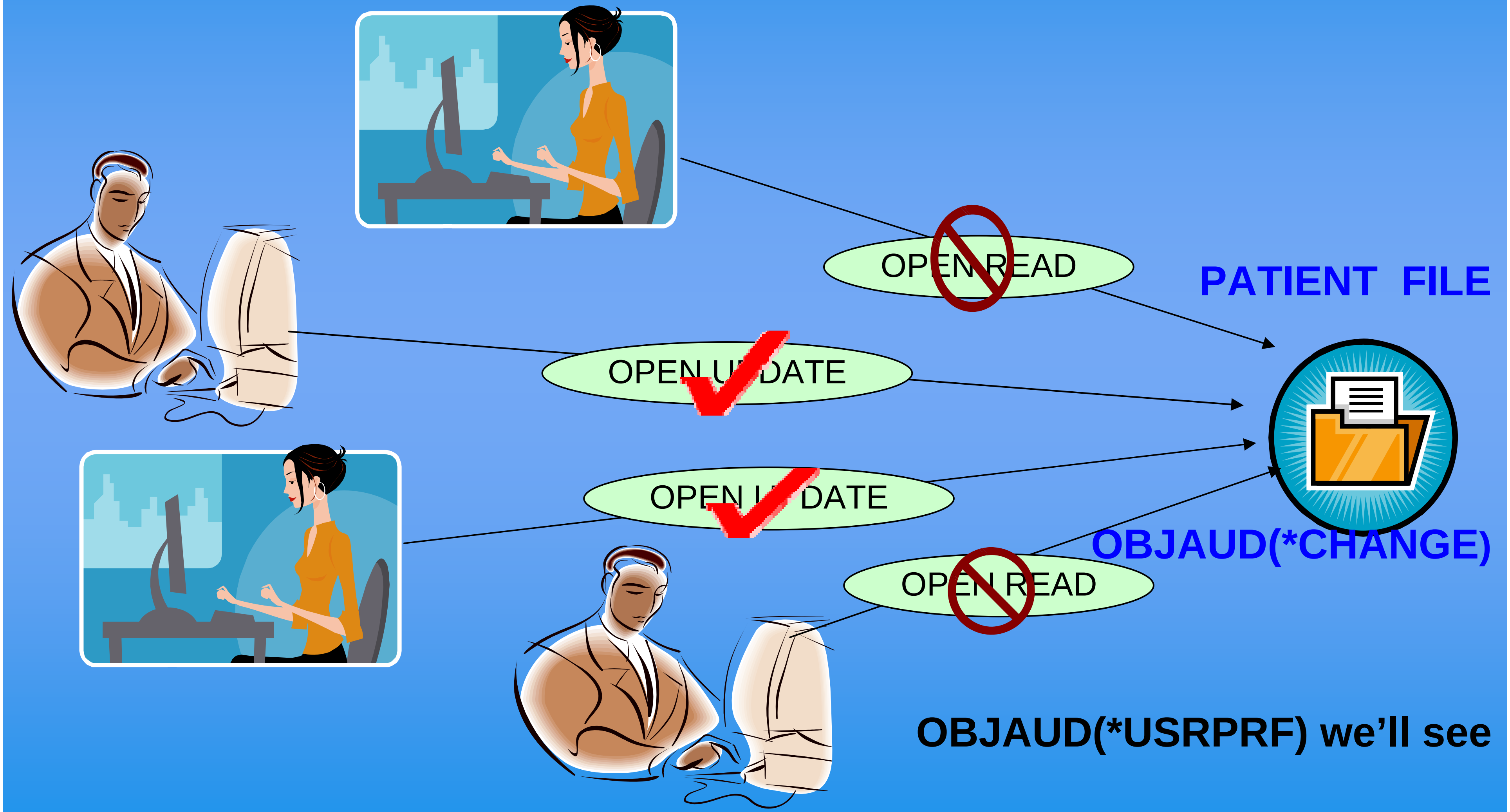


THE OBJECT IS IN CHARGE!

Using CHGOBJAUD … OBJAUD(*ALL)



Using CHGOBJAUD …OBJAUD(*CHANGE)



OPEN READ

OPEN UPDATE

OPEN UPDATE

OPEN READ

PATIENT FILE

OBJAUD(*CHANGE)

OBJAUD(*USRPRF) we'll see

What can be Audited for what Objects?

- IBM Security Reference Guide… Appendix

- Operations Common to All Object Types:
  - Read operation (**ZR** and other Journal Types)
    - **CRTDUPOBJ** Create Duplicate Object (with caveats)
    - **DMPOBJ** Dump Object
    - **DMPSYSOBJ** Dump System Object
    - **SAVxxx commands**

What can be Audited for Objects?

- Operations Common to All Object Types:
  - Change operation (ZC and other Journal Types)
    - **APYJRNCHG** Apply Journaled Changes
    - **CHGJRNOBJ** Change Journaled Object
    - **CHGOBJD** Change Object Description
    - **CHGOBJOWN** Change Object Owner
    - **DLTxxxxxx** Delete object (with Caveats)
    - **ENDJRNxxx** End Journaling
    - **GRTOBJAUT** Grant Object Authority
    - **Many more…**

What can be Audited for Objects?

- Operations for Command (*CMD):
  - Read operation
    - **Run - When command is run**
    - **Generates a CD Journal entry, not catchall ZR**

```
CHGOBJAUD OBJ(QSYS/WRKACTJOB) OBJTYPE(*CMD) OBJAUD(*ALL)
```

-
  - **Change operation (ZC Journal Entry)**
    - **CHGCMD - Change Command**
    - **CHGCMDDFT - Change Command Default**

What can be Audited for Objects?

- Operations for File (*FILE): (PF-DTA and LF)
  - Read operation (**ZR** and other Journal Types)
    - **CPYF - Copy File**
    - **Open - Open of a file for read in RPG, COBOL, CL…**
    - **DSPPFM - Display Physical File Member**
    - **ODBC Select**
    - **FTP GET**

```
CHGOBJAUD OBJ(PAYLIB/PAYMAST) OBJTYPE(*FILE) OBJAUD(*ALL)
```

NOTE: You DO NOT get any audit trail of record level activity.

What can be Audited for Objects?

- Operations for File Objects (*FILE): (PF-DTA and LF)
- Examples: Change operations (ZC and other Journal Types)
  - **Open** Open a file for update
  - **ADDLFM** Add Logical File Member
  - **ADDPFM** Add Physical File Member
  - **ADDPFTRG** Add Physical File Trigger
  - **CHGDDMF** Change DDM File
  - **CHGPF** Change Physical File
  - **CHGPFM** Change Physical File Member
  - **CLRPFM** Clear Physical File Member
  - **INZPFM** Initialize Physical File Member
  - **RGZPFM** Reorganize Physical File Member
  - **RMVM** Remove Member
  - **RNMM** Rename Member

Specifying Auditing for New Objects Created

- System Value **QCRTOBJAUD** – Controls auditing of new objects
  - ***NONE** – Set newly created objects to OBJAUD(*NONE). This is the shipped default value
  - ***CHANGE** – Set newly created objects to OBJAUD(*CHANGE) Typically used in HA solutions to ensure *CHANGE auditing of all new objects
  - ***ALL** – Set newly created objects to OBJAUD(*ALL)
  - ***USRPRF** - Set newly created objects to OBJAUD(*USRPRF)

This System value can be overridden at the Library/Directory level, using the **CRTOBJAUD** property of the Library/Directory.

Specifying Auditing for New Objects Created

- Consider making any **CRTOBJAUD** changes at the Library level
  - Specify the desired value for the Library's **CRTOBJAUD** value. This will control the **OBJAUD** value of 'Newly Created' objects in the Library/Directory

CRTLIB/CHGLIB LIB(PAYLIB) CRTOBJAUD(*SYSVAL)

*SYSVAL is the default

  - If you want to start auditing newly created objects in a library, change the library **CRTOBJAUD** value, Not the System Value

CRTLIB/CHGLIB LIB(PAYLIB) CRTOBJAUD(*CHANGE)

Note: Some H/A Solutions require that the System Value QCRTOBJAUD to be set to *CHANGE, and each in-scope library to be set to *SYSVAL or *CHANGE.

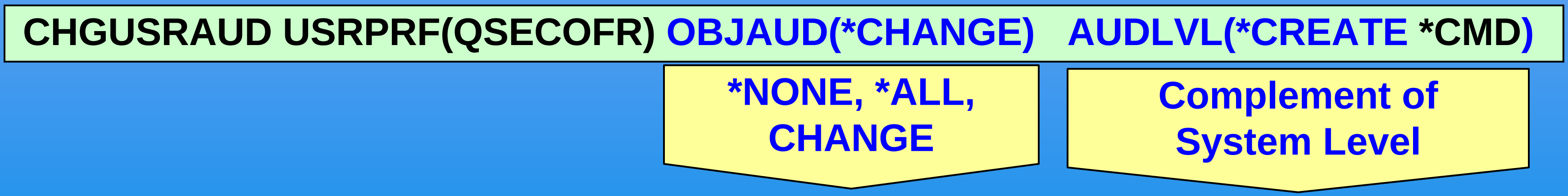
Auditing Users - CHGUSRAUD

- Individual user profiles can be audited
  - Powerful profiles QSECOFR, ZSECOFR, MYADMIN
  - Troublesome users
  - Past problems have occurred

- **QAUDCTL** system value must include the value ***OBJAUD** or ***AUDLVL**

- **CHGUSRAUD** command can start/stop auditing for a User
- Entries are written to the security audit journal **QAUDJRN**

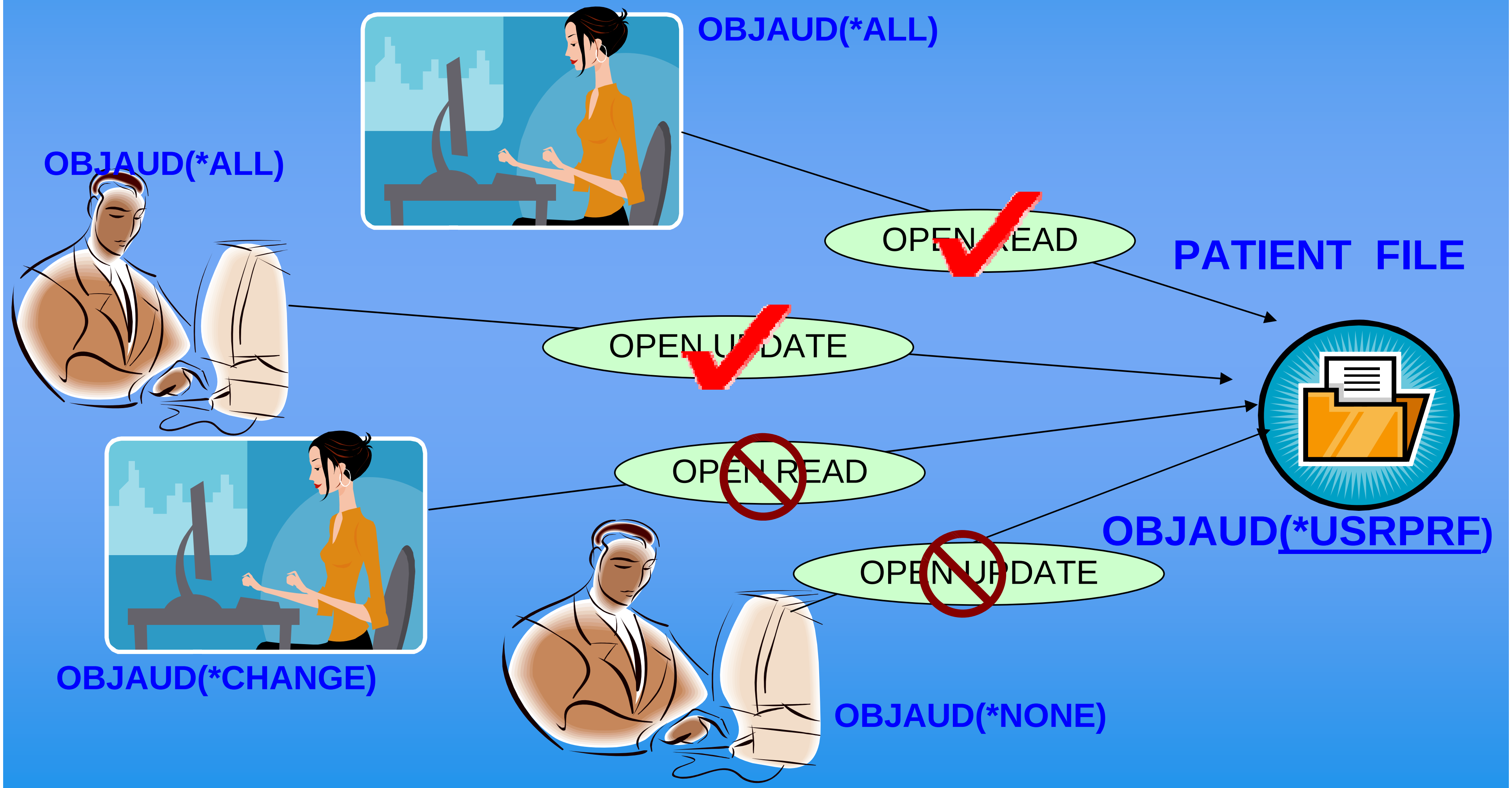
- User's **AUDLVL** can contain ***CMD** to audit all CL commands run by the user. (Can then filter command line commands)



```
CHGUSRAUD USRPRF(QSECOFR) OBJAUD(*CHANGE)   AUDLVL(*CREATE *CMD)
```

Using CHGOBJAUD   OBJAUD(*USRPRF)

The User Profile's OBJAUD value is ONLY evaluated if the Object's OBJAUD value is set to *USRPRF



OBJAUD(*ALL)

OBJAUD(*ALL)

OPEN READ

PATIENT FILE

OPEN UPDATE

OPEN READ

OBJAUD(*USRPRF)

OPEN UPDATE

OBJAUD(*CHANGE)

OBJAUD(*NONE)

Object auditing Lessons

- If you want to record all access (Read-only or update mode) to a sensitive file, set the file’s **OBJAUD** value to ***ALL**.

```
CHGOBJAUD OBJ(PAYLIB/PAYFILE) OBJTYPE(*FILE) OBJAUD(*ALL)
```

- If you want to record all access in update mode, set the file’s **OBJAUD** value to ***CHANGE**.

```
CHGOBJAUD OBJ(PAYLIB/PAYFILE) OBJTYPE(*FILE) OBJAUD(*CHANGE)
```

- If you only want to record access by a selected group of users, set the file’s **OBJAUD** value to ***USRPRF**

```
CHGOBJAUD OBJ(PAYLIB/PAYFILE) OBJTYPE(*FILE) OBJAUD(*USRPRF)
```

  - And set the user profile’s **OBJAUD** value to ***ALL** or ***CHANGE**

```
CHGUSRAUD USRPRF(MYUSER) OBJAUD(*CHANGE)
```

```
CHGUSRAUD USRPRF(MYUSER2) OBJAUD(*ALL)
```

Audit Reporting Tools - Reporting Events

- Once you have set up the security auditing function, you can use a commercial security software product to analyze and report on the audit journal data. Enhancements and new journal entry types are popping up in each new release.

- IBM has stopped providing enhancements for the **DSPAUDJRNE** command.

  “The command does not support all security audit record types, and the command does not list all the fields for the records it does support.” (IBM V5R3 Security Reference)

- New in V5R4 is the CL command **CPYAUDJRNE**, which will write selected audit journal entries to an *OUTFILE. It supports new audit journal entry types. Experiment with the command.

- The **DSPJRN** command is the most flexible, and provides the most selection criteria of Journal Entry types. Use the *Outfile capability with the *TYPE5 *Outfile format.

Journal Entry Types

See the attached Appendix from the IBM i/OS Security Reference

It is a ‘must’ for building your own security audit journal reporting system.

www.SecureMyi.com

Thank you!

Any Questions?

Dan Riehl
dan.riehl@SecureMyi.com

www.Cilasoft.com

- The detailed entry type. Some journal entry types are used to log more than one type of event. The detailed entry type field in the journal entry identifies the type of event.
- The ID of the message that can be used to define the entry-specific information in the journal entry.

Table 132. Security auditing journal entries

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
Action Auditing:				
*ATNEVT	IM	QASYIMJ5	P	A potential intrusion has been detected. Further evaluation is required to determine if this is an actual intrusion or an expected and permitted action.
*AUTFAIL	AF	QASYAFJE/J4/J5	A	An attempt was made to access an object or perform an operation to which the user was not authorized.
			B	Restricted instruction
			C	Validation failure
			D	Use of unsupported interface, object domain failure
			E	Hardware storage protection error, program constant space violation
			F	ICAPI authorization error.
			G	ICAPI authentication error.
			H	Scan exit program action.
			I	System Java inheritance not allowed
			J	An attempt was made to submit or schedule a job under a job description which has a user profile specified. The submitter did not have *USE authority to the user profile.
			K	An attempt was made to perform an operation for which the user did not have the required special authority.
			N	The profile token was not a regenerable profile token.
			O	Optical Object Authority failure
			P	An attempt was made to use a profile handle that is not valid on the QWTSETP API.
			R	Hardware protection error
			S	Default signon attempt.
			T	Not authorized to TCP/IP port.
			U	A user permission request was not valid.
			V	The profile token was not valid for generating new profile token.
			W	The profile token was not valid for exchange.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			X	System violation, see description of AF (Authority Failure) journal entries for details
			Y	Not authorized to the current JUID field during a clear JUID operation.
			Z	Not authorized to the current JUID field during a set JUID operation.
	CV	QASYCVJ4/J5	E	Connection ended abnormally.
			R	Connection rejected.
	DI	QASYDIJ4/J5	AF	Authority failures.
			PW	Password failures.
	GR	QASYGRJ4/J5	F	Function registration operations.
	KF	QASYKFJ4/J5	P	An incorrect password was entered.
	IP	QASYIPJE/J4/J5	F	Authority failure for an IPC request.
	PW	QASYPWJE/J4/J5	A	APPC bind failure.
			C	CHKPWD failure.
			D	An incorrect service tool user ID was entered.
			E	An incorrect service tool user ID password was entered.
			P	An incorrect password was entered.
			Q	Attempted signon (user authentication) failed because user profile was disabled.
			R	Attempted signon (user authentication) failed because password was expired.
			S	SQL decrypt a password that was not valid.
			U	User name not valid.
			X	Service tools user is disabled.
			Y	Service tools user not valid.
			Z	Service tools password not valid.
	VC	QASYVCJE/J4/J5	R	A connection was rejected because of incorrect password.
	VO	QASYVOJ4/J5	U	Unsuccessful verification of a validation list entry.
	VN	QASYVNJE/J4/J5	R	A network logon was rejected because of expired account, incorrect hours, incorrect user ID, or incorrect password.
	VP	QASYVPJE/J4/J5	P	An incorrect network password was used.
	X1	QASYX1J5	F	Delegate of identity token failed.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			U	Get user from identity token failed.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*CMD [1]	CD	QASYCDJE/J4/J5	C	A command was run.
			L	An S/36E control language statement was run.
			O	An S/36E operator control command was run.
			P	An S/36E procedure was run.
			S	Command run after command substitution took place.
			U	An S/36E utility control statement was run.
*CREATE [2]	CO	QASYCOJE/J4/J5	N	Creation of a new object, except creation of objects in QTEMP library.
			R	Replacement of existing object.
	DI	QASYDIJ4/J5	CO	Object created.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*DELETE [2]	DO	QASYDOJE/J4/J5	A	Object deleted.
			C	Pending delete committed.
			D	Pending create rolled back.
			P	Delete pending.
			R	Pending delete rolled back.
	DI	QASYDIJ4/J5	DO	Object deleted.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*JOBBAS	JS	QASYJSJ5	A	The ENDJOBABN command was used.
			B	A job was submitted.
			C	A job was changed.
			E	A job was ended.
			H	A job was held.
			I	A job was disconnected.
			N	The ENDJOB command was used.
			P	A program start request was attached to a prestart job.
			Q	Query attributes changed.
			R	A held job was released.
			S	A job was started.
			U	CHGUSRTRC command.
*JOBCHGUSR	JS	QASYJSJ5	M	Change profile or group profile.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			T	Change profile or group profile using a profile token.
*JOBDTA	JS	QASYJSJE/J4/J5	A	The ENDJOBABN command was used.
			B	A job was submitted.
			C	A job was changed.
			E	A job was ended.
			H	A job was held.
			I	A job was disconnected.
			M	Change profile or group profile.
			N	The ENDJOB command was used.
			P	A program start request was attached to a prestart job.
			Q	Query attributes changed.
			R	A held job was released.
			S	A job was started.
			T	Change profile or group profile using a profile token.
			U	CHGUSRTRC command.
	SG	QASYSGJE/J4/J5	A	Asynchronous i5/OS signal process.
			P	Asynchronous Private Address Space Environment (PASE) signal processed.
	VC	QASYVCJE/J4/J5	S	A connection was started.
			E	A connection was ended.
	VN	QASYVNJE/J4/J5	F	Logoff requested.
			O	Logon requested.
	VS	QASYVSJE/J4/J5	S	A server session was started.
			E	A server session was ended.
*NETBAS	CV	QASYCVJE/J4/J5	C	Connection established.
			E	Connection ended normally.
			R	Rejected connection.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file.
			N	IP rules have been unloaded for an IP Security connection.
			P	IP rules have been loaded for an IP Security connection.
			R	IP rules have been read and copied to a file.
			U	IP rules have been unloaded (removed).
	IS	QASYISJ4/J5	1	Phase 1 negotiation.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A violation was detected by the APPN Filter support when the Directory search filter was audited.
	NE	QASYNEJE/J4/J5	A	A violation is detected by the APPN Filter support when the End point filter is audited.
*NETCLU	CU	QASYCUJE/J4/J5	M	Creation of an object by the cluster control operation.
			R	Creation of an object by the Cluster Resource Group (*GRP) management operation.
*NETCMN	CU	QASYCUJE/J4/J5	M	Creation of an object by the cluster control operation.
			R	Creation of an object by the Cluster Resource Group (*GRP) management operation.
	CV	QASYCVJ4/J5	C	Connection established.
			E	Connection ended normally.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file.
			N	IP rule have been unloaded for an IP Security connection.
			P	IP rules have been loaded for an IP Security connection.
			R	IP rules have been read and copied to a file.
			U	IP rules have been unloaded (removed).
	IS	QASYISJ4/J5	1	Phase 1 negotiation.
			2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A violation was detected by the APPN Filter support when the Directory search filter was audited.
	NE	QASYNEJE/J4/J5	A	A violation is detected by the APPN Filter support when the End point filter is audited.
	SK	QASYSKJ4/J5	A	Accept
			C	Connect
			D	DHCP address assigned
			F	Filtered mail
			P	Port unavailable
			R	Reject mail
			U	DHCP address denied
*NETFAIL	SK	QASYSKJ4/J5	P	Port unavailable
*NETSCK	SK	QASYSKJ4/J5	A	Accept

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			C	Connect
			D	DHCP address assigned
			F	Filtered mail
			R	Reject mail
			U	DHCP address denied
*OBJMGT [2]	DI	QASYDIJ4/J5	OM	Object rename
	OM	QASYOMJE/J4/J5	M	An object was moved to a different library.
			R	An object was renamed.
*OFCSRV	ML	QASYMLJE/J4/J5	O	A mail log was opened.
	SD	QASYSDJE/J4/J5	S	A change was made to the system distribution directory.
*OPTICAL	O1	QASY01JE/J4/J5	R	Open file or directory
			U	Change or retrieve attributes
			D	Delete file directory
			C	Create directory
			X	Release held optical file
	O2	QASY02JE/J4/J5	C	Copy file or directory
			R	Rename file
			B	Back up file or directory
			S	Save held optical file
			M	Move file
	O3	QASY03JE/J4/J5	I	Initialize volume
			B	Backup volume
			N	Rename volume
			C	Convert backup volume to primary
			M	Import
			E	Export
			L	Change authorization list
			A	Change volume attributes
			R	Absolute read
*PGMADP	AP	QASYAPJE/J4/J5	S	A program started that adopts owner authority. The start entry is written the first time adopted authority is used to gain access to an object, not when the program enters the call stack.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			E	A program ended that adopts owner authority. The end entry is written when the program leaves the call stack. If the same program occurs more than once in the call stack, the end entry is written when the highest (last) occurrence of the program leaves the stack.
			A	Adopted authority was used during program activation.
*PGMFAIL	AF	QASYAFJE/J4/J5	B	A program ran a restricted machine interface instruction.
			C	A program which failed the restore-time program validation checks was restored. Information about the failure is in the *Validation Value Violation Type* field of the record.
			D	A program accessed an object through an unsupported interface or callable program not listed as a callable API.
			E	Hardware storage protection violation.
			R	Attempt made to update an object that is defined as read-only. (Enhanced hardware storage protection is logged only at security level 40 and higher)
*PRTDTA	PO	QASYPOJE/J4/J5	D	Printer output was printed directly to a printer.
			R	Output sent to remote system to print.
			S	Printer output was spooled and printed.
*SAVRST [2]	OR	QASYORJE/J4/J5	N	A new object was restored to the system.
			E	An object was restored that replaces an existing object.
	RA	QASYRAJE/J4/J5	A	The system changed the authority to an object being restored. [3]
	RJ	QASYRJJE/J4/J5	A	A job description that contains a user profile name was restored.
	RO	QASYROJE/J4/J5	A	The object owner was changed to QDFTOWN during restore operation.[3]
	RP	QASYRPJE/J4/J5	A	A program that adopts owner authority was restored.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
	RQ	QASYRQJE/J4/J5	A	A *CRQD object with PROFILE(*OWNER) was restored.
	RU	QASYRUJE/J4/J5	A	Authority was restored for a user profile using the RSTAUT command.
	RZ	QASYRZJE/J4/J5	A	The primary group for an object was changed during a restore operation.
			O	Auditing of an object was changed with CHGOBJAUD command.
			U	Auditing for a user was changed with CHGUSRAUD command.
*SECCFG	AD	QASYADJE/J4/J5	D	Auditing of a DLO was changed with CHGDLOAUD command.
			O	Auditing of an object was changed with CHGOBJAUD or CHGAUD commands.
			S	The scan attribute was changed using CHGATR command or the Qp0lSetAttr API, or when the object was created.
			U	Auditing for a user was changed with CHGUSRAUD command.
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CP	QASYCPJE/J4/J5	A	Create, change, or restore operation of user profile when QSYSRESPA API is used.
	CQ	QASYCQJE/J4/J5	A	A *CRQD object was changed.
	CY	QASYCYJ4/J5	A	Access Control function
			F	Facility Control function
			M	Master Key function
	DO	QASYDOJE/J4/J5	A	Object was deleted not under commitment control
			C	A pending object delete was committed
			D	A pending object create was rolled back
			P	The object delete is pending (the delete was performed under commitment control)
			R	A pending object delete was rolled back
	DS	QASYDSJE/J4/J5	A	Request to reset DST QSECOFR password to system-supplied default.
			C	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
			C	Change.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			D	Delete.
			I	Initialize environment variable space.
	GR	QASYGRJ4/J5	A	Exit program added
			D	Exit program removed
			F	Function registration operation
			R	Exit program replaced
	JD	QASYJDJE/J4/J5	A	The USER parameter of a job description was changed.
	KF	QASYKFJ4/J5	C	Certificate operation.
			K	Key ring file operation.
			T	Trusted root operation.
	NA	QASYNAJE/J4/J5	A	A network attribute was changed.
	PA	QASYPAJE/J4/J5	A	A program was changed to adopt owner authority.
	SE	QASYSEJE/J4/J5	A	A subsystem routing entry was changed.
	SO	QASYSOJ4/J5	A	Add entry.
			C	Change entry.
			R	Remove entry.
	SV	QASYSVJE/J4/J5	A	A system value was changed.
			B	Service attributes were changed.
			C	Change to system clock.
			E	Change to option
			F	Change to system-wide journal attribute
	VA	QASYVAJE/J4/J5	S	The access control list was changed successfully.
			F	The change of the access control list failed.
			V	Successful verification of a validation list entry.
	VU	QASYVUJE/J4/J5	G	A group record was changed.
			M	User profile global information changed.
			U	A user record was changed.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Audit change.
			BN	Successful bind
			CA	Authority change
			CP	Password change
			OW	Ownership change
			PO	Policy change
			UB	Successful unbind

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
*SECIPC	IP	QASYIPJE/J4/J5	A	The ownership or authority of an IPC object was changed.
			C	Create an IPC object.
			D	Delete an IPC object.
			G	Get an IPC object.
*SECNAS	X0	QASYX0J4/J5	1	Service ticket valid.
			2	Service principals do not match.
			3	Client principals do not match.
			4	Ticket IP address mismatch.
			5	Decryption of the ticket failed
			6	Decryption of the authenticator failed
			7	Realm is not within client and local realms
			8	Ticket is a replay attempt
			9	Ticket not yet valid
			A	Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error
			B	Remote IP address mismatch
			C	Local IP address mismatch
			D	KRB_AP_PRIV or KRB_AP_SAFE timestamp error
			E	KRB_AP_PRIV or KRB_AP_SAFE replay error
			F	KRB_AP_PRIV KRB_AP_SAFE sequence order error
			K	GSS accept - expired credential
			L	GSS accept - checksum error
			M	GSS accept - channel bindings
			N	GSS unwrap or GSS verify expired context
			O	GSS unwrap or GSS verify decrypt/decode
			P	GSS unwrap or GSS verify checksum error
			Q	GSS unwrap or GSS verify sequence error
*SECRUN	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
*SECSCKD	GS	QASYGSJE/J4/J5	G	A socket descriptor was given to another job. (The GS audit record is created if it is not created for the current job.)
			R	Receive descriptor.
			U	Unable to use descriptor.
*SECURITY	AD	QASYADJE/J4/J5	D	Auditing of a DLO was changed with CHGDLOAUD command.
			O	Auditing of an object was changed with CHGOBJAUD or CHGAUD commands.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
			U	Auditing for a user was changed with CHGUSRAUD command.
	X1	QASYADJE/J4/J5	D	Delegate of identity token successful
			G	Get user from identity token successful
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	CP	QASYCPJE/J4/J5	A	Create, change, or restore operation of user profile when QSYRESPA API is used
	CQ	QASYCQJE/J4/J5	A	A *CRQD object was changed.
	CV	QASYCVJ4/J5	C	Connection established.
			E	Connection ended normally.
			R	Connection rejected.
	CY	QASYCYJ4/J5	A	Access Control function
			F	Facility Control function
			M	Master Key function
	DI	QASYDIJ4/J5	AD	Audit change
			BN	Successful bind
			CA	Authority change
			CP	Password change
			OW	Ownership change
			PO	Policy change
			UB	Successful unbind
	DO	QASYDOJE/J4/J5	A	Object was deleted not under commitment control
			C	A pending object delete was committed

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			D	A pending object create was rolled back
			P	The object delete is pending (the delete was performed under commitment control)
			R	A pending object delete was rolled back
	DS	QASYDSJE/J4/J5	A	Request to reset DST QSECOFR password to system-supplied default.
			C	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
			C	Change.
			D	Delete.
			I	Initialize environment variable space.
	GR	QASYGRJ4/J5	A	Exit program added
			D	Exit program removed
			F	Function registration operation
			R	Exit program replaced
	GS	QASYGSJE/J4/J5	G	A socket descriptor was given to another job. (The GS audit record is created if it is not created for the current job.)
			R	Receive descriptor.
			U	Unable to use descriptor.
	IP	QASYIPJE/J4/J5	A	The ownership or authority of an IPC object was changed.
			C	Create an IPC object.
			D	Delete an IPC object.
			G	Get an IPC object.
	JD	QASYJDJE/J4/J5	A	The USER parameter of a job description was changed.
	KF	QASYKFJ4/J5	C	Certificate operation.
			K	Key ring file operation.
			T	Trusted root operation.
	NA	QASYNAJE/J4/J5	A	A network attribute was changed.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PA	QASYPAJE/J4/J5	A	A program was changed to adopt owner authority.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.
	PS	QASYPSJE/J4/J5	A	A target user profile was changed during a pass-through session.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			E	An office user ended work on behalf of another user.
			H	A profile handle was generated through the QSYGETPH API.
			I	All profile tokens were invalidated.
			M	The maximum number of profile tokens have been generated.
			P	Profile token generated for user.
			R	All profile tokens for a user have been removed.
			S	An office user started work on behalf of another user.
			V	User profile authenticated.
	SE	QASYSEJE/J4/J5	A	A subsystem routing entry was changed.
	SO	QASYSOJ4/J5	A	Add entry.
			C	Change entry.
			R	Remove entry.
	SV	QASYSVJE/J4/J5	A	A system value was changed.
			B	Service attributes were changed.
			C	Change to system clock.
			E	Change to option
			F	Change to system-wide journal attribute
	VA	QASYVAJE/J4/J5	S	The access control list was changed successfully.
			F	The change of the access control list failed.
	VO		V	Successful verify of a validation list entry.
	VU	QASYVUJE/J4/J5	G	A group record was changed.
			M	User profile global information changed.
			U	A user record was changed.
	X0	QASYX0J4/J5	1	Service ticket valid.
			2	Service principals do not match
			3	Client principals do not match
			4	Ticket IP address mismatch
			5	Decryption of the ticket failed
			6	Decryption of the authenticator failed
			7	Realm is not within client and local realms
			8	Ticket is a replay attempt

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			9	Ticket not yet valid
			A	Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error
			B	Remote IP address mismatch
			C	Local IP address mismatch
			D	KRB_AP_PRIV or KRB_AP_SAFE timestamp error
			E	KRB_AP_PRIV or KRB_AP_SAFE replay error
			F	KRB_AP_PRIV KRB_AP_SAFE sequence order error
			K	GSS accept - expired credential
			L	GSS accept - checksum error
			M	GSS accept - channel bindings
			N	GSS unwrap or GSS verify expired context
			O	GSS unwrap or GSS verify decrypt/decode
			P	GSS unwrap or GSS verify checksum error
			Q	GSS unwrap or GSS verify sequence error
*SECVFY	PS	QASYPSJE/J4/J5	A	A target user profile was changed during a pass-through session.
	X1	QASYX1J5	D	Delegate of identity token successful
			G	Get user from identity token successful
			E	An office user ended work on behalf of another user.
			H	A profile handle was generated through the QSYGETPH API.
			I	All profile tokens were invalidated.
			M	The maximum number of profile tokens have been generated.
			P	Profile token generated for user.
			R	All profile tokens for a user have been removed.
			S	An office user started work on behalf of another user.
			V	User profile authenticated.
*SECVLDL	VO		V	Successful verification of a validation list entry.
*SERVICE	ST	QASYSTJE/J4/J5	A	A service tool was used.
	VV	QASYVVJE/J4/J5	C	The service status was changed.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			E	The server was stopped.
			P	The server paused.
			R	The server was restarted.
			S	The server was started.
*SPLFDTA	SF	QASYSFJE/J4/J5	A	A spooled file was read by someone other than the owner.
			C	A spooled file was created.
			D	A spooled file was deleted.
			H	A spooled file was held.
			I	An inline file was created.
			R	A spooled file was released.
			S	A spooled file was saved.
			T	A spooled file was restored.
			U	A spooled file was changed.
			V	Only non-security relevant spooled files attributes changed.
*SYSMGT	DI	QASYDIJ4/J5	CF	Configuration changes
			CI	Create instance
			DI	Delete instance
			RM	Replication management
	SM	QASYSMJE/J4/J5	B	Backup options were changed using xxxxxxxxxx.
			C	Automatic cleanup options were changed using xxxxxxxxxx.
			D	A DRDA* change was made.
			F	An HFS file system was changed.
			N	A network file operation was performed.
			O	A backup list was changed using xxxxxxxxxx.
			P	The power on/off schedule was changed using xxxxxxxxxx.
			S	The system reply list was changed.
			T	The access path recovery times were changed.
	VL	QASYVLJE/J4/J5	A	The account is expired.
			D	The account is disabled.
			L	Logon hours were exceeded.
			U	Unknown or unavailable.
			W	Workstation not valid.
Object Auditing:				
*CHANGE	DI	QASYDIJ4/J5	IM	LDAP directory import

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			ZC	Object change
	ZC	QASYZCJ4/J5	C	Object changes
			U	Upgrade of open access to an object
	AD	QASYADJEJ4/J5	D	Auditing of an object was changed with CHGOBJAUD command.
			O	Auditing of an object was changed with CHGOBJAUD command.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
			U	Auditing for a user was changed with CHGUSRAUD command.
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	OM	QASYOMJE/J4/J5	M	An object was moved to a different library.
			R	An object was renamed.
	OR	QASYORJE/J4/J5	N	A new object was restored to the system.
			E	An object was restored that replaces an existing object.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.
	RA	QASYRAJE/J4/J5	A	The system changed the authority to an object being restored.
	RO	QASYROJE/J4/J5	A	The object owner was changed to QDFTOWN during restore operation.
	RZ	QASYRZJE/J4/J5	A	The primary group for an object was changed during a restore operation.
	GR	QASYGRJ4/J5	F	Function registration operations[5]
	LD	QASYLDJE/J4/J5	L	Link a directory.
			U	Unlink a directory.
	VF	QASYVFJE/J4/J5	A	The file was closed because of administrative disconnection.
			N	The file was closed because of normal client disconnection.
			S	The file was closed because of session disconnection.
	VO	QASYVOJ4/J5	A	Add validation list entry.
			C	Change validation list entry.
			F	Find validation list entry.
			R	Remove validation list entry.

Table 132. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
	VR	QASYVRJE/J4/J5	F	Resource access failed.
			S	Resource access was successful.
	YC	QASYYCJE/J4/J5	C	A document library object was changed.
	ZC	QASYZCJE/J4/J5	C	An object was changed.
			U	Upgrade of open access to an object.
*ALL [4]	CD	QASYCDJ4/J5	C	Command run
	DI	QASYDIJ4/J5	EX	LDAP directory export
			ZR	Object read
	GR	QASYGRJ4/J5	F	Function registration operations[5]
	LD	QASYLDJE/J4/J5	K	Search a directory.
	YR	QASYYRJE/J4/J5	R	A document library object was read.
	ZR	QASYZRJE/J4/J5	R	An object was read.

[1] This value can only be specified for the AUDLVL parameter of a user profile. It is not a value for the QAUDLVL system value.

[2] If object auditing is active for an object, an audit record is written for a create, delete, object management, or restore operation even if these actions are not included in the audit level.

[3] See the topic “Restoring objects” on page 249 for information about authority changes which might occur when an object is restored.

[4] When *ALL is specified, the entries for both *CHANGE and *ALL are written.

[5] When the QUSRSYS/QUSEXRGOBJ *EXITRG object is being audited.

Planning the auditing of object access

The i5/OS operating system provides the ability to log accesses to an object in the security audit journal by using system values and the object auditing values for users and objects. This is called *object auditing*.

The QAUDCTL system value, the OBJAUD value for an object, and the OBJAUD value for a user profile work together to control object auditing. The OBJAUD value for the object and the OBJAUD value for the user who is using the object determine whether a specific access should be logged. The QAUDCTL system value starts and stops the object auditing function.

Table 133 shows how the OBJAUD values for the object and the user profile work together.

Table 133. How object and user auditing work together

	OBJAUD value for user		
OBJAUD value for object	***NONE**	***CHANGE**	***ALL**
*NONE	None	None	None
*USRPRF	None	Change	Change and Use
*CHANGE	Change	Change	Change
*ALL	Change and Use	Change and Use	Change and Use