

iSeries and AS/400 Security

All you want to know about:

Security Tools

Presented by

Wayne O. Evans



DISCLAIMER

2

The security recommendations and any programming source are offered "AS IS" for your consideration. Wayne O Evans Consulting, Inc. makes no warranties or representations as to the quality of the examples. **ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE, ARE SPECIFICALLY DISCLAIMED.**

Wayne O. Evans
WOEvans@AOL.com
5677 West Circle Z St
Tucson, AZ 85713
Tel (520)-578-7785
Fax (520)-578-7786



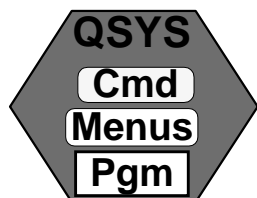
Security Toolkit

3



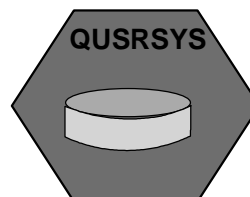
Security tools are included in OS/400 V3R2 and V3R7 and beyond

4



The security tool programs and commands are in the QSYS library with *EXCLUDE public authority.

The security tool commands create files in the QUSRSYS library with *EXCLUDE public authority.



Security Tools

5

You should sign on as a security officer when you use the security tools.

The security tools commands require *ALLOBJ special authority.

Some of the commands require *SECADM, *AUDIT, or *IOSYSCFG special authority.



This authority can be adopted so that users do not need to be given powerful authority

The implementation details are explained later in the question and answers section.

Outline

6

Security Tools

– **Interactive Options**

– **Batch Report**

– **Scheduling Reports**

– **General Options**

Interactive Security Tools

7

Security Management menu options

- Check for default password use
- Disable inactive profiles
- Limit access by time of day
- Schedule Deactivate/Delete of profile
- Set up audit

Security reporting

- User profiles
- Subsystems & communications
- JOB D with user names
- Others

Recommend: Interactive reporting does not make good use of system. Use batch options for reports

Default Passwords

8

```
SECTOOLS                Security Tools                System:  MCRISC
Select one of the following:

Work with profiles
  1. Analyze default passwords
  2. Display active profile list
  3. Change active profile list
  4. Analyze profile activity
  5. Display activation schedule
  6. Change activation schedule en
  7. Display expiration schedule
  8. Change expiration schedule enru
More..

Selection or command 1
===> _____

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Find user profiles with password = user profile name.

The profile last used used date is reset when the password matches the profile

Run option 4 first

Default Passwords

9

Analyze Default Passwords (ANZDFTPWD)

Type choices, press Enter.

Action taken against profiles . ACTION *NONE

- *NONE** No action take against profiles with a default password
- *DISABLE** The user profile STATUS field set to *DISABLED
- *PWDEXP** The user profile PWDEXP field set to *YES

Default Passwords

10

User profiles with default passwords Page 1
5716SS1 V4R2M0 971108 MCRISC 06/14/98 03:13:44

Action taken against profiles . . : *NONE

User

Profile	STATUS	PWDEXP	Text
LAURENT	*ENABLED	*NO	tim laurent -- CAE author
MALAGAX	*ENABLED	*NO	Ernie Malaga
PENCE	*ENABLED	*NO	Doug Pence
PWRUSR	*ENABLED	*NO	Power User
QD1SRM4	*DISABLED	*NO	ManageWare/400
QD1SRM4DLO	*DISABLED	*NO	ManageWare/400
TSTPRF	*ENABLED	*NO	Test user
USER1	*ENABLED	*NO	
USER2	*ENABLED	*NO	
USER3	*ENABLED	*NO	
WOEDELETE	*ENABLED	*NO	

* * * * * E N D O F L I S T I N G * * * * *

Active Profiles

11

SECTOOLS

Security Tools

System: MCRISC

Select one of the following:

Work with profiles

1. Analyze default passwords
2. Display active profile list
3. Change active profile list
4. Analyze profile activity
5. Display activation schedule
6. Change activation schedule entry
7. Display expiration schedule
8. Change expiration schedule entry

List profiles that are never checked for activity

More..

Selection or command

===> 2

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Active Profiles

12

Active Profile List

All profiles except those listed below will be set to *DISABLED after they have been inactive for the specified number of days : 045

User Profile	User Profile	User Profile
GREEN		
HOLT		
WOEPGMR		
WOEVANS		

This list should the profiles you do not want to disable

- ▶ Profiles for sending and receiving network files
- ▶ Seldom used profiles for backup purposes

Active Profiles

13

```
SECTOOLS                Security Tools                System:  MCRISC

Select one of the following:

Work with profiles
  1. Analyze default passwords
  2. Display active profile list
  3. Change active profile list
  4. Analyze profile activity
  5. Display activation schedule
  6. Change activation schedule entry
  7. Display expiration schedule
  8. Change expiration schedule entry
  More..

Selection or command 3
===> _

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Change list of profiles that are never checked for activity

Change Active Profile List

14

```
Change Active Profile List (CHGACTPRFL)

Type choices, press Enter.

User profile . . . . . USRPRF          WOETEST
                                     + for more values  QUSER
Action . . . . . ACTION                *ADD

Bottom

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

Profiles added to list are not checked for activity

Active Profiles

15

```
SECTOOLS                Security Tools                System:  MCRISC

Select one of the following:

Work with profiles
  1. Analyze default passwords
  2. Display active profile list
  3. Change active profile list
  4. Analyze profile activity
  5. Display activation schedule
  6. Change activation schedule entry
  7. Display expiration schedule
  8. Change expiration schedule entru

Selection or command 4
===> _____

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Set the number of days to check for inactivity. Disable inactive profiles

More..

Profile Activity

16

```
Analyze Profile Activity (ANZPRFACT)

Type choices, press Enter.

Number of inactive days . . . . INACDAYS    45

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

Caution: This option will disable all profiles that have been inactive for 45 days unless the profile is listed

Bottom

Active Profiles 17

SECTOOLS Security Tools System: MCRISC

Select one of the following:

Work with profiles

1. Analyze default passwords
2. Display active profile list
3. Change active profile list
4. Analyze profile activity
5. Display activation schedule
6. Change activation schedule entry
7. Display expiration schedule
8. Change expiration schedule entru

More..

Selection or command **2**

===> _

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Active Profiles 18

Active Profile List

All profiles except those listed below will be set to *DISABLED after they have been inactive for the specified number of days : 045

User Profile	User Profile	User Profile
GREEN		
HOLT		
QUSER		
WOEPGMR		
WOETEST		
WOEVANS		

User profiles added

Number of days to check for inactivity

19

Scheduled Job

DSPJOBSCDE

Last attempted submission:

```

Status . . . . . : Job not previously submitted.

Schedule day . . . . . : *ALL
Schedule time . . . . . : 01:00:00
Frequency . . . . . : *WEEKLY
Recovery action . . . . . : *SBMRLS
Next submit date . . . . . : 06/07/98
Command . . . . . : QSYS/CALL PGM(QSYS/QSECIDL2) PARM('045')

Job queue . . . . . : *JOBQ
Library . . . . . :
Job queue status . . . . . :
  
```

Schedules job every day of week to detect inactive profiles

Expiration interval

20

Activation Schedule

SECTOOLS Security Tools System: MCRISC

Select one of the following:

Work with profiles

1. Analyze default passwords
2. Display active profile list
3. Change active profile list
4. Analyze profile activity
5. Display activation schedule
6. Change activation schedule entry
7. Display expiration schedule
8. Change expiration schedule entry

More..

Selection or command **6**

===> _____

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Change Profile Activation Schedule

21

Change Activation Scd Entry (CHGACTSCDE)

Type choices, press Enter.

```

User profile . . . . . USRPRF      WOETEST
Enable time  . . . . . ENBTIME     5:00
Disable time . . . . . DSBTIME     18:00
Days . . . . . DAYS               *MON
                                      *TUE
                                      *WED
                                      THU
                                      *FRI
                                      ---
                                      ---

```

+ for more values

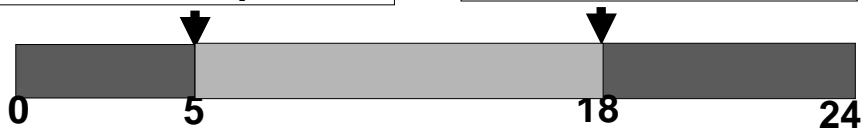
Technical detail

22

CHGACTSCDE

Schedules job at
start of the interval
to *ENABLE profile

Schedules job at
end of the interval
to *DISABLE profile



```

Next submit date . . : 06/02/98
Command . . . . . :
    QSYS/CALL PGM(QSYS/QSEACT5) PARM('WOEDELETE ' x)

Job queue . . . . . : *JOBQ
Library . . . . . :
Job queue status . . :
Job description . . : *USRPRF
Library . . . . . :

```

D = Disable
E = Enable

Activation Schedule

23

```
SECTOOLS                Security Tools                System:  MCRISC
Select one of the following:

Work with profiles
1. Analyze default passwords

2. Display active profile list
3. Change active profile list
4. Analyze profile activity

5. Display activation schedule
6. Change activation schedule entry

7. Display expiration schedule
8. Change expiration schedule entru

More..

Selection or command 5
===> _

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Profile Activation Schedule

24

User Profile Activation Schedule

User	Enable	Disable	Days
Profile	Time	Time	
WOEPGMR	05:30:00	19:00:00	*ALL
WOETEST	05:00:00	18:00:00	*MON *TUE *WED *THU *FRI

If user is active at disable time they can continue to work

Expiration Schedule

25

```
SECTOOLS                Security Tools                System:  MCRISC
Select one of the following:

Work with profiles
1. Analyze default passwords

2. Display active profile list
3. Change active profile list
4. Analyze profile activity

5. Display activation schedule
6. Change activation schedule entry

7. Display expiration schedule
8. Change expiration schedule entru

More..

Selection or command 8
===> _

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Expiration Schedule

26

```
Change Expiration Scd Entry (CHGEXPCDE)

Type choices, press Enter.

User profile . . . . . USRPRF          WQEPGMR
                                     + for more values
Expiration date . . . . . EXPDATE      6/20/98
Action . . . . . ACTION                *DISABLE
```

Use *DISABLE if you know the individual is planning to return

Expiration Schedule

Change Expiration Scd Entry (CHGEXPSCDE)

Type choices, press Enter.

```

User profile . . . . . USRPRF      > WOETEST
                                     + for more values
Expiration date . . . . . EXPDATE   > '6/30/98'
Action . . . . . ACTION           > *DELETE
Owned object option:      OWNOBJOPT
  Owned object value . . . . .      *CHGOWN
  User profile name if *CHGOWN      QDFTOWN
Primary group option:     PGPOPT
  Primary group value . . . . .     *NOCHG
  New primary group . . . . .      _____
  New primary group authority .    _____

```

When specifying ***DELETE** must also specify action for owned objects

Expiration Schedule

SECTOOLS Security Tools system: MCRISC

Select one of the following:

- Work with profiles
1. Analyze default passwords
 2. Display active profile list
 3. Change active profile list
 4. Analyze profile activity
 5. Display activation schedule
 6. Change activation schedule entry
 7. Display expiration schedule
 8. Change expiration schedule entry

More..

Selection or command **7**
 ===>

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Expiration Schedule

29

User Profile Expiration Schedule

User Profile	Expiration Date	Action	Owned Object Option	New Owner
WOEPGMR	06/20/98	*DISABLE		
WOETEST	06/30/98	*DELETE	*CHGOWN	QDFTOWN

Schedule deletion for users that will not return.

Use the *CHGOWN option to change owned objects

Security Auditing

30

SECTOOLS

Security Tools

System: MCRISC

Select one of the following:

Work with auditing

- 10. Change security auditing
- 11. Display security auditing

Reports

- 20. Submit or schedule security report
- 21. Adopting objects
- 22. Audit journal entries
- 23. Authorization list authorities
- 24. Command authority
- 25. Communications security
- 26. Document authority
- 27. File authority

Selection or command

More..

===> =

10

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Change audit system values and create audit journal objects

Security Audit Attributes

31

Change Security Auditing (CHGSECAUD)

Type choices, press Enter.

```
QAUDCTL system value . . . . . QAUDCTL      *SAME
                                     + for more values
QAUDLVL system value . . . . . QAUDLVL      *SAME
                                     + for more values
Initial journal receiver . . . . INLJRNRCV   AUDRCV0001
Library . . . . .                      QGPL
```

Useful when you first set up auditing

Can be done by changing the individual system values

Security Auditing

32

SECTOOLS Security Tools System: MCRISC

Select one of the following:

- Work with auditing
 - 10. Change security auditing
 - 11. Display security auditing

Display audit system values and audit journal objects

- Reports
 - 20. Submit or schedule security report
 - 21. Adopting objects
 - 22. Audit journal entries
 - 23. Authorization list authorities
 - 24. Command authority
 - 25. Communications security
 - 26. Document authority
 - 27. File authority

Selection or command **11** More..
===> _

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Security Audit Settings

33

Current Security Auditing Values

Security Auditing Journal Values

Security journal QAUDJRN exists : YES
Journal receiver attached to QAUDJRN . . : AUDJRN0009
Library : QGPL

Security Auditing System Values

Current QAUDCTL system value : *AUDLVL *NOQTEMP *OBJAUD
Current QAUDLVL system value : *AUTFAIL *SERVICE *SECURITY
*PGMFAIL

Quick check to see if auditing is active

Press Enter to continue.

F3=Exit F12=Cancel

Security Batch Reports

34

SECTOOLS

Security Tools

System: MCRISC

Select one of the following:

- Work with auditing
 - 10. Change security auditing
 - 11. Display security auditing

- Reports
 - 20. Submit or schedule security report
 - 21. Adopting objects
 - 22. Audit journal entries
 - 23. Authorization list authorities
 - 24. Command authority
 - 25. Communications security
 - 26. Document authority
 - 27. File authority

Selection or command

===> _

20 or GO SECBATCH

More..

Options 21-40 run interactively inefficient use of system



F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Outline

Security Tools

- Interactive Options
- **Batch Reports**
- Scheduling Reports
- General Options

Batch Security Tools



Useful Reports for

- Security Officers
- Auditors



General Security reporting

- System security attributes
- User profiles
- Subsystems & communications
- JOBD with user names
- Others

Specialized Security reporting

- Trigger Programs
- Adoptive authority
- User objects in QSYS library
- Command authorization
- Others

Batch Reports



General Options

Advanced Options

Scheduling Reports



System Security Attributes

```

SECBATCH  Submit or Schedule Security Reports To Batch
system:   MCRISC

Select one of the following:

  14. User profile authority
  15. Job and output queue authority
  16. Subsystem authority
  17. System security attributes
  18. Trigger programs
  19. User objects
  20. User profile information

  21. Check object integrity

Schedule Batch Reports
  30. Adopting objects
  31. Audit journal entries
  32. Authorization list authorities      More...

Selection or command
===> 17
_____

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
  
```

System Security Attributes

39

Submit Job (SBNJOB)

Type choices, press Enter.

Command to run CMD > PRSYSSECA

...

Job name	JOB	SYSVAL
Job description	JOB0	#USRPRF
Library		
Job queue	JOBQ	#JOBQ
Library		
Job priority (on JOBQ)	JOBPTY	#JOBQ
Output priority (on OUTQ)	OUTPTY	#JOBQ
Print device	PRTDEV	#CURRENT

Set job name

System Security Attributes

40

System Security Attributes

5716SS1 V4R2M0 961108

System Value

Name	Current value	Recommended value
QALWBJRST	*ALL	*NONE
QALWUSRDMN	*ALL	QTEMP
QATNPGM	QEZMAIN QSYS	*NONE
QAUDENDACN	*NOTIFY	*NOTIFY
QAUDFRCLVL	*SYS	*SYS
QAUDCTL	*AUDLVL *NOQTEMP	*AUDLVL *OBJAUD
QAUDLVL	*AUTFAIL *SERVICE *SECURITY *PGMFAIL	*NOQTEMP *AUTFAIL *CREATE *DELETE *SECURITY *SAVRST
QAUTOCFG	1	0
QAUTORMT	0	0
QAUTOVRT	999	0

Recommended values are very tight may not be the best tradeoff for usability

System Security Attributes

System Security Attributes

5716SS1 V4R2M0 961108

System Value

Name	Current value	Recommended value
QCMNRCYLMT	0 0	0 0
QCRTAUT	*CHANGE	Control at library
QCRTOBJAUD	*NONE	Control at library
QDEVRCYACN	*MSG	*DSCMSG
QDSCJOBIV	240	120
QDSPSGNINF	0	1
QINACTIV	*NONE	60
QINACTMSGQ	*ENDJOB	*ENDJOB
QLMTDEVSSN	0	1
QLMTSECOFR	0	1
QMAXSGNACN	3	3
QMAXSIGN	5	3

System Security Attributes

Name	Current value	Recommended value
QPWDEXPITV	60	60
QPWDLMTAJC	0	1
QPWDLMTCHR	*NONE	AEIOU@ \$#
QPWDLMTREP	0	1
QPWDMAXLEN	10	8
QPWDMINLEN	5	6
QPWDPOSDIF	0	1
QPWDRQDDGT	0	1
QPWDRQDDIF	0	1
QPWDVLDPGM	*NONE	*NONE
QRETSVRSEC	0	0
QRMTIPL	0	0
QRMTSIGN	*FRCSIGNON	*FRCSIGNON
QRMTSRVATR	0	0
QSECURITY	30	50
QSRVDMP	*DMPUSRJOB	*NONE

System Security Attributes

43

```
System Security Attributes                Page  2
5716SS1 V3R7M0  961108
Network Attribute
Name          Current value          Recommended value
DDMACC       *OBJAUT                    *REJECT
JOBACN       *FILE                       *REJECT
PCSACC       *OBJAUT                    *REJECT
* * * * *   E N D   O F   L I S T I N G   * * * * *
```

PRTSYSSECA command shows both security and security related system values and network attributes

User Profile Information

44

```
SECBATCH  Submit or Schedule Security Reports To Batch
system:   MCRISC
Select one of the following:

  14. User profile authority
  15. Job and output queue authority
  16. Subsystem authority
  17. System security attributes
  18. Trigger programs
  19. User objects
  20. User profile information
  21. Check object integrity

Schedule Batch Reports
  30. Adopting objects
  31. Audit journal entries
  32. Authorization list authorities      More...
Selection or command:
===> = 20
```

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

User Profile Information

45

```

User Profile Information
Report type . . . . . : *AUTINFO
Select by . . . . . : *SPCAUT
Special authorities . . . . . : *ALL
-----Special Authorities-----
*IO
User Profile Group *ALL *AUD SYS *JOB *SAV *SEC *SER *SPL User Group Group Author Limit
Profiles Profiles OBJ IT CFG CTL SYS ADM VICE CTL Class Owner Auth Type Capab
DENON *NONE X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
FENDT *NONE *USER *USRPRF *NONE *PRIVATE *NO
HOFFMAN *NONE X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
HOLT QPGMR X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
HOOPES *NONE X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
KLIMA *NONE X X X X X X X X *PGMR *USRPRF *NONE *PRIVATE *NO
LAURENT *NONE *USER *USRPRF *NONE *PRIVATE *NO
MALAGA *NONE X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
MALAGAX *NONE X X X X X X X X *SECOFR *USRPRF *NONE *PRIVATE *NO
PENCE GRP1 X X X X X X X X *SECOFR *GRPPRF *NONE *PRIVATE *NO
* * * truncated output * * *

```

Use User Profile Information report to check for:

- Excessive special authority
- Use of group profiles profiles
- Command line access

User Profile Information

46

```

User Profile Group *ALL *AUD SYS *JOB *SAV *SEC *SER *SPL User
Profiles Profiles OBJ IT CFG CTL SYS ADM VICE CTL Class
DENON *NONE X X X X X X X X *SECOFR
FENDT *NONE *USER
HOFFMAN *NONE *USER
HOLT QPGMR X X *PGMR
HOOPES *NONE X X *SYSOPR
KLIMA QPGMR X X *PGMR
LAURENT *NONE *USER
* * * truncated output * * *

```

Check for following User Profile Information:

- Excessive special authority
- Use of group profiles profiles
- Command line access

User Profile Information

47

Page 3

5716SS1 V3R7M0 961108 MCRISC 12/14/96 04:32:54

Report type : *ENVINFO
 Select by : *SPCAUT
 Special authorities : *ALL

User Profile	Current Library	Menu/ Library	Initial Library	Job Descr Library	Message Queue/ Library	Output Queue/ Library	Attention Program/ Library
DENON	*CRTDFT	MAIN	QCMD	QDFTJOB	DENON	*WRKSTN	QCMD
		*LIBL	*LIBL	QGPL	QUSRSYS		*LIBL
FENDT	*CRTDFT	MAIN	QCMD	QDFTJOB	FENDT	*WRKSTN	QCMD
		*LIBL	*LIBL	QGPL	QUSRSYS		*LIBL
HOFFMAN	*CRTDFT	MAIN	*NONE	QDFTJOB	HOFFMAN	*WRKSTN	*SYSVAL
		*LIBL		QGPL	QUSRSYS		
HOLT	*CRTDFT					HOLT	*SYSVAL
						HOLT	
HOOPES	\$HOOPES					WRKSTN	QCMD
							*LIBL
KLIMA	*CRTDFT					WRKSTN	QUSCMDLN
							*LIBL
LAURENT	*CRTDFT	MAIN	*NONE	STOTOM	LAURENT	*WRKSTN	*SYSVAL
		*LIBL		STOTOM	QUSRSYS		

Use report to check for:

- Initial program
- Initial menu
- Attention program

User Profile Information

48

Page 6

5716SS1 V3R7M0 961108 MCRISC 12/14/96 04:32:54

Report type : *PWDINFO
 Select by : *SPCAUT
 Special authorities : *ALL
 QPWDEXPITV system value : 60

User Profile	Status	Not Valid Sign-ons	No Password	Previous Sign-on	Password Changed	Expiration Interval	Password Expired
DENON	*ENABLED	0		12/09/96	10/14/96	*SYSVAL	*NO
FENDT	*ENABLED	0		10/07/96	09/20/96	*SYSVAL	*YES
HOFFMAN	*ENABLED	0	X	/ /	12/02/96	*SYSVAL	*NO
HOLT	*ENABLED	0		/ /	/ /	*SYSVAL	*YES
HOOPES	*DISABLED	0		09/26/96	07/29/96	*SYSVAL	*NO
KLIMA	*ENABLED	1		12/13/96	12/05/96	*SYSVAL	*NO
LAURENT	*ENABLED	0	X	/ /	12/10/96	*SYSVAL	*NO
MALAGA	*ENABLED	0		12/12/96	11/27/96	*NOMAX	*NO

Use report to check for

- Date last sign-on
- Use of *SYSVAL for password expiration

User Profile Authority

49

```

SECBATCH  Submit or Schedule Security Reports To Batch
                                     system:  MCRISC
Select one of the following:

    14. User profile authority
    15. Job and output queue authority
    16. Subsystem authority
    17. System security attributes
    18. Trigger programs
    19. User objects
    20. User profile information

    21. Check object integrity

Schedule Batch Reports
    30. Adopting objects
    31. Audit journal entries
    32. Authorization list authorities      More...
Selection or command
====>  14

```

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

User Profile Authority

50

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run CMD > PRTPUBAUT OBJTYPE(*USRPRF) CHGR
PONLY(*NO)

...
Job name JOB USRPRFAUT
Job description JOB0 *USRPRF
Library _____
Job queue JOBQ *JOB0
Library _____
Job priority (on JOBQ) JOBPTY *JOB0
Output priority (on OUTQ) OUTPTY *JOB0
Print device PRTDEV *CURRENT

User Profile Authority

51

```
Publicly Authorized Objects (Full Report)          Page 1
5716SS1 V3R7M0 961108                          MCRISC 12/14/96 04:28:12
Object type . . . . . : *USRPRF
Specified library . . : QSYS
-----Object----- -----Data-----
Library Object  Owner Authority Opr Mgt Exist Alter Ref Read Add Upd Dlt Exec
QSYS  QDBSHR  QSYS  USER DEF
QSYS  QSPLJOB  QSYS  *USE      X
QSYS  QTMLPD   QSYS  USER DEF  X
***** END OF LISTING *****
```

The profiles QDBSHR, QSPLJOB and QTMLPD are expected. Any other user profiles should be questioned

If users have *USE authority to user profiles, The SBMJOB command can be used to submit jobs as the other user profile.

Job Description Report

52

```
SECBATCH Submit or Schedule Security Reports To Batch
system: MCRISC
Select one of the following:
Submit Reports to Batch
1. Adopting objects
2. Audit journal entries
3. Authorization list authorities
4. Command authority
5. Communications security
6. Document authority
7. File authority
8. Folder authority
9. Job description authority
10. Library authority
11. Object authority
12. Private authority
13. Program authority
Selection or command 9 More.
===> =
F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel
```

Find JOBID with user names with PUBLIC access

Find JOBD that Name Profiles

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run CMD > PRTJOBDAUT LIB(*ALL)
CHGRPTONLY(*NO)

```

...
Job name . . . . . JOB          JOBD
Job description . . . . . JOBD   *USRPRF
  Library . . . . .
Job queue . . . . . JOBQ        *JOBD
  Library . . . . .
Job priority (on JOBQ) . . . . . JOBPTY *JOBD
Output priority (on OUTQ) . . . . . OUTPTY *JOBD
Print device . . . . . PRTDEV     *CURRENT
    
```

JOBD with User Profiles Named

Job Descriptions with Excess Authority (Full Report) Page 1
 5716SS1 V3R7M0 961108 MCRISC 12/14/96 03:15:57
 Specified library : *ALL

				-----Special Authorities-----										
Library	Job Description	Owner	User Profile	*ALL	*AUD	*IOSYS	*JOB	*SAV	*SEC	*SER	*SPL			
				OBJ	IT	CFG	CTL	SYS	ADM	VICE	CTL			
C51LIB	AUTOSTART2	QPGMR	QPGMR				X	X						
C51LIB	AUTOTEST	QPGMR	QPGMR				X	X						
QAUTOMON	QAUTOMON	QSYS	QAUTOMON				X	X						
QBRM	QBRMSYNC	QBRMS	QPGMR				X	X						
QBRM	Q1ACNETJD	QBRMS	QBRMS											
QBRM	Q1ASTRJD	QBRMS	QBRMS											
QDMT	QDMT	QSYS	QPGMR											
QDMT	QDNNOTIFY	QSYS	QPGMR											
QDMT	SERVER	QSYS	QPGMR											
QGPL	QAUTOMON	QSYS	QAUTOMON											
QGPL	QPFRCOL	QPGMR	QPGMR											
QGPL	QSPLAFPW	QSPL	QSPLJOB											
QGPL	QSPLDBR	QSPL	QSPLJOB											
QGPL	QSPLDKTR	QSPL	QSPLJOB											
QGPL	QSPLDKTW	QSPL	QSPLJOB											
QGPL	QSPLPRTW	QSPL	QSPLJOB											
QGPL	QSPLRMTW	QSPL	QSPLJOB											
QGPL	QSPLSTRWTR	QSPL	QSPLJOB											

Look for profiles that
 ► Own production objects
 ► With special authority
 - *ALLOBJ
 - *SERVICE
 - *SPLCTL

QSPLJOB is not an exposure

* * * * Report truncated * * *

Batch Reports

General Options

Advanced Options

Scheduling Reports



AUDITORS



Communications Security

SECBATCH Submit or Schedule Security Reports To Batch
system: MCRISC

Select one of the following:

Submit Reports to Batch

1. Adopting objects
2. Audit journal entries
3. Authorization list authorities
4. Command authority
5. Communications security
6. Document authority
7. File authority
8. Folder authority
9. Job description authority
10. Library authority
11. Object authority
12. Private authority
13. Program authority

**Security
attributes of
communication
configuration**

Selection or command **5**

More.

===> _

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Communications Security

57

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run CMD > PRTCMNSEC CHGRPTONLY(*NO)

```

...
Job name . . . . . JOB          COM_____
Job description . . . . . JOB0D  *USRPRF_____
  Library . . . . .
Job queue . . . . . JOBQ       *JOB0_____
  Library . . . . .
Job priority (on JOBQ) . . . . . JOBPTY  *JOB0_____
Output priority (on OUTQ) . . . . . OUTPTY  *JOB0_____
Print device . . . . . PRTDEV    *CURRENT_____

```

More...

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

Communication Information

58

Communications Information (Full Report) Page 1
 5716SS1 V3R7M0 961108 MCRISC 12/14/9 03:16:11
 Object type : *DEVD

Object Name	Object Type	Device Categ	Secure Locatio	Location Password	APPN Capabl	Single Session	Establish Session
DSP01	*DEVD	*DSP					
ETHLITCP	*DEVD	*NET					
MCEDIT	*DEVD	*APPC	*NO	*NO	*YES	*NO	*NO
OPT01	*DEVD	*OPT					
QANRDEVA	*DEVD	*APPC	*NO	*NO	*NO	*NO	*NO
QANRDEVB	*DEVD	*APPC	*NO	*NO	*NO	*NO	*NO
QCONSOLE	*DEVD	*DSP					
QESPAP	*DEVD	*APPC	*NO	*NO			
QIADSP	*DEVD	*HOST					
QIAPRT	*DEVD	*HOST					
QPADEV0001	*DEVD	*DSP					
QPADEV0002	*DEVD	*DSP					
QQAHOST	*DEVD	*APPC	*NO	*NO			
QTIDA	*DEVD	*APPC	*NO	*NO			
QTIDA2	*DEVD	*APPC	*NO	*NO			
QYCTSOC	*DEVD	*APPC	*NO	*NO	*YES	*NO	*NO
TAP01	*DEVD	*TAP					
TAP02	*DEVD	*TAP					

IF device is SECURELOC(*YES) recommend using a location password

Communication Information

59

```
Object type . . . . . : *CTLD
```

Object Name	Object Type	Controll Category	Auto Create	Switched	Call APPN	CP	Disc	Delete	Device	
CTL01	*CTLD	*LWS	*YES	*NO			0	0	DSP01	
ETHLINET	*CTLD	*NET	*YES	*NO			0	0	ETHLITCP	
MCEDIT	*CTLD	*APPC	*YES	*YES	DIAL	*YES	*YES	30	1440	MCEDIT
QANRCTLD	*CTLD	*APPC	*YES	*NO		*NO	*YES	30	1440	QANRDEVA
QCTL	*CTLD	*LWS	*YES	*NO			0	0	QCONSOLE	
QESCTL	*CTLD	*HOST	*YES	*YES	DIAL		0	0	QESPAP	
QILANM3601	*CTLD	*APPC	*YES	*NO		*YES	*YES	30	1440	*NONE
QPACTL01	*CTLD	*VWS	*YES	*NO			0	0	QPADEV000	
QTICTL	*CTLD	*HOST	*YES	*YES	*DIAL		0	0	QTIDA	
QVIRCD0001	*CTLD	*VWS	*YES	*NO			0	0	DVSERVERS	

Object type : *LIND

Communications Information (Full Report)

```
5716SS1 V3R7M0 961108 RISC 12
```

Object Name	Object Type	Line Category	Auto Create	Auto Delete	Auto Answer	Auto Dial
ETHLIN01	*LIND	*ETH	*NO	1440	*NO	*NO
QESLINE	*LIND	*SDLC	*NO	0	*YES	*NO
QTILINE	*LIND	*SDLC	*NO	0	*YES	*NO

Command Authority

60

SECBATCH Submit or Schedule Security Reports To Batch
system: MCRISC

Select one of the following:

- Submit Reports to Batch
1. Adopting objects
 2. Audit journal entries
 3. Authorization list authorities
 4. Command authority
 5. Communications security
 6. Document authority
 7. File authority
 8. Folder authority
 9. Job description authority
 10. Library authority
 11. Object authority
 12. Private authority
 13. Program authority

Security of CL commands

Selection or command **4** More.
===> =

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Command Authority

61

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run CMD > PRTPUBAUT OBJTYPE(*CMD)
 CHGRPTONLY(*NO)
 LIB(*ALL)

...
 Job name JOB *JOB0
 Job description JOB0 *USRPRF
 Library
 Job queue JOBQ *JOB0
 Library
 Job priority (on JOBQ) JOBPTY *JOB0
 Output priority (on OUTQ) OUTPTY *JOB0
 Print device PRTDEV *CURRENT

Command Authority

62

Publicly Authorized Objects (Full Report)

5716SS1 V3R7M0 961108

Object type : *CMD
 Specified library : *ALL

Library	Object	Owner	List	Authority	Opr	Mgt	Exist	Alter	Ref	Read	Add	Upd	Dlt	Exc
\$HOOPE	DLTPFRDTA2	HOOPE\$	*NONE	*CHANGE	X				X	X	X	X		X
\$KLIMA	CVTRPGCAS	KLIMA	*NONE	*CHANGE	X				X	X	X	X		X
\$KLIMA	DSPRDCNT	QDFTOWN	*NONE	*USE	X				X					X
\$KLIMA	EXTUTILS	KLIMA	*NONE	*CHANGE	X				X	X	X	X		X
QSMU	DLTSBMCRO	QSYS	QSM1AUTL	*USE	X				X					X
QSMU	DSPSBMCRO	QSYS	*NONE	*USE	X				X					X
QSMU	DSPSBMCROA	QSYS	*NONE	*USE	X				X					X
QSMU	DSPSBMCROQM	QSYS	*NONE	*USE	X				X					X
QSMU	DSPSRVPVDA	QSYS	*NONE	*USE	X				X					X
QSMU	EDTSMWAUT	QSYS	*NONE	*USE	X				X					X
QSMU	ENDSBMCROA	QSYS	QSM1AUTL	*USE	X				X					X
QSMU	HLDSBMCROA	QSYS	QSM1AUTL	*USE	X				X					X
QSMU	RLSSBMCROA	QSYS	QSM1AUTL	*USE	X				X					X
QSMVSS	QCQUPRUP	QSYS	*NONE	*USE	X				X					X
QSMVSS	WRKRCVCRQA	QSYS	QMGLAUTL											X
QSYS	ADDADMLANG	QSYS	*NONE											X
QSYS	ADDADMTYPE	QSYS	*NONE											X
QSYS	ADDAJE	QSYS	*NONE											X
QSYS	ADDALRACNE	QSYS	*NONE											X
QSYS	ADDALRD	QSYS	*NONE											X
QSYS	ADDALRSLTE	QSYS	*NONE											X
QSYS	WRKWTR	QSYS	*NONE	*USE	X				X					X

Use report to check for:
 ➤ **Access to powerful commands**

*** Report Truncated Many Pages ***

Job and Output Queue Authority

63

```

SECBATCH  Submit or Schedule Security Reports To Batch
system:    MCRISC

Select one of the following:

  14. User profile authority
  15. Job and output queue authority
  16. Subsystem authority
  17. System security attributes
  18. Trigger programs
  19. User objects
  20. User profile information

  21. Check object integrity

Schedule Batch Reports
  30. Adopting objects
  31. Audit journal entries
  32. Authorization list authorities      More...

Selection or command
===> 15
_____
F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
  
```

Job and Output Queue Authority

64

```

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run . . . . . CMD          > PRTQAUT LIB(*ALL)
                                           CHGRPTONLY(*NO)
_____
_____
_____
_____
...
Job name . . . . . JOB                QUEUES__
Job description . . . . . JOB0         *USRPRF__
Library . . . . .                      _____
Job queue . . . . . JOBQ              *JOB0__
Library . . . . .                      _____
Job priority (on JOBQ) . . . . . JOBPTY *JOB0__
Output priority (on OUTQ) . . . . . OUTPTY *JOB0__
Print device . . . . . PRTDEV         *CURRENT__
                                           More...

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

Job and Output Queue Authority

65

```

Queue Authority (Full Report)                               Page 1
5716SS1 V3R7M0 961108                                     MCRISC 12/16/96 13:17:00
Specified library . . . . . : *ALL
Library  Object      Type  Owner      Authority  DSPDTA  OPRCTL  AUTCHK
ERNIE    ERNIE         *OUTQ MALAGA   *USE      *NO     *YES    *OWNER
EVANS    EVANS         *OUTQ WOEVANS *USE      *NO     *YES    *OWNER
HOLT     HOLT          *OUTQ QDFTOWN *USE      *NO     *YES    *OWNER
HOLT     SECUREOUTQ    *OUTQ QDFTOWN *EXCLUDE  *NO     *NO     *OWNER
QADSM    QADSM         *OUTQ QSYS     *USE
QAUTOMON QAUTOMON      *JOBQ QSYS     *USE
QBRM     Q1ABRMNET    *JOBQ QBRMS   *USE
QGPL     QPFROUTQ     *OUTQ QSYS     *CHANGE
* * * Truncated Output * * *
  
```

OUTQs for sensitive output should be DSPDTA(*NO) OPTCTL(*NO) AUTCHK(*OWNER)

The Changed Report shows changes from the previous time the report was run

```

Queue Authority (Changed Report)                           Page 3
5716SS1 V3R7M0 961108                                     MCRISC 12/16/96 13:17:00
Specified library . . . . . : *ALL
Last changed report . . . . . : 12/14/96 05:42:10
Library  Object      Type  Owner      Authority  DSPDTA  OPRCTL  AUTCHK
(There are no queues to list)
* * * * * E N D   O F   L I S T I N G   * * * * *
  
```

Trigger Programs

66

```

SECBATCH  Submit or Schedule Security Reports To Batch
system:    MCRISC

Select one of the following:

  14. User profile authority
  15. Job and output queue authority
  16. Subsystem authority
  17. System security attributes
  18. Trigger programs
  19. User objects
  20. User profile information

  21. Check object integrity

Schedule Batch Reports
  30. Adopting objects
  31. Audit journal entries
  32. Authorization list authorities      More...

Selection or command
===> = 18

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
  
```

Trigger Programs

67

```

Submit Job (SBNJOB)

Type choices, press Enter.

Command to run . . . . . CMD          > PRTRTRPGM LIB(*ALL)
                                           CHGRPTONLY(*NO)

. . .
Job name . . . . . JOB                TRIGGERPGM
Job description . . . . . JOB0         @USRPF
Library . . . . .
Job queue . . . . . JOBQ              *JOBQ
Library . . . . .
Job priority (on JOBQ) . . . . . JOBPTY *JOBQ
Output priority (on OUTQ) . . . . . OUTPTY *JOBQ
Print device . . . . . PRTDEV         *CURRENT
                                           More...

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

Trigger Programs

68

Trigger Programs (Full Report) Page 1

5716SS1 V3R7M0 961108 MCRISC 12/14/96 04:32:42

Specified library : *ALL

Library	File	Trigger Library	Trigger Program	Trigger Time	Trigger Event	Trigger Condition	Allow Repeated Change
HOLT	CUSTMAS	HOLT	UPDSALES	After	Update	Change	No
HOLT	CUSTMAS2	HOLT	UPDSALES	After	Update	Change	No
MAGCHECK	CUST_MSTR	\$KLIROB	CHK_CREDIT	After	Update	Always	No
MAGWORK	ACT001PF	MAGWORK	ACT003RG	Before	Insert		No
MAGWORK	ACT001PF	MAGWORK	ACT003RG	Before	Update	Change	No
MAGWORK	TRIGPF	MAGWORK	TRIGPGM	Before	Update	Always	Yes
QUSRSYS	QAVATALNP	QSVMS	QVATTRIG	After	Insert		No
QUSRSYS	QAVATALNP	QSVMS	QVATTRIG	After	Delete		No
QUSRSYS	QAVATALNP	QSVMS	QVATTRIG	After	Update	Always	No

Trigger programs run when users access files. Users are often not aware of that the trigger program exit runs when they access data. In a high security environment, the function of trigger programs should be reviewed

User Objects in QSYS Library

69

```

SECBATCH  Submit or Schedule Security Reports To Batch
                                                    system:  MCRISC
Select one of the following:

    14. User profile authority
    15. Job and output queue authority
    16. Subsystem authority
    17. System security attributes
    18. Trigger programs
    19. User objects
    20. User profile information

    21. Check object integrity

Schedule Batch Reports
    30. Adopting objects
    31. Audit journal entries
    32. Authorization list authorities           More...
Selection or command
====>  19

```

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

User Objects in QSYS

70

```

Submit Job (SBMJOB)

Type choices, press Enter.

Command to run . . . . . CMD          > PRTUSROBJ LIB(QSYS)
                                                    CHGRPTONLY(*NO)

```

```

...
Job name . . . . . JOB                *JOBQ
Job description . . . . . JOBQ        *JOBQ
Library . . . . .                    *JOBQ
Job queue . . . . . JOBQ             *JOBQ
Library . . . . .                    *JOBQ
Job priority (on JOBQ) . . . . . JOBPTY *JOBQ
Output priority (on OUTQ) . . . . . OUTPTY *JOBQ
Print device . . . . . PRTDEV         *CURRENT

```

User Objects in QSYS

71

```

User Objects (Full Report)                               Page 1
5716SS1 V3R7M0                                         MCRISC 12/30/96 01:13:17
Specified library . . . . . : QSYS
Libr Object Type Attr Owner Description
QSYS GLOOP *LIB PROD WOEVANS COLLECTION - created by SQL
QSYS GRP_WOE *USRPRF WOEVANS Group profile for Wayne Evans
QSYS DSP01 *DEVD DSPLCL QPGMR CREATED BY AUTO-CONFIGURATION
QSYS DSP02 *DEVD DSPLCL QPGMR CREATED BY AUTO-CONFIGURATION
QSYS ETHLIN01 *LIND ETH PLUTH Ethernet line on NWS
QSYS SLIP *LIND ASC KLIMA
QSYS APPCOVRT *CTLD APPC STOTOM
QSYS CTL01 *CTLD LWS QPGMR CREATED BY AUTO-CONFIGURATION
QSYS QHST963A *FILE PF QSYS 09612240458080961228001002
QSYS QHST966A *FILE PF QSYS 09612280010020961230010013
QSYS DSP01 *MSGQ QSYS Work Station Message Queue
QSYS DSP02 *MSGQ QSYS Work Station Message Queue
QSYS VFYOPCCN *CMD QSYS
QSYS QNTBIBM *NTBD QSYS This NTBD is IBM Supplied
QSYS QDCIPX1 *IPXD QSYS This IPXD is IBM Supplied
QSYS QDCIPX2 *IPXD QSYS This IPXD is IBM Supplied
QSYS QMOTRACE *

```

Use report to check for:
 ➤ **User Commands**
 ➤ **Production files**

Batch Reports



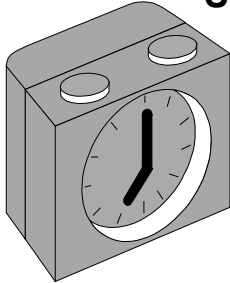
General Options

Advanced Options

Scheduling Reports

72

Scheduled Security Reports 73



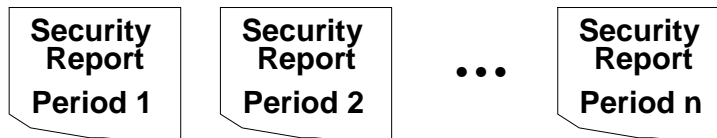
Useful for repeated use of reports

Reports can be scheduled for

- Daily
- Weekly
- Month End or start

Uses OS/400 job scheduling functions

All of security reports can be scheduled.



Schedule Audit Journal Report 74

```
SECBATCH  Submit or Schedule Security Reports To Batch
system:   MCRISC

Select one of the following:

  14. User profile authority
  15. Job and output queue authority
  16. Subsystem authority
  17. System security attributes
  18. Trigger programs
  19. User objects
  20. User profile information

  21. Check object integrity

Schedule Batch Reports
  30. Adopting objects
  31. Audit journal entries
  32. Authorization list authorities      More...

Selection or command
===> = 31
```

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Schedule Audit Journal Report 75

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name JOB
 Command to run CMD > DSPAUDJRNE ENTYP(AF) USRPRF(*#
 L) JRNRCV(*CURRENT)

**Put cursor in
CMD field**

F4

**Prompt for
submitted
command**

Frequency FRQ
 Schedule date, or SCDDATE *CURRENT
 Schedule day SCDDAY *NONE
 + for more values
 Schedule time SCDTIME *CURRENT

Prompting can be used to customize report

Bottom

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

Audit Journal Report 76

Display Audit Journal Entries (DSPAUDJRNE) Level: 2

Type choices, press Enter.

Journal entry types ENTYP > AE
 + for more values > **+**
 User profile USRPRF > *ALL
 Journal receiver searched: JRNRCV > *CURRENT
 Starting journal receiver
 Library
 Ending journal receiver
 Library
 Starting date and time: FROMTIME
 Starting date *FIRST
 Starting time
 Ending date and time: TOTIME
 Ending date *LAST
 Ending time
 Output OUTPUT *PRINT

**Enter "+"
to expand
field**

Bottom

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

Select Audit Journal Event Types

77

Specify More Values for Parameter ENTTYP

Type choices, press Enter.

Journal entry types > AF
PW
CO
CA
SC
—
—
—
—
—
—
—
—
—
—

Enter additional journal entry types

Schedule Audit Journal Report

78

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Provide job name

Job name JOB AUDJRN
Command to run CMD DSPAUDJRNE
ENTTYP(AF PW CA CO CP) USRPRF(*ALL) JRNRCV(*CURRENT)

Frequency FRQ *NONE
Schedule date, or SCDDATE
Schedule day SCDDAY *SUN
+ for more values
Schedule time SCDTIME 00:00:01

Provide time when job should be scheduled

Scheduled Jobs								79	
WRKJOBSCDE SCDBY(WOEVANS)									
Work with Job Schedule Entries						MCRISC			
						06/09/98 02:18:55			
Type options, press Enter.									
2=Change		3=Hold		4=Remove		5=Display details		6=Release	
8=Work with last submission				10=Submit immediately					
-----Schedule-----									
Opt	Job	Status	Date	Time	Frequency	Recovery Action	Next Submit Date		
5	AUDJRN	SCD	*SUN	00:00:01	*WEEKLY	*SBMRLS	06/14/98		
—	QSECACT1	SCD	USER DEF	05:00:00	*WEEKLY	*SBMRLS	06/09/98		
—	QSECACT1	SCD	USER DEF	18:00:00	*WEEKLY	*SBMRLS	06/09/98		
—	QSECACT1	SCD	*ALL	05:30:00	*WEEKLY	*SBMRLS	06/09/98		
—	QSECACT1	SCD	*ALL	19:00:00	*WEEKLY	*SBMRLS	06/09/98		
—	QSECEXP1	SCD	*ALL	00:01:00	*WEEKLY	*SBMRLS	06/10/98		
—	QSECIDL1	SCD	*ALL	01:00:00	*WEEKLY	*SBMRLS	06/10/98		
								Bottom	
Parameters or command									
===>									
F3=Exit		F4=Prompt		F5=Refresh		F6=Add		F9=Retrieve	
F11=Display job queue data			F12=Cancel		F17=Top		F18=Bottom		

Scheduled Jobs								80
Display Job Schedule Entry Details								
						System: MCRISC		
Job:	AUDJRN	Entry number:	000095	Status:	SCD			
Last attempted submission:								
Status	Job not previously submitted.							
Schedule day	*SUN							
Schedule time	00:00:01							
Frequency	*WEEKLY							
Recovery action	*SBMRLS							
Next submit date	06/14/98							
Command	DSPAUDJRNE ENTYP(AF PW CA CO CP) USRPRF(*AL) JRNRCV(*CURRENT)							
Job queue	*JOBQ							
Library								
Job queue status								

Scheduled Jobs										81
Work with Job Schedule Entries										MCRISC
										06/09/98 02:18:55
Type options, press Enter.										
2=Change 3=Hold 4=Remove 5=Display details 6=Release										
8=Work with last submission 10=Submit immediately										
Opt	Job	Status	Date	Time	-----Schedule-----					
—	AUDJRN	SCD	*SUN	00:00						Submit
—	QSECACT1	SCD	USER DEF	05:00						14/98
—	QSECACT1	SCD	USER DEF	18:00:00	*WEEKLY	*SAMEDAY				09/98
—	QSECACT1	SCD	*ALL	05:30:00	*WEEKLY	*SBMRLS				09/98
—	QSECACT1	SCD	*ALL	19:00:00	*WEEKLY	*SBMRLS				06/09/98
—	QSECEXP1	SCD	*ALL	00:01:00	*WEEKLY	*SBMRLS				06/09/98
—	QSECIDL1	SCD	*ALL	01:00:00	*WEEKLY	*SBMRLS				06/10/98
										Bottom
Parameters or command										
===>										
F3=Exit F4=Prompt F5=Refresh F6=Add F9=Retrieve										
F11=Display job queue data F12=Cancel F17=Top F18=Bottom										

Use the other options of WRKSCDJOB to change/remove scheduled jobs

Outline		82
Security Tools		
—	Interactive Options	
—	Batch Report	
—	Scheduling Reports	
—	General Options	

General Security Options

83

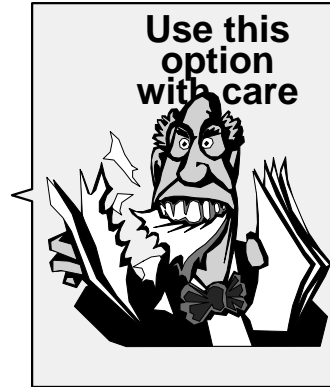
SECTOOLS

Security Tools

Select one of the following:

- General system security
 - 50. Configure system security
 - 51. Revoke public authority to objects
 - 52. Check object integrity

- 70. Related security tasks



Bottom

Selection or command

==> **50**

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Configure System Security

84

Do not use this option blindly or your system will be very secure and difficult to use

```
.....
*
*   This command activates system security features by turning on
*   security auditing, changing system values, and modifying system
*   supplied user profiles. Only run this command if you know what
*   features are being activated by this command.
*
*
*   To determine what security features are activated, issue the
*   Retrieve CL Source (RTVCLSRC) command against the program
*   QSECCFGS and examine the source file created.
*
*
*.....
```

RECOMMEND Retrieve the source of QSECCFGS and modify for your installation

Press Enter to confirm your choices to run the command.
Press F12 to cancel your request.

[View Source](#)

QSECCFGS Configure Security

85

```

/*****
/*
/* 5716SS1 V3R7M0 961108      RTVCLSRC Output      12/27/96 04:56:02  */
/*
/* Program name . . . . . : QSECCFGS      PN*/
/* Library name . . . . . : QSYS          PL*/
/* Original source file . . . . . :      SN*/
/* Library name . . . . . :              SL*/
/* Original source member . . . . . :     SM*/
/* Source file change
/*   date/time . . . . . :              SC*/
/* Patch option . . . . . : *NOPATCH      PO*/
/* User profile . . . . . : *USER        UP*/
/* Text . . . . . :                    TX*/
/* Owner . . . . . : QSYS              OW*/
/* Patch change ID . . . . . :          PC*/
/* Patch APAR ID . . . . . :           PA*/
/* User mod flag . . . . . : *NO        UM*/
/*
/******
      QSYS/PGM
      DCL  VAR(&IBMREG) TYPE(*CHAR) LEN(300) VALUE('Copyright, -
5799XDH, 5763SS1, 5716SS1, (C) Copyright IBM Corp. 1996. All Rights -
Reserved; US Government Users Restricted Rights - Use, duplication or-
disclosure restricted by GSA ADP Schedule Contract with IBM Corp. -
Licensed Materials - Property of IBM.  ')

```

QSECCFGS Configure Security

86

```

DCL  VAR(&IBMREG2) TYPE(*CHAR) LEN(300)
DCL  VAR(&LMTCHRTXTM) TYPE(*CHAR) LEN(7) VALUE('CPXB302')
DCL  VAR(&DFTVALUE) TYPE(*CHAR) LEN(10)
DCL  VAR(&APPID) TYPE(*CHAR) LEN(8)
DCL  VAR(&PNLGRP) TYPE(*CHAR) LEN(20) VALUE('QGSECCSS *LIBL')
DCL  VAR(&FUNC) TYPE(*CHAR) LEN(4) VALUE(' ')
DCL  VAR(&ENTERVALUE) TYPE(*DEC) LEN(4) VALUE(100)
DCL  VAR(&ERRCD) TYPE(*CHAR) LEN(8) VALUE(X'0000000000000000')
DCL  VAR(&AUTIND) TYPE(*CHAR) LEN(1)
DCL  VAR(&AUTS) TYPE(*CHAR) LEN(30)-
      VALUE('*ALLOBJ *SECADM *AUDIT ')
DCL  VAR(&NUMAUTS) TYPE(*CHAR) LEN(4) VALUE(X'00000003')
DCL  VAR(&CALLLVL) TYPE(*CHAR) LEN(4) VALUE(X'00000000')
QSYS/MONMSG MSGID(CPF0000)
QSYS/CHGVAR VAR(&IBMREG2) VALUE(&IBMREG)
QSYS/CALL PGM(QSYS/QSYCUSRS) PARM(&AUTIND *CURRENT &AUTS -
&NUMAUTS &CALLLVL &ERRCD)
QSYS/IF COND(&AUTIND *EQ 'N') THEN(QSYS/SNDPGMMSG MSGID(CPFB304)-
MSGF(*LIBL/QCPFMSG) MSGTYPE(*ESCAPE))
QSYS/CALL PGM(QSYS/QUIOPNDA) PARM(&APPID &PNLGRP -1 0 N &ERRCD)
QSYS/MONMSG MSGID(CPF0000) EXEC(GOTO CMDLBL(SKIPUIM))
QSYS/CALL PGM(QSYS/QUIDSPP) PARM(&APPID &FUNC 'CONCSS' N &ERRCD)
QSYS/CALL PGM(QSYS/QUICLOA) PARM(&APPID M &ERRCD)
QSYS/IF COND(%BIN(&FUNC) *NE &ENTERVALUE) THEN(QSYS/RETURN)
SKIPUIM:

```

QSECCFGS Configure Security

87

```
QSYS/CHGSECAUD QAUDCTL(*ALL) QAUDLVL(*DFTSET)
QSYS/CHGSYSVAL SYSVAL(QALWOBJRST) VALUE(' *NONE' ) /* *ALL */
QSYS/CHGSYSVAL SYSVAL(QAUTOCFG) VALUE('0') /* 1 */
QSYS/CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(0) /* 1 */
QSYS/CHGSYSVAL SYSVAL(QDEVRCYACN) VALUE(' *DSCMSG' )
QSYS/CHGSYSVAL SYSVAL(QDSCJOBITV) VALUE('120')
QSYS/CHGSYSVAL SYSVAL(QDSPSGNINF) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QINACTITV) VALUE('60')
QSYS/CHGSYSVAL SYSVAL(QINACTMSGQ) VALUE(' *ENDJOB' ) /* *DSCJOB */
QSYS/CHGSYSVAL SYSVAL(QLMTDEVSSN) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QMAXSGNACN) VALUE('3')
QSYS/CHGSYSVAL SYSVAL(QMAXSIGN) VALUE('3')
QSYS/CHGSYSVAL SYSVAL(QRMTSIGN) VALUE(' *FRCSIGNON' )
QSYS/CHGSYSVAL SYSVAL(QRMTSRVATR) VALUE('0')
QSYS/CHGSYSVAL SYSVAL(QSECURITY) VALUE('50') /* 40 */
QSYS/CHGSYSVAL SYSVAL(QPWDEXPITV) VALUE('60')
QSYS/CHGSYSVAL SYSVAL(QPDMINLEN) VALUE(6)
QSYS/CHGSYSVAL SYSVAL(QPDMAXLEN) VALUE(8) /* 8-10 */
QSYS/CHGSYSVAL SYSVAL(QPWDPOSDIF) VALUE('1') /* 0 */
```

QSECCFGS Configure Security

88

```
QSYS/RTVMSG MSGID(&LMTCHRTXTM) MSGF(QCPFMSG) MSG(&DFTVALUE)
QSYS/CHGSYSVAL SYSVAL(QPWDLMTCHR) VALUE(&DFTVALUE) /* # $ @ */
QSYS/CHGSYSVAL SYSVAL(QPWDLMTAJC) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QPWDLMTREP) VALUE('2')
QSYS/CHGSYSVAL SYSVAL(QPWDRQDDGT) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QPWDRQDDIF) VALUE('1') /* 0 */
QSYS/CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(' *NONE' ) /* pgm */
/ *** Set password of user profiles *** /
QSYS/CHGUSRPRF USRPRF(QSYSOPR) PASSWORD(*NONE)
QSYS/CHGUSRPRF USRPRF(QPGMR) PASSWORD(*NONE)
QSYS/CHGUSRPRF USRPRF(QUSER) PASSWORD(*NONE)
QSYS/CHGUSRPRF USRPRF(QSRV) PASSWORD(*NONE)
QSYS/CHGUSRPRF USRPRF(QSRVBAS) PASSWORD(*NONE)
QSYS/ENDPGM
```

Change source for installation defaults before running the program

General Security Options

89

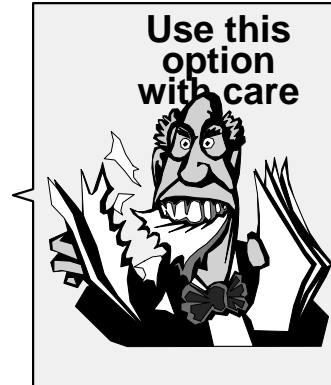
SECTOOLS

Security Tools

Select one of the following:

- General system security
 - 50. Configure system security
 - 51. Revoke public authority to objects
 - 52. Check object integrity

- 70. Related security tasks



Bottom

Selection or command

==> **51**

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

Configure System Security

90

Confirm Revoke Public Authority

Do not use this option blindly or your system will be very secure and difficult to use

This command limits the use of commands and programs by changing the public authority to #EXCLUDE. Only run this command if you know what commands and programs have their public authority set by this command.

To determine what command and program authorities are changed, issue the Retrieve CL Source (RTVCLSRC) command against the program QSECRVKP and examine the source file created.

RECOMMEND Retrieve the source of QSECRVKP and modify for your installation

Press Enter to confirm your choices to run the command.
Press F12 to cancel your request.

General Security Options

91

SECTOOLS

Security Tools

System: MCRISC

Select one of the following:

General system security

- 50. Configure system security
- 51. Revoke public authority to objects
- 52. Check object integrity

- 70. Related security tasks

Long running function to check all objects in system. Use only in high security environments.

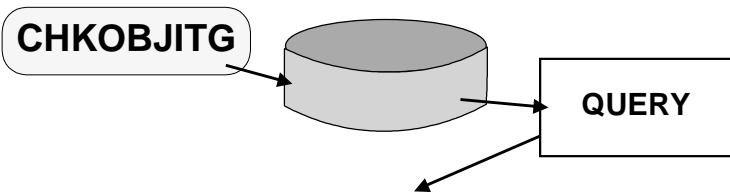
Selection or command

==> **52**

F1=Help F3=Exit F4=Prompt F9=Retrieve F12=Cancel

CHKOBJITG Report

92



VIOLATION	OBJECT	LIBRARY	TYPE	OWNER
NOTTRANS	SGN001CL	MAGWORK	*PGM	QSECOFR
NOTTRANS	SWAP	MAGWORK	*PGM	QSECOFR
NOTTRANS	RISPRFCL	POINT51	*PGM	QSECOFR
NOTTRANS	QHJWX6ER	QPWXCGY	*PGM	OSYS

Violations Types	
DMN	DMN The domain is not correct for the object type
DMN	PGMMOD The object has been modified
DMN	NOTTRANS Object has not been converted to RISC format

The NOTTRANS objects can be translated by CHGPGM or recompile

PROBLEM

Security tools shipped by IBM require ***ALLOBJ** and ***IOSYSCFG** special authority.



Administrators that want auditors to use tools do not want to give these users powerful authority.

Adoption of Authority

QUESTION

Is there a way to give someone other than a user with powerful special authority access to the security tools?

ANSWER

Yes, the special authorities ***ALLOBJ** and ***IOSYSCFG** can be adopted.

Adoption of Authority

QUESTION

Can I give users access by adopting before I display the security tool menu?

ANSWER

YES it is possible to adopt before you issue the GO SECTOOLS command

NOT RECOMMENDED

1. The security tools menu has a command line.

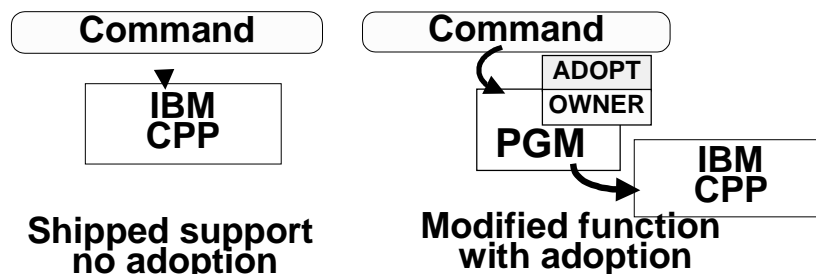
**Adoption Rule 1
DO NOT GIVE USERS A COMMAND LINE
WHEN ADOPTING**

2. Adopted authority will not work for batch reports.

Adoption of Authority

QUESTION How can I get the security tools to adopt?

ANSWER Change the security tools commands to call your program.
Your program will adopt and then call the IBM CPP (Command Processing Program)



WARNING: Changing the IBM commands is not recommended by IBM BUT IT WORKS!!

Adopting Authority for Security Tools ⁹⁷

1. Create authorization list to secure function

```
CRTAUTL SECTOOLS AUT(*EXCLUDE)
```

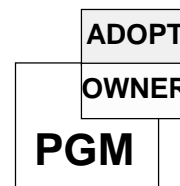
The security tools were limited to users with *ALLOBJ authority.

After these changes you must secure the use of tools

Adopting Authority for Security Tools ⁹⁸

2. Create a program to adopt and call IBM CPP

- Store the program in library QSYS
- Have the program adopt authority
- Secure the program using the SECTOOLS authorization list



```
CRTCLPGM QSYS/Q$SECJOBDO SRCFILE()  
USRPRF(*OWNER) AUT(SECTOOLS)
```

```
PGM (&P1 &P2 &P3)  
DCL &P1 *CHAR 1  
DCL &P2 *CHAR 1  
DCL &P3 *CHAR 1  
CALL QSYS/Q$SECJOBDO +  
(&p1 &p2 &p3)  
ENDPGM
```

Adopting Authority for Security Tools ⁹⁹

3. Create a backup copy of the IBM command

```
CRTDUPOBJ PRTJOBDAUT QSYS *CMD  
TOLIB(QSYSSAVE)
```

This step is important should you need to remove changes.

4. Change command to call that adopts
(This is the program created in step 2)

```
CHGCMD QSYS/PRTJOBDAUT  
PGM(QSYS/Q$SECJOBDO)
```

Adopting Authority for Security Tools ¹⁰⁰

5. Secure the command with SECTOOLS authorization list

```
GRTOBJAUT QSYS/PRTJOBDAUT *CMD  
AUTL(SECTOOLS)
```

6. Add user profiles to the SECTOOLS authorization list

```
EDTAUTL AUTL(SECTOOLS)
```

INFORMATION SOURCES

101

- **MANUALS**

- **SC41-5300 Tips and Tools for Securing Your AS/400**
- **SC41-5301 AS/400 Security Basic**
- **SC41-5302 AS/400 Security Reference**
- **S325-6321 IBM Secure Way AS/400 and the Internet**

102

End of Presentation

WOEvans@AOL.com