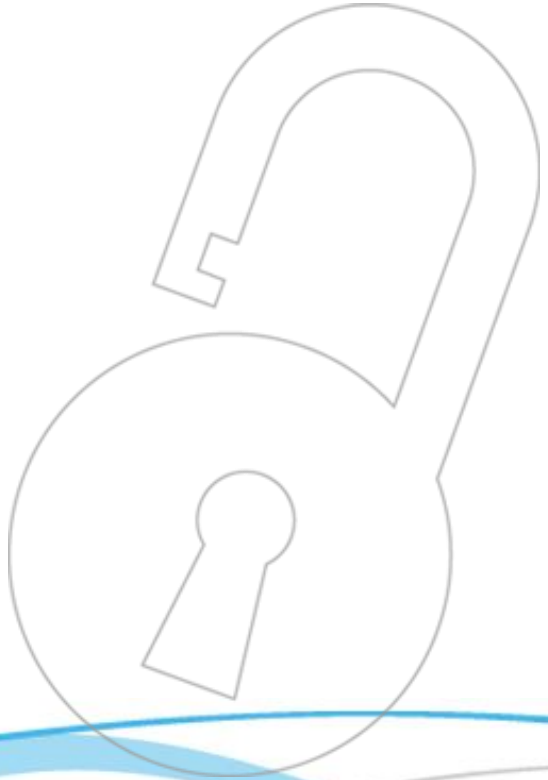


Authority on Demand

Control Authority Rights & Emergency Access

iSecurity

SRC Secure Solutions

RAZ-LEE The iSeries Security Experts

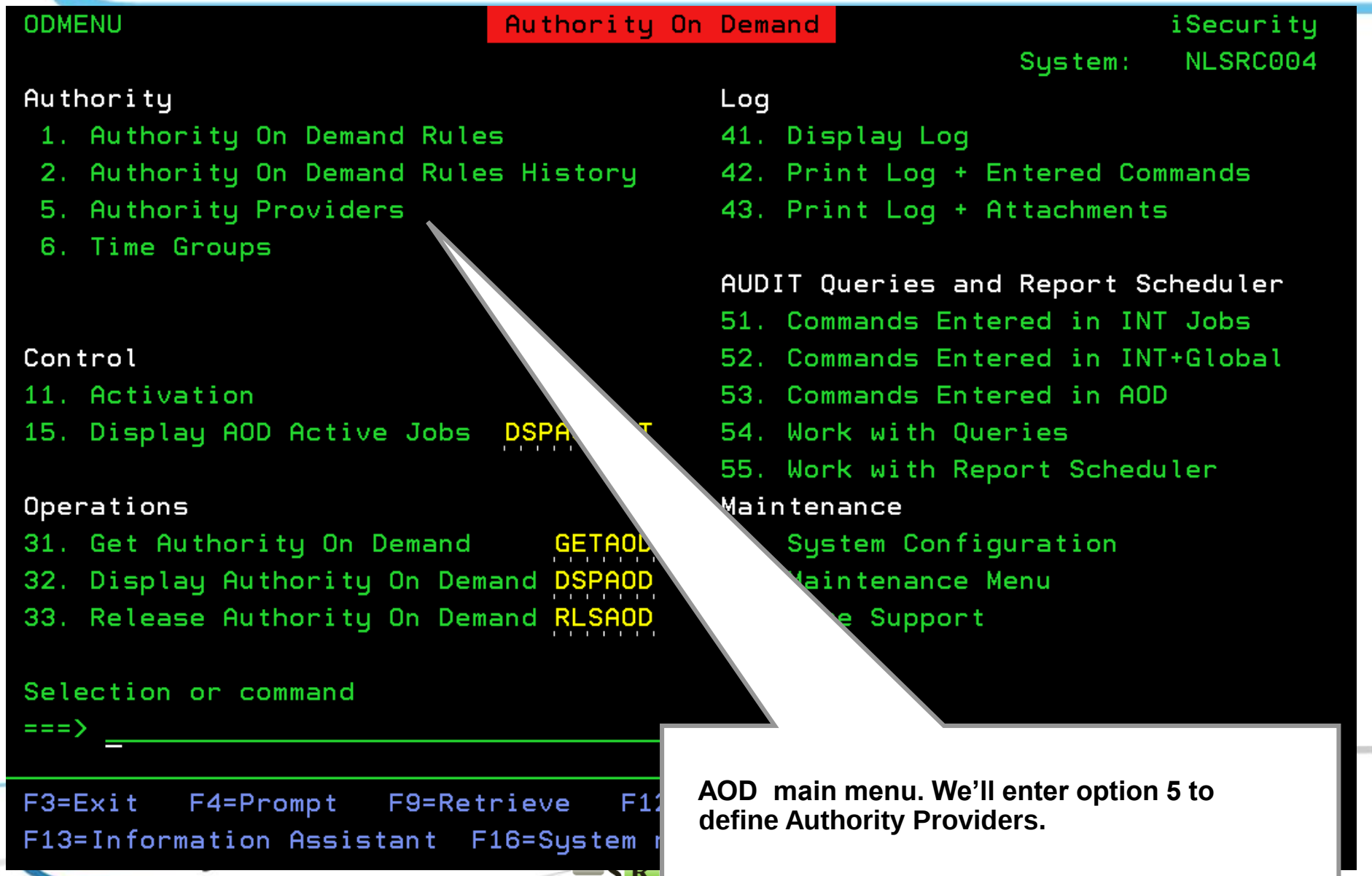
The Challenge

- System i sites define user's security levels and allocate security rights corresponding to the different job responsibilities in the organization
- Emergency access to critical application data and processes is a potentially serious security breach which is often uncovered in System i audits.
- Manual approaches to this problem are not only error-prone, but do not comply with regulations and auditor's often stringent security requirements.

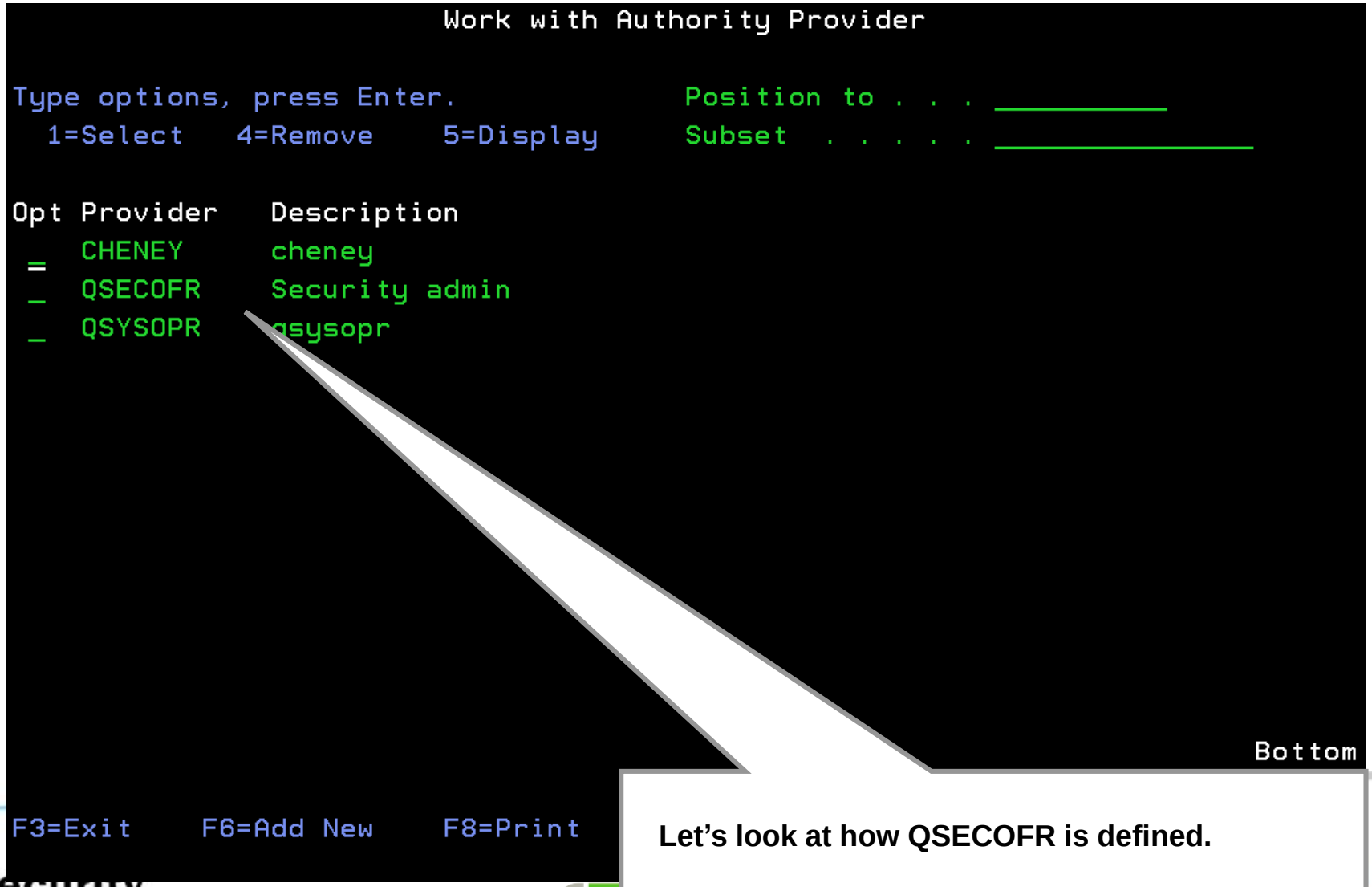
AOD Features

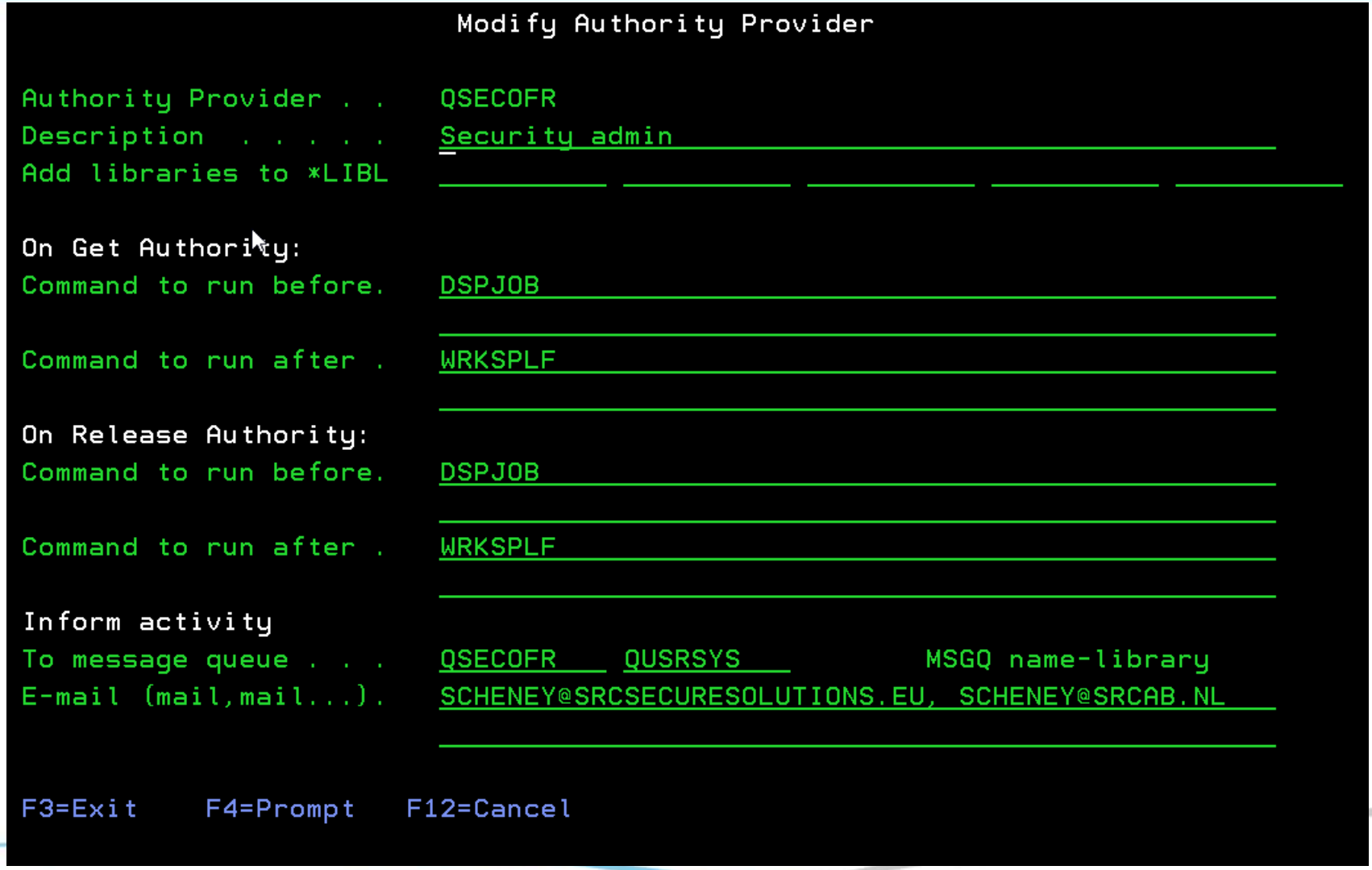
- ADD and SWAP Security Levels (**feature unique to AOD**) – can ADD additional security rights to current user profile or grant a new security authority level.
- Global Add SPCAUT
- Authority Transfer On-Demand Rules & Providers - pre-define special authority "providers" and authority transfer rules.
- Safe Recovery from Emergency – recover from emergency situations with minimum risk of human error and maximum reporting of activities while running with higher special authority.
- Full Monitoring Capabilities - logs and monitors all relevant activities, and sends audit reports and real-time e-mail alerts when higher authority rights are provided.
- Simple, Controlled Access – Only authorized users can grant authority or access critical data and processes and incorporates easy-to-use reporting and monitoring mechanisms.
- Part of Comprehensive Solution - solidifies iSecurity's position as the most comprehensive security solution for System i environments.

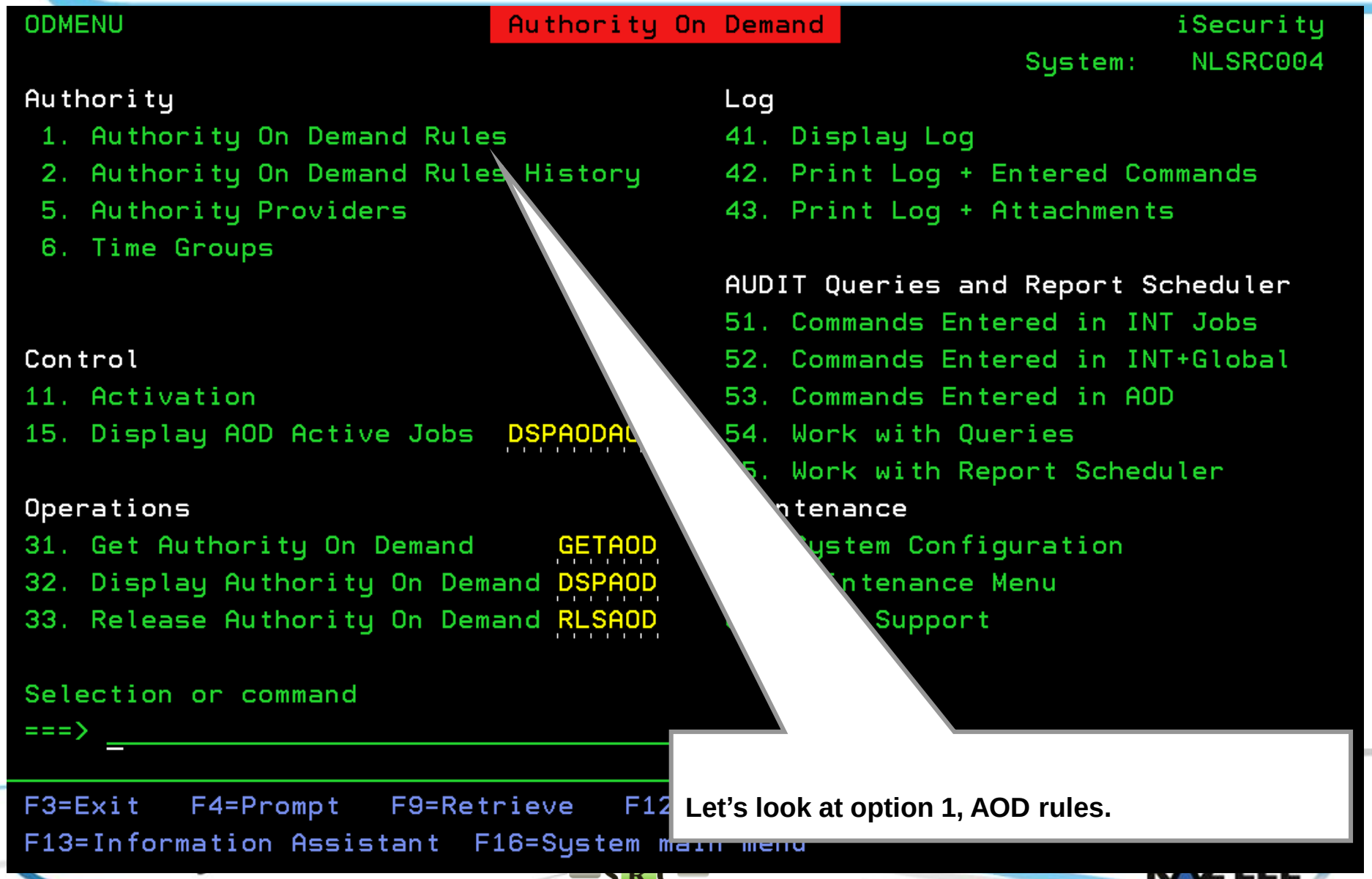
Authority on Demand Training



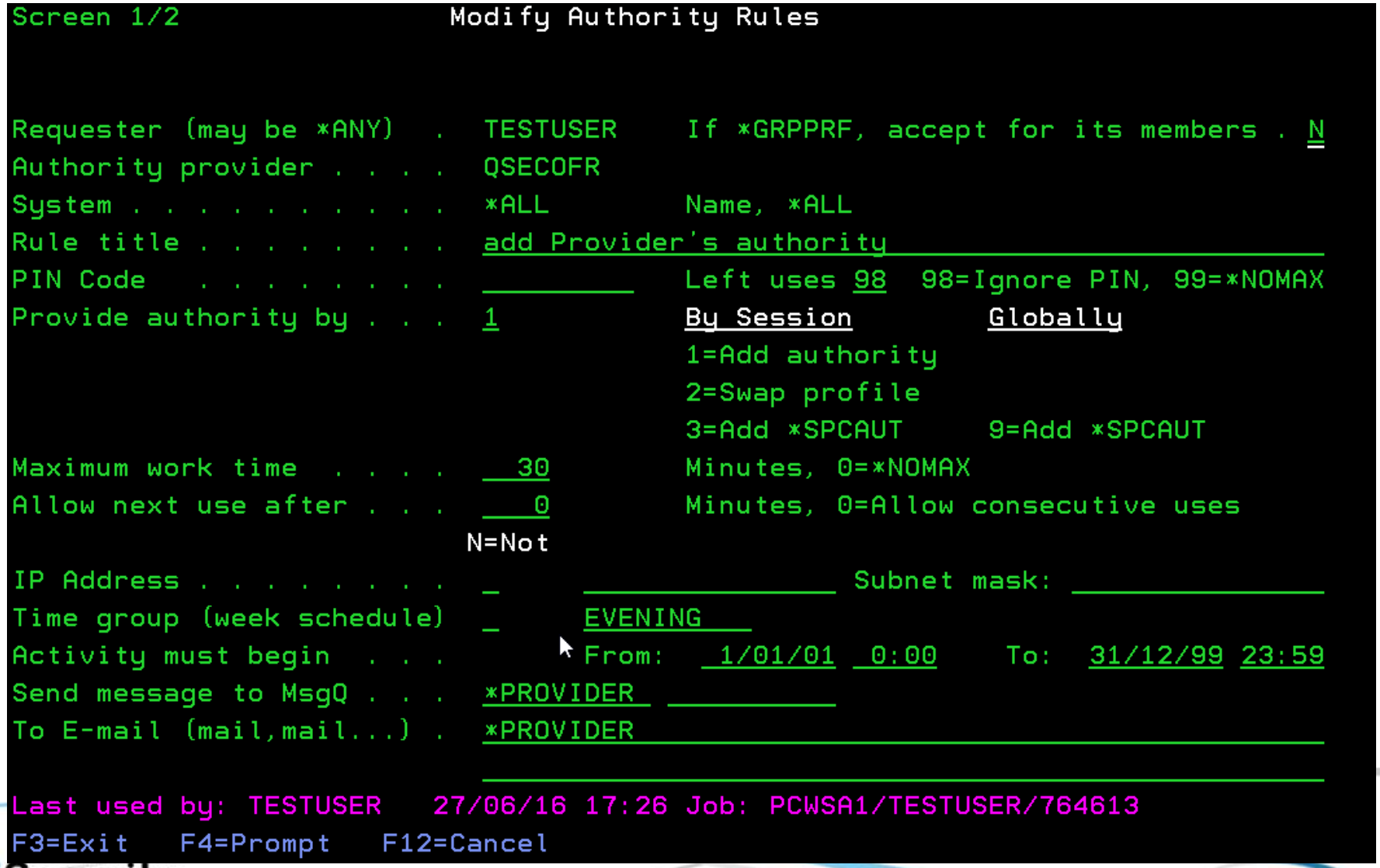
AOD main menu. We'll enter option 5 to define Authority Providers.

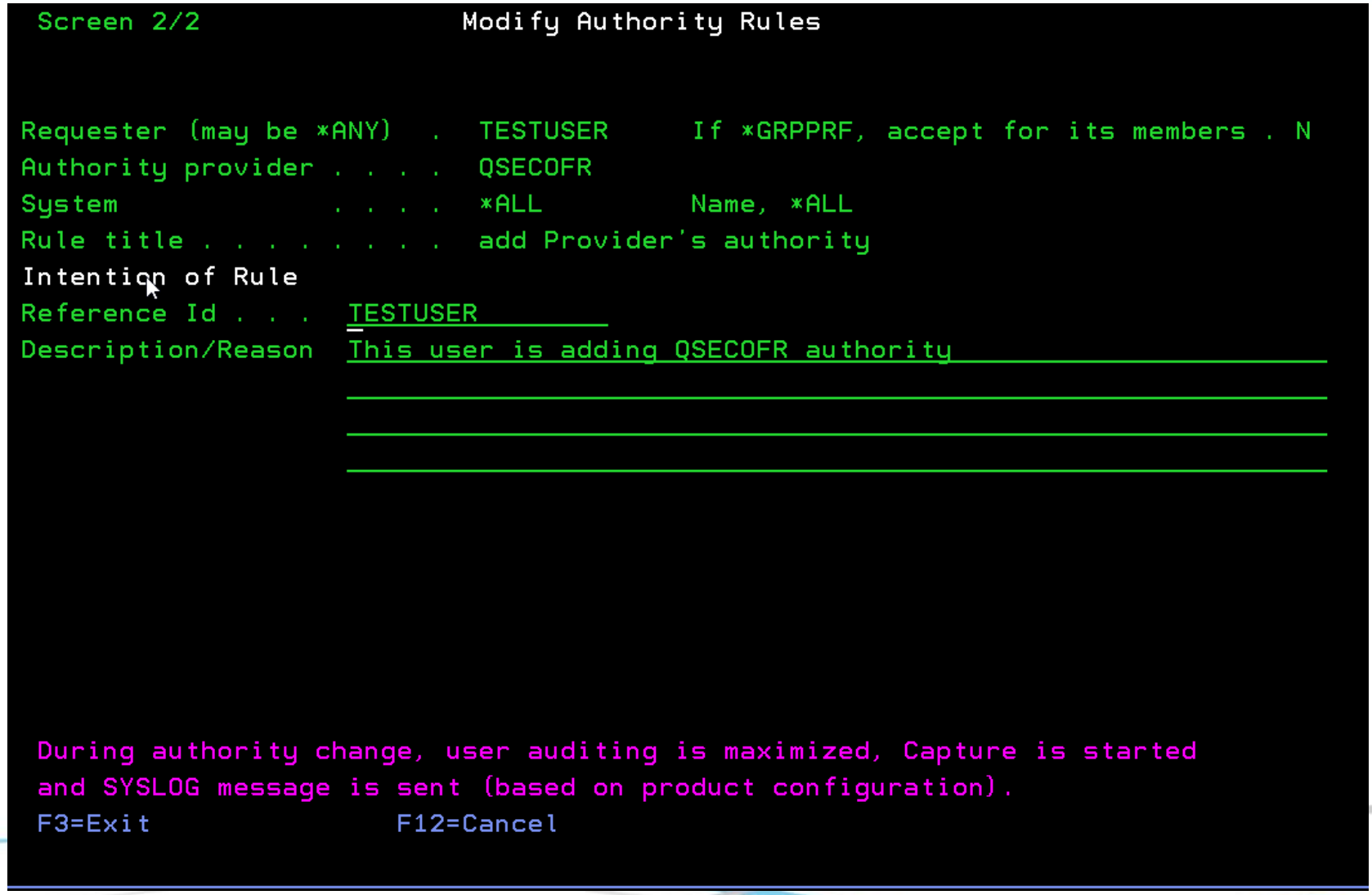

Work with Authority Provider
Type options, press Enter.
1=Select 4=Remove 5=Display
Position to . . . _____
Subset . . . . . _____
Opt Provider Description
CHENEY cheney
QSECOFR Security admin
QSYSOPR qsysopr
Bottom
F3=Exit F6=Add New F8=Print
Let's look at how QSECOFR is defined.

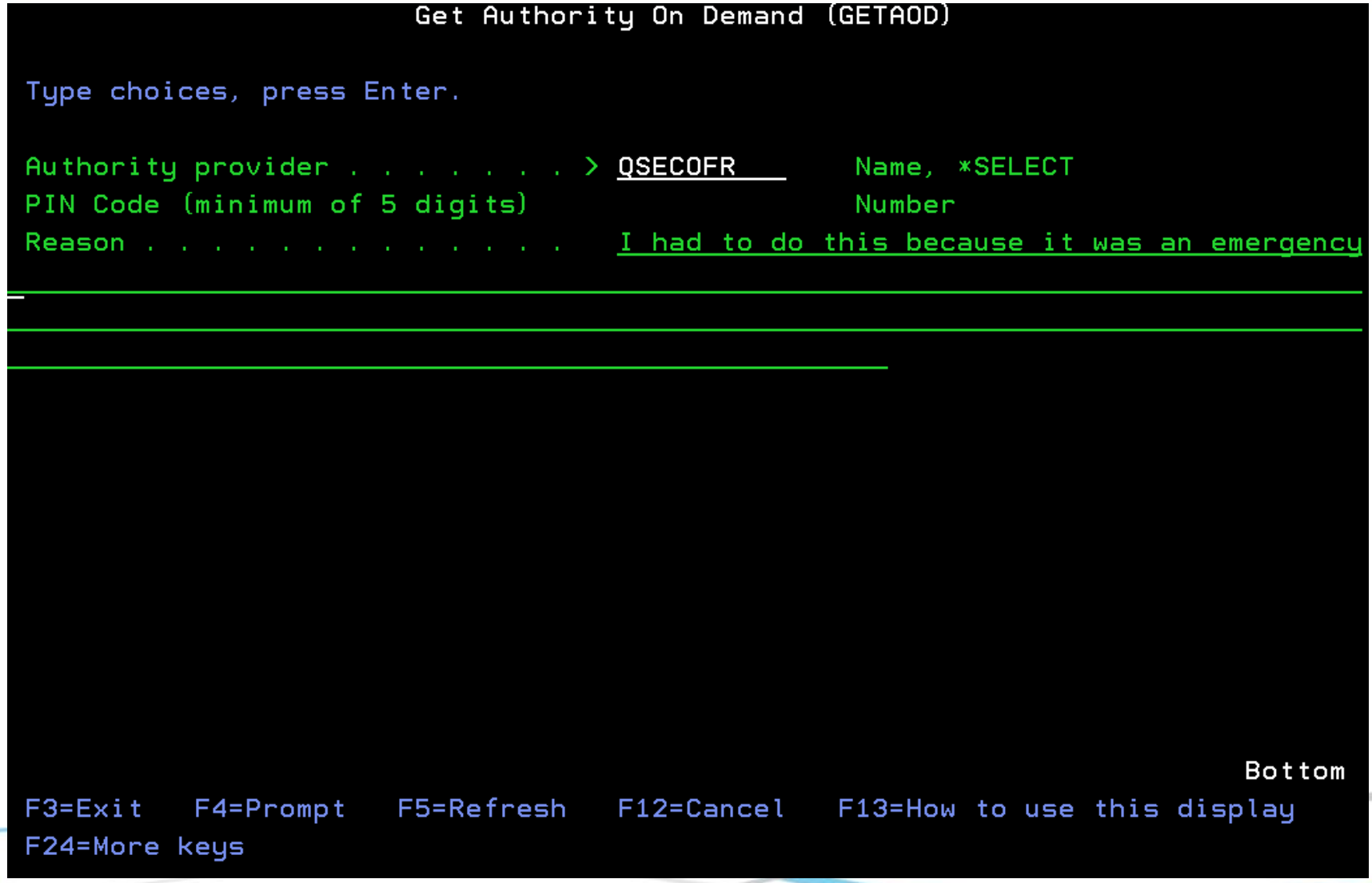

Modify Authority Provider
Authority Provider . . QSECOFR
Description . . . . . Security admin
Add libraries to *LIBL
On Get Authority:
Command to run before. DSPJOB
Command to run after . WRKSPLF
On Release Authority:
Command to run before. DSPJOB
Command to run after . WRKSPLF
Inform activity
To message queue . . . QSECOFR QUSRSYS MSGQ name-library
E-mail (mail,mail...). SCHENEY@SRCSECURESOLUTIONS.EU, SCHENEY@SRCAB.NL
F3=Exit F4=Prompt F12=Cancel

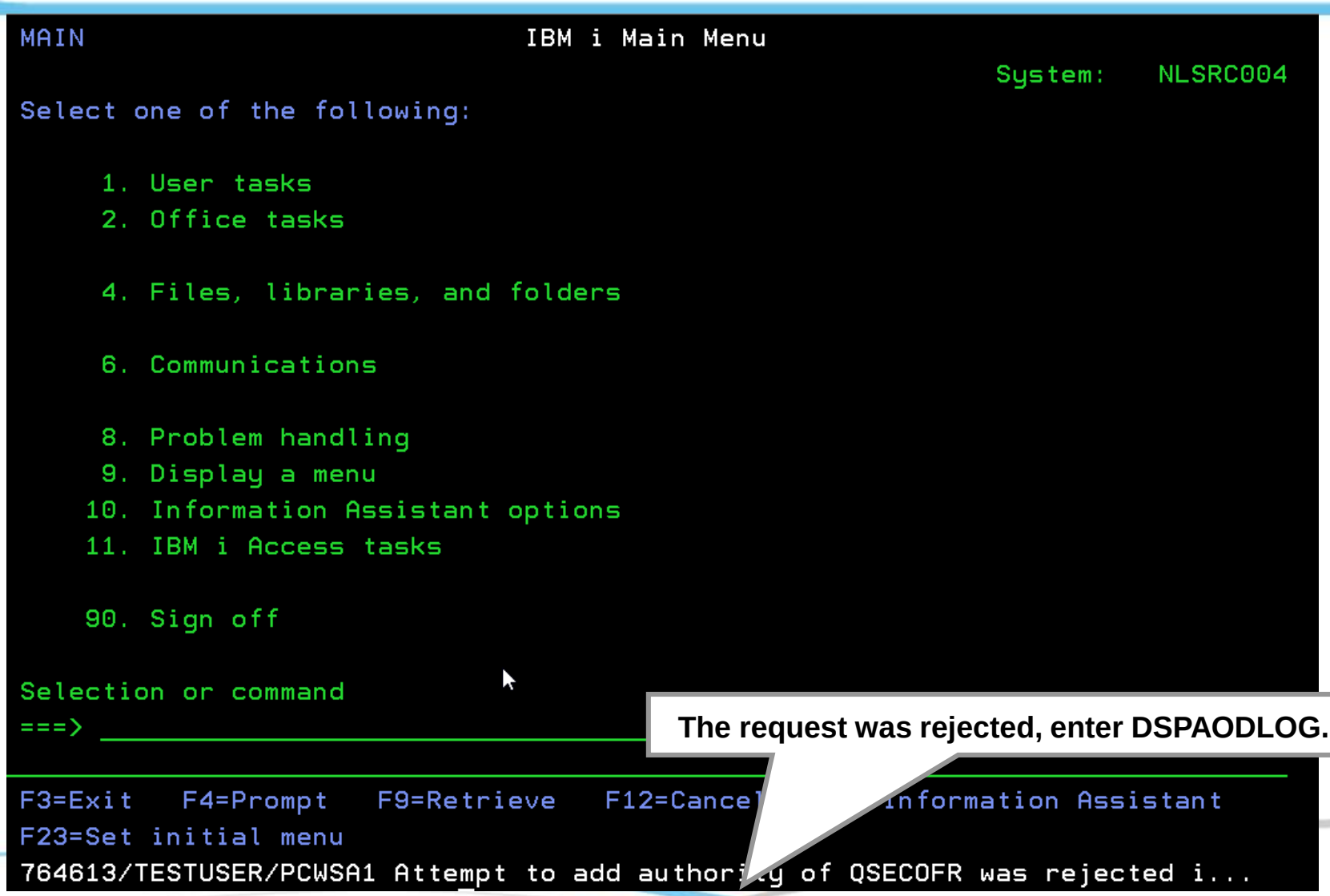

ODMENU
Authority On Demand
iSecurity
System: NLSRC004
Authority
1. Authority On Demand Rules
2. Authority On Demand Rules History
5. Authority Providers
6. Time Groups
Control
11. Activation
15. Display AOD Active Jobs DSPAODAU
Operations
31. Get Authority On Demand GETAOD
32. Display Authority On Demand DSPAOD
33. Release Authority On Demand RLSAOD
Log
41. Display Log
42. Print Log + Entered Commands
43. Print Log + Attachments
AUDIT Queries and Report Scheduler
51. Commands Entered in INT Jobs
52. Commands Entered in INT+Global
53. Commands Entered in AOD
54. Work with Queries
5. Work with Report Scheduler
ntenance
ystem Configuration
ntenance Menu
Support
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12
F13=Information Assistant F16=System main menu
Let's look at option 1, AOD rules.


Work with Authority Rules
Role in product .
Type options, press Enter.
Position to . . . _____
1=Select 3=Copy 4=Remove 5=Display
Subset . . . . . _____
9=Select for Export
Opt Provider Requester System Provide auth.by
_ CHENEY TESTUSER3 *ALL Add Add authority
_ QSECOFR *ANY *ALL Add test
_ QSECOFR CHENEY *ALL Add test
1 QSECOFR TESTUSER *ALL Add add Provider's authority
_ QSECOFR TESTUSER2 *ALL GlbSpc global add *SPCAUT
_ QSYSOPR TESTUSER *ALL Swap test swap
_ QSYSOPR TESTUSER2 *ALL Swap test swap
Bottom
You can define regular or Emergency rules. When needed, an authorized operator can enable or modify emergency rules.
F3=Exit F6=Add New F7=Add Emergency F8=Print F12=Cancel

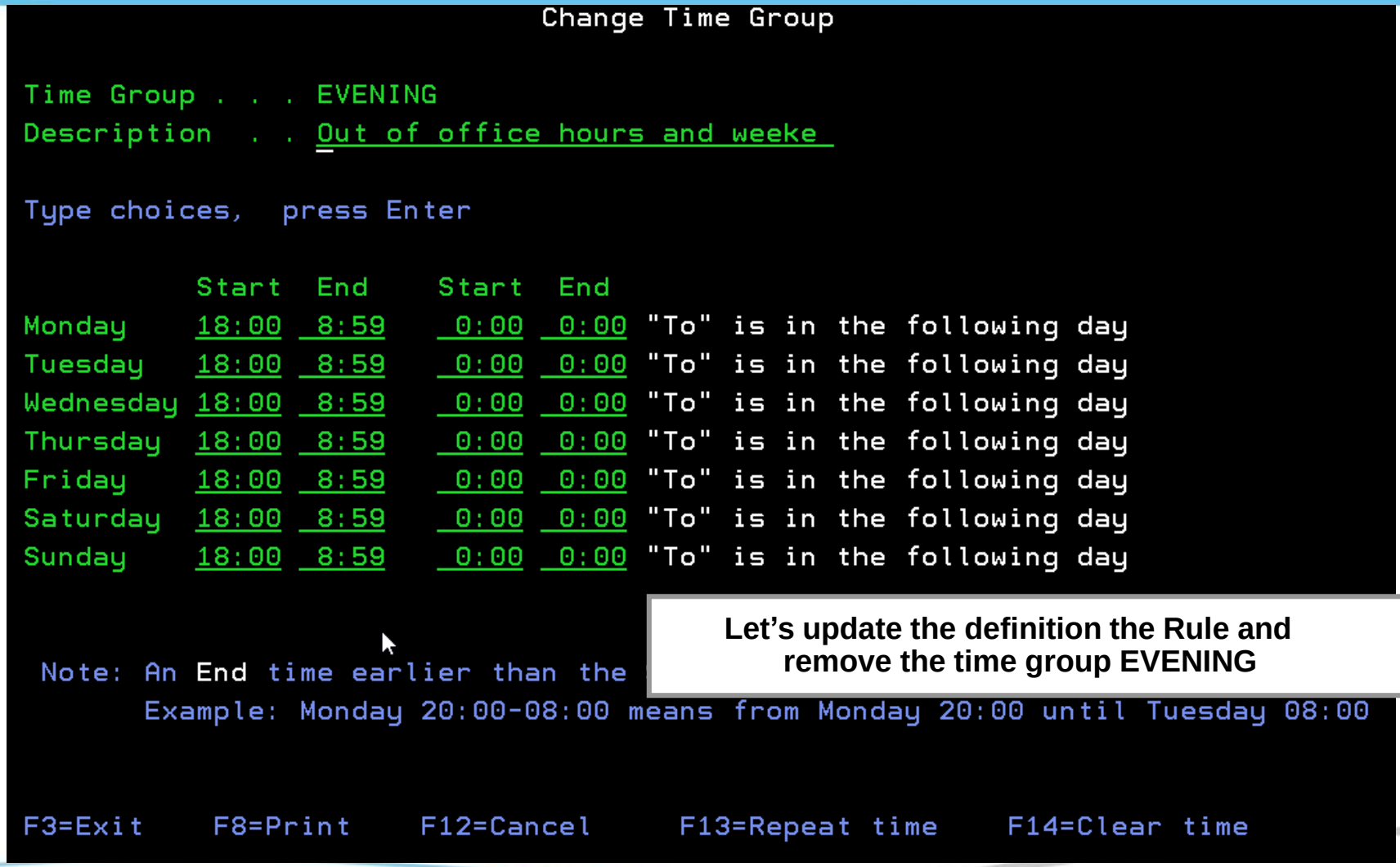

Screen 1/2 Modify Authority Rules
Requester (may be *ANY) . TESTUSER If *GRPPRF, accept for its members . N
Authority provider . . . . QSECOFR
System . . . . . *ALL Name, *ALL
Rule title . . . . . add Provider's authority
PIN Code . . . . . Left uses 98 98=Ignore PIN, 99=*NOMAX
Provide authority by . . . 1 By Session Globally
1=Add authority
2=Swap profile
3=Add *SPCAUT 9=Add *SPCAUT
Maximum work time . . . . 30 Minutes, 0=*NOMAX
Allow next use after . . . 0 Minutes, 0=Allow consecutive uses
N=Not
IP Address . . . . . Subnet mask:
Time group (week schedule) EVENING
Activity must begin . . . From: 1/01/01 0:00 To: 31/12/99 23:59
Send message to MsgQ . . . *PROVIDER
To E-mail (mail,mail...) . *PROVIDER
Last used by: TESTUSER 27/06/16 17:26 Job: PCWSA1/TESTUSER/764613
F3=Exit F4=Prompt F12=Cancel


Screen 2/2 Modify Authority Rules
Requester (may be *ANY) . TESTUSER If *GRPPRF, accept for its members . N
Authority provider . . . . QSECOFR
System . . . . *ALL Name, *ALL
Rule title . . . . . add Provider's authority
Intention of Rule
Reference Id . . . TESTUSER
Description/Reason This user is adding QSECOFR authority
During authority change, user auditing is maximized, Capture is started
and SYSLOG message is sent (based on product configuration).
F3=Exit F12=Cancel

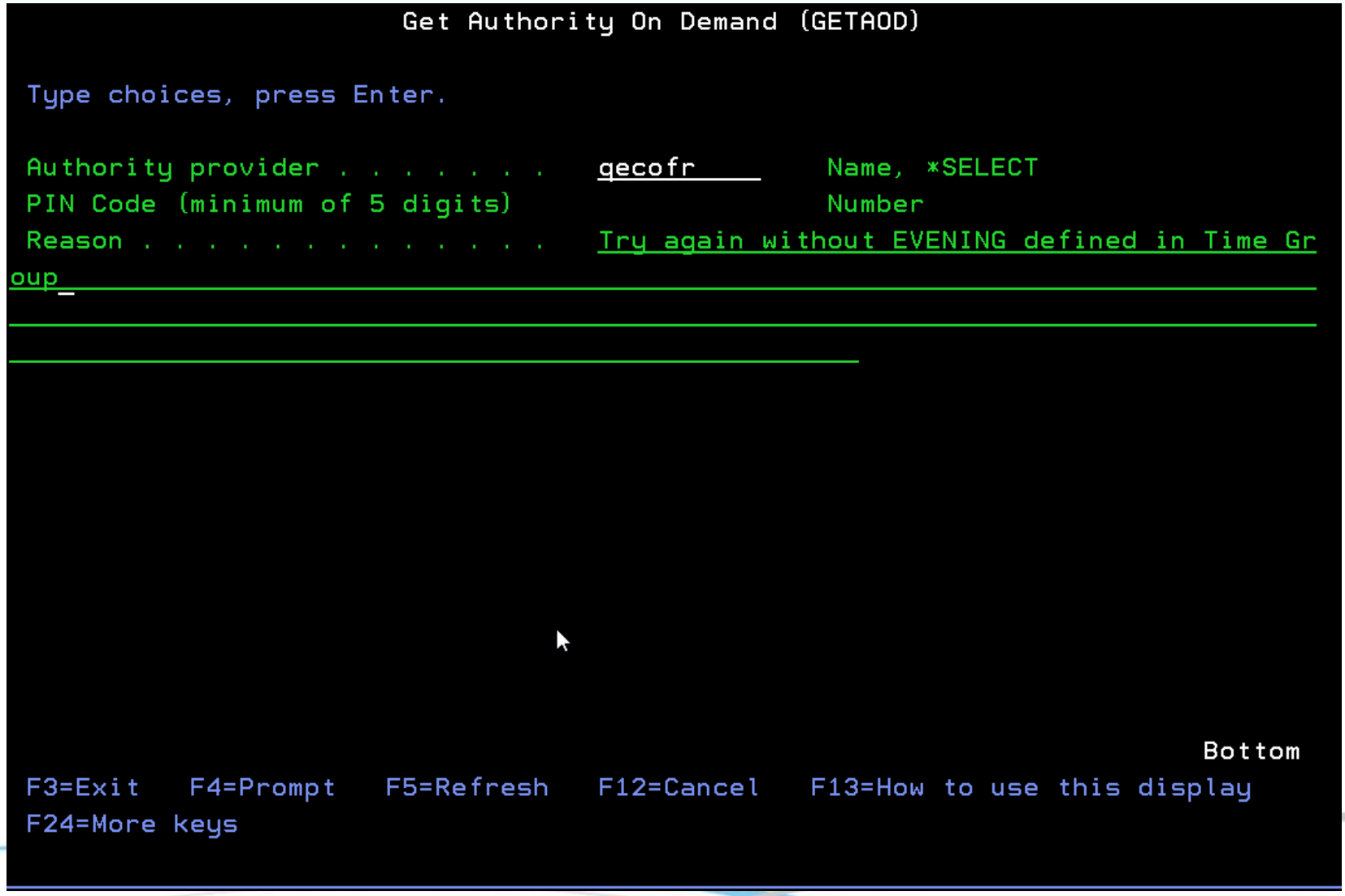

Get Authority On Demand (GETAOD)
Type choices, press Enter.
Authority provider . . . . . > QSECOFR
Name, *SELECT
PIN Code (minimum of 5 digits)
Number
Reason . . . . . I had to do this because it was an emergency
Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

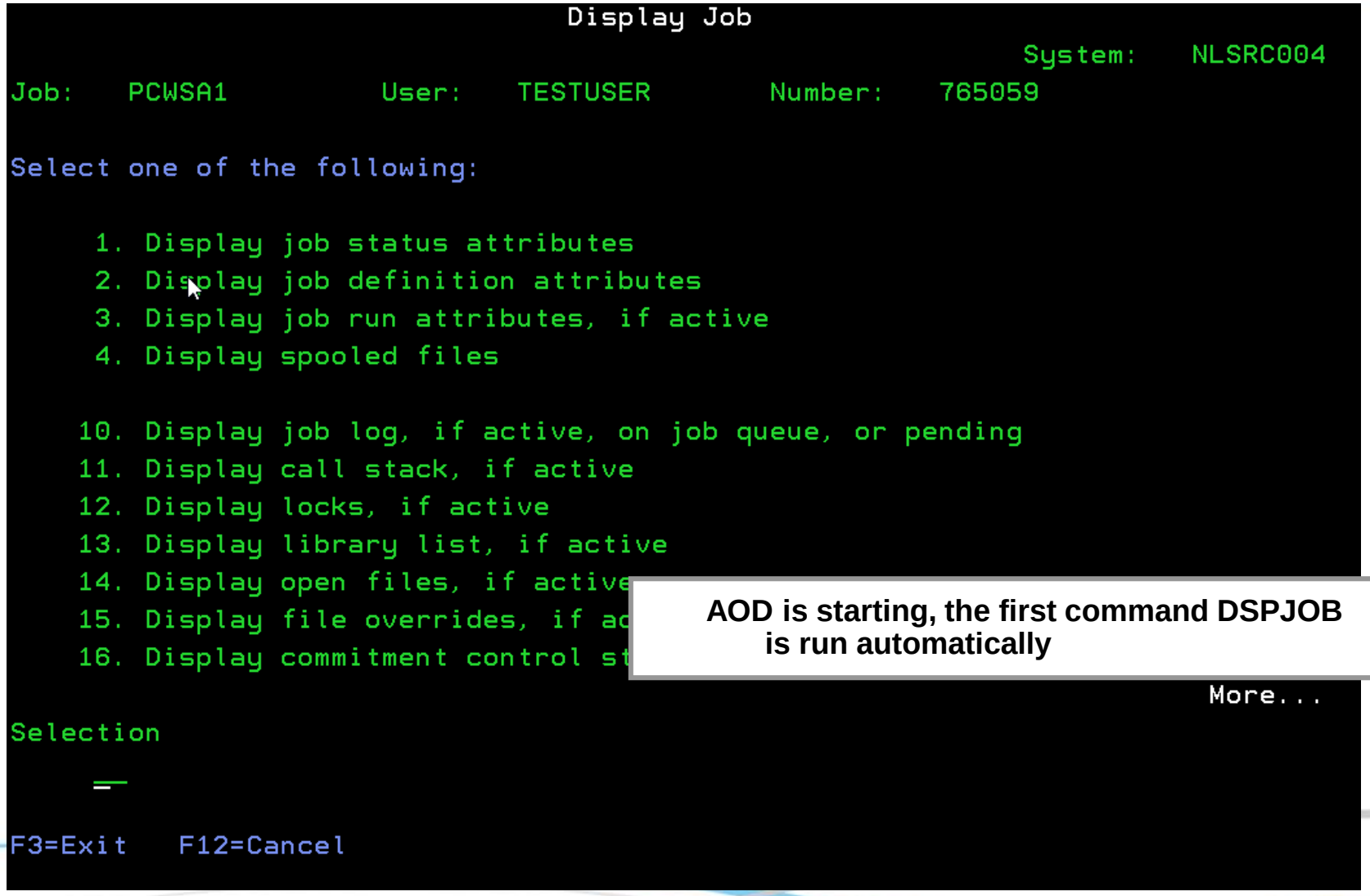

MAIN IBM i Main Menu
System: NLSRC004
Select one of the following:
1. User tasks
2. Office tasks
4. Files, libraries, and folders
6. Communications
8. Problem handling
9. Display a menu
10. Information Assistant options
11. IBM i Access tasks
90. Sign off
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12=Cancel
nformation Assistant
F23=Set initial menu
764613/TESTUSER/PCWSA1 Attempt to add authority of QSECOFR was rejected i...
The request was rejected, enter DSPAODLOG...


Additional Message Information System: NLSRC004
Message ID . . . . . : ODE4211 User profile . . . . . : TESTUSER
Date sent . . . . . : 27/06/16 Time sent . . . . . : 17:31:14
Job . . . . . : 764613/TESTUSER/PCWSA1
764613/TESTUSER/PCWSA1 Attempt to add authority of QSECOFR was rejected in NLSRC004. Rejected because of Time Group. IP address 192.168.100.83. Rule text: add Provider's authority. Reason: I had to do this because it was an emergency.
… because it was not requested during off hours.
F3=Exit F9=Tracing of activity F12=Cancel

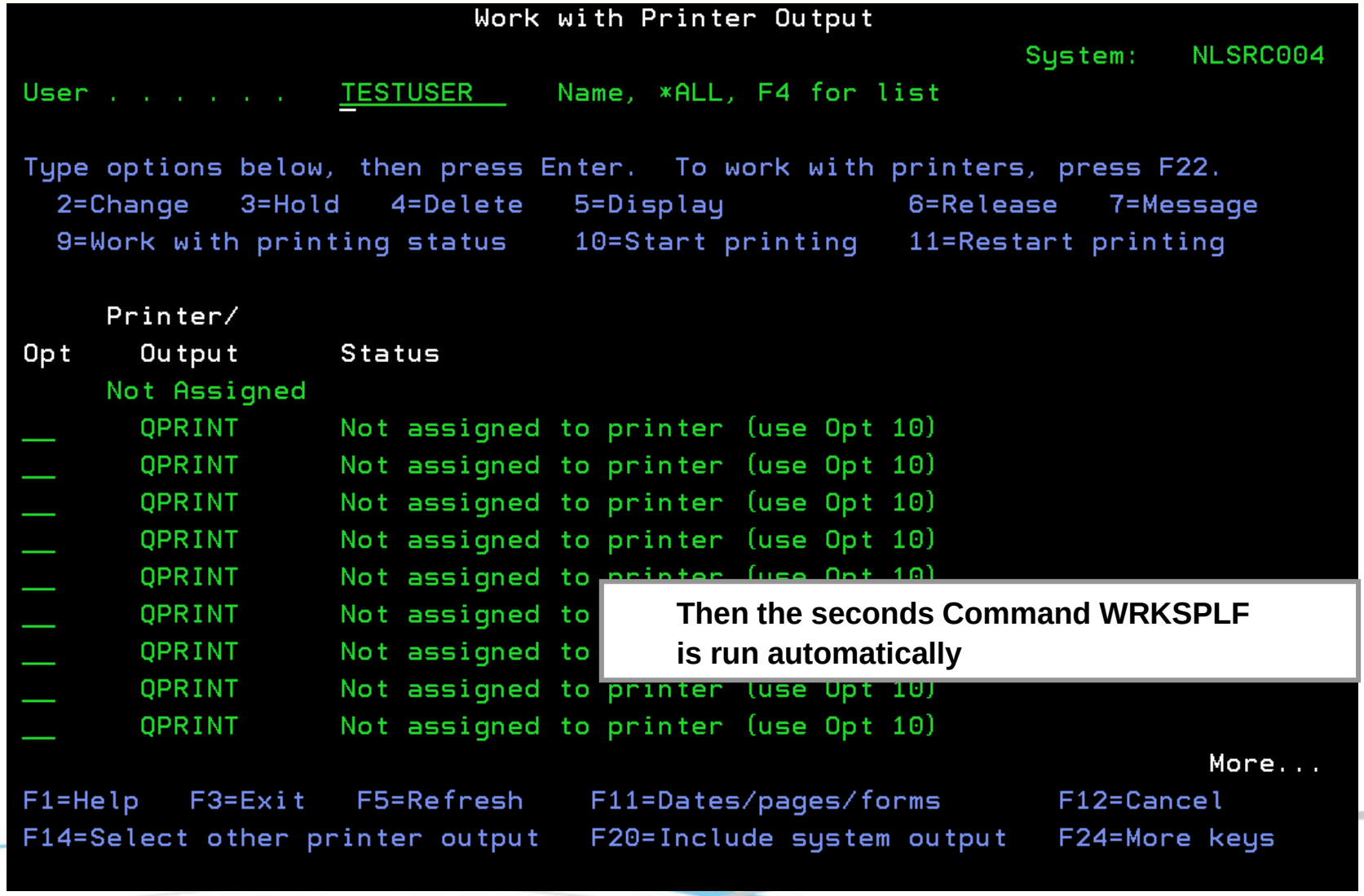


Let's update the definition the Rule and remove the time group EVENING

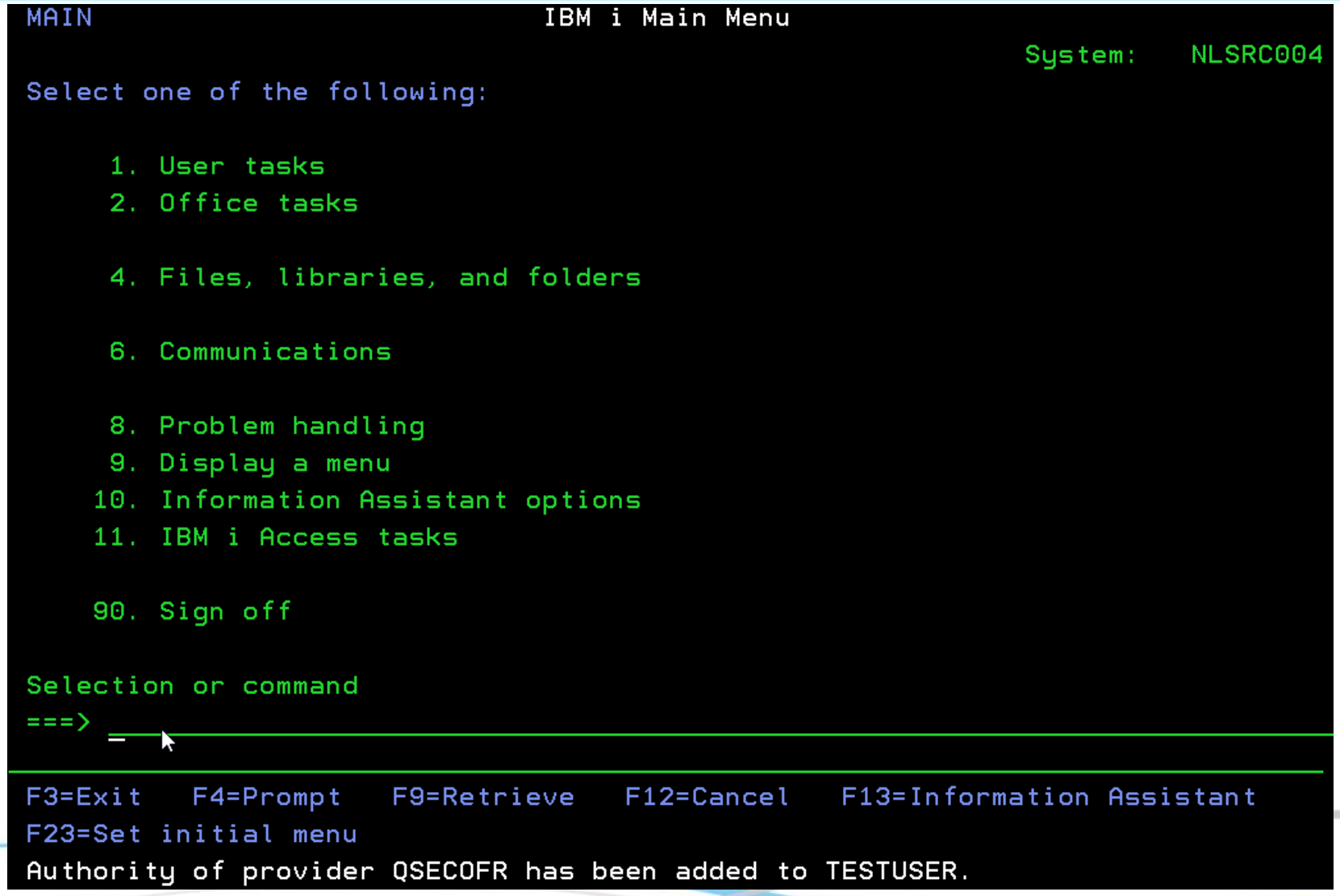

Get Authority On Demand (GETAOD)
Type choices, press Enter.
Authority provider . . . . . gecofr Name, *SELECT
PIN Code (minimum of 5 digits) Number
Reason . . . . . Try again without EVENING defined in Time Gr
oup
Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

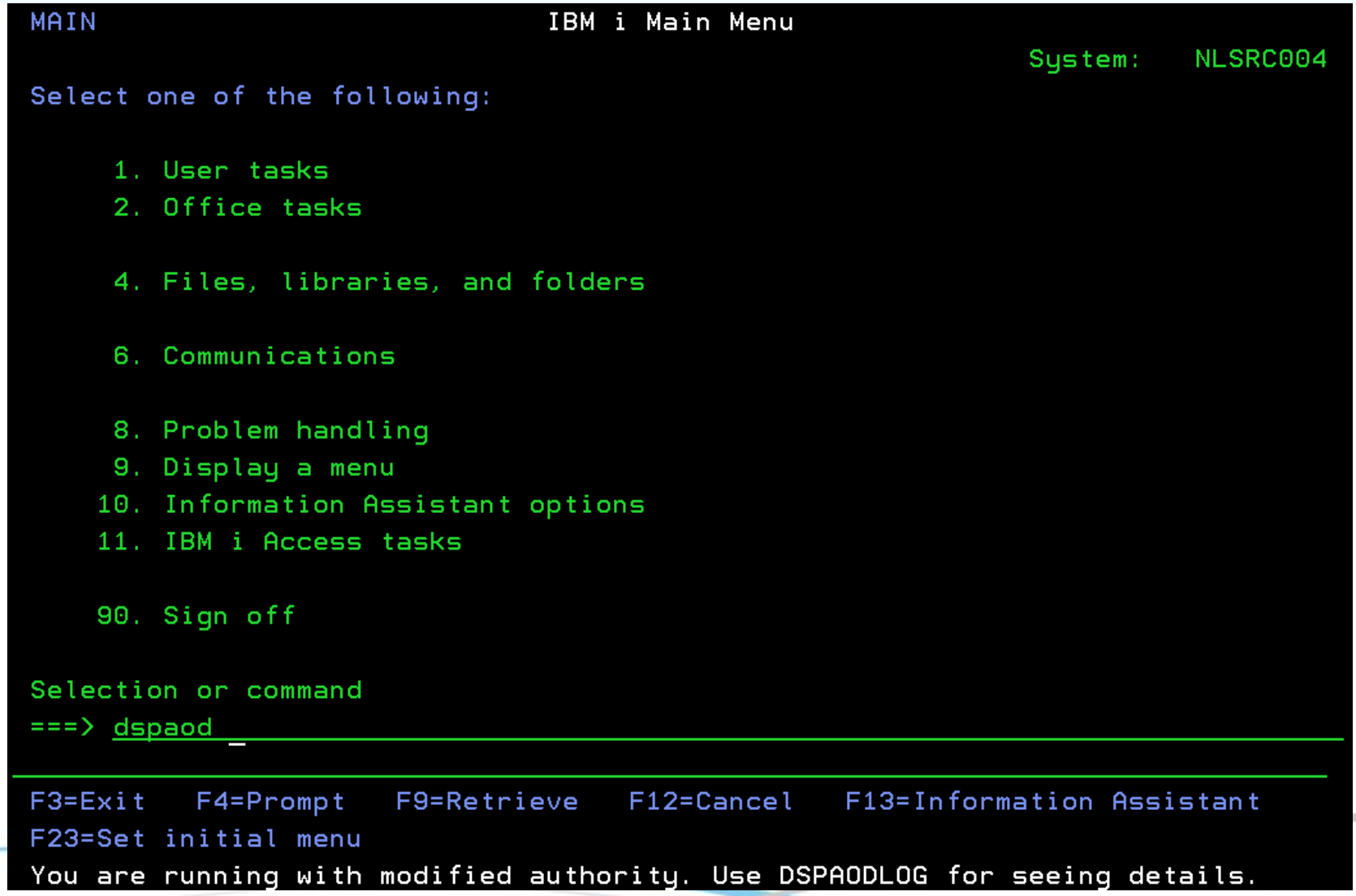


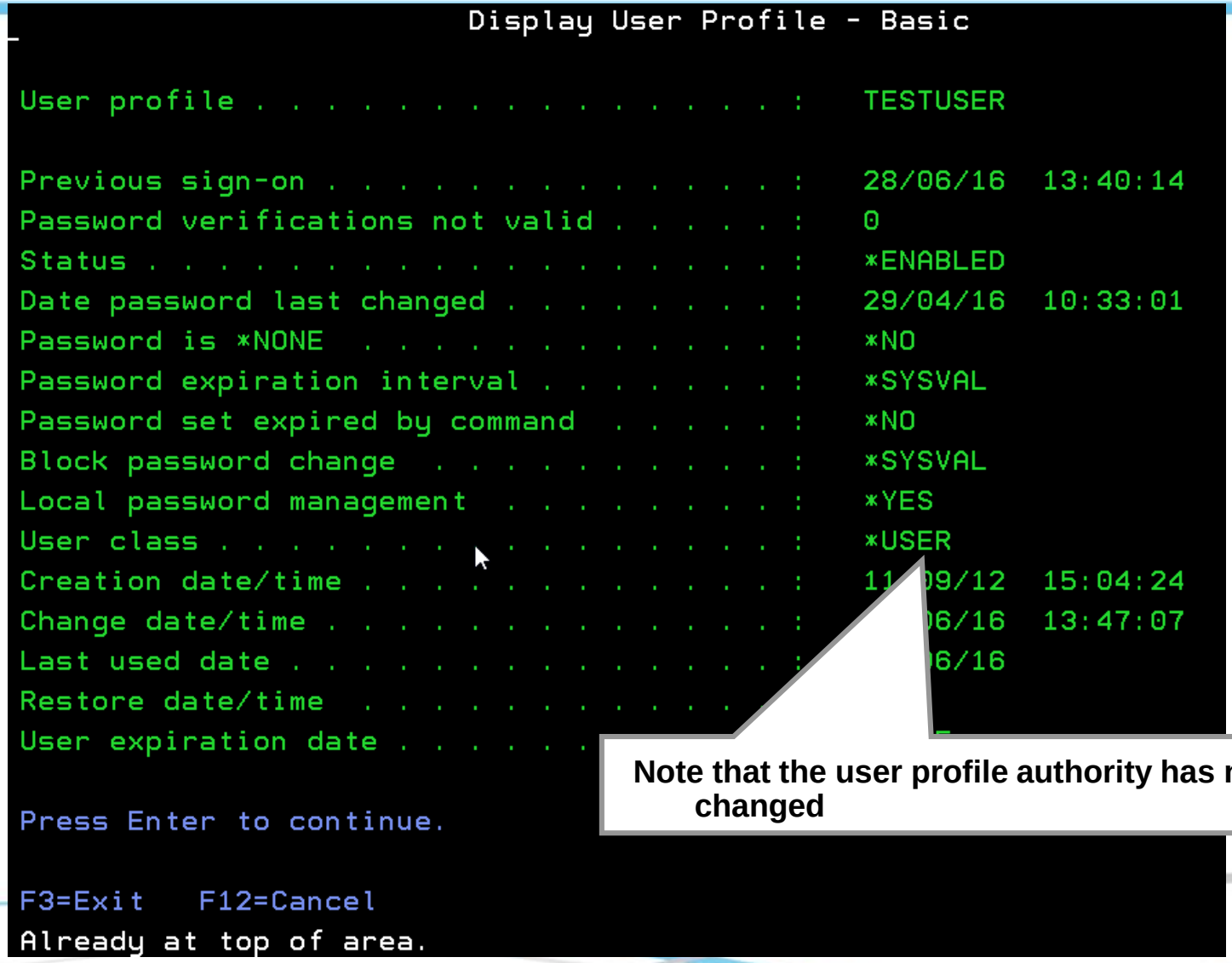
AOD is starting, the first command DSPJOB is run automatically

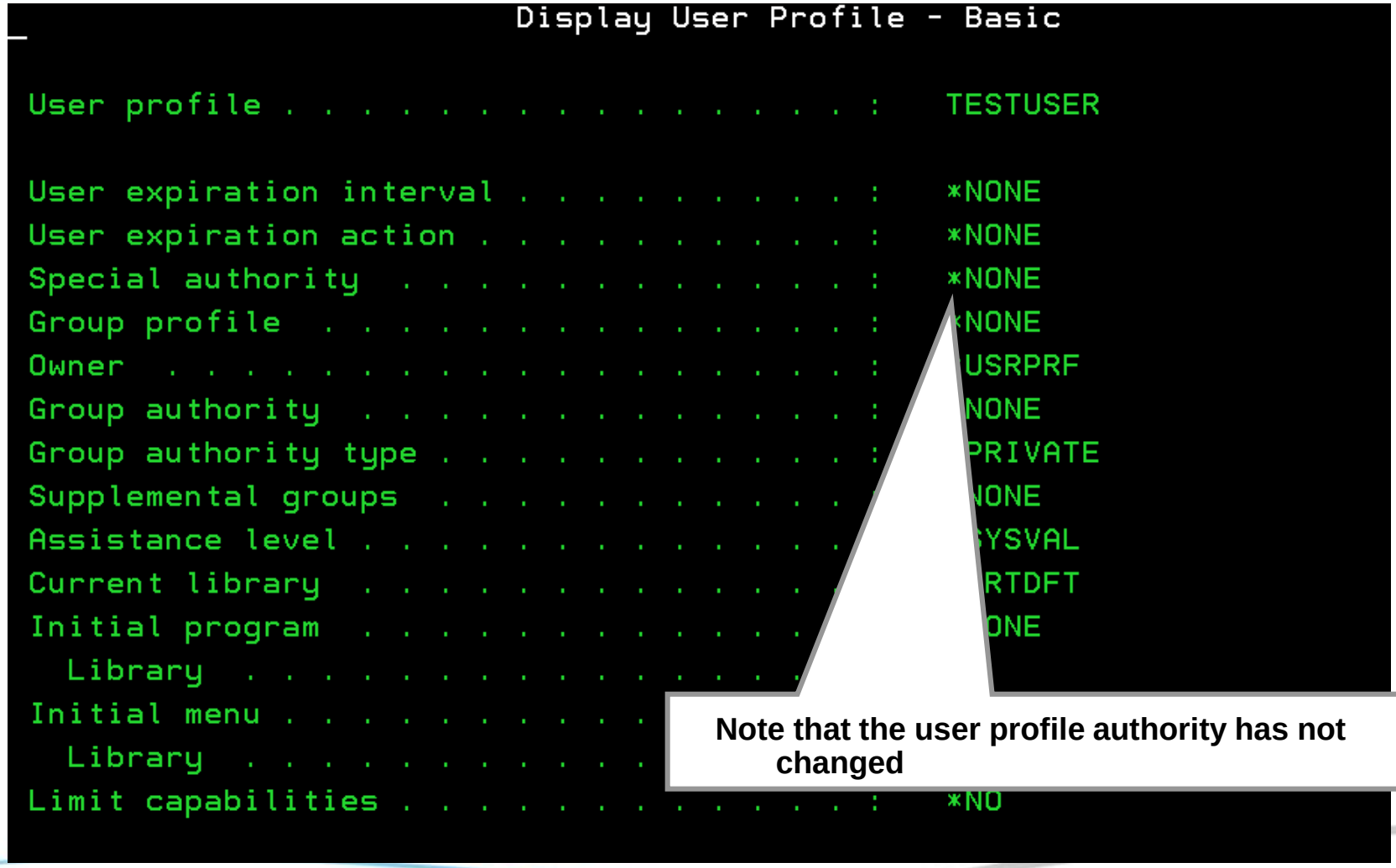


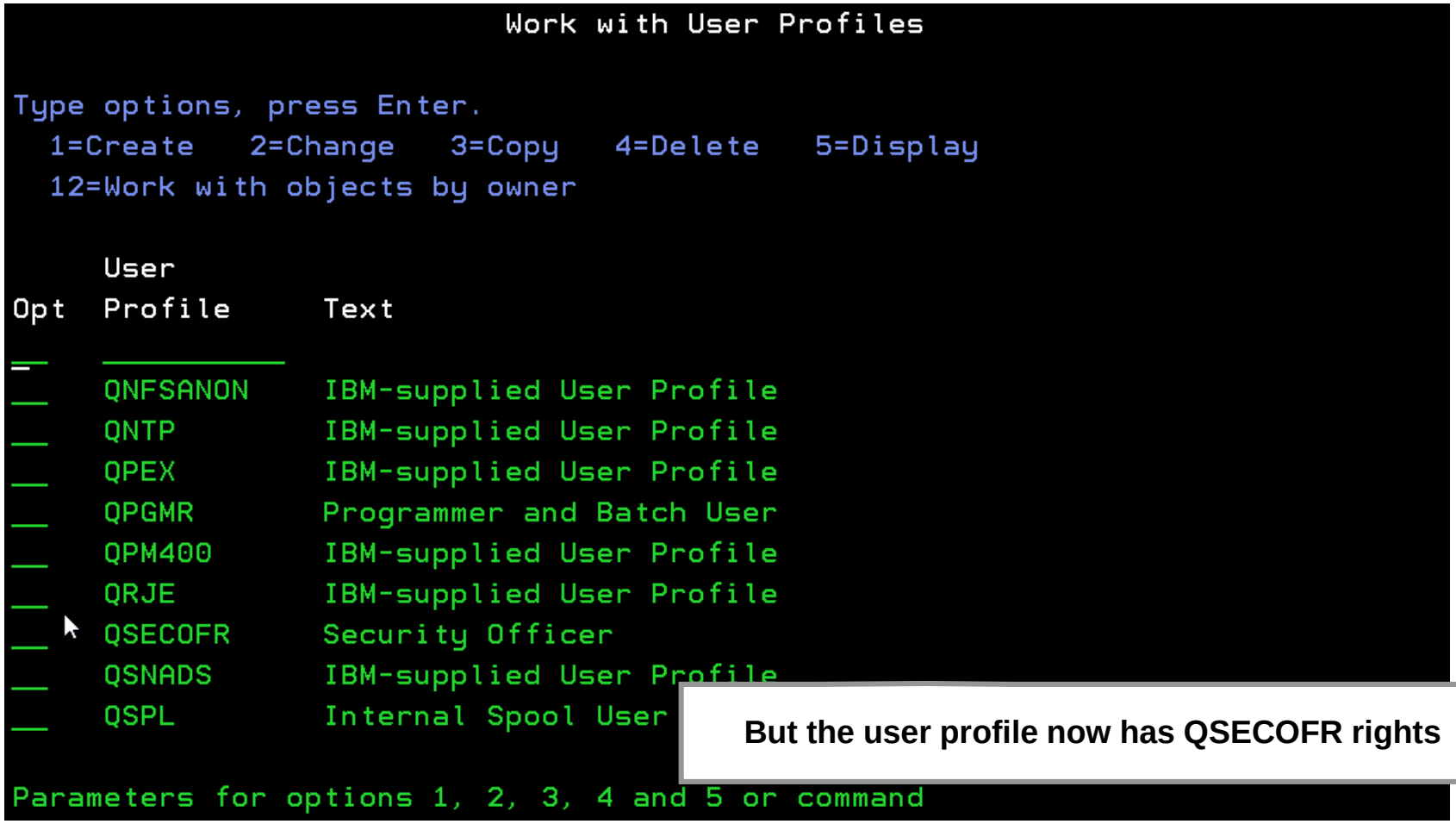
Then the seconds Command WRKSPLF is run automatically


MAIN
IBM i Main Menu
System: NLSRC004
Select one of the following:
1. User tasks
2. Office tasks
4. Files, libraries, and folders
6. Communications
8. Problem handling
9. Display a menu
10. Information Assistant options
11. IBM i Access tasks
90. Sign off
Selection or command
===>
F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant
F23=Set initial menu
Authority of provider QSECOFR has been added to TESTUSER.


MAIN IBM i Main Menu
System: NLSRC004
Select one of the following:
1. User tasks
2. Office tasks
4. Files, libraries, and folders
6. Communications
8. Problem handling
9. Display a menu
10. Information Assistant options
11. IBM i Access tasks
90. Sign off
Selection or command
===> dspaod
F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant
F23=Set initial menu
You are running with modified authority. Use DSPAODLOG for seeing details.


Display User Profile - Basic
User profile . . . . . : TESTUSER
Previous sign-on . . . . . : 28/06/16 13:40:14
Password verifications not valid . . . . . : 0
Status . . . . . : *ENABLED
Date password last changed . . . . . : 29/04/16 10:33:01
Password is *NONE . . . . . : *NO
Password expiration interval . . . . . : *SYSVAL
Password set expired by command . . . . . : *NO
Block password change . . . . . : *SYSVAL
Local password management . . . . . : *YES
User class . . . . . : *USER
Creation date/time . . . . . : 11 09/12 15:04:24
Change date/time . . . . . : 06/16 13:47:07
Last used date . . . . . : 06/16
Restore date/time . . . . . :
User expiration date . . . . . :
Press Enter to continue.
F3=Exit F12=Cancel
Already at top of area.
Note that the user profile authority has not changed


Display User Profile - Basic
User profile . . . . . : TESTUSER
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *NONE
Group profile . . . . . : *NONE
Owner . . . . . : USRPRF
Group authority . . . . . : NONE
Group authority type . . . . . : PRIVATE
Supplemental groups . . . . . : NONE
Assistance level . . . . . : SYSVAL
Current library . . . . . : RTDFT
Initial program . . . . . : ONE
Library . . . . . :
Initial menu . . . . . :
Library . . . . . :
Limit capabilities . . . . . : *NO
Note that the user profile authority has not changed



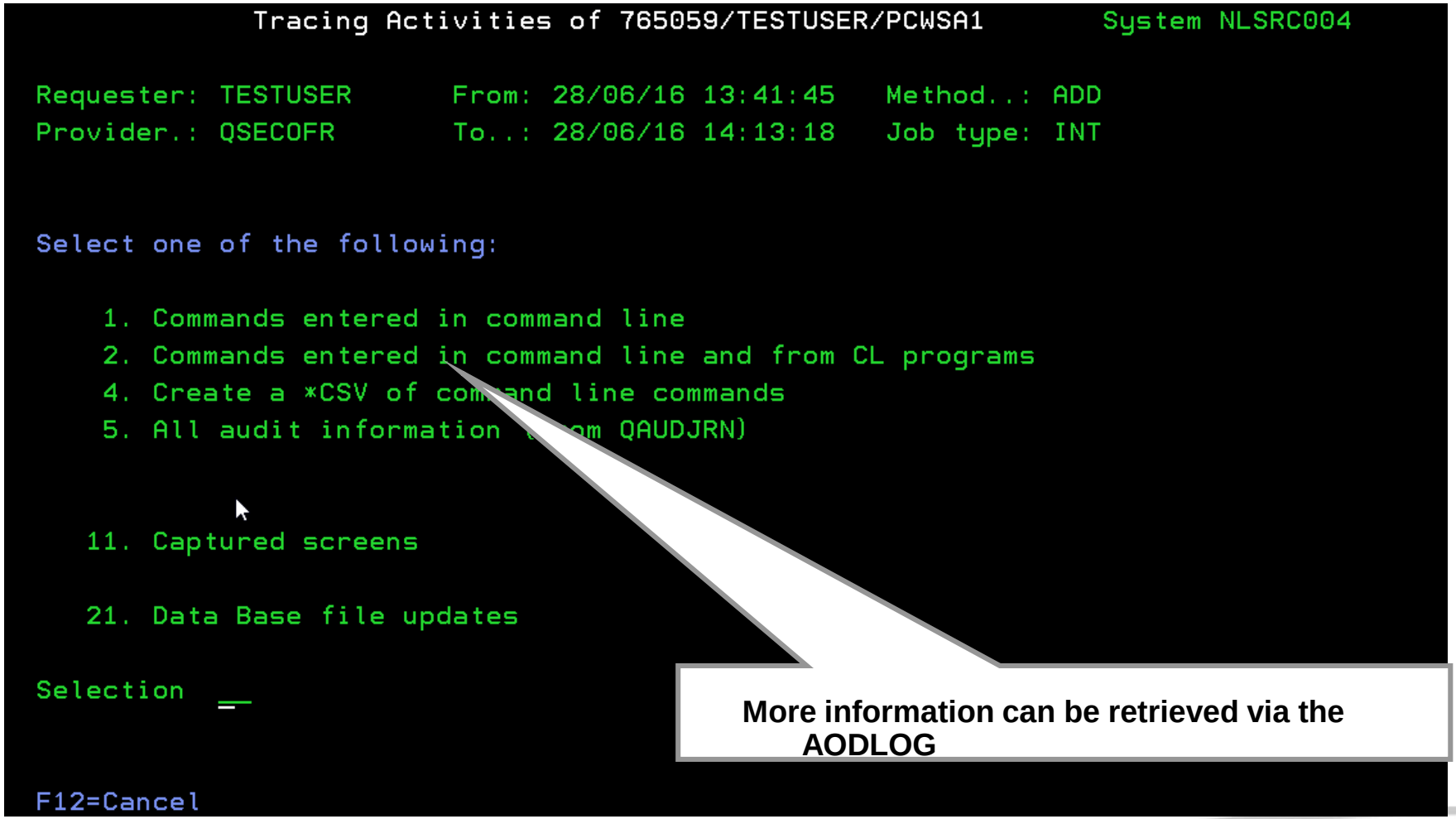
But the user profile now has QSECOFR rights

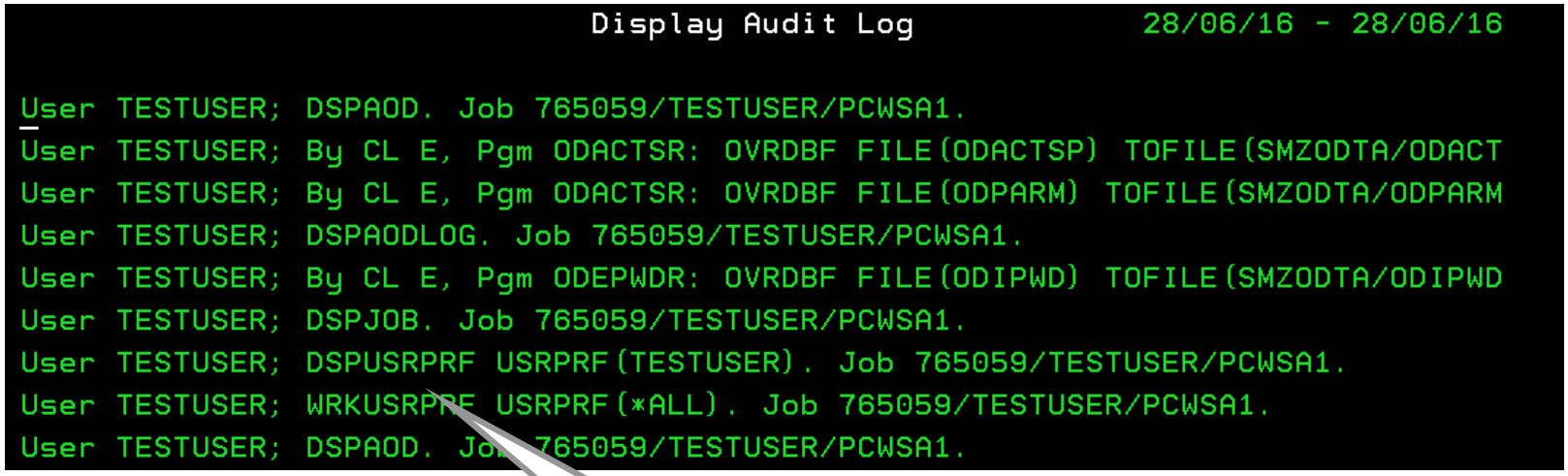
28/06/16 13:41:45 765059/TESTUSER/PCWSA1 Start add authority of QSECOFR in NLSRC004.
IP address 192.168.100.83. Rule text: add Provider's authority. Reason: Try again
without EVENING defined in Time Group.

```
Message ID . . . . . :   ODE4001
Date sent  . . . . . :   28/06/16      Time sent  . . . . . :   13:45:00

Message . . . . :   765059/TESTUSER/PCWSA1 Start add authority of QSECOFR in
  NLSRC004.

28/06/16 13:41:45 765059/TESTUSER/PCWSA1 Start add authority of QSECOFR in
  NLSRC004. IP address 192.168.100.83. Rule text: add Provider's authority.
  Reason: Try again without EVENING defined in Time Group.
```

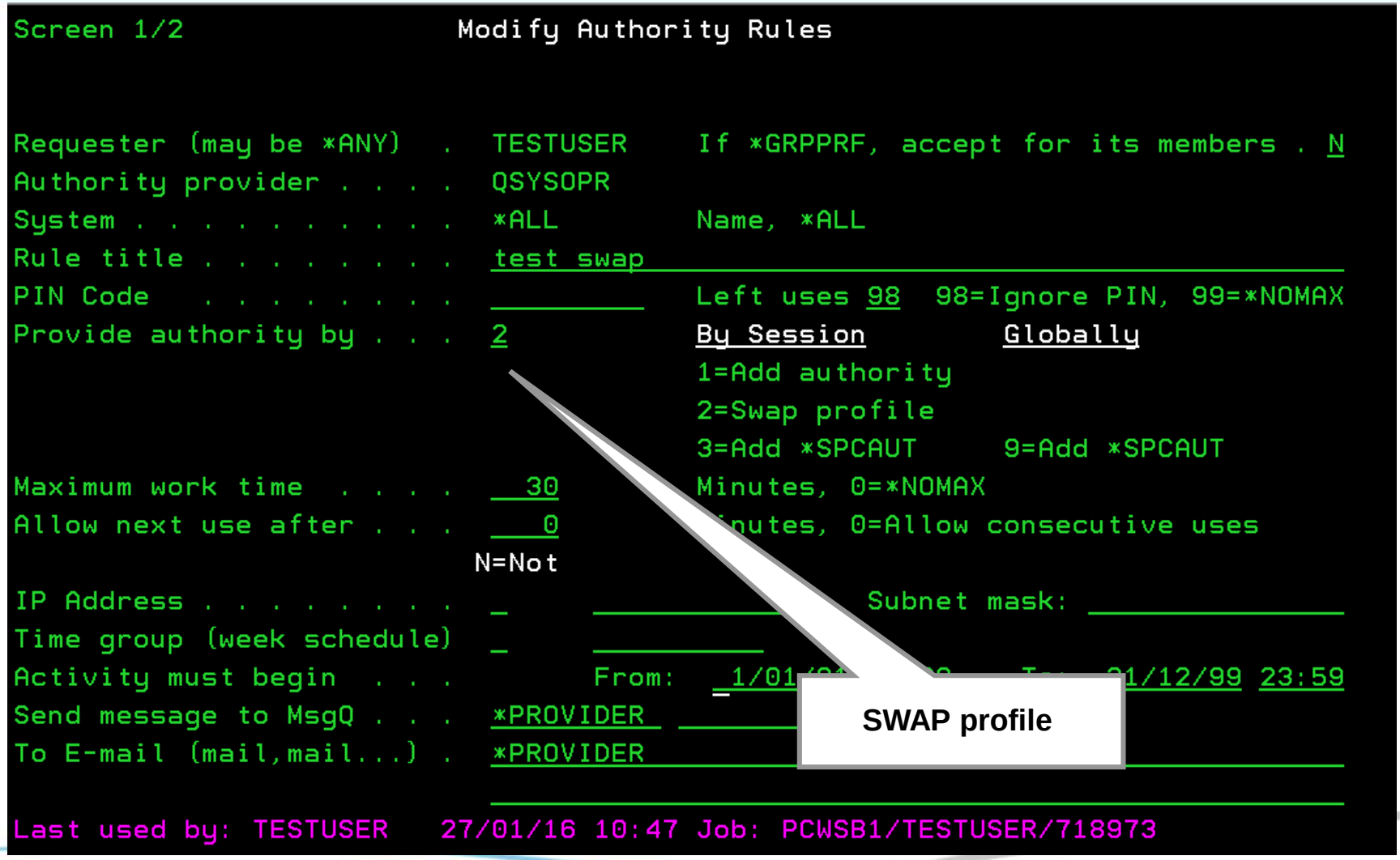
```
                    Display Authority on Demand Log     28/06/16 - 28/06/16

765059/TESTUSER/PCWSA1 Start add authority of QSECOFR in NLSRC004.
765059/TESTUSER/PCWSA1 End add authority
```

Reporting, an email is sent, a message is sent, a log is written

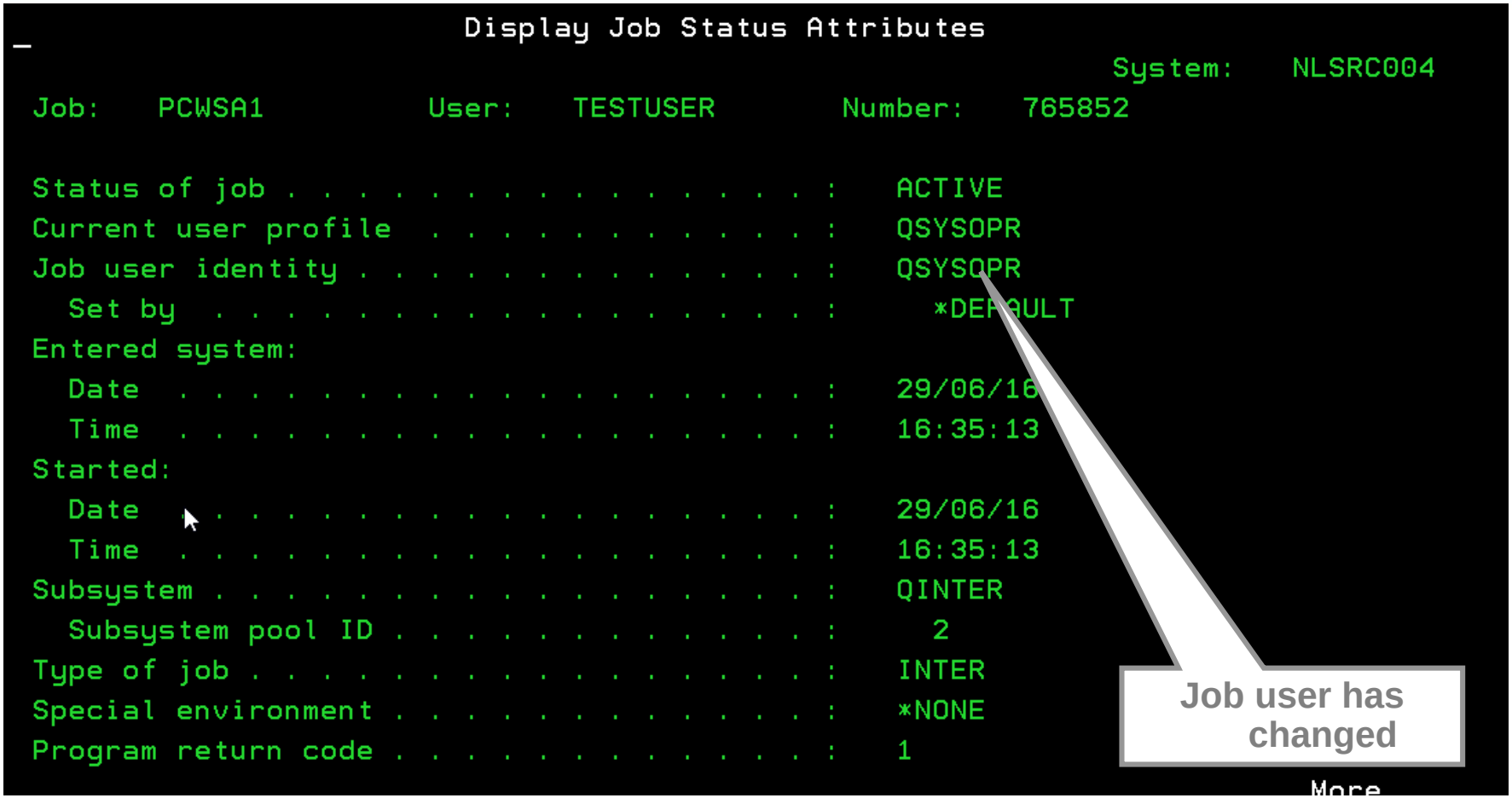

Tracing Activities of 765059/TESTUSER/PCWSA1 System NLSRC004
Requester: TESTUSER From: 28/06/16 13:41:45 Method..: ADD
Provider.: QSECOFR To..: 28/06/16 14:13:18 Job type: INT
Select one of the following:
1. Commands entered in command line
2. Commands entered in command line and from CL programs
4. Create a *CSV of command line commands
5. All audit information (from QAUDJRN)
11. Captured screens
21. Data Base file updates
Selection
F12=Cancel
More information can be retrieved via the AODLOG



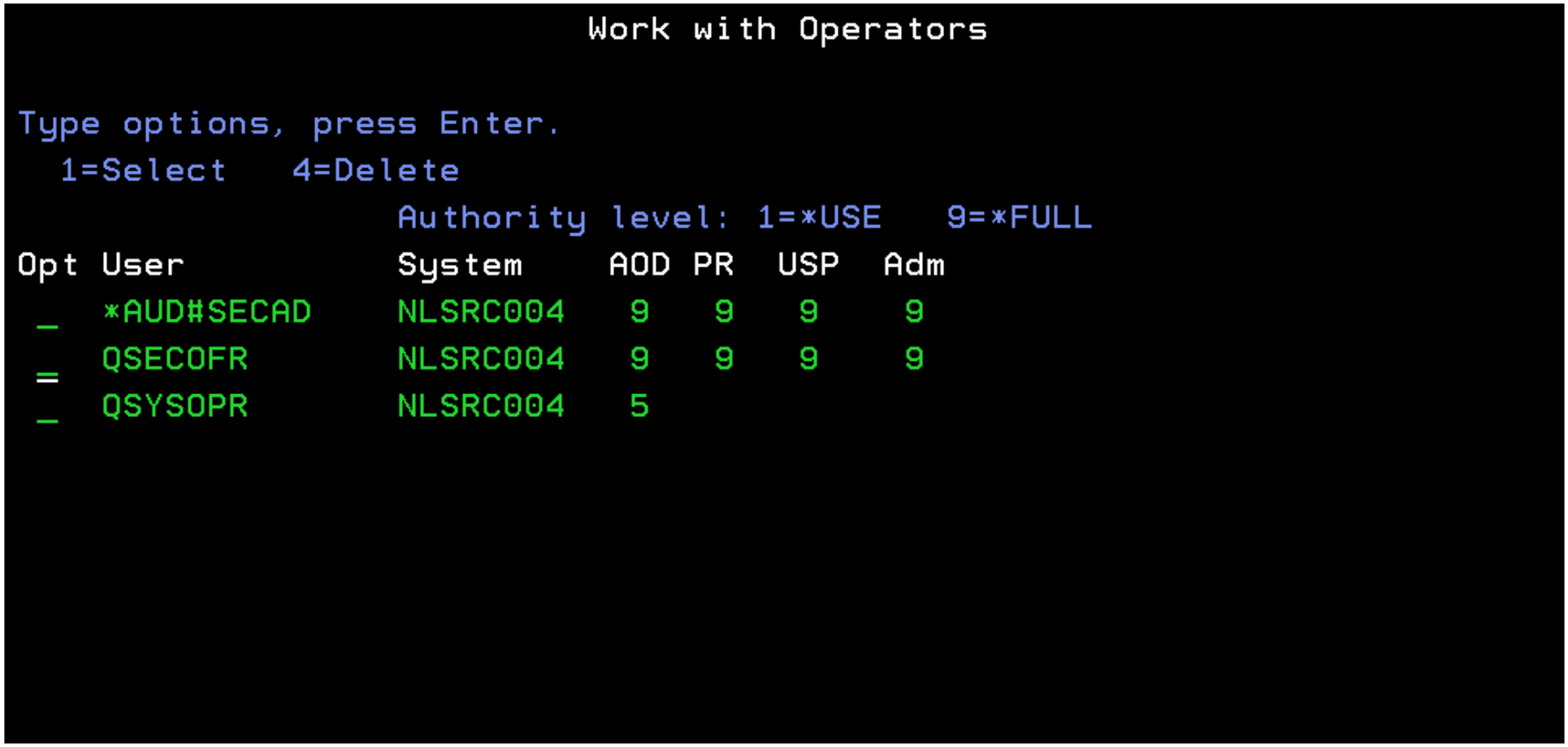
More information can be retrieved via the AODLOG

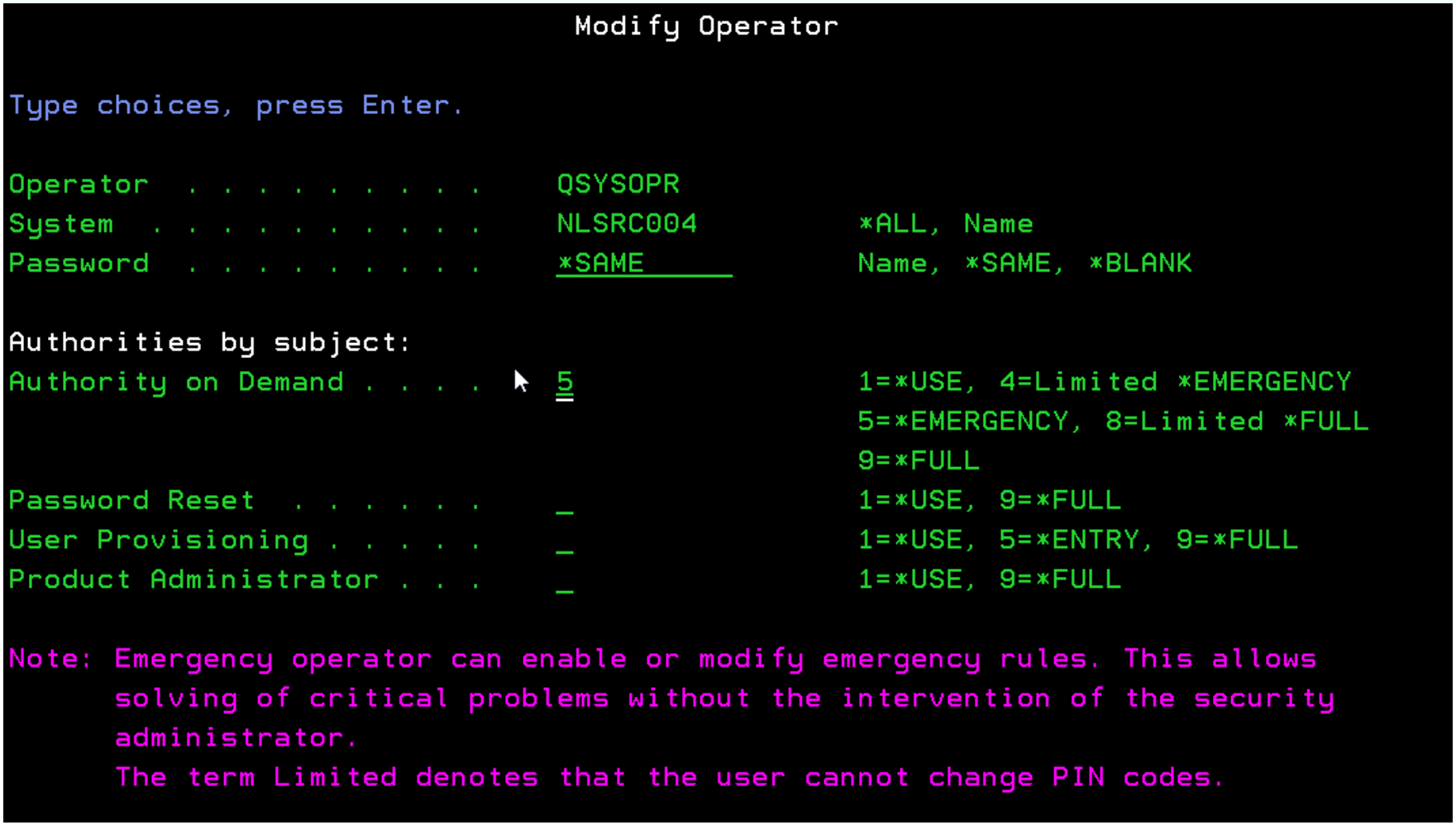

Screen 1/2 Modify Authority Rules
Requester (may be *ANY) . TESTUSER If *GRPPRF, accept for its members . N
Authority provider . . . . QSYSOPR
System . . . . . *ALL Name, *ALL
Rule title . . . . . test swap
PIN Code . . . . . Left uses 98 98=Ignore PIN, 99=*NOMAX
Provide authority by . . . 2 By Session Globally
1=Add authority
2=Swap profile
3=Add *SPCAUT 9=Add *SPCAUT
Maximum work time . . . . 30 Minutes, 0=*NOMAX
Allow next use after . . . 0 inutes, 0=Allow consecutive uses
N=Not
IP Address . . . . . Subnet mask:
Time group (week schedule)
Activity must begin . . . From: 1/01 1/12/99 23:59
Send message to MsgQ . . . *PROVIDER
To E-mail (mail,mail...) . *PROVIDER
Last used by: TESTUSER 27/01/16 10:47 Job: PCWSB1/TESTUSER/718973
SWAP profile

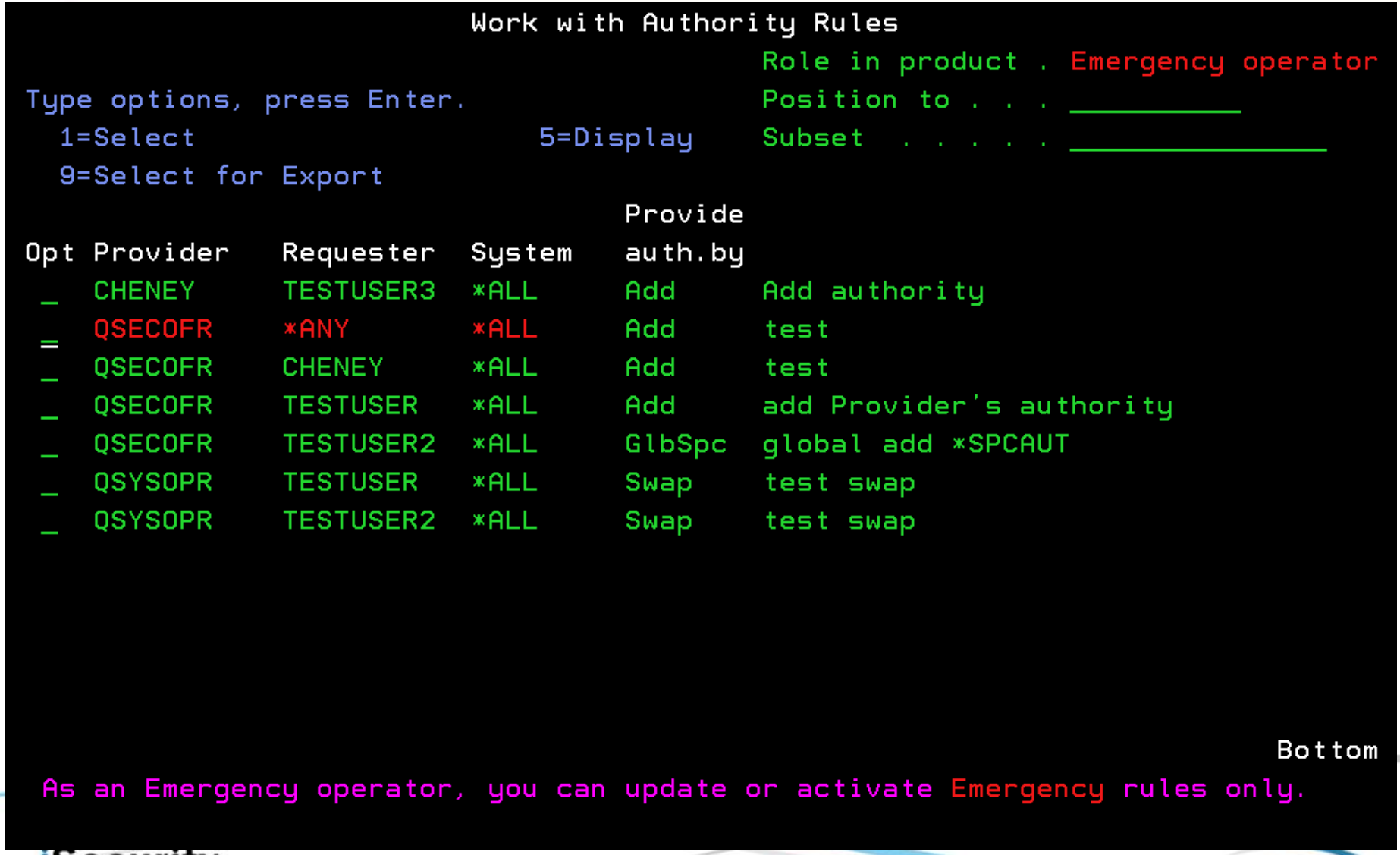

Get Authority On Demand (GETAOD)
Type choices, press Enter.
Authority provider . . . . . qsysopr Name, *SELECT
PIN Code (minimum of 5 digits) Number
Reason . . . . . *BYPIN


Display Job Status Attributes
System: NLSRC004
Job: PCWSA1 User: TESTUSER Number: 765852
Status of job . . . . . : ACTIVE
Current user profile . . . . . : QSYSOPR
Job user identity . . . . . : QSYSOPR
Set by . . . . . : *DEFAULT
Entered system:
Date . . . . . : 29/06/16
Time . . . . . : 16:35:13
Started:
Date . . . . . : 29/06/16
Time . . . . . : 16:35:13
Subsystem . . . . . : QINTER
Subsystem pool ID . . . . . : 2
Type of job . . . . . : INTER
Special environment . . . . . : *NONE
Program return code . . . . . : 1
More
Job user has changed

Provide authority by	Description
1 = Add	**Current user** = Requester **Object authorities** = Added ***SPCAUT** = Added ***USRCLS** = No change **LMTCPB( )** = No change Operating System restraints do not allow for changes to the USRCLS or LMTCPB
2 = Swap	**Current user** = Provider **Object authorities** = Provider ***SPCAUT** = Provider ***USRCLS** = Provider **LMTCPB( )** = Provider
3 = Add SPC	**Current user** = Requester **Object authorities** = No Change ***SPCAUT** = Added ***USRCLS** = No change **LMTCPB( )** = No change Operating System restraints do not allow for changes to the USRCLS or LMTCPB
9 = Add SPC Globally	**Current user** = Requester **Object authorities** = Added ***SPCAUT** = Added ***USRCLS** = Provider **LMTCPB( )** = Provider


Work with Operators
Type options, press Enter.
1=Select 4=Delete
Authority level: 1=*USE 9=*FULL
Opt User System AOD PR USP Adm
_ *AUD#SECAD NLSRC004 9 9 9 9
_ QSECOFR NLSRC004 9 9 9 9
_ QSYSOPR NLSRC004 5


Modify Operator
Type choices, press Enter.
Operator . . . . . QSYSOPR
System . . . . . NLSRC004 *ALL, Name
Password . . . . . *SAME Name, *SAME, *BLANK
Authorities by subject:
Authority on Demand . . . . 5 1=*USE, 4=Limited *EMERGENCY
5=*EMERGENCY, 8=Limited *FULL
9=*FULL
Password Reset . . . . . _ 1=*USE, 9=*FULL
User Provisioning . . . . . _ 1=*USE, 5=*ENTRY, 9=*FULL
Product Administrator . . . _ 1=*USE, 9=*FULL
Note: Emergency operator can enable or modify emergency rules. This allows
solving of critical problems without the intervention of the security
administrator.
The term Limited denotes that the user cannot change PIN codes.


Work with Authority Rules
Role in product . Emergency operator
Type options, press Enter.
Position to . . . _____
1=Select
5=Display
Subset . . . . . _____
9=Select for Export
Opt Provider Requester System Provide auth.by
_ CHENEY TESTUSER3 *ALL Add Add authority
= QSECOFR *ANY *ALL Add test
_ QSECOFR CHENEY *ALL Add test
_ QSECOFR TESTUSER *ALL Add add Provider's authority
_ QSECOFR TESTUSER2 *ALL GlbSpc global add *SPCAUT
_ QSYSOPR TESTUSER *ALL Swap test swap
_ QSYSOPR TESTUSER2 *ALL Swap test swap
Bottom
As an Emergency operator, you can update or activate Emergency rules only.

Thank You!

Please visit us at
www.srcsecuresolutions.eu

SRC
Secure Solutions