SEA™

SOFTWARE ENGINEERING OF AMERICA®

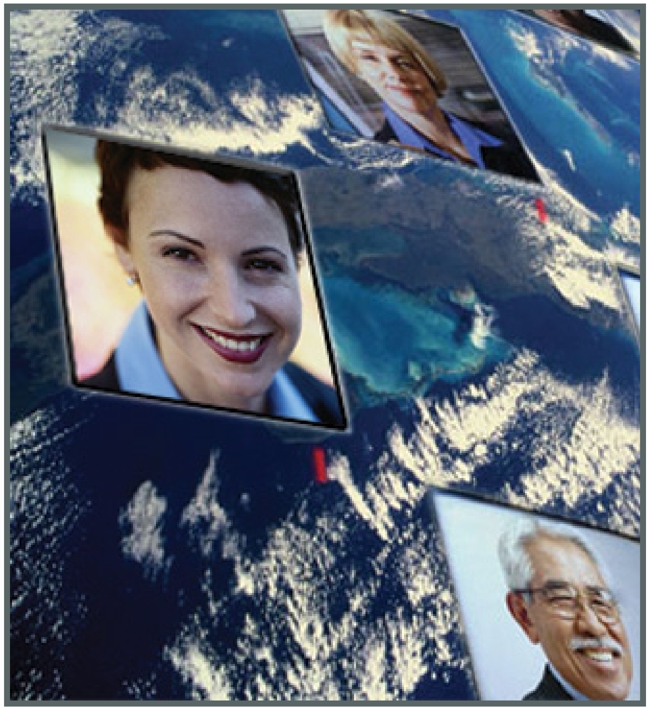
www.seasoft.com

Assessing
Your Security on the Power i

iSecurity
System i Security Solutions

Company Overview

Company Overview

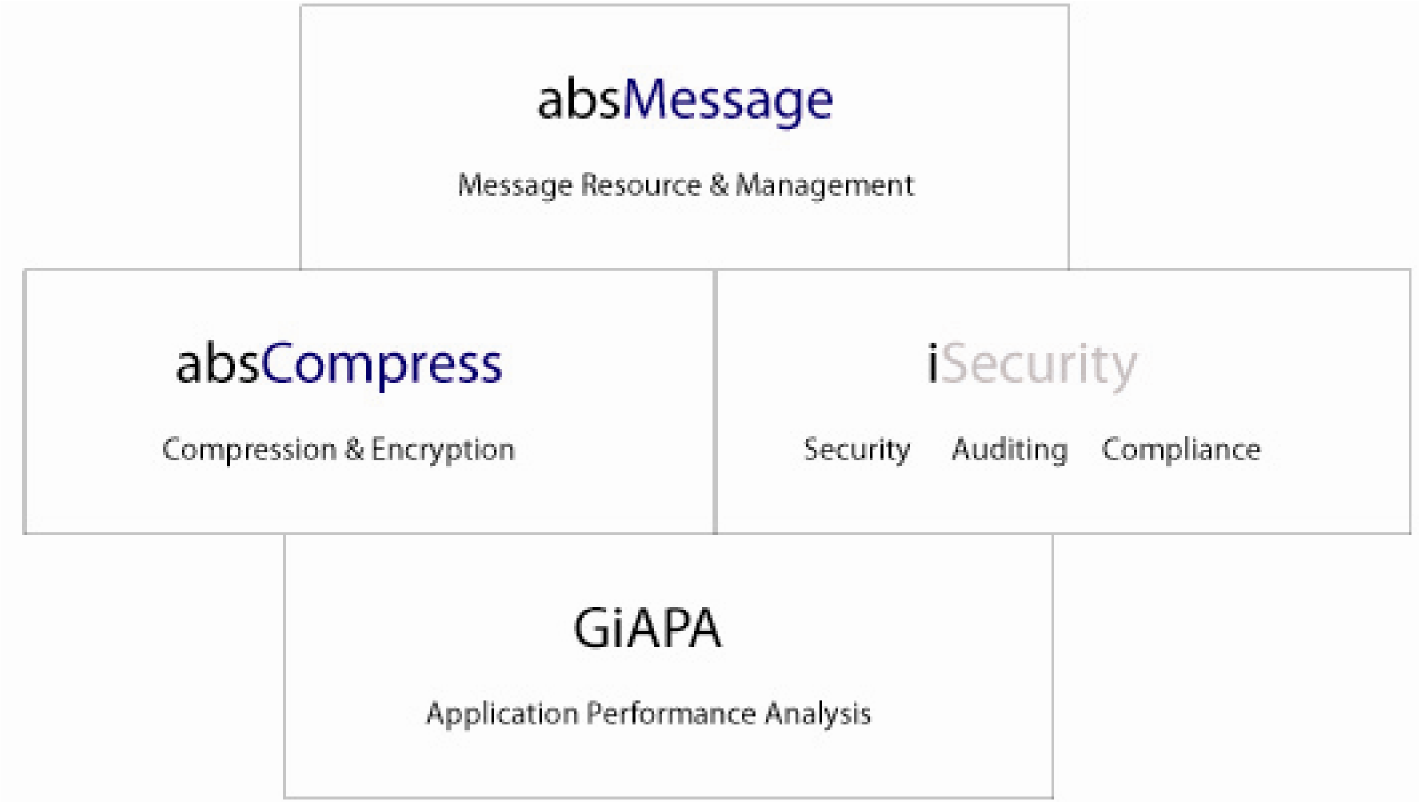


- 30 Years of Excellence
- 9 of the Fortune 10
- 85% of the Fortune 500
- Licenses in over 50 Countries

Company Overview

- **Support -**
  Live Operator 24x7x365
- **SEA Employee**
- **Training**
- **Conversions**
- **Consulting**

Company Overview



absMessage

Message Resource & Management

absCompress

Compression & Encryption

iSecurity

Security Auditing Compliance

GiAPA

Application Performance Analysis

iSecurity

System i Security Solutions

Assessing Your Security on the Power i

Where Does IBM “Hide” Security?

SYSTEM VALUES

USER PROFILES

NETWORK ATTRIBUTE

AUTHORIZATION LISTS

OBJECT SECURITY

EXIT POINTS

- SYSTEM VALUES
- USER PROFILES
- NETWORK ATTRIBUTES
- EXIT POINTS

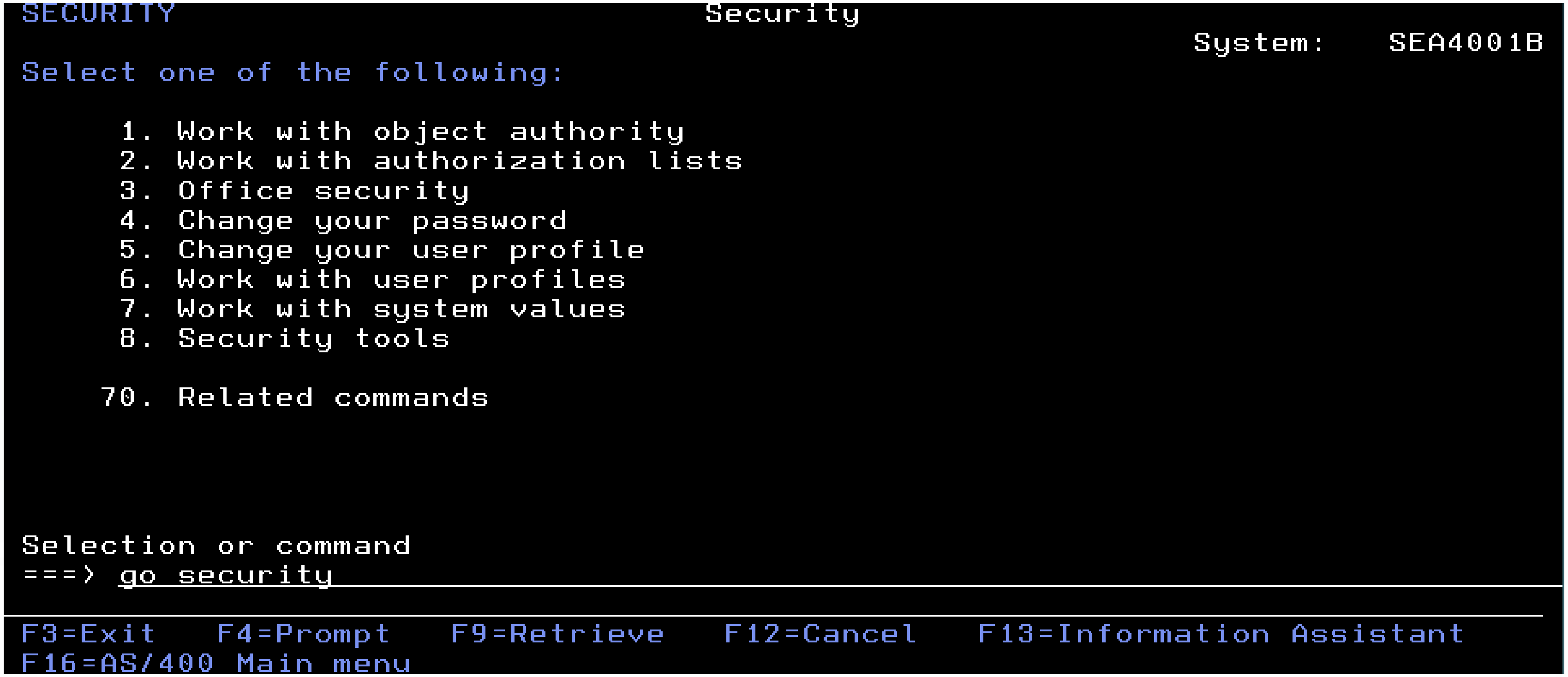
- AUTHORIZATION LIST
- OBJECTS
  - PROGRAMS, FILES, COMMANDS, etc.

How to Monitor Your iSeries

- MESSAGE QUEUES
- QHST
- QAUDJRN
- EXIT POINT PROGRAMMING
- REPORTS OVER USER PROFILES, OBJECT AUTHORITY ETC.

Assistance from IBM

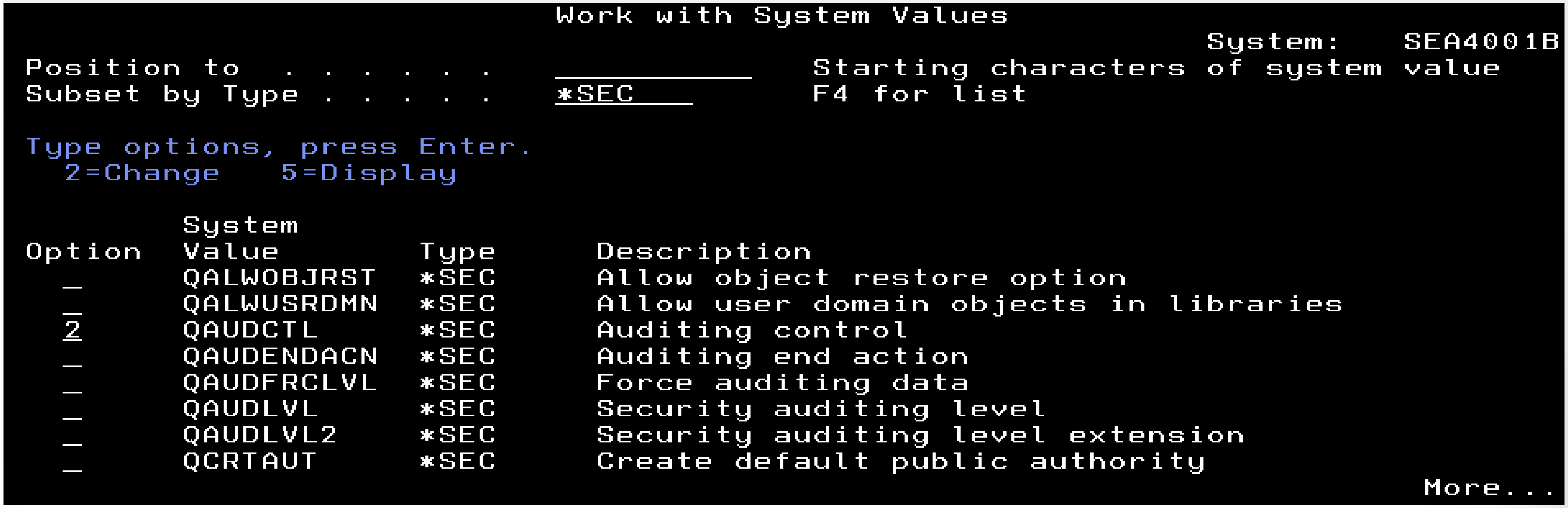
GO SECURITY



```
SECURITY                                    Security
                                                                 System:   SEA4001B
Select one of the following:

     1. Work with object authority
     2. Work with authorization lists
     3. Office security
     4. Change your password
     5. Change your user profile
     6. Work with user profiles
     7. Work with system values
     8. Security tools

    70. Related commands




Selection or command
===> go security

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

WORKING WITH SYSTEM VALUES

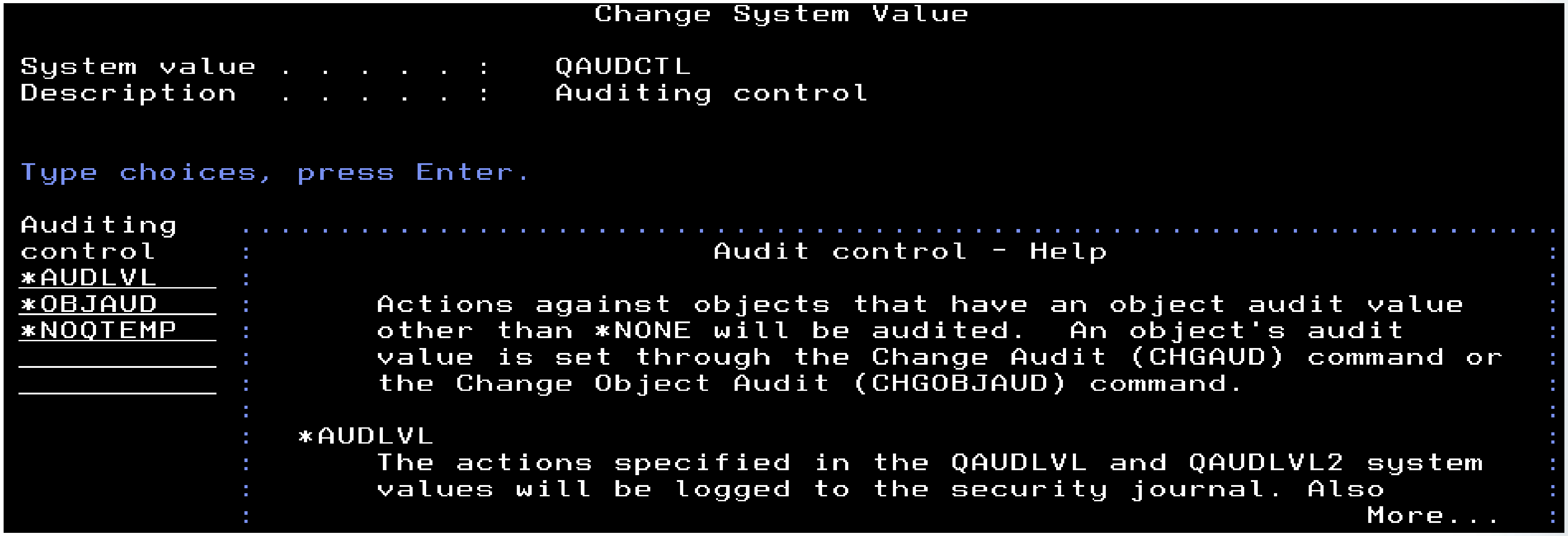
WRKSYSVAL *SEC



```
                           Work with System Values
                                                            System:   SEA4001B
Position to . . . . . . .  __________    Starting characters of system value
Subset by Type . . . . .   *SEC___       F4 for list

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

        System
Option  Value        Type      Description
  _     QALWOBJRST   *SEC      Allow object restore option
  _     QALWUSRDMN   *SEC      Allow user domain objects in libraries
  2     QAUDCTL      *SEC      Auditing control
  _     QAUDENDACN   *SEC      Auditing end action
  _     QAUDFRCLVL   *SEC      Force auditing data
  _     QAUDLVL      *SEC      Security auditing level
  _     QAUDLVL2     *SEC      Security auditing level extension
  _     QCRTAUT      *SEC      Create default public authority
                                                                       More...
```

WORKING WITH SYSTEM VALUES

OS400 provides valuable help text, press F1 for help



```
                              Change System Value

System value . . . . . :    QAUDCTL
Description  . . . . . :    Auditing control


Type choices, press Enter.

Auditing     ..................................................................
control      :                     Audit control - Help                       :
*AUDLVL____  :                                                                :
*OBJAUD____  :       Actions against objects that have an object audit value  :
*NOQTEMP___  :       other than *NONE will be audited.  An object's audit     :
__________   :       value is set through the Change Audit (CHGAUD) command or :
__________   :       the Change Object Audit (CHGOBJAUD) command.             :
             :                                                                :
             :   *AUDLVL                                                      :
             :       The actions specified in the QAUDLVL and QAUDLVL2 system :
             :       values will be logged to the security journal. Also      :
             :                                                     More...    :
```

System Values

WRKSYSVAL *SEC

- Allow object restore option (QALWOBJRST)
- Auditing control (QAUDCTL)
- Security auditing level (QAUDLVL)
- default auditing level of newly created (QCRTOBJAUD)
- default public authority to objects (QCRTAUT)

System Values

- Inactive interactive job time-out (QINACTITV)
- Sign-on display information control (QDSPSGNINF)
- Action to take for failed sign on attempts (QMAXSGNACN)
- Password Control (multiple system values)
- Adopted Authority (QUSEADPAUT)

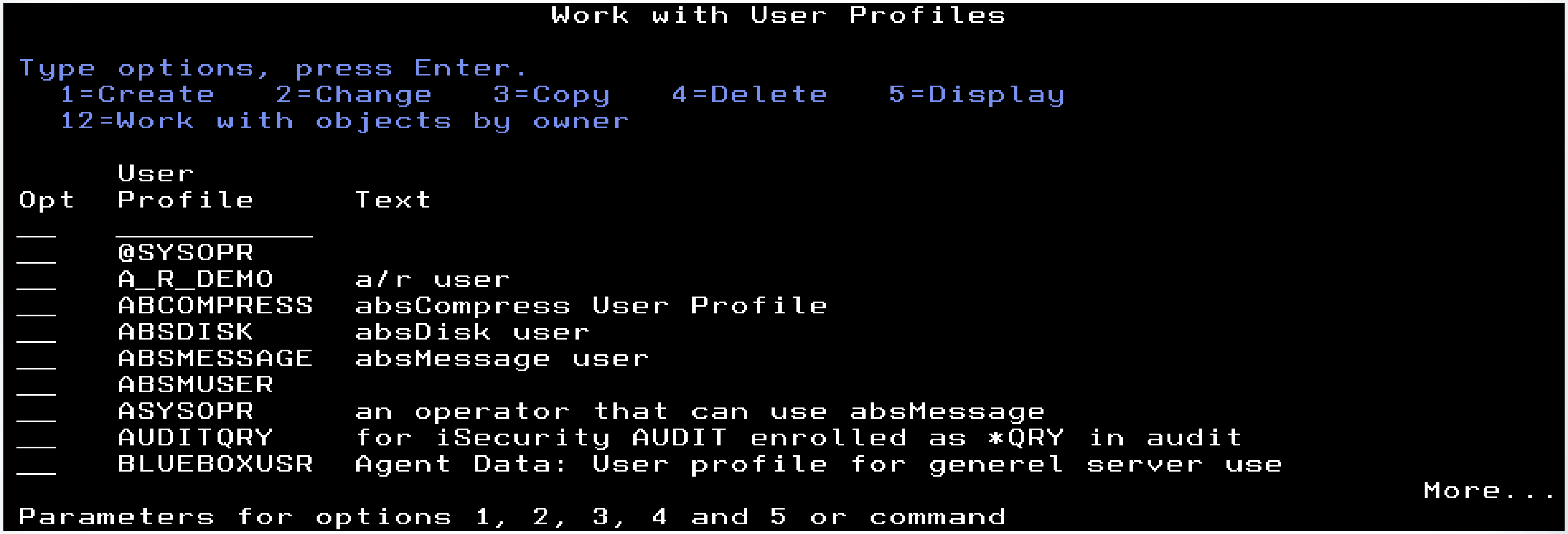
Adopted Authority

- A system value determines which users can work with programs with adopted authorities. Adopted authority adds the authority of a program owner to the authority of the user running the program

- Programs should adopt the authority of a user profile that has only enough authority to do the necessary functions, not excessive authority!

Working With User Profiles

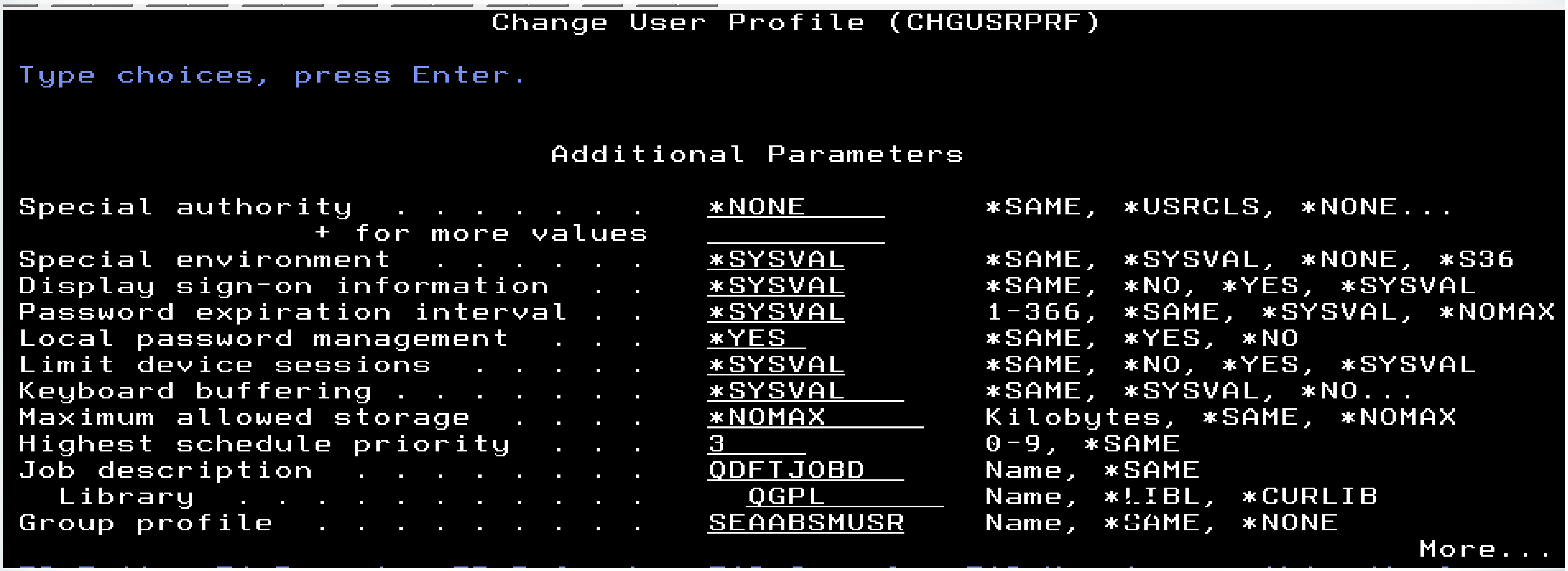
- WRKUSRPRF *ALL



```
                                Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile      Text
__   __________
__   @SYSOPR
__   A_R_DEMO     a/r user
__   ABCOMPRESS   absCompress User Profile
__   ABSDISK      absDisk user
__   ABSMESSAGE   absMessage user
__   ABSMUSER
__   ASYSOPR      an operator that can use absMessage
__   AUDITQRY     for iSecurity AUDIT enrolled as *QRY in audit
__   BLUEBOXUSR   Agent Data: User profile for generel server use
                                                                           More...
Parameters for options 1, 2, 3, 4 and 5 or command
```

Working With User Profiles

– security can be individualized by user



```
                         Change User Profile (CHGUSRPRF)

 Type choices, press Enter.


                            Additional Parameters

 Special authority . . . . . . .   *NONE            *SAME, *USRCLS, *NONE...
               + for more values
 Special environment . . . . . .   *SYSVAL          *SAME, *SYSVAL, *NONE, *S36
 Display sign-on information  . .  *SYSVAL          *SAME, *NO, *YES, *SYSVAL
 Password expiration interval . .  *SYSVAL          1-366, *SAME, *SYSVAL, *NOMAX
 Local password management  . . .  *YES             *SAME, *YES, *NO
 Limit device sessions  . . . . .  *SYSVAL          *SAME, *NO, *YES, *SYSVAL
 Keyboard buffering . . . . . . .  *SYSVAL          *SAME, *SYSVAL, *NO...
 Maximum allowed storage  . . . .  *NOMAX           Kilobytes, *SAME, *NOMAX
 Highest schedule priority  . . .  3                0-9, *SAME
 Job description  . . . . . . . .  QDFTJOBD         Name, *SAME
   Library  . . . . . . . . . . .    QGPL           Name, *LIBL, *CURLIB
 Group profile  . . . . . . . . .  SEAABSMUSR       Name, *SAME, *NONE
                                                                         More...
```

OS400 User Profiles

Besides the user id and password

- **Default password**
- **Job control**

  - initial program

  - initial menu

  - job description

  - change job attributes
- **Display sign-on information**

OS400 User Profiles

Besides the user id and password

- Used to grant or revoke authority to OS400 objects
- Contain password expiration timeframe
- Limited capabilities
- Special authorities
- Spool and print control

OS400 User Profiles

Besides the user id and password

- **Limit device session**

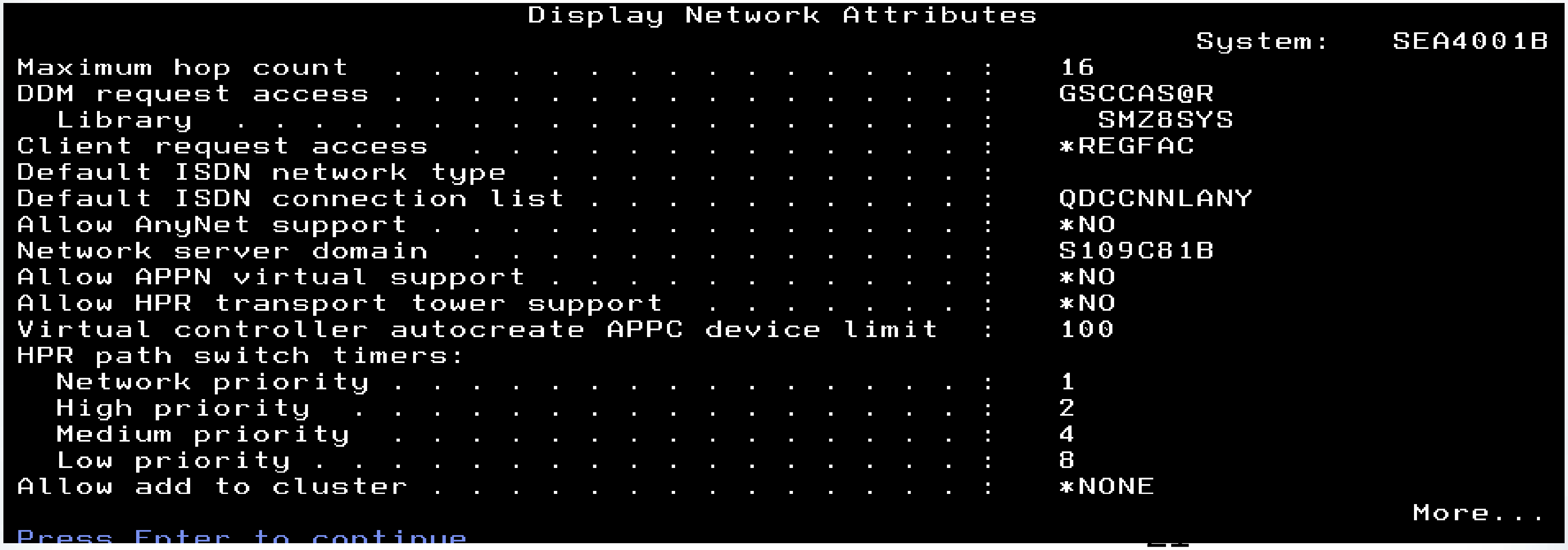
- **Group profile membership**

A *group profile* is a special type of user profile. You can use a group profile to define authority for a group of users, rather than for giving authority to each user individually. A group profile can own objects too

NETWORK ATTRIBUTES

DSPNETA or CHGNETA

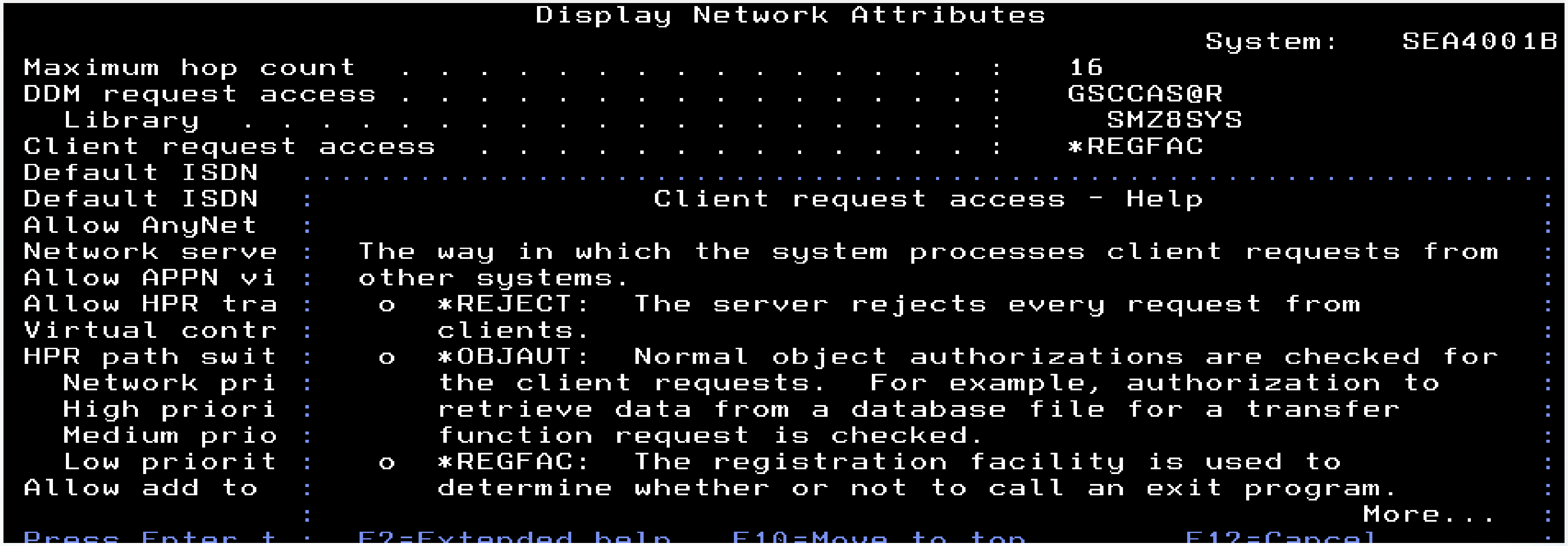
Distributed Data Management = DDM



```
                          Display Network Attributes
                                                            System:   SEA4001B
Maximum hop count  . . . . . . . . . . . . . . . . :   16
DDM request access . . . . . . . . . . . . . . . . :   GSCCAS@R
  Library  . . . . . . . . . . . . . . . . . . . . :     SMZ8SYS
Client request access  . . . . . . . . . . . . . . :   *REGFAC
Default ISDN network type  . . . . . . . . . . . . :
Default ISDN connection list . . . . . . . . . . . :   QDCCNNLANY
Allow AnyNet support . . . . . . . . . . . . . . . :   *NO
Network server domain  . . . . . . . . . . . . . . :   S109C81B
Allow APPN virtual support . . . . . . . . . . . . :   *NO
Allow HPR transport tower support  . . . . . . . . :   *NO
Virtual controller autocreate APPC device limit    :   100
HPR path switch timers:
  Network priority . . . . . . . . . . . . . . . . :   1
  High priority  . . . . . . . . . . . . . . . . . :   2
  Medium priority  . . . . . . . . . . . . . . . . :   4
  Low priority . . . . . . . . . . . . . . . . . . :   8
Allow add to cluster . . . . . . . . . . . . . . . :   *NONE
                                                                      More...
Press Enter to continue
```

NETWORK ATTRIBUTES

F1 for help from OS400



```
                          Display Network Attributes
                                                              System:   SEA4001B
 Maximum hop count  . . . . . . . . . . . . . . . . :   16
 DDM request access . . . . . . . . . . . . . . . . :   GSCCAS@R
   Library  . . . . . . . . . . . . . . . . . . . . :     SMZ8SYS
 Client request access  . . . . . . . . . . . . . . :   *REGFAC
 Default ISDN   . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
 Default ISDN   :                Client request access - Help                    :
 Allow AnyNet   :                                                                :
 Network serve  :  The way in which the system processes client requests from   :
 Allow APPN vi  :  other systems.                                                :
 Allow HPR tra  :   o   *REJECT:   The server rejects every request from         :
 Virtual contr  :       clients.                                                 :
 HPR path swit  :   o   *OBJAUT:   Normal object authorizations are checked for  :
   Network pri  :       the client requests.  For example, authorization to      :
   High priori  :       retrieve data from a database file for a transfer        :
   Medium prio  :       function request is checked.                             :
   Low priorit  :   o   *REGFAC:   The registration facility is used to          :
 Allow add to   :       determine whether or not to call an exit program.        :
                :                                                    More...     :
 Press Enter t  :  F2=Extended help    F10=Move to top        F12=Cancel         :
```

Network Attributes

DSPNETA

- System name
- DDM request
- Client access request

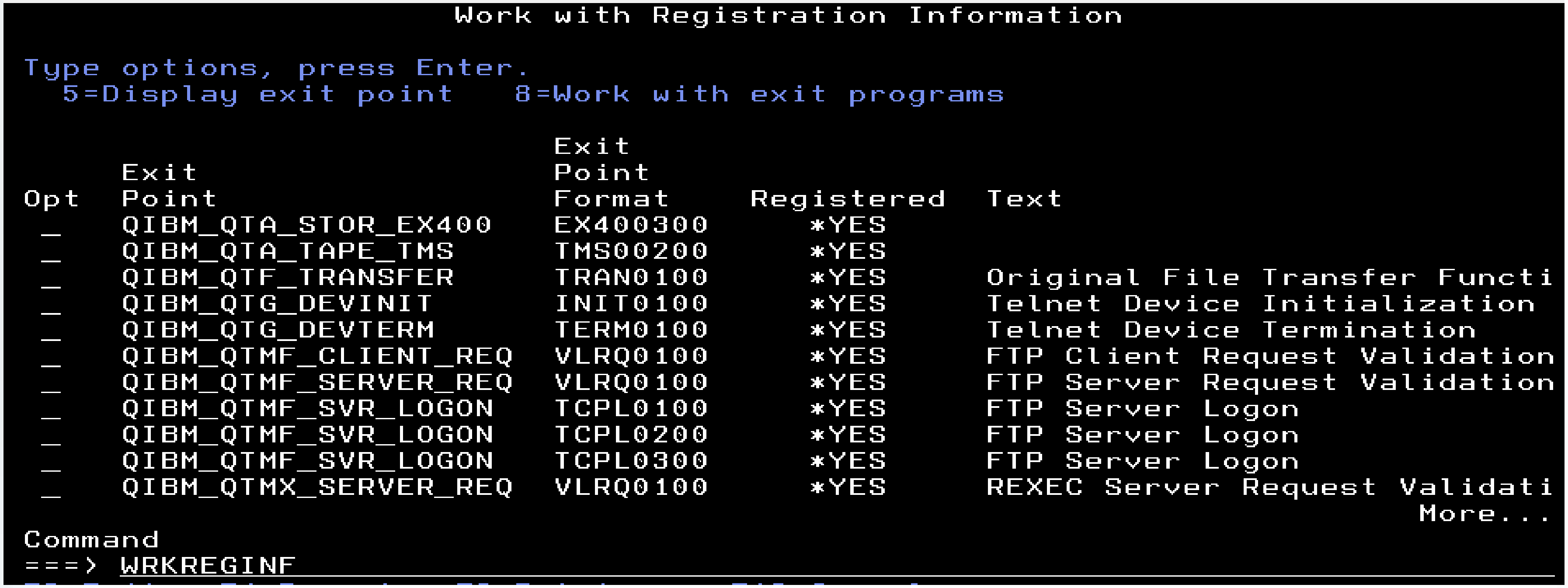
Network Monitoring & Protection

NOT PROVIDED BY OS400!

- OS400 provides EXIT Points to register YOUR programs to perform this critical function
- WRKREGINF

EXIT POINTS

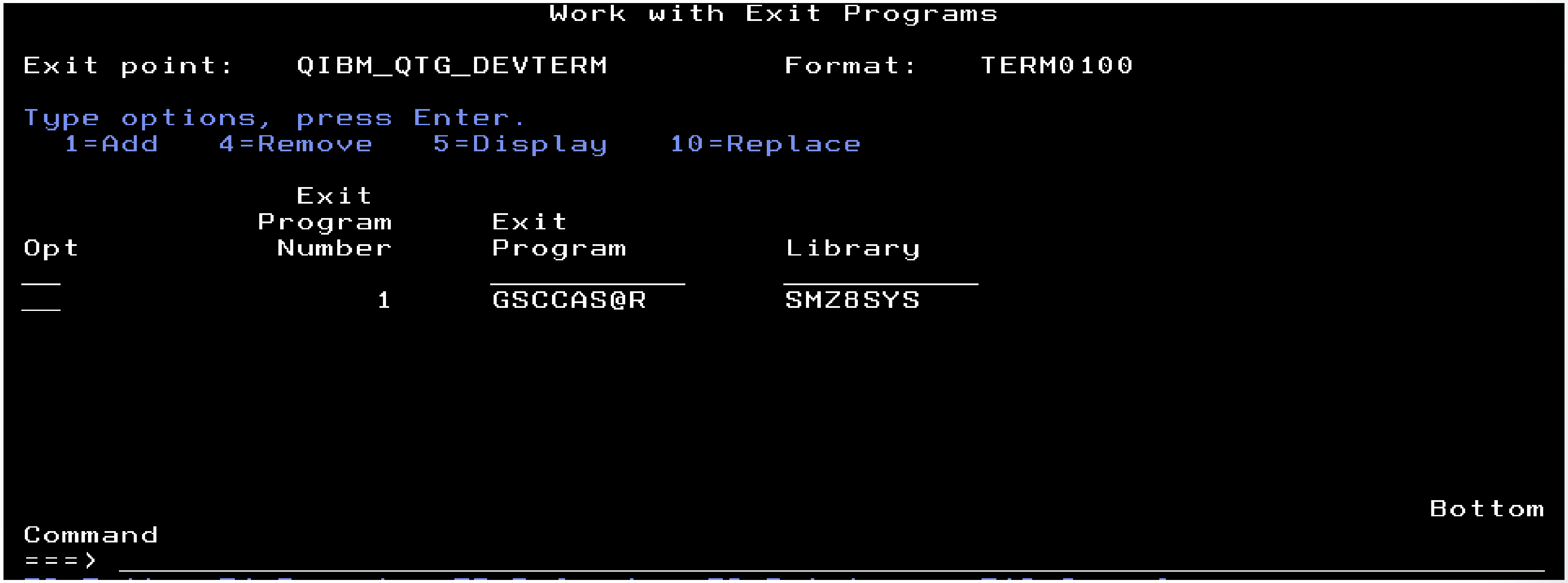
– WRKREGINF



```
                      Work with Registration Information

Type options, press Enter.
  5=Display exit point   8=Work with exit programs

                           Exit
     Exit                  Point
Opt  Point                 Format    Registered  Text
 _   QIBM_QTA_STOR_EX400   EX400300     *YES
 _   QIBM_QTA_TAPE_TMS     TMS00200     *YES
 _   QIBM_QTF_TRANSFER     TRAN0100     *YES     Original File Transfer Functi
 _   QIBM_QTG_DEVINIT      INIT0100     *YES     Telnet Device Initialization
 _   QIBM_QTG_DEVTERM      TERM0100     *YES     Telnet Device Termination
 _   QIBM_QTMF_CLIENT_REQ  VLRQ0100     *YES     FTP Client Request Validation
 _   QIBM_QTMF_SERVER_REQ  VLRQ0100     *YES     FTP Server Request Validation
 _   QIBM_QTMF_SVR_LOGON   TCPL0100     *YES     FTP Server Logon
 _   QIBM_QTMF_SVR_LOGON   TCPL0200     *YES     FTP Server Logon
 _   QIBM_QTMF_SVR_LOGON   TCPL0300     *YES     FTP Server Logon
 _   QIBM_QTMX_SERVER_REQ  VLRQ0100     *YES     REXEC Server Request Validati
                                                                       More...
Command
===> WRKREGINF
```

EXIT POINTS

– PROGRAMS BEGINNING WITH Q ARE USUALLY NOT SECURITY PROGRAMS



```
                          Work with Exit Programs

Exit point:    QIBM_QTG_DEVTERM          Format:    TERM0100

Type options, press Enter.
  1=Add    4=Remove    5=Display    10=Replace

              Exit
            Program      Exit
Opt          Number      Program         Library
___                      __________      __________
___               1      GSCCAS@R        SMZ8SYS






                                                                      Bottom
Command
===> ____________________________________________________________________________
```

Network Protection

- **Should provide for MONITORING**
- **Should provide for CONTROLLING – FIREWALL Function**
  - Is this server available to be used?
  - What ip address's can use this server
  - What users can use this server
  - What objects can be accessed
  - Method of access, read, update, delete, run commands remotely

Network Protection

- **EXIT POINTS**
  - Virus Scan of the IFS
  - Before and After images of changed User Profiles
  - FTP
  - Remote Commands
  - SQL, ODBC, FILE TRANSFER
  - Pass Through

Authorization List

CRTAUTL, EDTAUTL

Authorization lists are a tool that helps to manage authority to objects (libraries, files, programs, commands, etc.) when all of the objects need to be authorized in the same way.

For example as when many users need the same authority to a lot of objects.

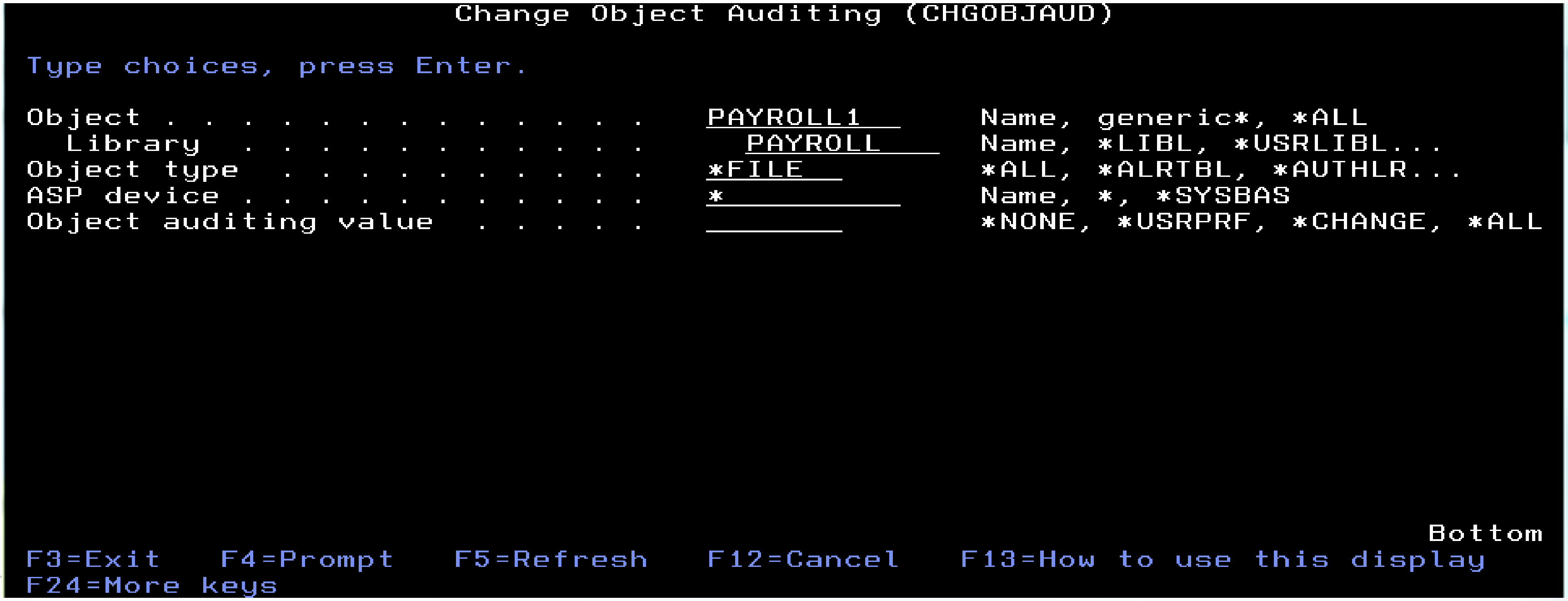
Object Security

- DSPOBJAUT
- DSPOBJD
- Who owns object
- Is object audited
- Private authorities
- User Profiles are objects too

Object Security

– Control auditing at the object level

– DSPOBJD and CHGOBJAUD

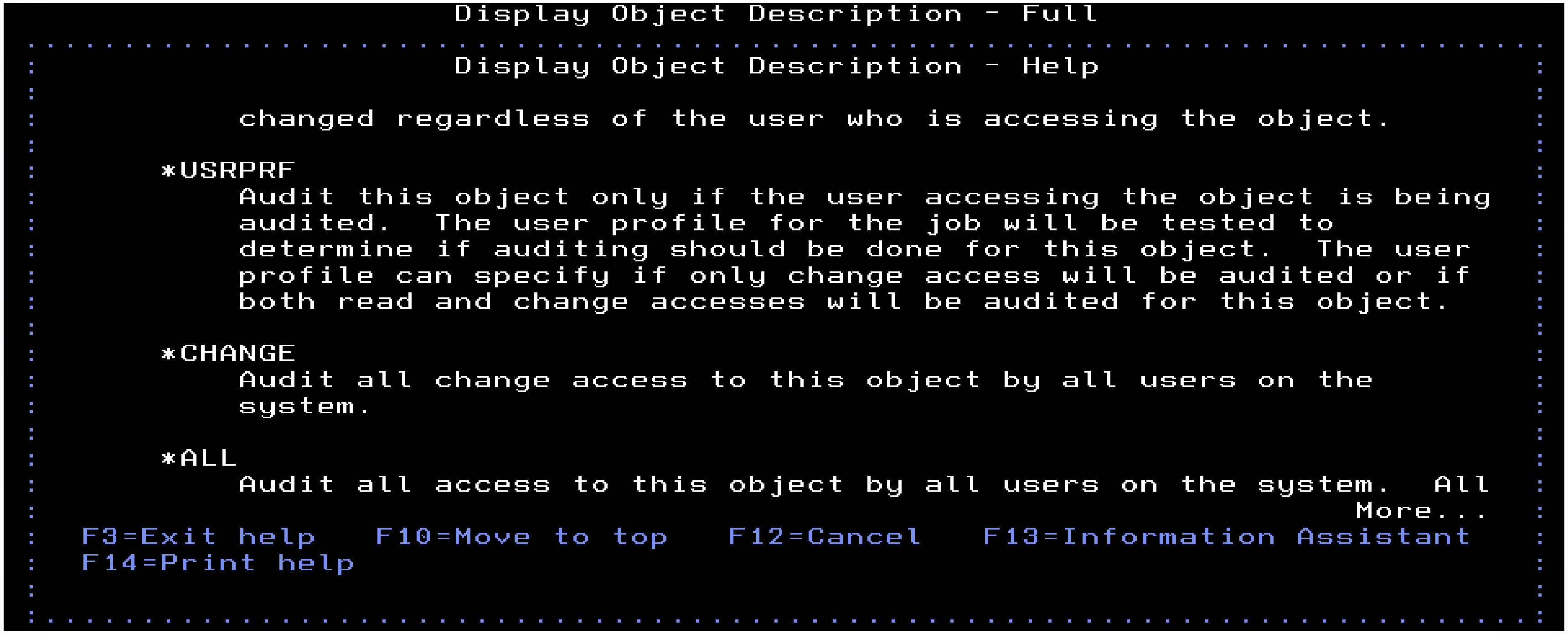


```
                      Change Object Auditing (CHGOBJAUD)

 Type choices, press Enter.

 Object . . . . . . . . . . . . . . . PAYROLL1        Name, generic*, *ALL
   Library  . . . . . . . . . . . . .   PAYROLL       Name, *LIBL, *USRLIBL...
 Object type  . . . . . . . . . . . . *FILE           *ALL, *ALRTBL, *AUTHLR...
 ASP device . . . . . . . . . . . . . *               Name, *, *SYSBAS
 Object auditing value  . . . . . .                   *NONE, *USRPRF, *CHANGE, *ALL










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

Object Security

– Control auditing at the object level

– DSPOBJD and CHGOBJAUD



```
                         Display Object Description - Full
 :.............................................................................:
 :                       Display Object Description - Help                     :
 :                                                                             :
 :          changed regardless of the user who is accessing the object.       :
 :                                                                             :
 :      *USRPRF                                                                :
 :          Audit this object only if the user accessing the object is being  :
 :          audited.  The user profile for the job will be tested to          :
 :          determine if auditing should be done for this object.  The user   :
 :          profile can specify if only change access will be audited or if   :
 :          both read and change accesses will be audited for this object.    :
 :                                                                             :
 :      *CHANGE                                                                :
 :          Audit all change access to this object by all users on the        :
 :          system.                                                            :
 :                                                                             :
 :      *ALL                                                                   :
 :          Audit all access to this object by all users on the system.  All  :
 :                                                                   More...   :
 :  F3=Exit help   F10=Move to top   F12=Cancel   F13=Information Assistant    :
 :  F14=Print help                                                             :
 :                                                                             :
 :.............................................................................:
```

What Auditors are Looking For

BEST PRACTICES

- Written Policy that all employees understand
- Continuous Monitoring of Security Activity
- Rules to Enforce Security Policy
- Real-time Alerts of Exceptions to Policy

What Auditors are Looking For

BEST PRACTICES

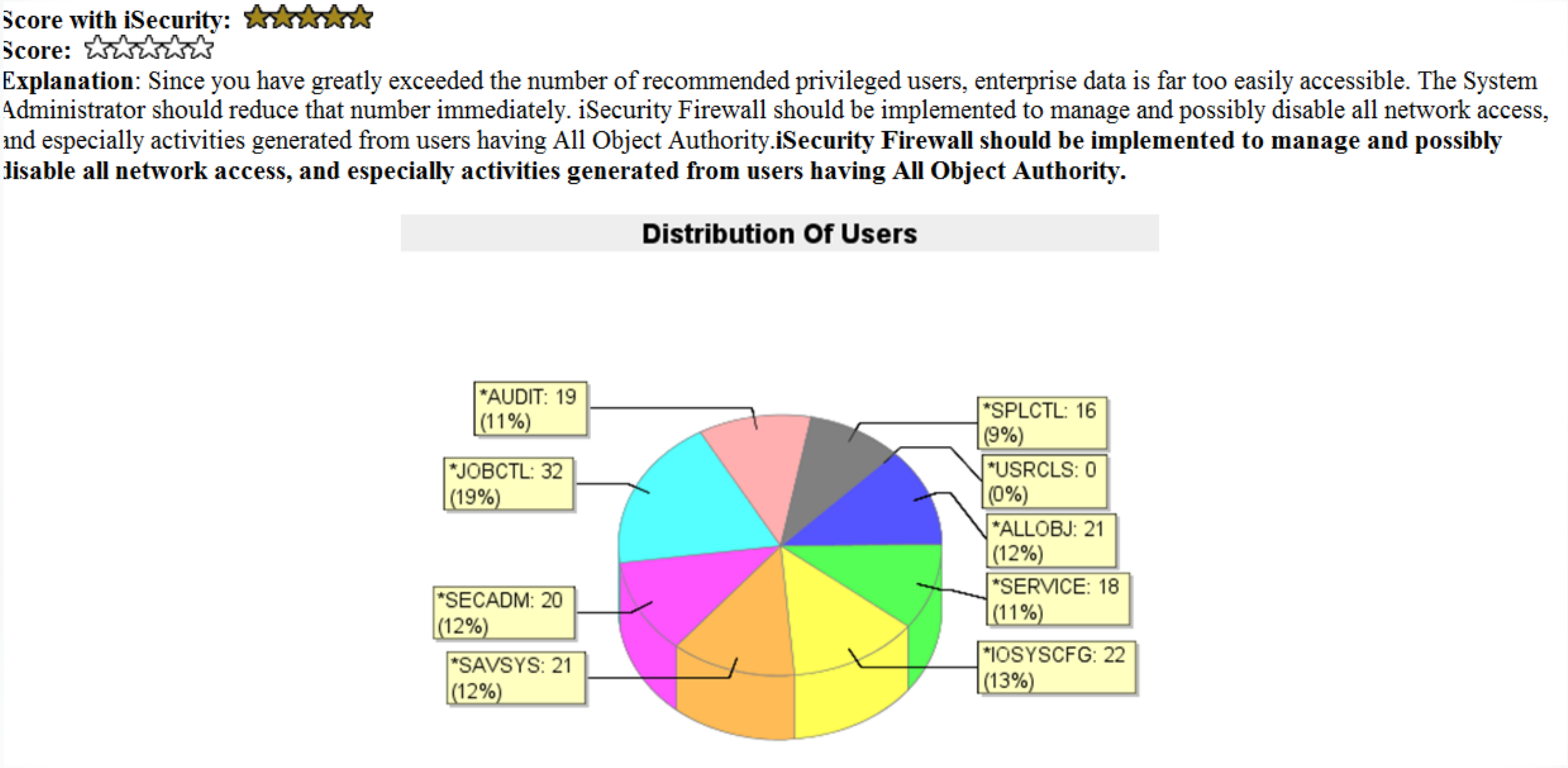
- Data Retention
- Relevant Reports for mgmt and auditors
- Being pro active

What is My Current Status

- Assessment Utility
- Installs on and Runs from PC
- Easy to use
- Intuitive
- Graphics
- Written analysis

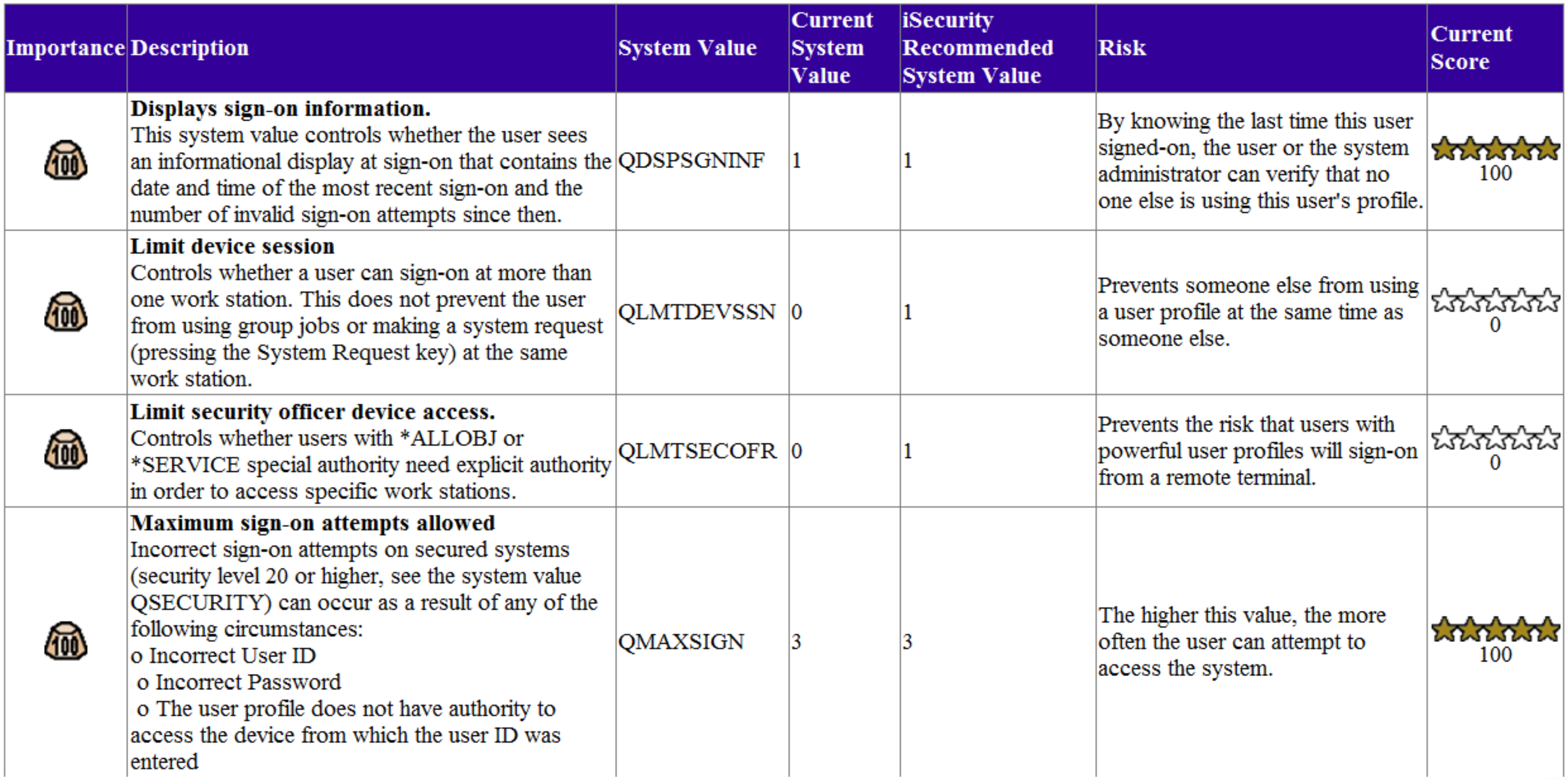
- 516-328-7000 or sales@seasoft.com

Assessment Utility



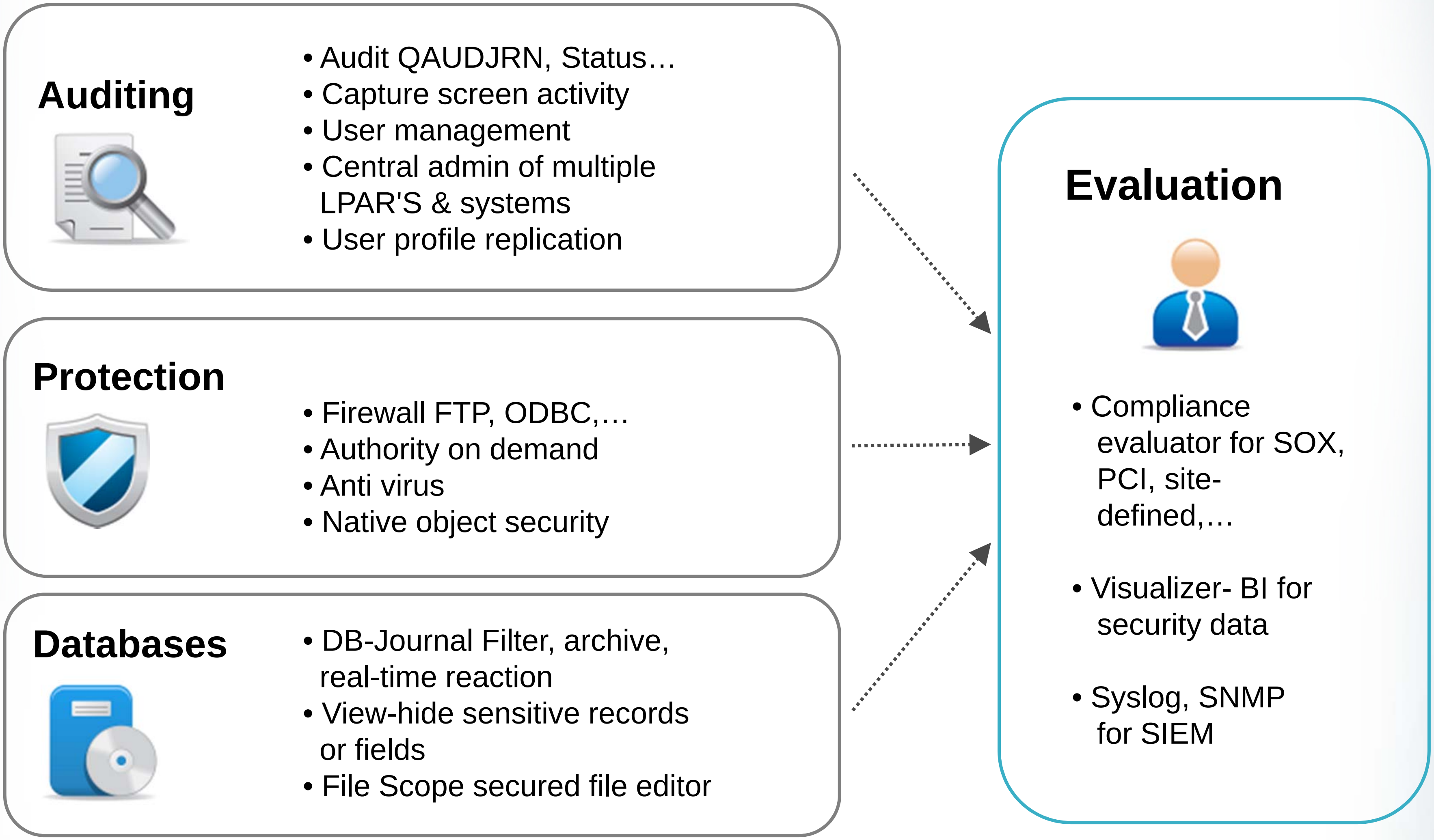
Score with iSecurity: ★★★★★
Score: ☆☆☆☆☆
Explanation: Since you have greatly exceeded the number of recommended privileged users, enterprise data is far too easily accessible. The System Administrator should reduce that number immediately. iSecurity Firewall should be implemented to manage and possibly disable all network access, and especially activities generated from users having All Object Authority.**iSecurity Firewall should be implemented to manage and possibly disable all network access, and especially activities generated from users having All Object Authority.**

Assessment Utility



Importance	Description	System Value	Current System Value	iSecurity Recommended System Value	Risk	Current Score
100	**Displays sign-on information.** This system value controls whether the user sees an informational display at sign-on that contains the date and time of the most recent sign-on and the number of invalid sign-on attempts since then.	QDSPSGNINF	1	1	By knowing the last time this user signed-on, the user or the system administrator can verify that no one else is using this user's profile.	★★★★★ 100
100	**Limit device session** Controls whether a user can sign-on at more than one work station. This does not prevent the user from using group jobs or making a system request (pressing the System Request key) at the same work station.	QLMTDEVSSN	0	1	Prevents someone else from using a user profile at the same time as someone else.	☆☆☆☆☆ 0
100	**Limit security officer device access.** Controls whether users with *ALLOBJ or *SERVICE special authority need explicit authority in order to access specific work stations.	QLMTSECOFR	0	1	Prevents the risk that users with powerful user profiles will sign-on from a remote terminal.	☆☆☆☆☆ 0
100	**Maximum sign-on attempts allowed** Incorrect sign-on attempts on secured systems (security level 20 or higher, see the system value QSECURITY) can occur as a result of any of the following circumstances: o Incorrect User ID o Incorrect Password o The user profile does not have authority to access the device from which the user ID was entered	QMAXSIGN	3	3	The higher this value, the more often the user can attempt to access the system.	★★★★★ 100

iSecurity Solutions



Auditing

- Audit QAUDJRN, Status…
- Capture screen activity
- User management
- Central admin of multiple LPAR'S & systems
- User profile replication

Protection

- Firewall FTP, ODBC,…
- Authority on demand
- Anti virus
- Native object security

Databases

- DB-Journal Filter, archive, real-time reaction
- View-hide sensitive records or fields
- File Scope secured file editor

Evaluation

- Compliance evaluator for SOX, PCI, site-defined,…
- Visualizer- BI for security data
- Syslog, SNMP for SIEM

Watch Your E-mail

for a complimentarily copy of the SEA's
guide to assessing your
security on the iSeries

Thank You!

Visit Us at:

www.seasoft.com

sales@seasoft.com

516-328-7000