CXL SECURE

AZScan

Report for
Demo

07-Dec-2008 18:24

Report for	Demo
Company	CXL Finance
Business Unit	Finance Division
Location	London
System	FINSYS202

Report Name	c:\tbxnew-works\reports\myrepa.doc
Report Date	07-Dec-2008 18:24

Key to colors

Risks	L Low risk	M Medium risk	H High risk
Results	L Correct or low risk	M Medium impact	H Major problem

1 SYSSETSystem settings

1.1	QSEC	M Security level	L 40
1.2	QAUTOC	L Auto configuration	M 1=On
1.3	QAUTOVRT	L Auto virtual	H 10
1.4	QCRTAUT	M Default public authority	L *EXCLUDE
1.5	QALWUD	L Allow user domain	L *ALL
1.6	QAOR	L Allow object restore	L All
1.7	QATNPGM	M Attention program	L ASSIST

2 SYSPWDSSystem passwords

2.1	QPWDLVL	L Password level	L Setting 0
2.2	QPWDEXPITV	H Password expiration interval	L 60 days.
2.3	QPWDLMTAJC	L Password limit adjacent digits	M 0 - allowed
2.4	QPWDLMTCHR	L Password limit characters	L *NONE
2.5	QPWDLMTREP	L Password limit repetition	L Duplicate characters not allowed.
2.6	QPWDMINLEN	H Password minimum length	L 6 characters.
2.7	QPWDMAXLEN	L Password maximum length	L 10
2.8	QPWDPOSDIF	L Password position different	M 0
2.9	QPWDRQDDGT	M Password does not require digits	L 1
2.10	QPWDRQDDIF	H Password required to be different	L 7
2.11	QPWDVLDPGM	L Password validation program	L *NONE

3 USERSUsers

3.1	UCLASS	H User Classes	M *User 52 *Sysopr 6 *Secofr 3 *Pgmr 7 *Secadm 1

3.2	DISPROF	L Users with disabled profiles	L 7disabled.
3.3	CURLIB	L Users current library	M 68 users - no current library.
3.4	INLPGM	L Users initial programs	M 68 users - no initial program set.
3.5	INLMNU	L Users initial menu	H 66 - users without initial menus set.
3.6	DSPSGNINF	M Users display sign-on information	H 65 users - no sign-on information.
3.7	LMTCPB	L Users limit capability	H 68 users - without limited capability.
3.8	QLMTDEVSSN	L Users with limited device sessions	H 63 users can sign on to >1 terminal.
3.9	SPCENV	L Users with special environments	L 60 users.

4 SPAUTHORTYSpecial Authorities

4.1	ALLOBJ	H Users with all objects authority	M *USER=1 *PGMR=0 *SYSOPR=2 *SECOFR=3 *SECADM=0
4.2	SECADM	H Users with security administration authority	M *USER=1 *PGMR=0 *SYSOPR=2 *SECOFR=3 *SECADM=0
4.3	JOBCTL	M Users with job control authority	M *USER=2 *PGMR=5 *SYSOPR=6 *SECOFR=3 *SECADM=0
4.4	SPLCTL	M Users with spool control Authority	M *USER=1 *PGMR=0 *SYSOPR=0 *SECOFR=3 *SECADM=0
4.5	SAVSYS	M Users with save system authority	M *USER=1 *PGMR=1 *SYSOPR=4 *SECOFR=3 *SECADM=0
4.6	SERVICE	M Users with service authority	M *USER=1 *PGMR=1 *SYSOPR=1 *SECOFR=3 *SECADM=0
4.7	AUDIT	L Users with audit authority	M *USER=1 *PGMR=0 *SYSOPR=0 *SECOFR=3 *SECADM=0
4.8	IOSYSCFG	L Users with system configuration authority	M *USER=3 *PGMR=1 *SYSOPR=3 *SECOFR=3 *SECADM=0

5 UPASSWORDUser passwords

5.1	PWDEXPITV	M Users password expiry interval	M 60 days.
5.2	PWDEXPD	M Users with password set to expired	L 0users.
5.3	PWDLCHG	M Users password last changed	M 0
5.4	PWDIBMPRO	L IBM system profiles where password <> *NONE	H 2
5.5	PWDNOTLO	M Users who have not logged on	H 55
5.6	PWDLASTLO	M Users last logon date	H 14

6 SIGNONSignon attempts allowed

6.1	QMAXSIGN	M Maximum sign-on attempts	M 5
6.2	QMAXSGNACN	L Maximum sign-On attempt action	L 3
6.3	QRMTSIGN	M Remote sign-on	L *REJECT
6.4	QLMTESCOFR	L Limit security officer	H 0

6.5	QDSPSGNINF	M Display sign-on information	L 1
6.6	QLMTDEVSSN	L Limit device sessions	H 0
6.7	QINACTITV	M Inactive Interval	M *NONE
6.8	QINACTMSGQ	L Inactive Message Queue	L *DSCJOB

7 GROUPSGroups

7.1	GROUPS	L Users in each group	L 1

8 AUDITINGAuditing

8.1	QAUDCTL	L Audit control	L 2
8.2	QAUDLVL	M Audit level	L 24
8.3	QAEA	L Audit end action	L 2
8.4	QAFREQ	L Audit frequency level	L 2
8.5	QCRTOBJAUD	L Create object audit	L *USRPRF

1 SYSSET - System settings

RISKS

In this section we look at some of the basic system settings which effect the security of the system.

1.1 QSEC - Security level

M

RISKS

This is the security level of the system known as QSECURITY and ranges from 10 to 50.
Level 10 provides no security protection and is not supported by IBM.
Level 50 is used for high security systems and is required for C2 certification.
The system requires a password to sign-on and users must have authority to access objects and system resources.
Level 40 is the preferred option.

ACTIONS

Preferred 40, minimum 30

L

RESULTS

Current setting: Level 40
The user must have an active user profile and password to sign-on.
The user must have authority specifically granted to them if authority other than 'Public' authority for an object is required.
This level provides operating system integrity checks and logging of foreign programs, (e.g., 'viruses'), usage of unsupported interfaces, and restricted system instructions.
Security-related exposures that surface at level 40 are usually attributed to lack of familiarity with the AS/400 security features or poor protection schemes that makes security administration difficult.

1.2 QAUTOC - Auto configuration

L

RISKS

This parameter should be set to off (0) during normal operation.
It can be turned on (1) periodically to automatically configure new devices, but is reset to 'off' once the configuration process is complete.

ACTIONS

Recommended value 0

M

RESULTS

This is currently set to 1.

1.3 QAUTOVRT - Auto virtual

L

RISKS

This value represents the maximum number of virtual devices that can be configured.
With automatic configuration active, the actual threshold limit on invalid sign-on attempts ('QMAXSIGN') is increased by the multiple of the value specified in 'QAUTOVRT: to 500 (the default value).
The invalid sign-on threshold for sessions using the AS/400 pass-through facility (e.g., personal computers or other AS/400s within the network) is automatically increased to 1500.
Allowing automatic configuration of virtual devices in your system increases the likelihood of system break-in via pass-through.

ACTIONS

Recommended value 0Automatic virtual device configuration for pass-through sessions should either be eliminated or limited as appropriate.

H

RESULTS

This is currently set to 10

1.4 QCRTAUT - Default public authority

M

RISKS

Public authority is given to users who have no specific authority to an object - that is, those who have no specific authority granted for their user profiles, are not on an authorization list that supplies specific authority, or are not part of a group profile with specific authority.
Standard values are *ALL, *CHANGE, *USE, or *EXCLUDE
o *ALL The user can perform all operations on the object except those limited to the owner or controlled by authorization list management authority
o *CHANGE The user can perform all operations on the object except those limited to the owner or controlled by object existence authority and object management authority.
o *USE The user can perform basic operations on the object (e.g., opening the file and reading the records and executing the program).
o *EXCLUDE The user is specifically denied any access to the object
For created objects, the value should be set system-wide to be *USE.
If set inappropriately, changes to production objects could take place.

ACTIONS

Recommended value *EXCLUDEVerify that it has been changed from the default value of *CHANGE to a minimum of *EXCLUDE.

L

RESULTS

Correctly set to *EXCLUDE

1.5 QALWUD - Allow user domain

L

RISKS

Indicates that all libraries on the system can contain 'user domain objects' (*USRSPC, *USRIDX, and USRQ)

ACTIONS

Recommended value *ALL

L

RESULTS

Correctly set to *ALL

1.6 QAOR - Allow object restore

L

RISKS

Determines whether objects that are security-sensitive may be restored to your system. It can be used by individuals to prevent anyone from restoring a system state object or an object that adopts authority.

ACTIONS

Recommended value *ALL

L

RESULTS

Correctly set to *ALL

1.7 QATNPGM - Attention program

M

RISKS

This program runs when the Attention key is pressed. A malicious program could be inserted here.
The Operational Assistant menu should appear when the attention key is pressed.

ACTIONS

Recommended value *ASSIST

L

RESULTS
Correctly set to *ASSIST

2 SYSPWDS - System passwords

RISKS

This section looks at the security around the password settings for all users defined by the system. Some of these parameters can be amended within each user's individual profile.

2.1 QPWDLVL - Password level

L

RISKS

The password level of the system can be set to allow for user profile passwords from 1 through 10 characters or to allow for user profile passwords from 1 through 128 characters.
There are four possible values:
0 Short passwords using a limited character set.
1 Short passwords using a limited character set. Disable AS/400 Netserver on Windows 95/98/ME.
2 Long passwords using an unlimited character set.
3 Long passwords using an unlimited character set. Disable AS/400 Netserver on Windows 95/98/ME.
Level 2 or 3 cannot be used if other systems are not using release V5R1M0 or above or are set to levels 0 or 1.

ACTIONS

Consider very carefully before moving to level 2 or 3. Whilst these provide better security with longer passwords, network communication problems could result.

L

RESULTS

This is currently set to 0
Short passwords, limited character set.

2.2 QPWDEXPITV - Password expiration interval

H

RISKS

This controls the number of days a password is valid and forces passwords to be changed after a given time interval.
Users are notified seven days in advance of password expiration.
You can set QPWDEXPITV to an expiration interval of between 1 and 366 days, or you can set it to *NOMAX, which specifies that passwords will never expire and users will not be forced to change their passwords.

ACTIONS

Recommended value 30-90 daysThe 'QPWDEXPITV' value should be set, at a minimum, to 90 days. At this value, the user is required to change their password every 90 days.Note: This control can be further tailored at the user level via the user profile parameter 'Password Expiration Interval'(PWDEXPITV).For powerful and sensitive user-ids, we recommend that this value should be set to 30 days.If there is no PWDEXPITV value specified for a user profile, the profile will use the QPWDEXPITV system value for its expiration properties.If a user profile has a PWDEXPITV parameter that is different from the QPWDEXPITV system value, the PWDEXXPITV parameter will take precedence over QPWDEXXPITV.

L

RESULTS

The password expiry interval for 'ordinary' users is 60 days and for 'system' users it is 30 days.
This is correctly set to 60 days.

2.3 QPWDLMTAJC - Password limit adjacent digits

L

RISKS

Adjacent digits are not allowed in passwords.
Used to specify whether adjacent numeric characters are (0) or are not (1) allowed in a password.
This option prevents users from using birthdays, telephone numbers, or a sequence of numbers as passwords.

ACTIONS

Recommended value 1.

M

RESULTS

The value is currently set to 0

2.4 QPWDLMTCHR - Password limit characters

L

RISKS

Characters which are not valid on all international keyboard are restricted such as the number sign (#), dollar sign ($), at sign (@), and underscore (_)
This option could also be used to prevent users from using specific characters, such as vowels, in a password. Restricting vowels prevents users from forming actual words for their passwords.

ACTIONS

Recommended value #s@ or some commonly used characters

L

RESULTS

Currently set to *NONE - all characters are acceptable in passwords.

2.5 QPWDLMTREP - Password limit repetition

L

RISKS

Repeating adjacent characters in passwords are not allowed.
This limits repeating characters in a new password, thus eliminating the possibilities of a user having passwords such as, 11111, AAAAA, etc.

ACTIONS

Recommended value 1.The 'QPWDLMTREP' value should be set '1', so that the same character cannot be repeated more than once in a password.

L

RESULTS

Duplicate characters are allowed in passwords but not consecutively. (eg 'ABABABAB' is allowed)

2.6 QPWDMINLEN - Password minimum length

H

RISKS

This controls the minimum number of characters in a password, thus eliminating very short passwords that are more easily guessable.

ACTIONS

Recommended value 6 or higher.The 'QPWDMINLEN' value should ideally be set at 6 to 8 characters for effective password control.

L

RESULTS

Correctly set to 6 characters.

2.7 QPWDMAXLEN - Password maximum length

L

RISKS

Password can not be longer than x characters in length. The default value is 8.

ACTIONS

Recommended value 8 to 10.

L

RESULTS

Correctly set to 10

2.8 QPWDPOSDIF - Password position different

L

RISKS

New password cannot have characters in the same position as the previous password. This prevents changing just one character from the previous password when a user changes the password.

ACTIONS

Recommended value 1

M

RESULTS

This is currently set to 0

2.9 QPWDRQDDGT - Password does not require digits

M

RISKS

Designates whether digits are required to be present in every password. It is a good idea to include digits somewhere in the password since this makes it more difficult to guess them.

ACTIONS

Recommended value 1

L

RESULTS

Correctly set to 1

2.10 QPWDRQDDIF - Password required to be different

H

RISKS

New passwords are required to be different to previous passwords.

ACTIONS

Recommended value: 1 to 5This specifies that the new password must be different from between the 10 to 32 previous password values.The 'QPWDDRQDDIF' value should be set to '1', thus requiring that the new password value to be different to the previous value.

L

RESULTS

This is currently set to 7 and therefore only 6 previous passwords are checked for duplicates.

2.11 QPWDVLDPGM - Password validation program

L

RISKS

A special password validation program is used in addition to or in place of the standard AS/400 logic.
If a program is used, the program should not record user passwords or contain hard-coded passwords.

ACTIONS

Recommended value *NONE

L

RESULTS

Correctly set to *NONE

3 USERS - Users

RISKS

In this section we look at the individual user profiles and the various parameters which affect their security settings.

3.1 UCLASS - User Classes

H

RISKS

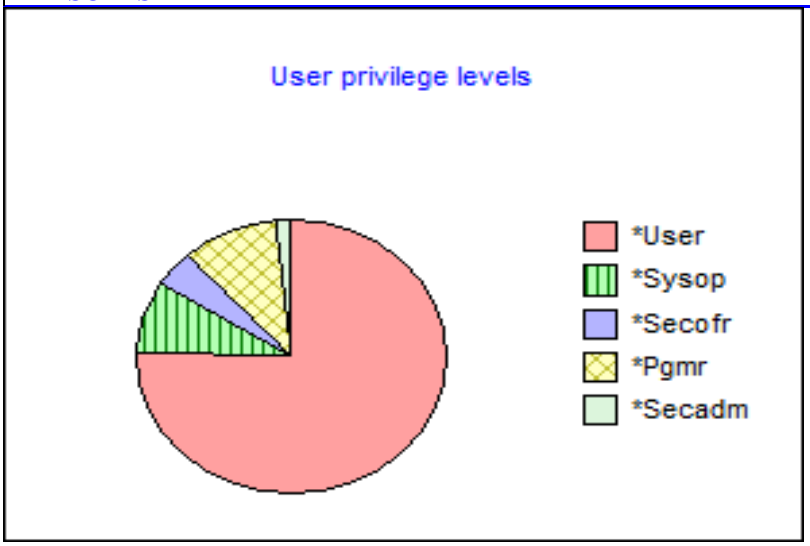
Classes, other than *USER, give default special authorities to users. This can then give them access to system functions which are greater than they need.

ACTIONS

Examine each user profile and ensure that they are correctly classified according to their job function.Most users should be set to *USER.Do not modify the IBM supplied profiles which begin with Q.

M

RESULTS



```
User class:   *User
User Name       Owner
----------------------
DAVID           USER PROFILE1
MANAGER6        USER PROFILE1
QBRMS           IBM-supplied User Profile
QCLUMGT         IBM-supplied User Profile
QCLUSTER        IBM-supplied User Profile
QCOLSRV         IBM-supplied User Profile
QDBSHR          Internal Data Base User Profile
QDBSHRDO        Internal Data Base User Profile
QDESADM         DB2 TEXT EXTENDER ADMINISTRATOR
QDESUSR         DB2 TEXT EXTENDER USER
QDFTOWN         Default Owner for System Objects
QDIRSRV         OS/400 Directory Services Server User Profile
QDLFM           IBM-supplied User Profile
QDOC            Internal Document User Profile
QDSNX           IBM-supplied User Profile
QEJB            IBM-supplied User Profile
QFNC            IBM-supplied User Profile
QGATE           IBM-supplied User Profile
QIPP            IBM-supplied User Profile
QMQM            MQSERIES PROFILE
QMQMADM         MQSERIES GROUP PROFILE
QMSF            Mail Server Framework Profile
QNETSPLF        Internal Spool Network Profile
QNFSANON        IBM-supplied User Profile
QNTP            IBM-supplied User Profile
QSNADS          IBM-supplied User Profile
QSPL            Internal Spool User Profile
QSPLJOB         Internal Spool User Profile
QTCM            IBM-supplied User Profile
QTFTP           IBM-supplied User Profile
QTMHHTP1        HTTP Server CGI User Profile
QTMHHTTP        HTTP Server User Profile
QTMPLPD         REMOTE REQUESTERS
QTMTWSG         5250 HTML WORKSTATION GATEWAY PROFILE
USER1           USER PROFILE1
USER10          USER PROFILE2
USER11          USER PROFILE2
USER12          USER PROFILE2
USER13          USER PROFILE2
USER14          USER PROFILE2
USER15          USER PROFILE2
USER16          USER PROFILE2
USER17          USER PROFILE2
USER18          USER PROFILE2
USER2           USER PROFILE1
USER3           USER PROFILE1
USER4           USER PROFILE1
USER5           USER PROFILE1
USER6           USER PROFILE1
USER7           USER PROFILE1
USER8           USER PROFILE1
USER9           USER PROFILE1

 52 profiles were found in this user class.

User class:   *Sysopr
User Name       Owner
----------------------
MANAGER5        System Operator
QLPAUTO         IBM-supplied User Profile
QLPINSTALL      IBM-supplied User Profile
QSVCDRCTR       IBM-supplied User Profile
QSYSOPR         System Operator
QTCP            Internal TCP/IP User Profile
```

3.2 DISPROF - Users with disabled profiles

L

RISKS

The users shown below have had their profiles disabled and cannot log onto the system. They may have left or changed jobs.

ACTIONS

Consider deleting these users if they have not been on the system for a long time.Do not delete IBM supplied profiles beginning with Q.

L

RESULTS

```
The following user profiles are disabled:

MANAGER5     System Operator
QSVCDRCTR    IBM-supplied User Profile
QSYSOPR      System Operator
QTCM         IBM-supplied User Profile
USER10       USER PROFILE2
USER15       USER PROFILE2
USER16       USER PROFILE2

 7 users are disabled.
```

3.3 CURLIB - Users current library

L

RISKS

The current library is searched before the libraries in the user portion of the library list for any objects specified as *LIBL.
If the user creates objects and specifies *CURLIB, the objects are put in the current library.
The current library is automatically added to the user's library list when the user signs on.
The user cannot change the current library if the Limit Capabilities field in the user profile is *YES or *PARTIAL.
If objects are created using *CURLIB on a create command, the library QGPL is used as the default current library.

ACTIONS

Examine each user's current library and ensure that the library is valid and appropriate for their work.

M

RESULTS

```
These users do not have a current library set.
Files created by users will be stored in QGPL.

DAVID          MANAGER1       MANAGER2       MANAGER3       MANAGER4
MANAGER5       MANAGER6       QBRMS          QCLUMGT        QCLUSTER
QCOLSRV        QDBSHR         QDBSHRDO       QDESADM        QDESUSR
QDFTOWN        QDIRSRV        QDLFM          QDOC           QDSNX
QEJB           QFNC           QGATE          QIPP           QLPAUTO
QLPINSTALL     QMQM           QMQMADM        QMSF           QNETSPLF
QNFSANON       QNTP           QPGMR          QPM400         QRJE
QSECOFR        QSNADS         QSPL           QSPLJOB        QSRV
QSRVBAS        QSVCDRCTR      QSYS           QSYSOPR        QTCM
QTFTP          QTMHHTP1       QTMHHTTP       QTMPLPD        QTMTWSG
USER1          USER10         USER11         USER12         USER13
USER14         USER15         USER16         USER17         USER18
USER2          USER3          USER4          USER5          USER6
USER7          USER8          USER9


The users have the following libraries:
               Current                          Current
User           Library          User            Library
-------------------------------------------------------
QTCP           QTCP
```

3.4 INLPGM - Users initial programs

L

RISKS

You can specify the name of a program to call when a user signs on. This program runs before the initial menu, if any, is displayed.
If the Limit Capabilities field in the user's profile is *YES or *PARTIAL, the user cannot specify an initial program on the Sign On display.
Initial programs are used for two main purposes:
o To restrict a user to a specific set of functions.
o To perform some initial processing, such as opening files or establishing the library list.
The initial program is called only if the user's routing program is QCMD or QCL.
Parameters cannot be passed to an initial program. If the initial program fails, the user is not able to sign on.

ACTIONS

Examine each user's initial program and ensure that it is valid and appropriate for their work.

M

RESULTS

```
These users do not have an initial program set:

DAVID          MANAGER1       MANAGER2       MANAGER3       MANAGER4
MANAGER5       MANAGER6       QBRMS          QCLUMGT        QCLUSTER
QCOLSRV        QDBSHR         QDBSHRDO       QDESADM        QDESUSR
QDFTOWN        QDIRSRV        QDLFM          QDOC           QDSNX
QEJB           QFNC           QGATE          QIPP           QLPINSTALL
QMQM           QMQMADM        QMSF           QNETSPLF       QNFSANON
QNTP           QPGMR          QPM400         QRJE           QSECOFR
QSNADS         QSPL           QSPLJOB        QSRV           QSRVBAS
QSVCDRCTR      QSYS           QSYSOPR        QTCM           QTCP
QTFTP          QTMHHTP1       QTMHHTTP       QTMPLPD        QTMTWSG
USER1          USER10         USER11         USER12         USER13
USER14         USER15         USER16         USER17         USER18
USER2          USER3          USER4          USER5          USER6
USER7          USER8          USER9


The users have the following initial programs set:
               Initial                          Initial
User           Program          User            Program
--------------------------------------------------------
QLPAUTO        QLPINATO
```

3.5 INLMNU - Users initial menu

L

RISKS

You can specify the name of a menu to be shown when the user signs on. The initial menu is displayed after the user's initial program runs.
The initial menu is called only if the user's routing program is QCMD or QCL.
If you want the user to run only the initial program, you can specify *SIGNOFF for the initial menu.
If the Limit capabilities field in the user's profile is *YES, the user cannot specify a different initial menu on the Sign On display. If a user is allowed to specify an initial menu on the Sign On display, the menu specified overrides the menu in the user profile.
Values:
MAIN - The AS/400 system Main Menu is shown.
*SIGNOFF - The system signs off the user when the initial program completes. Use this to limit users to running a single program.

ACTIONS

Examine the initial menu of each user and ensure that it exists and is appropriate for their work.

H

RESULTS

```
These users do not have an initial menu set:

DAVID          MANAGER1       MANAGER2       MANAGER3       MANAGER4
MANAGER5       MANAGER6       QBRMS          QCLUMGT        QCLUSTER
QCOLSRV        QDBSHR         QDBSHRDO       QDESADM        QDESUSR
QDFTOWN        QDIRSRV        QDLFM          QDOC           QDSNX
QEJB           QFNC           QGATE          QIPP           QLPINSTALL
QMSF           QNETSPLF       QNFSANON       QNTP           QPGMR
QPM400         QRJE           QSECOFR        QSNADS         QSPL
QSPLJOB        QSRV           QSRVBAS        QSVCDRCTR      QSYS
QSYSOPR        QTCM           QTCP           QTFTP          QTMHHTP1
QTMHHTTP       QTMPLPD        QTMTWSG        USER1          USER10
USER11         USER12         USER13         USER14         USER15
USER16         USER17         USER18         USER2          USER3
USER4          USER5          USER6          USER7          USER8
USER9


The users have the following initial menus:
               Initial          Initial
User           Menu             Menu Library
-----------------------------------------
QLPAUTO        *SIGNOFF
QMQM           *SIGNOFF
QMQMADM        *SIGNOFF
```

3.6 DSPSGNINF - Users display sign-on information

Ⓜ

RISKS

The Display Sign-on Information field specifies whether the Sign-on Information display is shown when the user signs on. It is useful to tell a user when their account was last used.
Password expiration information is also shown if the password expires within seven days.
Possible values are:

- *SYSVAL The QDSPSGNINF system value is used.
- *NO The Sign-on Information display is not shown when the user signs on.
- *YES The Sign-on Information display is shown when the user signs on.

ACTIONS

Having all users see this display is recommended.Users with special authority or authority to critical objects should be encouraged to use the display to make sure no one attempts to use their profiles.

Ⓗ

RESULTS

The following users do not have information displayed when they sign on:

DAVID	MANAGER1	MANAGER2	MANAGER3	MANAGER4
MANAGER5	MANAGER6	QBRMS	QCLUMGT	QCLUSTER
QCOLSRV	QDBSHRDO	QDESADM	QDESUSR	QDFTOWN
QDIRSRV	QDLFM	QDOC	QDSNX	QEJB
QFNC	QGATE	QIPP	QLPAUTO	QLPINSTALL
QMQM	QMQMADM	QMSF	QNETSPLF	QNFSANON
QNTP	QPGMR	QPM400	QRJE	QSECOFR
QSNADS	QSPL	QSPLJOB	QSRV	QSRVBAS
QSVCDRCTR	QSYS	QSYSOPR	QTCM	QTCP
QTFTP	QTMHHTP1	QTMHHTTP	QTMPLPD	QTMTWSG
USER10	USER11	USER12	USER13	USER14
USER15	USER16	USER17	USER18	USER2
USER3	USER4	USER5	USER7	USER8

65 out of 69 users.

3.7 LMTCPB - Users limit capability

L

RISKS

You can use the Limit Capabilities field to limit the user's ability to enter commands and to override the initial program, initial menu, current library, and attention-key-handling program specified in the user profile. It also prevents users from experimenting on the system.
A user with LMTCPB(*YES)can only run commands that are defined as Allow Limited User(ALWLMTUSR) *YES.
These commands are shipped by IBM with ALWLMTUSR(*YES):
- o Sign off (SIGNOFF)
- o Send message (SNDMSG)
- o Display messages (DSPMSG)
- o Display job (DSPJOB)
- o Display job log (DSPJOBLOG)
- o Start PC Organizer (STRPCO)
- o Work with Messages (WRKMSG)

The Limit capabilities field in the user profile and the ALWLMTUSR parameter on commands apply only to commands that are run from the command line, the Command Entry display or an option from a command grouping menu. Users are not restricted from doing the following:
- o Running commands in CL programs that are running a command as a result of taking an option from a menu
- o Running remote commands through applications, such as FTP.

You can allow the limited capability user to run additional commands, or remove some of these commands from the list, by changing the ALWLMTUSR parameter for a command.
If you create your own commands, you can specify the ALWLMTUSR parameter on the Create Command (CRTCMD) command.
*Partial allows use of system commands, but restricts the user from changing their initial program and menu at the sign-on screen . Users have the ability to change the initial menu via the change profile command (CHGPRF).
Possible values for Limit Capabilities and what functions are allowed for each value.

ACTIONS

Decide which users should be restricted and ensure that this is the case for the users shown below.

H

RESULTS

These users have limited capability:

QDIRSRV

These users do not have limited capability:

DAVID	MANAGER1	MANAGER2	MANAGER3	MANAGER4
MANAGER5	MANAGER6	QBRMS	QCLUMGT	QCLUSTER
QCOLSRV	QDBSHR	QDBSHRDO	QDESADM	QDESUSR
QDFTOWN	QDLFM	QDOC	QDSNX	QEJB
QFNC	QGATE	QIPP	QLPAUTO	QLPINSTALL
QMQM	QMQMADM	QMSF	QNETSPLF	QNFSANON
QNTP	QPGMR	QPM400	QRJE	QSECOFR
QSNADS	QSPL	QSPLJOB	QSRV	QSRVBAS
QSVCDRCTR	QSYS	QSYSOPR	QTCM	QTCP
QTFTP	QTMHHTP1	QTMHHTTP	QTMPLPD	QTMTWSG
USER1	USER10	USER11	USER12	USER13
USER14	USER15	USER16	USER17	USER18
USER2	USER3	USER4	USER5	USER6
USER7	USER8	USER9		

3.8 QLMTDEVSSN - Users with limited device sessions

L

RISKS

The Limit device sessions field controls whether a user can be signed on at more than one workstation at a time. The value does not restrict the use of the System Request menu or a second sign-on from the same device.
Possible Values for LMTDEVSSN:
*SYSVAL The QLMTDEVSSN system value is used.
*NO The user may be signed on to more than one device at the same time.
*YES The user may not be signed on to more than one device at the same time.
Limiting users to one workstation at a time is one way to discourage sharing user profiles.

ACTIONS

Set the QLMTDEVSSN system value to 1 (YES).If some users have a requirement to sign on at multiple workstations, use the Limit device sessions field in the user profile for those users.

H

RESULTS

```
The QLMTDEVSSN system value is used to determine whether the users can
sign-on to more than one device at a time.
The QLMTDEVSSN system value is currently set to 0 - No.
A 'S' next to a username indicates that this system setting is being used.

DAVID              MANAGER2     S    MANAGER3          MANAGER4     S
MANAGER5     S     MANAGER6     S    QBRMS        S    QCOLSRV      S
QDBSHR       S     QDBSHRDO          QDESADM      S    QDESUSR      S
QDFTOWN      S     QDIRSRV           QDLFM        S    QDOC         S
QDSNX        S     QEJB         S    QGATE        S    QIPP         S
QLPAUTO      S     QLPINSTALL   S    QMQM         S    QMSF         S
QNETSPLF     S     QNFSANON     S    QNTP         S    QPGMR        S
QPM400       S     QRJE              QSECOFR      S    QSNADS       S
QSPL         S     QSPLJOB      S    QSRV              QSRVBAS      S
QSVCDRCTR    S     QSYS         S    QSYSOPR      S    QTCM         S
QTCP         S     QTFTP        S    QTMHHTP1     S    QTMHHTTP     S
QTMPLPD            QTMTWSG      S    USER1        S    USER11       S
USER12       S     USER13       S    USER14       S    USER15       S
USER16       S     USER17       S    USER18       S    USER2        S
USER3              USER4        S    USER5        S    USER6        S
USER7              USER8        S    USER9        S

63 users can sign on to more than one terminal.
```

3.9 SPCENV - Users with special environments

L

RISKS

Special Environment determines the environment the user operates in after signing on.
The user can operate in the AS/400, the System/36, or the System/38 environment. When the user signs on, the system uses the routing program and the special environment in the user's profile to determine the user's environment.
*SYSVAL The QSPCENV system value is used to determine the environment when the user signs on, if the user's routing program is QCMD.
*NONE The user operates in the AS/400 environment.
*S36 The user operates in the System/36 environment if the user's routing program is QCMD.

ACTIONS

Review all users shown below and ensure that they are all working in appropriate environments.

L

RESULTS

These users operate in the AS/400 environment:

QCLUMGT	QCLUSTER	QDIRSRV	QLPAUTO	QLPINSTALL
QNETSPLF	QSVCDRCTR	QTCM	QTCP	

The QSPCENV system value is used to determine the environment when the user signs on, if the user's routing program is QCMD.
The QSPCENV system value is currently set to *NONE.

DAVID	MANAGER1	MANAGER2	MANAGER3	MANAGER4
MANAGER5	MANAGER6	QBRMS	QCOLSRV	QDBSHR
QDBSHRDO	QDESADM	QDESUSR	QDFTOWN	QDLFM
QDOC	QDSNX	QEJB	QFNC	QGATE
QIPP	QMQM	QMQMADM	QMSF	QNFSANON
QNTP	QPGMR	QPM400	QRJE	QSECOFR
QSNADS	QSPL	QSPLJOB	QSRV	QSRVBAS
QSYS	QSYSOPR	QTFTP	QTMHHTP1	QTMHHTTP
QTMPLPD	QTMTWSG	USER1	USER10	USER11
USER12	USER13	USER14	USER15	USER16
USER17	USER18	USER2	USER3	USER4
USER5	USER6	USER7	USER8	USER9

4 SPAUTHORTY - Special Authorities

RISKS

Special Authorities give users special access to a number of important system functions.

4.1 ALLOBJ - Users with all objects authority

H

RISKS

All-object special authority allows the user to access any resource on the system whether or not private authority exists for the user.
Even if the user has *EXCLUDE authority to an object, *ALLOBJ special authority still allows the user to access the object.
The user can view, change, or delete any object. The user can also grant to other users the authority to use objects.
A user with *ALLOBJ authority cannot directly perform operations that require another special authority.
For example, *ALLOBJ special authority does not allow a user to create another user profile, because creating user profiles requires *SECADM special authority. However, a user with *ALLOBJ special authority can submit a batch job to run using a profile that has the needed special authority. Giving *ALLOBJ special authority essentially gives a user access to all functions on the system.

ACTIONS

Only qualified users should have this special authority.

M

RESULTS

```
The following *USER users have *ALLOBJ special authority:
USER3       USER PROFILE1

1 users.

No *PGMR users have ALLOBJ authority.

0 users.

The following *SYSOPR users have *ALLOBJ special authority:
QLPAUTO     IBM-supplied User Profile
QLPINSTALL  IBM-supplied User Profile

2 users.

The following *SECOFR users have *ALLOBJ special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have ALLOBJ authority.

0 users.
```

4.2 SECADM - Users with security administration authority

H

RISKS

Security administrator (*SECADM) special authority allows a user to create, change, and delete user profiles.
A user with *SECADM special authority can:
o Add users to the system distribution directory.
o Display authority for documents or folders.
o Add and remove access codes to the system.
o Give and remove a user's access code authority.
o Give and remove permission for users to work on another user's behalf.
o Delete documents and folders.
o Delete document lists.
o Change distribution lists created by other users.
Only a user with *SECADM and *ALLOBJ special authority can give *SECADM special authority to another user.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

M

RESULTS

```
The following *USER users have *SECADM special authority:
USER3       USER PROFILE1

1 users.

No *PGMR users have *SECADM authority.

0 users.

The following *SYSOPR users have *SECADM special authority:
QLPAUTO     IBM-supplied User Profile
QLPINSTALL  IBM-supplied User Profile

2 users.

The following *SECOFR users have *SECADM special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *SECADM authority.

0 users.
```

4.3 JOBCTL - Users with job control authority

M

RISKS

Job control (*JOBCTL) special authority allows the user to:
- Change, delete, hold, and release all files on any output queues specified as OPRCTL(*YES).
- Display, send, and copy all files on any output queues specified as DSPDTA(*YES or *NO) and OPRCTL(*YES).
- Hold, release, and clear job queues specified as OPRCTL(*YES).
- Hold, release, and clear output queues specified as OPRCTL(*YES).
- Hold, release, change, and cancel other users' jobs.
- Start, change, end, hold, and release writers, if the output queue is specified as OPRCTL(*YES).
- Change the running attributes of a job, such as the printer for a job.
- Stop subsystems.
- Perform an initial program load (IPL).

You can change the job priority (JOBPTY) and the output priority (OUTPTY) of your own job without job control special authority. You must have *JOBCTL special authority to change the run priority (RUNPTY) of your own job.
Changes to the output priority and job priority of a job are limited by the priority limit (PTYLMT) in the profile of the user making the change.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

M

RESULTS

```
The following *USER users have *JOBCTL special authority:
QMQM         MQSERIES PROFILE
USER3        USER PROFILE1

2 users.

The following *PGMR users have *JOBCTL special authority:
QPGMR        Programmer and Batch User
QPM400       IBM-supplied User Profile
QRJE         IBM-supplied User Profile
QSRV         Service User Profile
QSRVBAS      Basic Service User Profile

5 users.

The following *SYSOPR users have *JOBCTL special authority:
MANAGER5     System Operator
QLPAUTO      IBM-supplied User Profile
QLPINSTALL   IBM-supplied User Profile
QSVCDRCTR    IBM-supplied User Profile
QSYSOPR      System Operator
QTCP         Internal TCP/IP User Profile

6 users.

The following *SECOFR users have *JOBCTL special authority:
MANAGER4     Security Officer
QSECOFR      Security Officer
QSYS         Internal System User Profile

3 users.

No *SECADM users have *JOBCTL authority.

0 users.
```

4.4 SPLCTL - Users with spool control Authority

M

RISKS

The user with *SPLCTL special authority can perform any operation on any spooled file in the system. Confidential spooled files cannot be protected from a user with *SPLCTL special authority.
Spool control special authority allows the user to perform all spool control functions, such as changing, deleting, displaying, holding and releasing spooled files. The user can perform these functions on all output queues, regardless of any authorities for the output queue or the OPRCTL parameter for the output queue.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

M

RESULTS

```
The following *USER users have *SPLCTL special authority:
USER3       USER PROFILE1

1 users.

No *PGMR users have *SPLCTL authority.

0 users.

No *SYSOPR users have *SPLCTL authority.

0 users.

The following *SECOFR users have *SPLCTL special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *SPLCTL authority.

0 users.
```

4.5 SAVSYS - Users with save system authority

Ⓜ

RISKS

Save system (*SAVSYS) special authority gives the user the authority to save, restore, and free storage for all objects on the system, whether or not the user has object existence authority to the objects.
The user with *SAVSYS special authority can:

- Save an object and take it to another AS/400 system to be restored (and viewed).
- Save an object and display the tape to view the data.
- Save an object and free storage, thus deleting the data portion of the object.
- Save a document and delete it.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

Ⓜ

RESULTS

```
The following *USER users have *SAVSYS special authority:
USER3       USER PROFILE1

1 users.

The following *PGMR users have *SAVSYS special authority:
QPGMR       Programmer and Batch User

1 users.

The following *SYSOPR users have *SAVSYS special authority:
MANAGER5    System Operator
QLPAUTO     IBM-supplied User Profile
QLPINSTALL  IBM-supplied User Profile
QSYSOPR     System Operator

4 users.

The following *SECOFR users have *SAVSYS special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *SAVSYS authority.

0 users.
```

4.6 SERVICE - Users with service authority

M

RISKS

A user with *SERVICE special authority can display and change confidential information using service functions. The user must have *ALLOBJ special authority to change the information using service functions.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

M

RESULTS

```
The following *USER users have *SERVICE special authority:
USER3       USER PROFILE1

1 users.

The following *PGMR users have *SERVICE special authority:
QSRV        Service User Profile

1 users.

The following *SYSOPR users have *SERVICE special authority:
QSVCDRCTR   IBM-supplied User Profile

1 users.

The following *SECOFR users have *SERVICE special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *SERVICE authority.

0 users.
```

4.7 AUDIT - Users with audit authority

(L)

RISKS

Audit (*AUDIT) special authority gives the user the ability to change auditing characteristics. The user can:
- Change the system values that control auditing.
- Use the CHGOBJAUT, CHGDLOAUD, and CHGAUD commands to change auditing for objects.
- Use the CHGUSRAUD command to change auditing for a user.

A user with *AUDIT special authority can stop and start auditing on the system or prevent auditing of particular actions. Note: Only a user with *ALLOBJ, *SECADM, and *AUDIT special authorities can give another user *AUDIT special authority.

ACTIONS

If having an audit record of security-relevant events is important for your system, carefully control and monitor the use of *AUDIT special authority.Review all users shown below. Ensure that only appropriate users have this authority.

(M)

RESULTS

```
The following *USER users have *AUDIT special authority:
USER3       USER PROFILE1

1 users.

No *PGMR users have *AUDIT authority.

0 users.

No *SYSOPR users have *AUDIT authority.

0 users.

The following *SECOFR users have *AUDIT special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *AUDIT authority.

0 users.
```

4.8 IOSYSCFG - Users with system configuration authority

L

RISKS

System configuration (*IOSYSCFG) special authority gives the user the ability to change how the system is configured. For example, adding or removing communications configuration information, working with TCP/IP servers, and configuring the internet connection server (ICS). Most commands for configuring communications require *IOSYSCFG special authority.
Note: You need *ALLOBJ to be able to change data using service functions.
Recommendations for Special Authorities: Giving special authorities to users represents a security exposure. For each user, carefully evaluate the need for any special authorities. Keep track of which users have special authorities and periodically review their requirement for the authority.
In addition, you should control the following situations for user profiles and programs:
o Whether user profiles with special authorities can be used to submit jobs
o Whether programs created by these users can run using the authority of the program owner.
Programs adopt the *ALLOBJ special authority of the owner if:
o The programs are created by users who have *ALLOBJ special authority
o The user specifies USRPRF(*OWNER) parameter on the command that creates the program.

ACTIONS

Review all users shown below. Ensure that only appropriate users have this authority.

M

RESULTS

```
The following *USER users have *IOSYSCFG special authority:
QCLUMGT     IBM-supplied User Profile
QCLUSTER    IBM-supplied User Profile
USER3       USER PROFILE1

3 users.

The following *PGMR users have *IOSYSCFG special authority:
QPM400      IBM-supplied User Profile

1 users.

The following *SYSOPR users have *IOSYSCFG special authority:
QLPAUTO     IBM-supplied User Profile
QLPINSTALL  IBM-supplied User Profile
QSVCDRCTR   IBM-supplied User Profile

3 users.

The following *SECOFR users have *IOSYSCFG special authority:
MANAGER4    Security Officer
QSECOFR     Security Officer
QSYS        Internal System User Profile

3 users.

No *SECADM users have *IOSYSCFG authority.

0 users.
```

5 UPASSWORD - User passwords

RISKS

Passwords are the most important means of securing access to your system.

5.1 PWDEXPITV - Users password expiry interval

M

RISKS

Requiring users to change their passwords after a specified length of time reduces the risk of an unauthorized person accessing the system. The password expiration interval controls the number of days that a valid password can be used before it must be changed.
When a user's password has expired, the user receives a message at sign-on. The user can either press the Enter key to assign a new password or press F3 (Exit) to cancel the sign-on attempt without assigning a new password. If the user chooses to change the password, the Change Password display is shown and full password validation is run for the new password.

ACTIONS

Set the QPWDEXPITV system value for an appropriate interval, such as 60 to 90 days.Use the password expiration interval field in the user profile for individual users who should change their passwords more frequently, such as security administrators.Use the user profile password interval to require profiles with *SERVICE, *SAVSYS, or *ALLOBJ special authorities to change passwords more frequently than other users.o *SYSVAL The QPWDEXPITV system value is used.o *NOMAX The system does not require the user to change the password.Specify a number from 1 through 366.

M

RESULTS

The system parameter QPWDEXPITV is set to 60 days.
Your company standard is 60 days for ordinary users and 30 for 'system' users.
This setting will be over-ridden by any users which have individual password expiration intervals.

5.2 PWDEXPD - Users with password set to expired

M

RISKS

CHANGE THIS FROM IBM
The Set password to expired field allows a security administrator to indicate in the user profile that the user's password is expired and must be changed the next time the user signs on. This value is reset to *NO when the password is changed. You can change the password by using either the CHGPWD or CHGUSRPRF command, or the QSYCHGPW API, or as part of the next sign-on process.
This field can be used when a user cannot remember the password and a security administrator must assign a new one. Requiring the user to change the password assigned by the security administrator prevents the security administrator from knowing the new password and signing on as the user.
When a user's password has expired, the user receives a message at sign-on. The user can either press the Enter key to assign a new password or press F3 (Exit) to cancel the sign-on attempt without assigning a new password. If the user chooses to change the password, the Change Password display is shown and password validation is run for the new password.

ACTIONS

Examine users with expired passwords and determine why they have not signed-on and changed their password.They may no longer need access to the system.

L

RESULTS

```
No users have expired passwords.
```

5.3 PWDLCHG - Users password last changed

M

RISKS

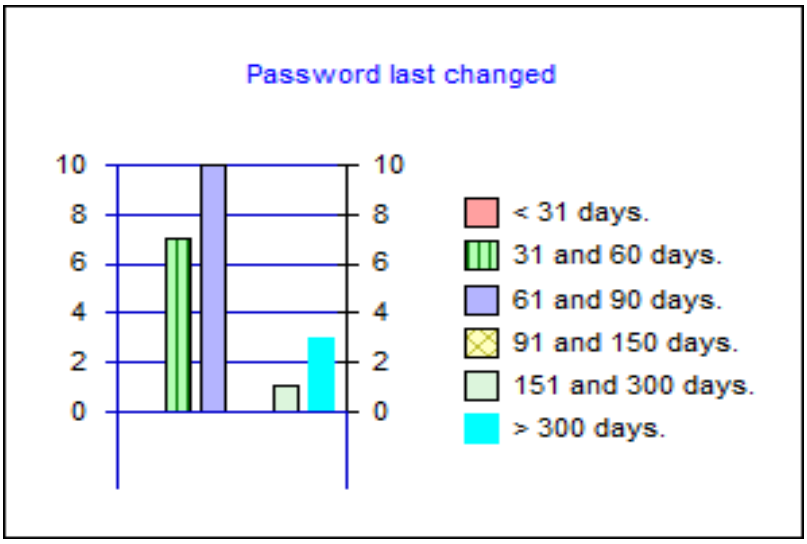
This shows when a user last changed their password.

ACTIONS

Passwords should have been changed recently, within the normal password change frequency. Examine those accounts which have not changed for many days.

M

RESULTS


Password last changed
10
8
6
4
2
0
10
8
6
4
2
0
< 31 days.
31 and 60 days.
61 and 90 days.
91 and 150 days.
151 and 300 days.
> 300 days.

IBM system profiles have been excluded from this list.

Range < 31 days.

No users in this range.

Range 31 and 60 days.

DAVID	13-Apr-2006	46	USER PROFILE1
MANAGER3	13-Apr-2006	46	USER PROFILE1
USER1	13-Apr-2006	46	USER PROFILE1
USER11	13-Apr-2006	46	USER PROFILE2
USER2	13-Apr-2006	46	USER PROFILE1
USER6	17-Apr-2006	42	USER PROFILE1
USER9	09-Apr-2006	50	USER PROFILE1

7 users.

Range 61 and 90 days.

MANAGER2	13-Mar-2006	77	USER PROFILE1
MANAGER4	18-Mar-2006	72	Security Officer
MANAGER6	13-Mar-2006	77	USER PROFILE1
USER12	13-Mar-2006	77	USER PROFILE2
USER13	13-Mar-2006	77	USER PROFILE2
USER14	13-Mar-2006	77	USER PROFILE2
USER18	13-Mar-2006	77	USER PROFILE2
USER3	23-Mar-2006	67	USER PROFILE1
USER4	11-Mar-2006	79	USER PROFILE1
USER5	16-Mar-2006	74	USER PROFILE1

10 users.

Range 91 and 150 days.

No users in this range.

Range 151 and 300 days.

USER17	13-Nov-2005	197	USER PROFILE2

1 users.

Range > 300 days.

MANAGER1	13-May-2005	381	USER PROFILE1
USER7	13-Feb-2005	470	USER PROFILE1
USER8	13-Feb-2005	470	USER PROFILE1

3 users.

5.4 PWDIBMPRO - IBM system profiles where password <> *NONE

L

RISKS

IBM has a number of standard system profiles which should not have a password and should not be signed on to.

ACTIONS

The profiles shown below should have a password set to *NONE but do not.

H

RESULTS

```
Some IBM system profiles do not have a password set to *NONE:

QSECOFR   Security Officer
QSYSOPR   System Operator
```

5.5 PWDNOTLO - Users who have not logged on

M

RISKS

The users shown below do not have a Previous Sign-On Date shown in the user file. This indicates that they have not logged on to the system.
Unused accounts represent an unnecessary risk to the system.

ACTIONS

Review these users and determine if the accounts are still needed. Remove any not needed being careful NOT to remove systems accounts.

H

RESULTS

The following user profiles have not signed on to the system.

DAVID	USER PROFILE1	Active
MANAGER1	USER PROFILE1	Active
MANAGER3	USER PROFILE1	Active
MANAGER6	USER PROFILE1	Active
QBRMS	IBM-supplied User Profile	Active
QCLUMGT	IBM-supplied User Profile	Active
QCLUSTER	IBM-supplied User Profile	Active
QCOLSRV	IBM-supplied User Profile	Active
QDBSHR	Internal Data Base User Profile	Active
QDBSHRDO	Internal Data Base User Profile	Active
QDESADM	DB2 TEXT EXTENDER ADMINISTRATOR	Active
QDESUSR	DB2 TEXT EXTENDER USER	Active
QDFTOWN	Default Owner for System Objects	Active
QDIRSRV	OS/400 Directory Services Server User Profile	Active
QDLFM	IBM-supplied User Profile	Active
QDOC	Internal Document User Profile	Active
QDSNX	IBM-supplied User Profile	Active
QEJB	IBM-supplied User Profile	Active
QFNC	IBM-supplied User Profile	Active
QGATE	IBM-supplied User Profile	Active
QIPP	IBM-supplied User Profile	Active
QLPAUTO	IBM-supplied User Profile	Active
QLPINSTALL	IBM-supplied User Profile	Active
QMQM	MQSERIES PROFILE	Active
QMQMADM	MQSERIES GROUP PROFILE	Active
QMSF	Mail Server Framework Profile	Active
QNETSPLF	Internal Spool Network Profile	Active
QNFSANON	IBM-supplied User Profile	Active
QNTP	IBM-supplied User Profile	Active
QPGMR	Programmer and Batch User	Active
QPM400	IBM-supplied User Profile	Active
QRJE	IBM-supplied User Profile	Active
QSNADS	IBM-supplied User Profile	Active
QSPL	Internal Spool User Profile	Active
QSPLJOB	Internal Spool User Profile	Active
QSRV	Service User Profile	Active
QSRVBAS	Basic Service User Profile	Active
QSVCDRCTR	IBM-supplied User Profile	Disabled
QSYS	Internal System User Profile	Active
QTCM	IBM-supplied User Profile	Disabled
QTCP	Internal TCP/IP User Profile	Active
QTFTP	IBM-supplied User Profile	Active
QTMHHTP1	HTTP Server CGI User Profile	Active
QTMHHTTP	HTTP Server User Profile	Active
QTMPLPD	REMOTE REQUESTERS	Active
QTMTWSG	5250 HTML WORKSTATION GATEWAY PROFILE	Active
USER10	USER PROFILE2	Disabled
USER11	USER PROFILE2	Active
USER2	USER PROFILE1	Active
USER3	USER PROFILE1	Active
USER4	USER PROFILE1	Active
USER5	USER PROFILE1	Active
USER6	USER PROFILE1	Active
USER8	USER PROFILE1	Active
USER9	USER PROFILE1	Active

55 users have not signed on to the system.

5.6 PWDLASTLO - Users last logon date

M

RISKS

Shown below are the last time users logged on to the system. Users who have not used their account for a long time may not need it anymore and represent a risk to the system.

ACTIONS

Review the users who have not used their account for a long time and determine if the accounts are still needed. Remove any accounts not needed being careful NOT to remove systems accounts.

H

RESULTS

Users signed on 0 days to 30 days.

No users have signed onto the system in this time period.

Users signed on 31 days to 60 days.

No users have signed onto the system in this time period.

Users signed on 61 days to 90 days.

No users have signed onto the system in this time period.

Users signed on 91 days to 150 days.

No users have signed onto the system in this time period.

Users signed on 150 days to 300 days.

User	Date	Days sign-on	Status
MANAGER2	30/11/2005	180	Active
MANAGER5	20/10/2005	221	Disabled
QSYSOPR	20/10/2005	221	Disabled
USER1	30/08/2005	272	Active
USER12	15/08/2005	287	Active
USER13	13/08/2005	289	Active
USER14	22/09/2005	249	Active
USER15	27/09/2005	244	Disabled
USER18	18/09/2005	253	Active
USER7	29/10/2005	212	Active

10 users last signed on in this time period.

Users signed on 301 days to 9999 days.

User	Date	Days sign-on	Status
MANAGER4	18/03/2005	437	Active
QSECOFR	18/03/2005	437	Active
USER16	30/07/2005	303	Disabled
USER17	12/07/2005	321	Active

4 users last signed on in this time period.

14 users have signed on

6 SIGNON - Signon attempts allowed

RISKS

Each user signs on to the system usually with a user-ID and a password. The number of attempts is limited to prevent people guessing passwords.

6.1 QMAXSIGN - Maximum sign-on attempts

M

RISKS

This controls the maximum number of invalid sign-on attempts permitted (for both local and remote users) by the system. A limit of 3 invalid sign-on attempts is allowed before the user profile is disabled. Once a successful sign-on has occurred, the counter is reset to zero.
Note: An invalid sign-on attempt can be caused by:
o entering an incorrect user-id
o entering an incorrect password
o by trying to sign-on to a display station that the user does not have the authority to use.

ACTIONS

Recommended value 3The QMAXSIGN value should be set to a low, yet feasible value, so that sign-on security controls can be effective. The industry standard for 'QMAXSIGN' is 3 to 5 invalid sign-ons.

M

RESULTS

This setting is a little high at 5

6.2 QMAXSGNACN - Maximum sign-On attempt action

L

RISKS

Action to prevent further attempts - once a user reaches the maximum number of invalid sign-ons:
1 disable device,
2 disable user profile,
3 disable both user profile and device.

ACTIONS

Recommended value 2 or 3

L

RESULTS

The users terminal and profile will be disabled with a setting of 3

6.3 QRMTSIGN - Remote sign-on

M

RISKS

This value controls whether a user accessing the system via the AS/400 pass-through facility will be required to undergo normal system sign-on prior to accessing any resources.
Remote sign-on are allowed, but the user must sign-on with a valid user profile and password. In this mode, it is assumed that the system(node) where the incoming user originated from, is adequately secured.

ACTIONS

Recommended value *FRCSIGNON The 'QRMTSIGN' should be set to *FRCSIGNON value so that all pass-through sessions that begin on the system must go through the normal sign-on.

L

RESULTS

This is currently set to *REJECT

6.4 QLMTESCOFR - Limit security officer

L

RISKS

Users with *ALLOBJ and *SERVICE special authority can sign-on to any display device configured to the system. This value restricts access to specific workstations.
QLMTSECOFR can be set to either 0 or 1. When set to 0, privileged users can sign on to any workstation.

ACTIONS

Recommended value 1Setting QLMTSECOFR to 1 restricts privileged users from signing on to any terminal for which they don't already have specific authorization. QLMTSECOFR has a limited effect when a privileged user is signed on to the system console. The shipped value is 1.

H

RESULTS

The value is currently set to 0

6.5 QDSPSGNINF - Display sign-on information

M

RISKS

The system will show an informational display at sign-on that contains the date and time last signed-on and the number of invalid sign-on attempts.
This controls whether or not the AS/400 will provide key sign-on information such as:
o date of last sign on,
o the number of invalid sign-on attempts,
o the number of days until the current password expires.

ACTIONS

Recommended value 1The 'QDSSGNINF' value should be set to '1', so that key sign-on information is displayed when a user completes a successful sign-on.This control allows a user to detect if someone has been tampering with their user-id/account.

L

RESULTS

Correctly set to 1

6.6 QLMTDEVSSN - Limit device sessions

L

RISKS

End users are limited in the number of concurrent devices they can be signed on to. The absence of this control increases the risk that a terminal may remain signed on and left unattended, thus allowing unauthorized access to the system and reducing the risk that users will share their User-IDs and passwords.
After signing on, the only additional jobs that can be started for that user are group jobs and system requests originating from the same terminal.

ACTIONS

Recommended value 1The 'QLMTDEVSSN' value should be set to a value of '1', so that users can only be signed on to one device at any given time.

H

RESULTS

The value is wrongly set to 0

6.7 QINACTITV - Inactive Interval

M

RISKS

This controls the amount of time a terminal can remain signed-on without any activity. Once the inactive threshold is reached, the system automatically logs-off the User-ID, requiring the user to undergo a regular sign-on session.
Note: Consideration should be given to the processing environment, e.g., shop floor operations, customer service, etc.
The absence of this control increases the risk that a terminal may remain signed on and left unattended, thus allowing unauthorized access to the system.
Terminals left unattended for an extended period of time may be used by unauthorized persons to perform functions that are available under that session, possibly affecting production data and processing.
In addition, unauthorized users of unattended terminals may remain unidentifiable.

ACTIONS

Recommended value 30The 'QINACTITV' threshold should be set to a value that is practical, yet effective.

M

RESULTS

This is set to NONE and terminals will not time-out.

6.8 QINACTMSGQ - Inactive Message Queue

L

RISKS

The action taken when interactive jobs time out.

ACTIONS

Recommended value *DSCJOB

L

RESULTS

Any dormant job will be disconnected. - *DSCJOB

7 GROUPS - Groups

RISKS

Users are grouped together in to groups which link their job functions and the actions they need to perform on the system.

7.1 GROUPS - Users in each group

RISKS

Users may be a member of a group.

ACTIONS

Examine the groups in which users reside and ensure that this is appropriate.

RESULTS

```
Group - QMQMADM
QMQM          QPGMR

Group - QMQMADM
QMQM          QPGMR
```

8 AUDITING - Auditing

RISKS

Auditing is a means of recording key actions of users.

8.1 QAUDCTL - Audit control

L

RISKS

Indicates what the system will audit based on those objects designated by the CHGOBJAUD command and by the system value QUADLVL.
If auditing is not turned on (i.e. *NONE), then it will be impossible to review security violations

ACTIONS

Recommended value *AUDLVLSet the audit level system value using CHGSYSVAL: CHGSYSVAL SYSVAL (QAUDCTL)+ VALUE('*AUDLVL *NOQTEMP')The value *NOQTEMP is optional but will reduce the volume of data recorded because the system does not have to record information about library QTEMP.If you would like to use a simple technique to set up auditing, use the Change Security Auditing (CHGSECAUD) command. The CHGSECAUD command will create the journal receiver and audit journal, and allow you to set the system values QAUDLVL and QAUDCTL in one operation.

L

RESULTS

Correctly set to *NOQTEMP,*AUDLVL

8.2 QAUDLVL - Audit level

M

RISKS

This controls which security related events are logged to the security journal (QAUDJRN).

ACTIONS

The 'QAUDLVL' value should be set at a minimum to:o *SECURITY (logs all system security modifications)o *AUTFAIL (logs all authorization failures)o *SAVRST (logs all security related objects restore activities).Proper evaluation of the system performance and resource requirements should be evaluated before selecting the 'QAUDLVL' options since logging does impact system performance and DASD utilization.Optional *CREATE *OBJMGT *PGMFAIL *JOBDTA *PRTDTA *DELETEAvoid for performance reasons global auditing of program adopt and spool file data.Avoid *PGMADP *SPLFDTAEntries in the audit journal that report authorization failures should be reviewed.

L

RESULTS

The following types of auditing are being employed:

*JOBDTA - start, change, hold, release, and end job operations are audited. This includes server sessions and remote connection jobs.

*NETCMN - violations detected by the APPN Filter support are audited.

*DELETE - the deletion of objects is audited.

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

*SAVRST - save and restore operations are audited.

*AUTFAIL - unsuccessful log-on attempts and unauthorized attempts to use sensitive objects are audited. These include rejected connection attempts, invalid network sign-on attempts, and attempts to perform an operation or access an object to which the user isn/t authorized.

*SERVICE - starting, pausing, and stopping servers and using service tools are audited.

*PGMFAIL - programs that run a restricted machine interface instruction or access objects via an unsupported interface are audited.

*SECURITY - a wide range of security-related activities are audited, including:
- changing an object/s audit value or a user/s audit setting
- changing an authorization list or an object/s authority
- changing an object/s ownership
- creating, restoring, or changing a user profile
- requests to reset the DST QSECOFR password
- generating a profile handle through the QSYGETPH API
- changing a network attribute, system value, or service attribute.

The following types of auditing are NOT being used:
*CREATE - the creation of new objects or objects that replace existing objects is audited.

*OBJMGT - object rename and move operations are audited.

*OFCSRV - OfficeVision for OS/400 tasks (e.g., changing the system distribution directory, opening a mail log) are audited.

*PGMADP - gaining access to objects via program adopted authority is audited.

*PRTDTA - printing job output is audited whether the output is sent directly to a printer, sent to a remote system, or spooled and printed on a local machine.

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

8.3 QAEA - Audit end action

L

RISKS

Indicates that the system operator is notified when the audit journal cannot receive records.

ACTIONS

Recommended value *NOTIFY

RESULTS

Correctly set to *NOTIFY

8.4 QAFREQ - Audit frequency level

RISKS

The system will determine when journal entries are written out from the security journal to auxiliary.

ACTIONS

Recommended value *SYS

RESULTS

Correctly set to *SYS

8.5 QCRTOBJAUD - Create object audit

RISKS

States default auditing when objects are created in a library whose Create Object Auditing value (CRTOBJAUD) is set to *SYSVAL.

ACTIONS

Recommended value *NONE

RESULTS

The value is currently set to *USRPRF