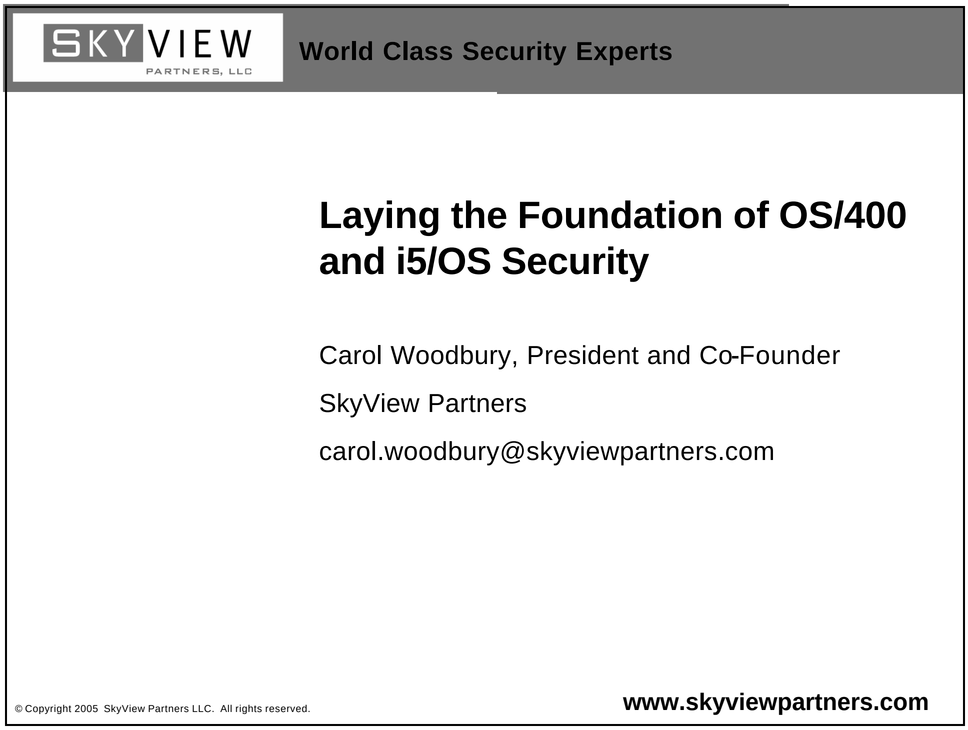


World Class Security Experts

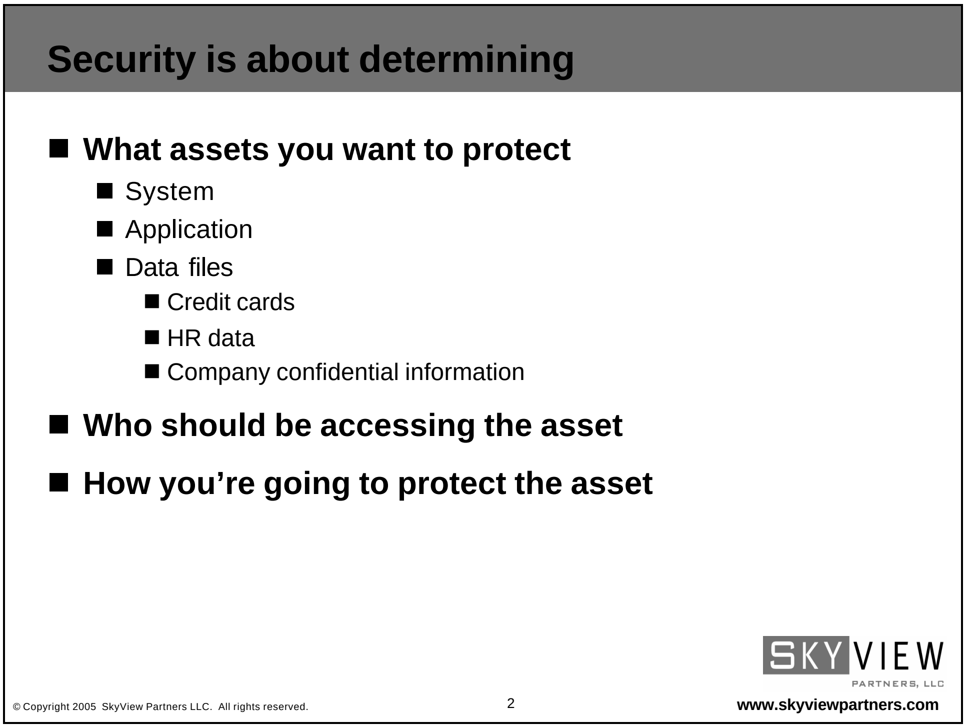
Laying the Foundation of OS/400 and i5/OS Security

Carol Woodbury, President and Co-Founder

SkyView Partners

carol.woodbury@skyviewpartners.com

www.skyviewpartners.com



Security is about determining

- **What assets you want to protect**
  - System
  - Application
  - Data files
    - Credit cards
    - HR data
    - Company confidential information
- **Who should be accessing the asset**
- **How you're going to protect the asset**

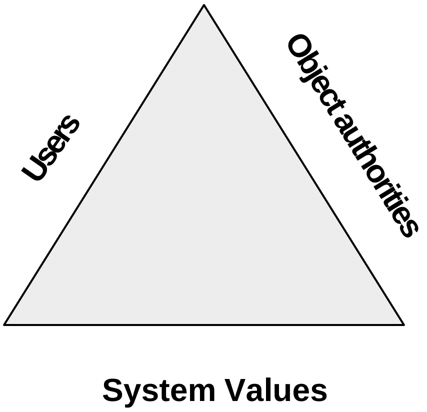
2

www.skyviewpartners.com

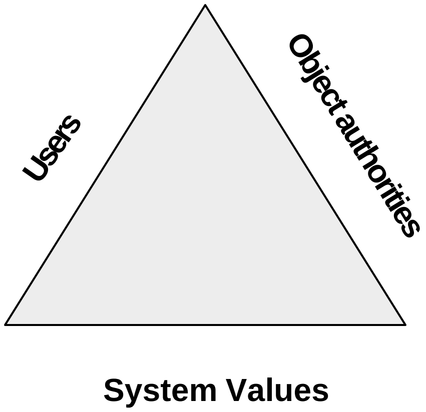
Agenda

- Securing objects – libraries, files, etc
- Defining users
- Authority search order
- Adopted authority
- Protecting your system
  - Security-relevant system values
  - Passwords
  - Auditing
- IFS security
- For more information …

Core of OS/400 Security

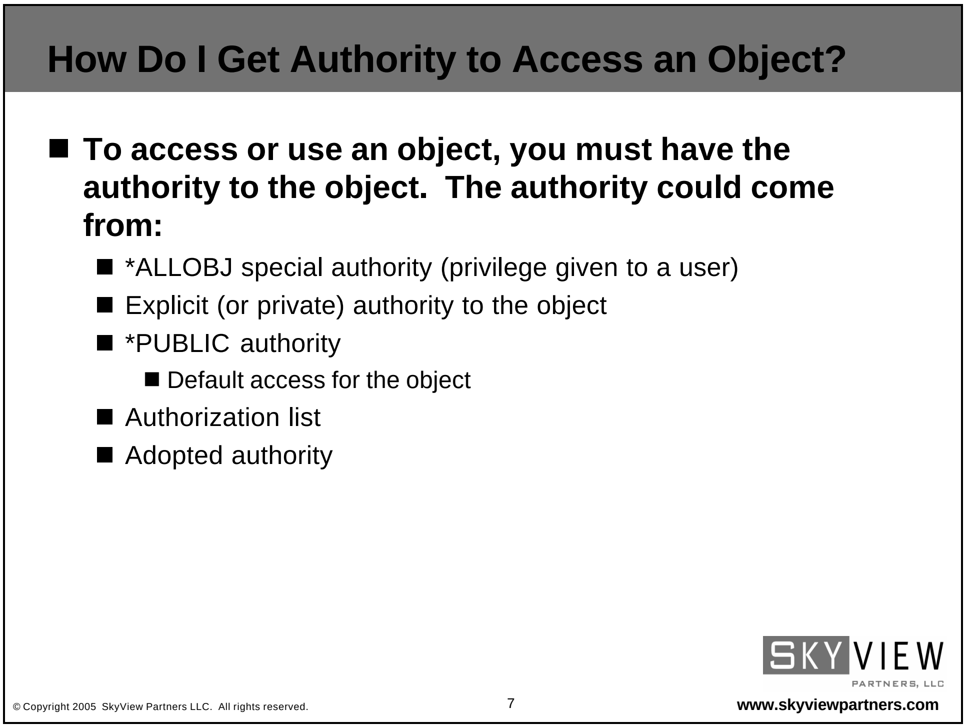


Protecting Assets



Protecting Assets

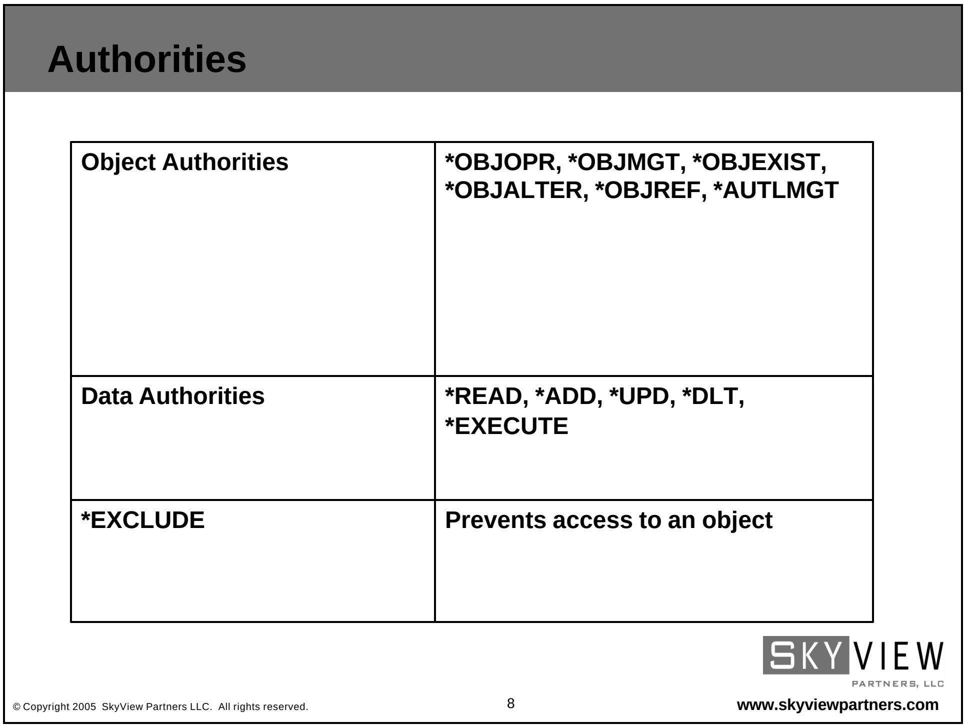
- **How should the asset be protected?**
  - Excluded, except for authorized users
  - OK for general public access – read only
  - OK for general public access - update



How Do I Get Authority to Access an Object?

- **To access or use an object, you must have the authority to the object. The authority could come from:**
  - *ALLOBJ special authority (privilege given to a user)
  - Explicit (or private) authority to the object
  - *PUBLIC authority
    - Default access for the object
  - Authorization list
  - Adopted authority

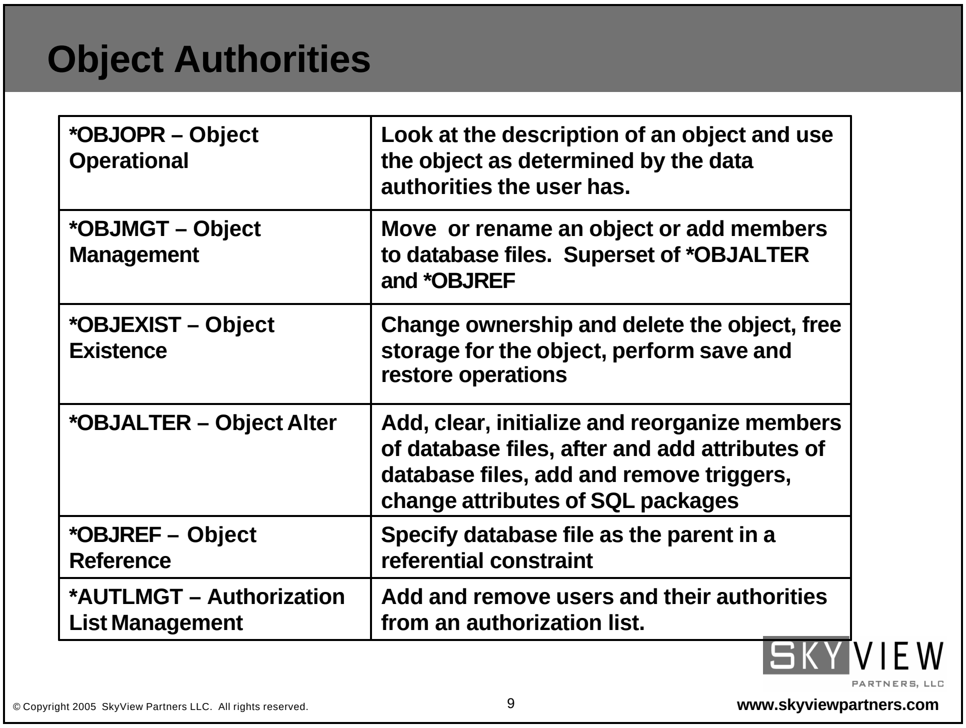
© Copyright 2005 SkyView Partners LLC. All rights reserved. 7 **www.skyviewpartners.com**



Authorities

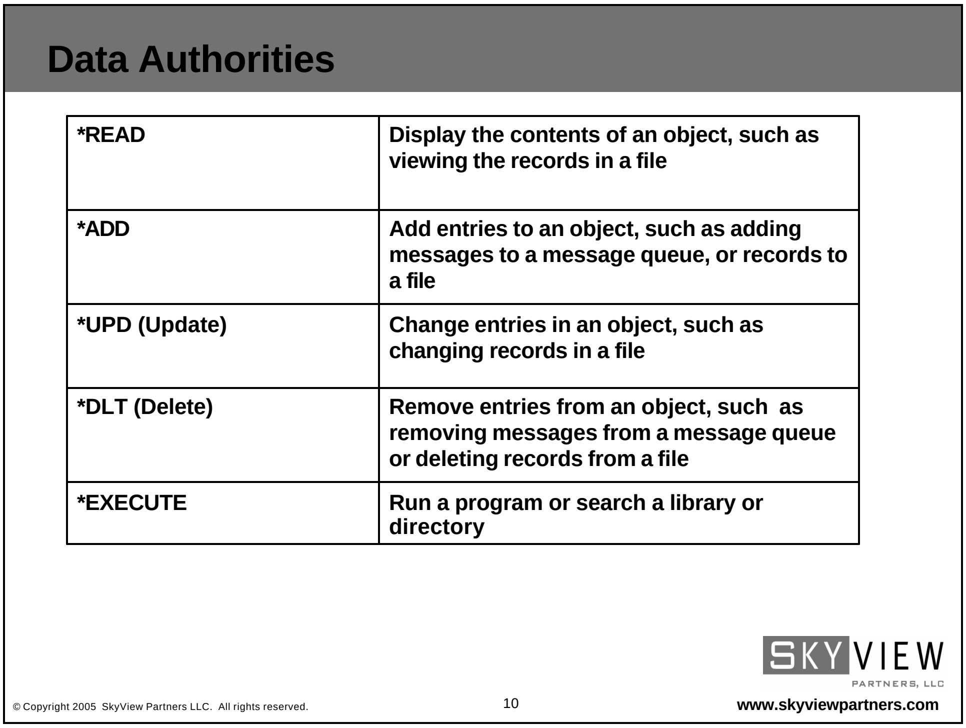
Object Authorities	***OBJOPR, *OBJMGT, *OBJEXIST, *OBJALTER, *OBJREF, *AUTLMGT**
Data Authorities	***READ, *ADD, *UPD, *DLT, *EXECUTE**
***EXCLUDE**	**Prevents access to an object**

© Copyright 2005 SkyView Partners LLC. All rights reserved. 8 **www.skyviewpartners.com**



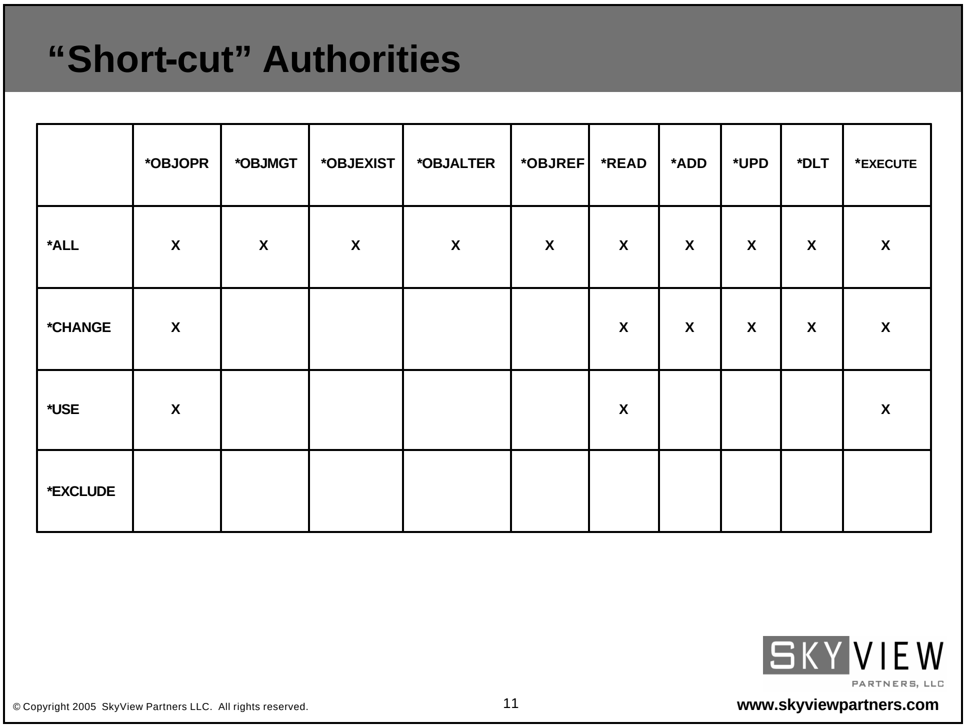
Object Authorities

*OBJOPR – Object Operational	Look at the description of an object and use the object as determined by the data authorities the user has.
*OBJMGT – Object Management	Move or rename an object or add members to database files. Superset of *OBJALTER and *OBJREF
*OBJEXIST – Object Existence	Change ownership and delete the object, free storage for the object, perform save and restore operations
*OBJALTER – Object Alter	Add, clear, initialize and reorganize members of database files, after and add attributes of database files, add and remove triggers, change attributes of SQL packages
*OBJREF – Object Reference	Specify database file as the parent in a referential constraint
*AUTLMGT – Authorization List Management	Add and remove users and their authorities from an authorization list.



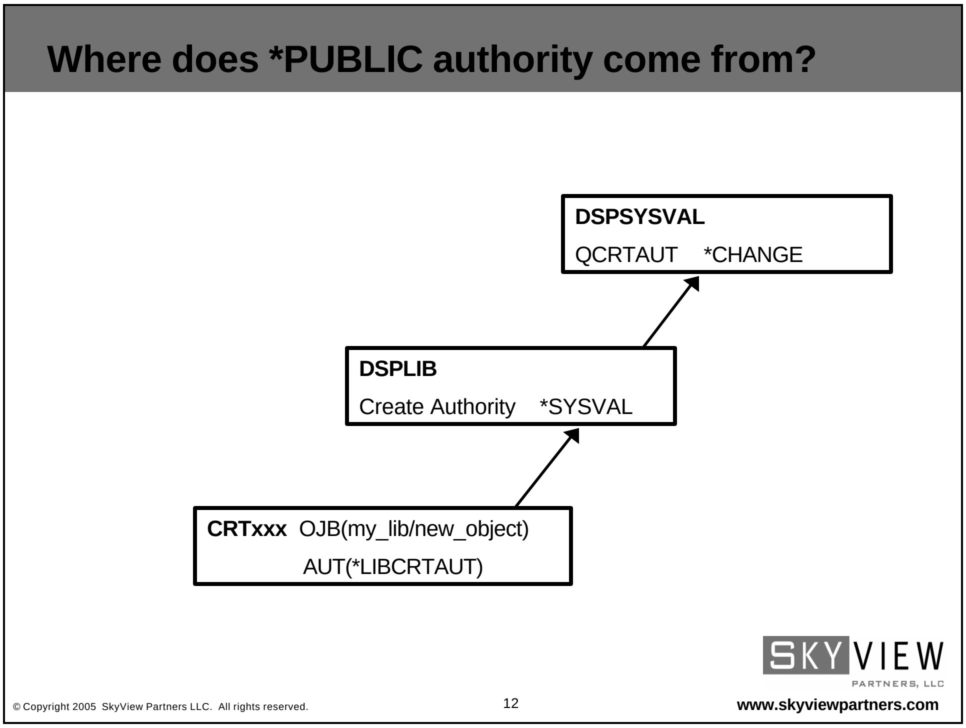
Data Authorities

*READ	Display the contents of an object, such as viewing the records in a file
*ADD	Add entries to an object, such as adding messages to a message queue, or records to a file
*UPD (Update)	Change entries in an object, such as changing records in a file
*DLT (Delete)	Remove entries from an object, such as removing messages from a message queue or deleting records from a file
*EXECUTE	Run a program or search a library or directory



“Short-cut” Authorities

	*OBJOPR	*OBJMGT	*OBJEXIST	*OBJALTER	*OBJREF	*READ	*ADD	*UPD	*DLT	*EXECUTE
*ALL	X	X	X	X	X	X	X	X	X	X
*CHANGE	X					X	X	X	X	X
*USE	X					X				X
*EXCLUDE										

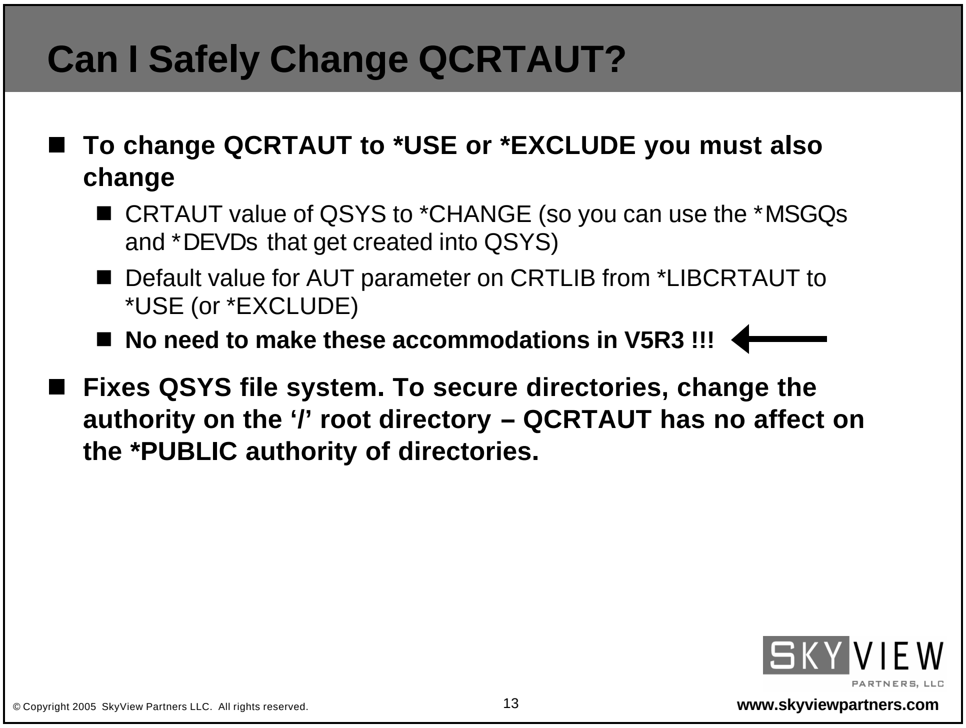


Where does *PUBLIC authority come from?

DSPSYSVAL
QCRTAUT *CHANGE

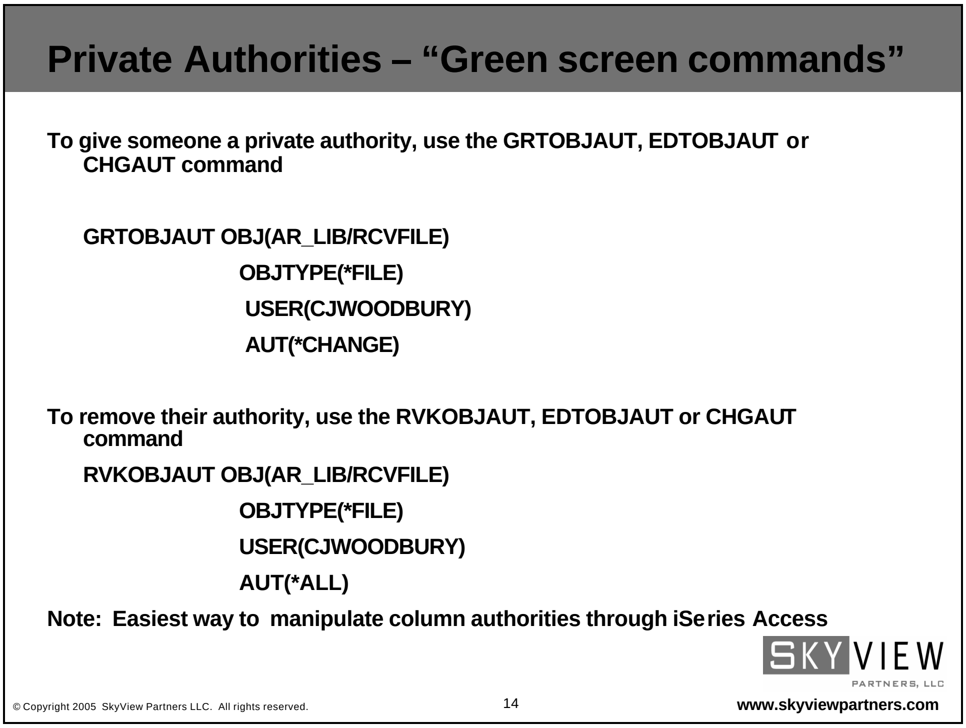
DSPLIB
Create Authority *SYSVAL

CRTxxx OJB(my_lib/new_object)
AUT(*LIBCRTAUT)



Can I Safely Change QCRTAUT?

- **To change QCRTAUT to *USE or *EXCLUDE you must also change**
  - CRTAUT value of QSYS to *CHANGE (so you can use the *MSGQs and *DEVDs that get created into QSYS)
  - Default value for AUT parameter on CRTLIB from *LIBCRTAUT to *USE (or *EXCLUDE)
  - **No need to make these accommodations in V5R3 !!!** ⟵
- **Fixes QSYS file system. To secure directories, change the authority on the '/' root directory – QCRTAUT has no affect on the *PUBLIC authority of directories.**



Private Authorities – "Green screen commands"

To give someone a private authority, use the GRTOBJAUT, EDTOBJAUT or CHGAUT command

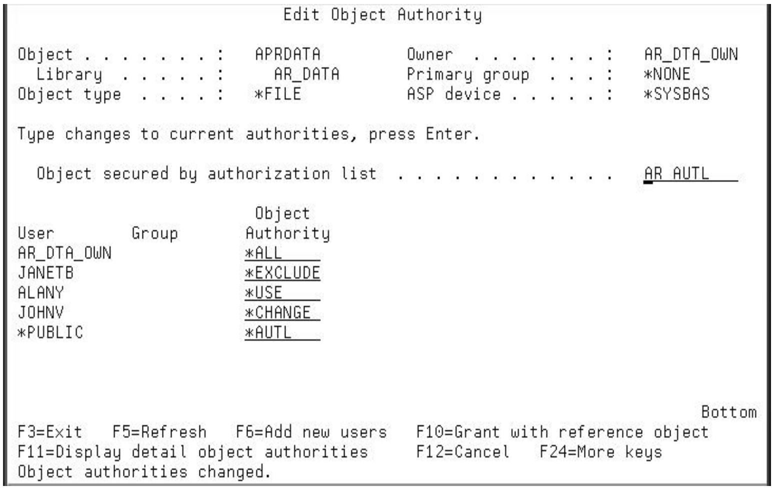
```
GRTOBJAUT OBJ(AR_LIB/RCVFILE)
                   OBJTYPE(*FILE)
                    USER(CJWOODBURY)
                    AUT(*CHANGE)
```

To remove their authority, use the RVKOBJAUT, EDTOBJAUT or CHGAUT command

```
RVKOBJAUT OBJ(AR_LIB/RCVFILE)
                   OBJTYPE(*FILE)
                   USER(CJWOODBURY)
                   AUT(*ALL)
```

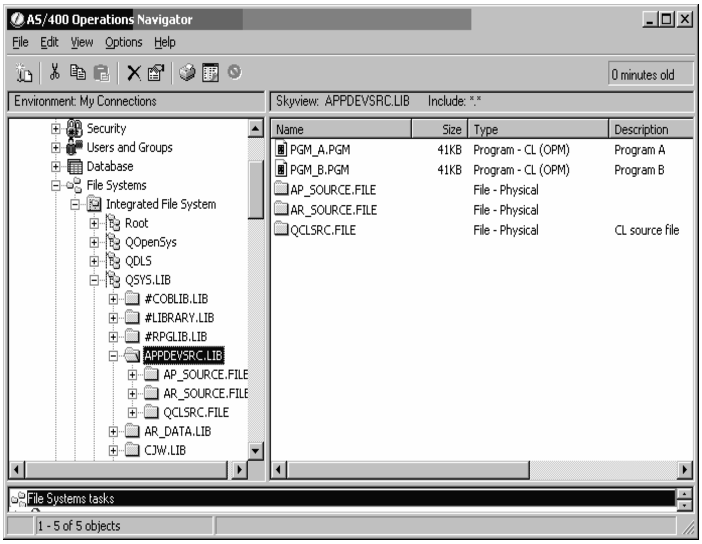
Note: Easiest way to manipulate column authorities through iSeries Access

EDTOBJAUT



```
                          Edit Object Authority

Object . . . . . . . :   APRDATA        Owner  . . . . . . . :   AR_DTA_OWN
  Library  . . . . . :     AR_DATA      Primary group  . . . :   *NONE
Object type  . . . . :   *FILE          ASP device . . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . . . .   AR_AUTL

                        Object
User        Group       Authority
AR_DTA_OWN              *ALL
JANETB                  *EXCLUDE
ALANY                   *USE
JOHNV                   *CHANGE
*PUBLIC                 *AUTL



                                                                     Bottom
F3=Exit   F5=Refresh   F6=Add new users   F10=Grant with reference object
F11=Display detail object authorities     F12=Cancel   F24=More keys
Object authorities changed.
```

Setting Authority on an Object



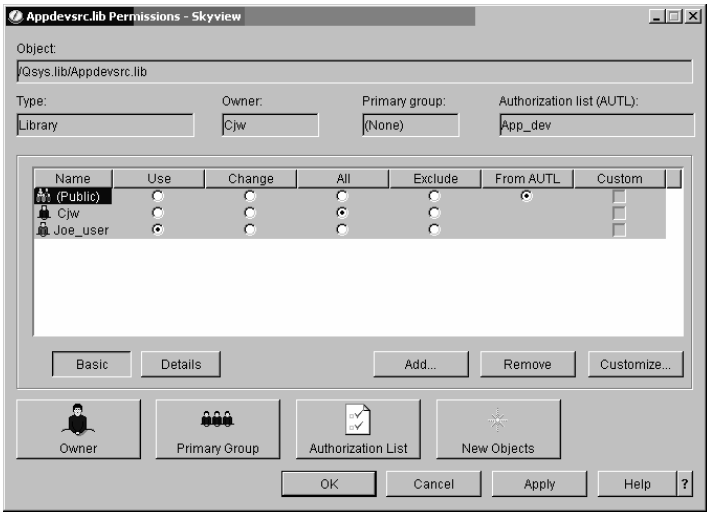
Skyview: APPDEVSRC.LIB Include: *.*

Name	Size	Type	Description
PGM_A.PGM	41KB	Program - CL (OPM)	Program A
PGM_B.PGM	41KB	Program - CL (OPM)	Program B
AP_SOURCE.FILE		File - Physical	
AR_SOURCE.FILE		File - Physical	
QCLSRC.FILE		File - Physical	CL source file

1 - 5 of 5 objects

- Right click on the object name, select Permissions

Permissions



Appdevsrc.lib Permissions - Skyview

Object: /Qsys.lib/Appdevsrc.lib

Type: Library

Owner: Cjw

Primary group: (None)

Authorization list (AUTL): App_dev

Name	Use	Change	All	Exclude	From AUTL	Custom
(Public)	○	○	○	○	●	□
Cjw	○	○	●	○		□
Joe_user	●	○	○	○		□

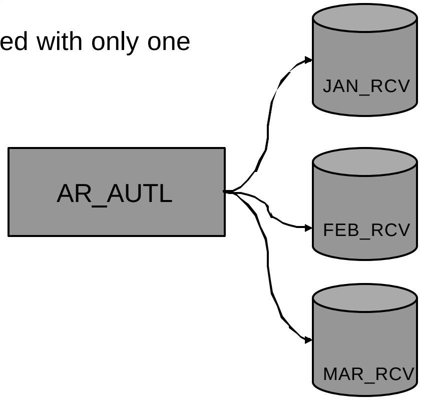
Authorization Lists

Way to group similar objects and only have to manage authority once

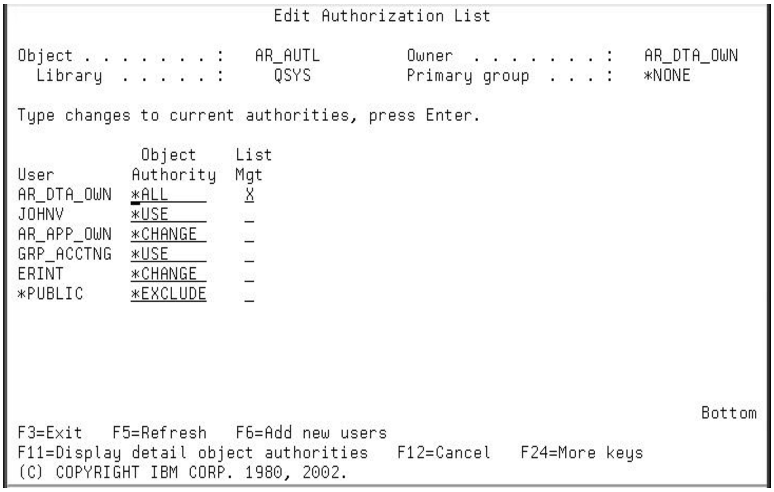
An object can be secured with only one authorization list

Grant Private Authorities:

KELSEY	*USE
TODD	*CHANGE
ABBY	*ALL
AVA	*USE
*PUBLIC(*EXCLUDE)	

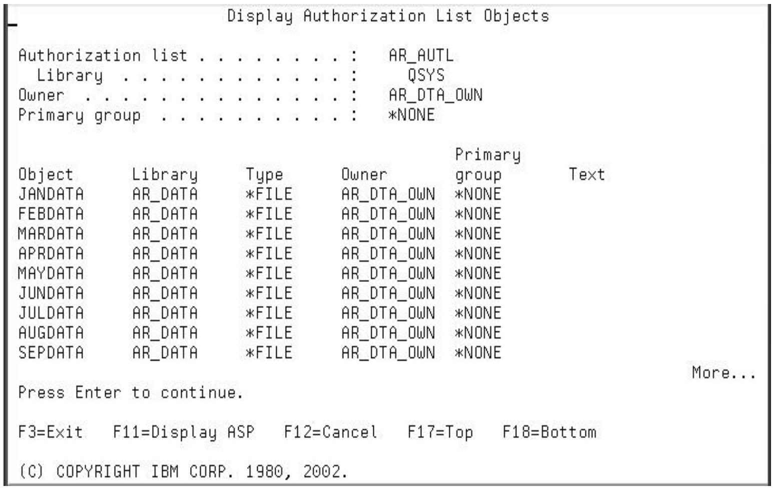


EDTAUTL



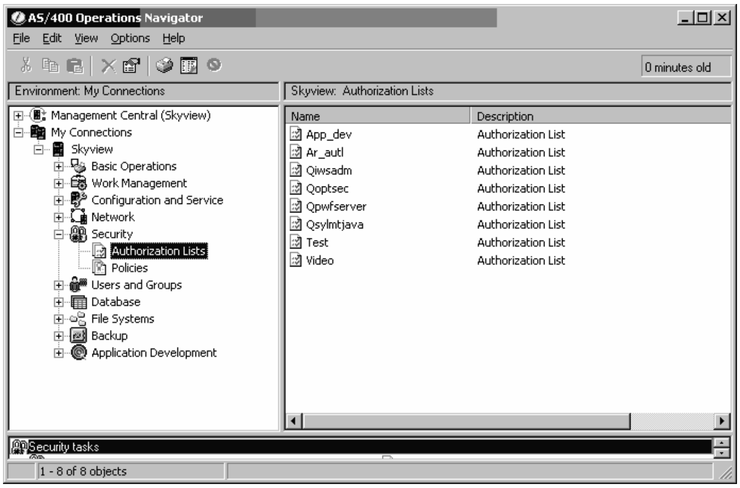
```
                           Edit Authorization List

Object . . . . . . . :   AR_AUTL        Owner  . . . . . . . :   AR_DTA_OWN
  Library  . . . . . :     QSYS         Primary group  . . . :   *NONE

Type changes to current authorities, press Enter.

             Object    List
User         Authority  Mgt
AR_DTA_OWN   *ALL        X
JOHNV        *USE        _
AR_APP_OWN   *CHANGE     _
GRP_ACCTNG   *USE        _
ERINT        *CHANGE     _
*PUBLIC      *EXCLUDE    _




                                                                      Bottom
F3=Exit   F5=Refresh   F6=Add new users
F11=Display detail object authorities   F12=Cancel   F24=More keys
(C) COPYRIGHT IBM CORP. 1980, 2002.
```

DSPAUTLOBJ



```
                      Display Authorization List Objects

Authorization list . . . . . . . . :   AR_AUTL
  Library  . . . . . . . . . . . . :     QSYS
Owner  . . . . . . . . . . . . . . :   AR_DTA_OWN
Primary group  . . . . . . . . . . :   *NONE

                                             Primary
Object      Library     Type       Owner       group       Text
JANDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
FEBDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
MARDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
APRDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
MAYDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
JUNDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
JULDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
AUGDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
SEPDATA     AR_DATA     *FILE      AR_DTA_OWN  *NONE
                                                                     More...
Press Enter to continue.

F3=Exit   F11=Display ASP   F12=Cancel   F17=Top   F18=Bottom

(C) COPYRIGHT IBM CORP. 1980, 2002.
```

Authorization Lists

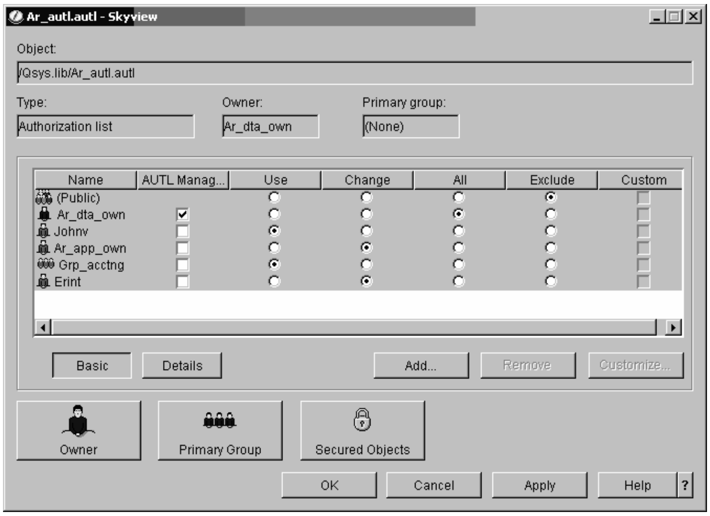


Skyview: Authorization Lists

Name	Description
App_dev	Authorization List
Ar_autl	Authorization List
Qiwsadm	Authorization List
Qoptsec	Authorization List
Qpwfserver	Authorization List
Qsylmtjava	Authorization List
Test	Authorization List
Video	Authorization List

1 - 8 of 8 objects

Authorization list authorities



Object: /Qsys.lib/Ar_autl.autl

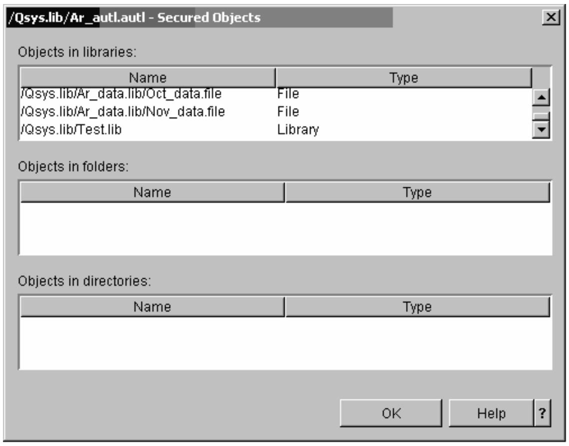
Type: Authorization list

Owner: Ar_dta_own

Primary group: (None)

Name	AUTL Manag...	Use	Change	All	Exclude	Custom
(Public)		○	○	○	●	□
Ar_dta_own	☑	○	○	●	○	□
Johnv	□	●	○	○	○	□
Ar_app_own	□	○	●	○	○	□
Grp_acctng	□	●	○	○	○	□
Erint	□	○	●	○	○	□

Objects secured by the authorization list



/Qsys.lib/Ar_autl.autl - Secured Objects

Objects in libraries:

Name	Type
/Qsys.lib/Ar_data.lib/Oct_data.file	File
/Qsys.lib/Ar_data.lib/Nov_data.file	File
/Qsys.lib/Test.lib	Library

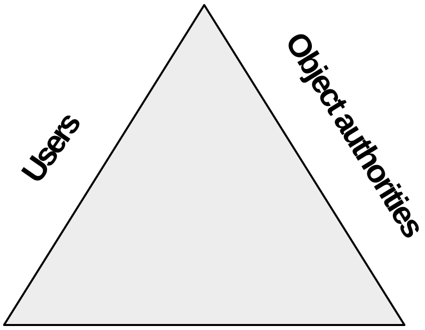
Objects in folders:

Name	Type

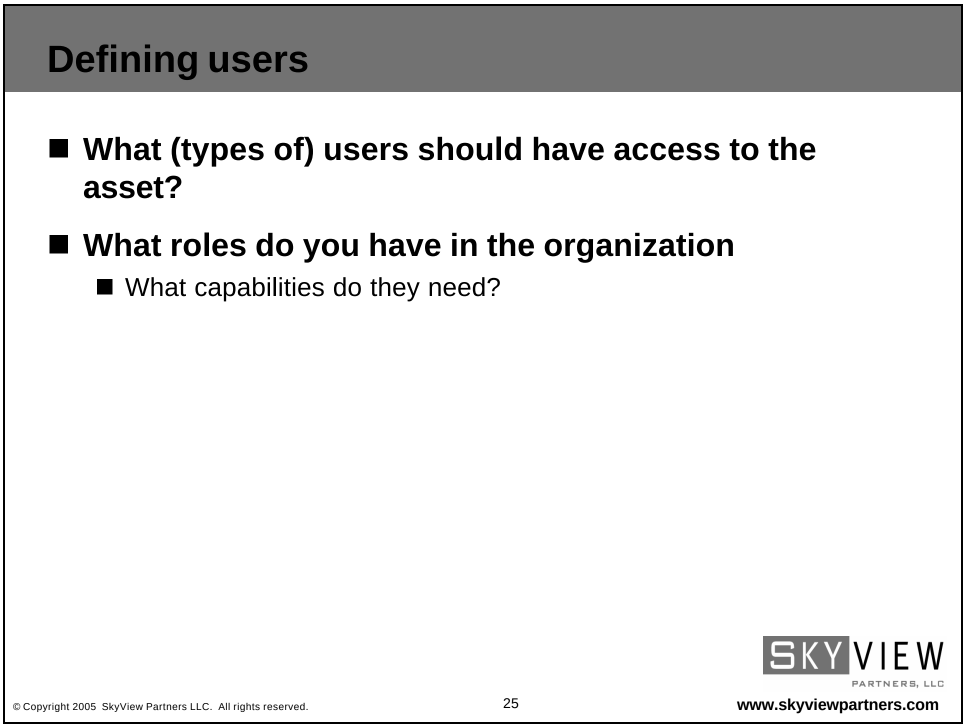
Objects in directories:

Name	Type

OS/400 Security Elements



System Values

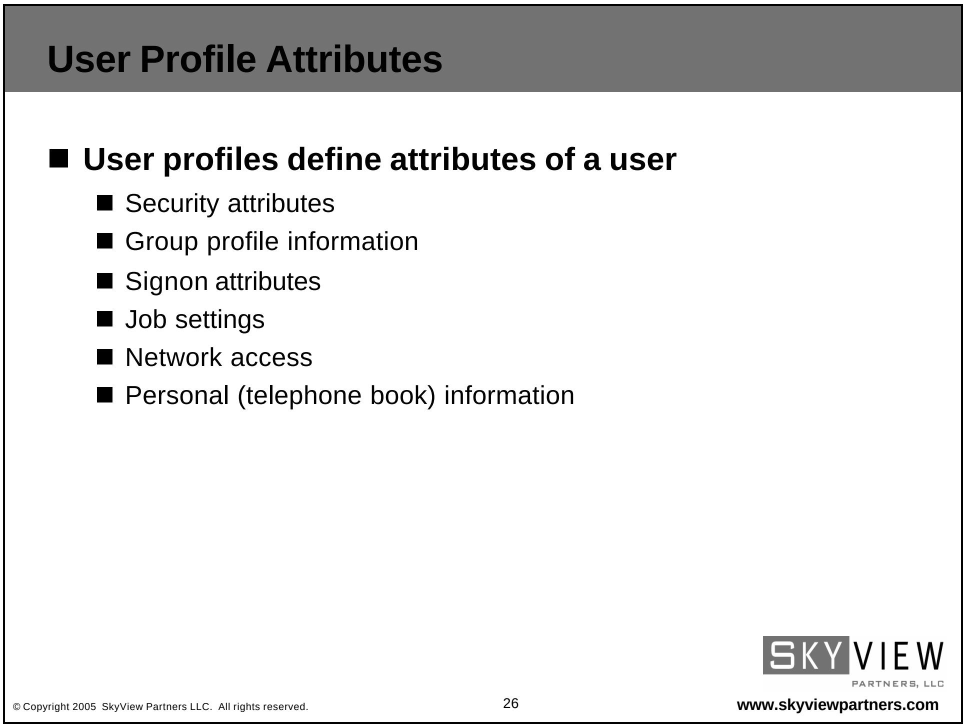


Defining users

- **What (types of) users should have access to the asset?**
- **What roles do you have in the organization**
  - What capabilities do they need?

25

www.skyviewpartners.com



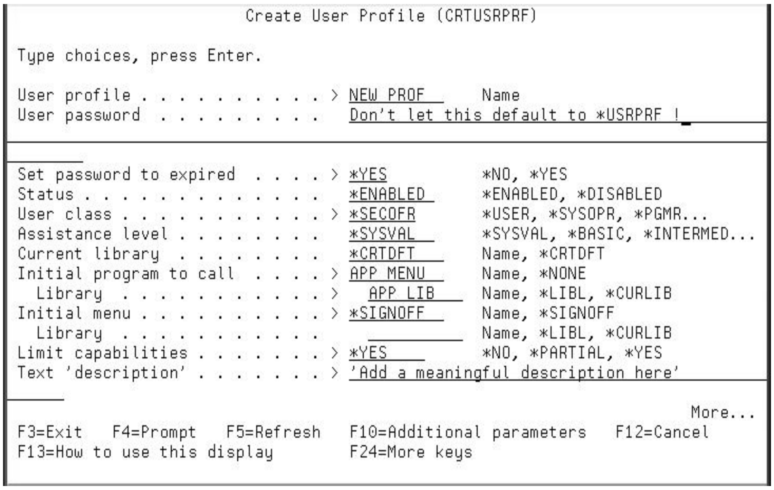
User Profile Attributes

- **User profiles define attributes of a user**
  - Security attributes
  - Group profile information
  - Signon attributes
  - Job settings
  - Network access
  - Personal (telephone book) information

26

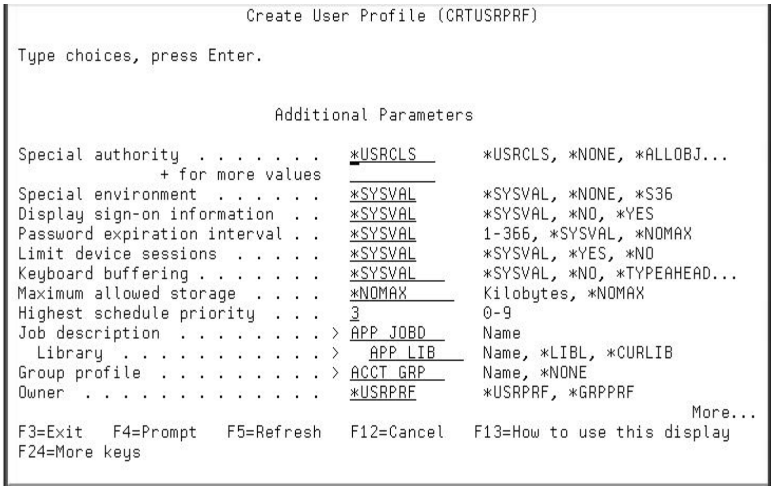
www.skyviewpartners.com

CRTUSRPRF – 1



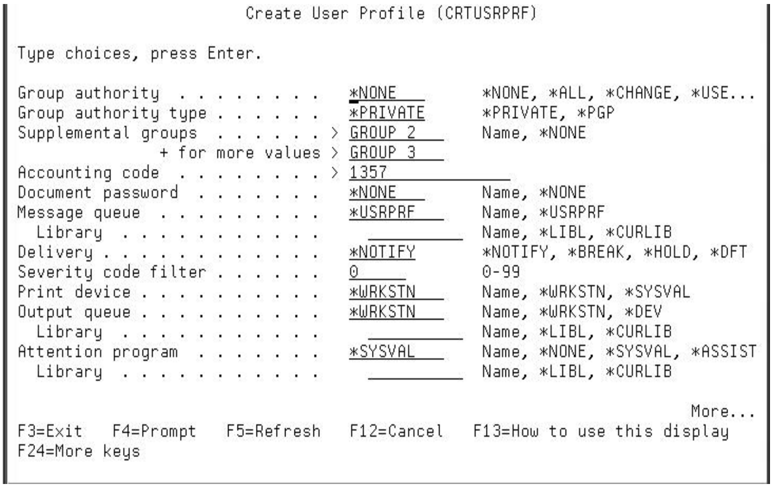
```
                        Create User Profile (CRTUSRPRF)

 Type choices, press Enter.

 User profile . . . . . . . . . . > NEW PROF      Name
 User password  . . . . . . . . .   Don't let this default to *USRPRF !_

 Set password to expired  . . . . > *YES          *NO, *YES
 Status . . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED
 User class . . . . . . . . . . . > *SECOFR       *USER, *SYSOPR, *PGMR...
 Assistance level . . . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
 Current library  . . . . . . . .   *CRTDFT       Name, *CRTDFT
 Initial program to call  . . . . > APP MENU      Name, *NONE
   Library  . . . . . . . . . . . >   APP LIB     Name, *LIBL, *CURLIB
 Initial menu . . . . . . . . . . > *SIGNOFF      Name, *SIGNOFF
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
 Limit capabilities . . . . . . . > *YES          *NO, *PARTIAL, *YES
 Text 'description' . . . . . . . > 'Add a meaningful description here'

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

CRTUSRPRF – 2



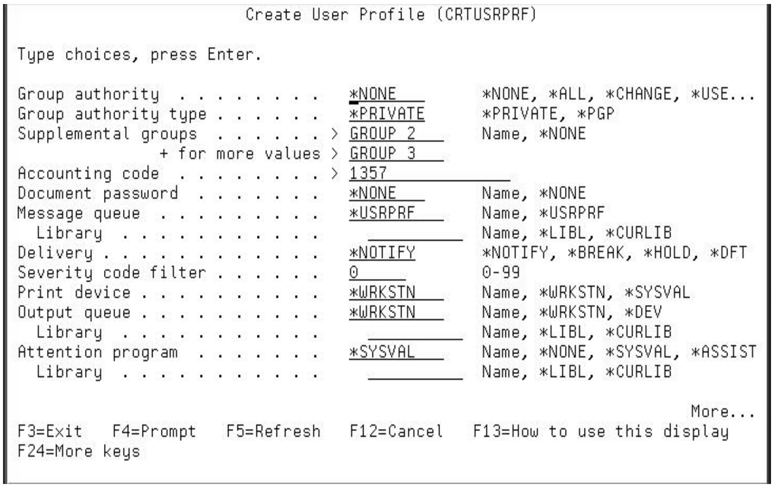
```
                        Create User Profile (CRTUSRPRF)

 Type choices, press Enter.


                             Additional Parameters

 Special authority  . . . . . . .   *USRCLS       *USRCLS, *NONE, *ALLOBJ...
                + for more values
 Special environment  . . . . . .   *SYSVAL       *SYSVAL, *NONE, *S36
 Display sign-on information  . .   *SYSVAL       *SYSVAL, *NO, *YES
 Password expiration interval . .   *SYSVAL       1-366, *SYSVAL, *NOMAX
 Limit device sessions  . . . . .   *SYSVAL       *SYSVAL, *YES, *NO
 Keyboard buffering . . . . . . .   *SYSVAL       *SYSVAL, *NO, *TYPEAHEAD...
 Maximum allowed storage  . . . .   *NOMAX        Kilobytes, *NOMAX
 Highest schedule priority  . . .   3             0-9
 Job description  . . . . . . . . > APP JOBD      Name
   Library  . . . . . . . . . . . >   APP LIB     Name, *LIBL, *CURLIB
 Group profile  . . . . . . . . . > ACCT GRP      Name, *NONE
 Owner  . . . . . . . . . . . . .   *USRPRF       *USRPRF, *GRPPRF
                                                                      More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

CRTUSRPRF – 3



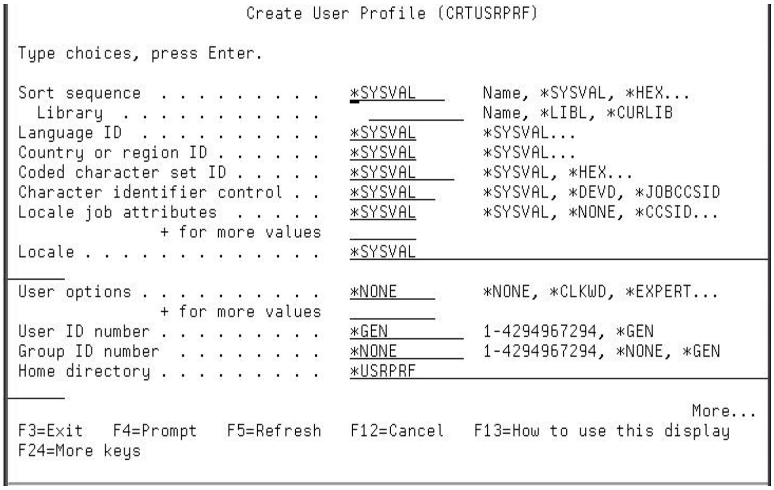
```
                         Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Group authority  . . . . . . . .   *NONE         *NONE, *ALL, *CHANGE, *USE...
Group authority type . . . . . .   *PRIVATE      *PRIVATE, *PGP
Supplemental groups  . . . . . . > GROUP 2       Name, *NONE
               + for more values > GROUP 3
Accounting code  . . . . . . . . > 1357
Document password  . . . . . . .   *NONE         Name, *NONE
Message queue  . . . . . . . . .   *USRPRF       Name, *USRPRF
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Delivery . . . . . . . . . . . .   *NOTIFY       *NOTIFY, *BREAK, *HOLD, *DFT
Severity code filter . . . . . .   0             0-99
Print device . . . . . . . . . .   *WRKSTN       Name, *WRKSTN, *SYSVAL
Output queue . . . . . . . . . .   *WRKSTN       Name, *WRKSTN, *DEV
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Attention program  . . . . . . .   *SYSVAL       Name, *NONE, *SYSVAL, *ASSIST
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB

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

CRTUSRPRF – 4



```
                         Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Group authority  . . . . . . . .   *NONE         *NONE, *ALL, *CHANGE, *USE...
Group authority type . . . . . .   *PRIVATE      *PRIVATE, *PGP
Supplemental groups  . . . . . . > GROUP 2       Name, *NONE
               + for more values > GROUP 3
Accounting code  . . . . . . . . > 1357
Document password  . . . . . . .   *NONE         Name, *NONE
Message queue  . . . . . . . . .   *USRPRF       Name, *USRPRF
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Delivery . . . . . . . . . . . .   *NOTIFY       *NOTIFY, *BREAK, *HOLD, *DFT
Severity code filter . . . . . .   0             0-99
Print device . . . . . . . . . .   *WRKSTN       Name, *WRKSTN, *SYSVAL
Output queue . . . . . . . . . .   *WRKSTN       Name, *WRKSTN, *DEV
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Attention program  . . . . . . .   *SYSVAL       Name, *NONE, *SYSVAL, *ASSIST
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB

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

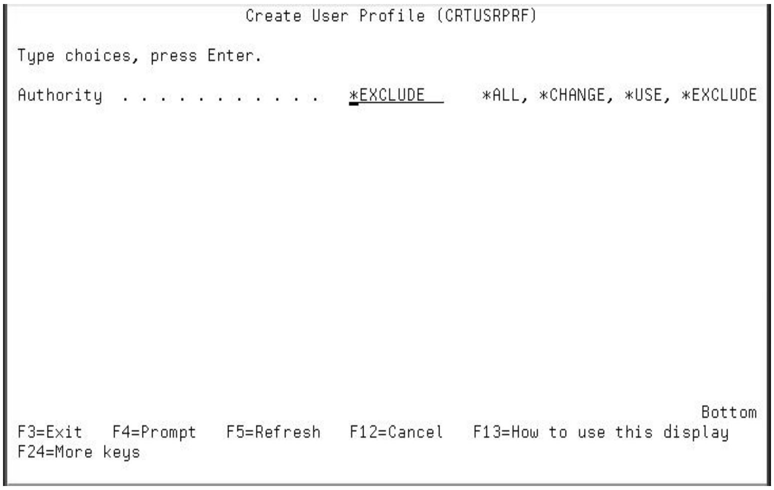
CRTUSRPRF – 5



```
                         Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Sort sequence  . . . . . . . . .   *SYSVAL       Name, *SYSVAL, *HEX...
  Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
Language ID  . . . . . . . . . .   *SYSVAL       *SYSVAL...
Country or region ID . . . . . .   *SYSVAL       *SYSVAL...
Coded character set ID . . . . .   *SYSVAL       *SYSVAL, *HEX...
Character identifier control . .   *SYSVAL       *SYSVAL, *DEVD, *JOBCCSID
Locale job attributes  . . . . .   *SYSVAL       *SYSVAL, *NONE, *CCSID...
               + for more values
Locale . . . . . . . . . . . . .   *SYSVAL

User options . . . . . . . . . .   *NONE         *NONE, *CLKWD, *EXPERT...
               + for more values
User ID number . . . . . . . . .   *GEN          1-4294967294, *GEN
Group ID number  . . . . . . . .   *NONE         1-4294967294, *NONE, *GEN
Home directory . . . . . . . . .   *USRPRF

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

31 www.skyviewpartners.com

CRTUSRPRF – 6



```
                         Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Authority  . . . . . . . . . . .   *EXCLUDE     *ALL, *CHANGE, *USE, *EXCLUDE















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

32 www.skyviewpartners.com

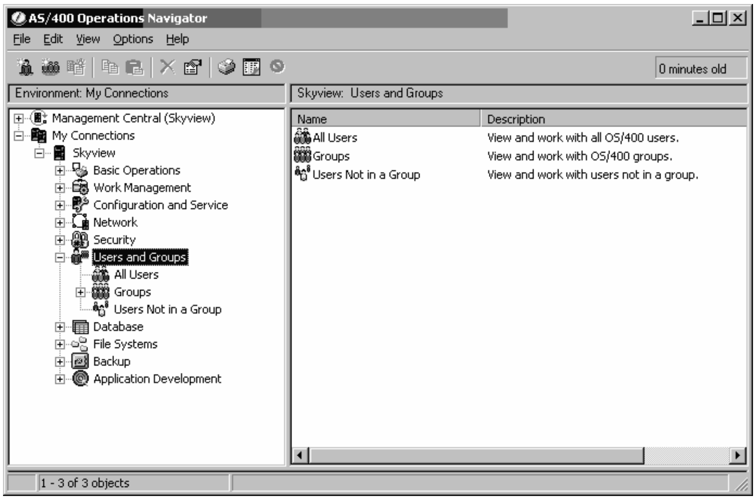
New Profile Parameters – V5R3

- **Local password management (LCLPWDMGT)**
  - *YES – password stored on local machine as it is today
  - *NO – password set to *NONE, then stored remotely to take advantage of single signon
    - iSeries Integration for Windows Server
- **EIM association (EIMASSOC)**

EIM identifier	*NOCHG, *USRPRF, name
Association type	*TARGET, *SOURCE, *TGTSRC, *ADMIN
Association action	*REPLACE, *ADD, *REMOVE
Create EIM identifier	*NOCRTEIMID, *CRTEIMID

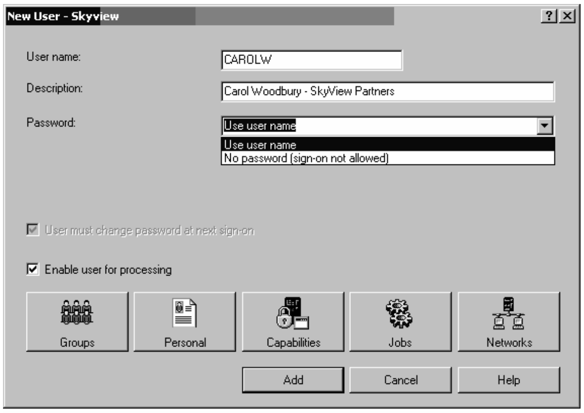
- **This enables writing a CL program to initially populate EIM**

Users and Groups



Name	Description
All Users	View and work with all OS/400 users.
Groups	View and work with OS/400 groups.
Users Not in a Group	View and work with users not in a group.

Add a New User



New User - Skyview

User name: CAROLW

Description: Carol Woodbury - SkyView Partners

Password: Use user name

Use user name
No password (sign-on not allowed)

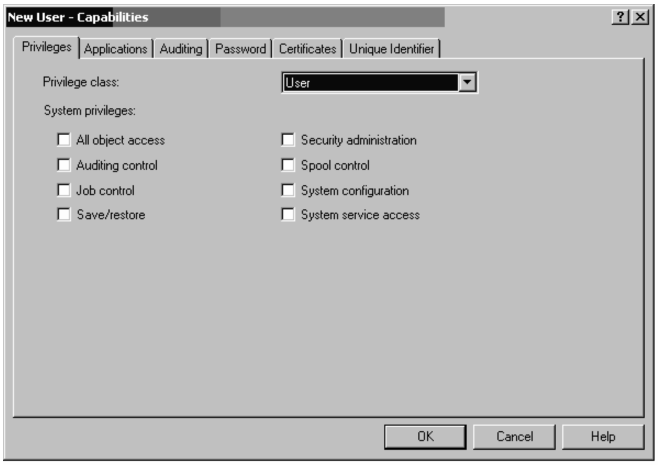
☑ User must change password at next sign-on

☑ Enable user for processing

- Right click on Users and Groups
- Select New User …

SKYVIEW PARTNERS, LLC

Capabilities - Privileges (Special Authorities)



New User - Capabilities

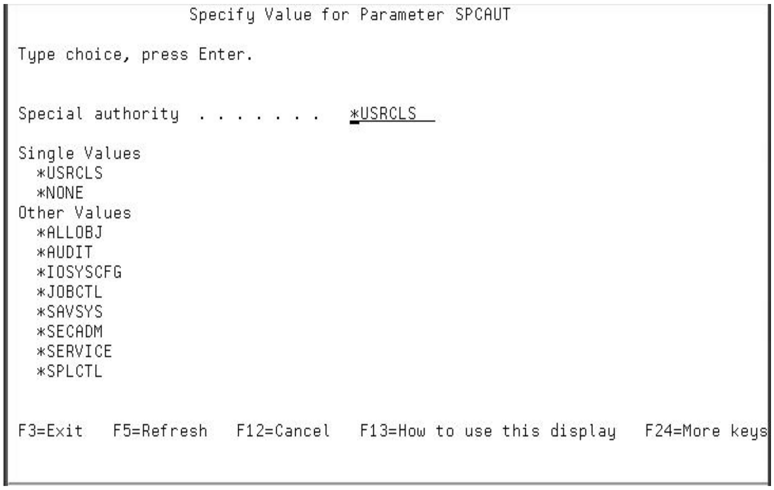
Privilege class: User

System privileges:

☐ All object access
☐ Auditing control
☐ Job control
☐ Save/restore
☐ Security administration
☐ Spool control
☐ System configuration
☐ System service access

SKYVIEW PARTNERS, LLC

Special Authorities – Green screen

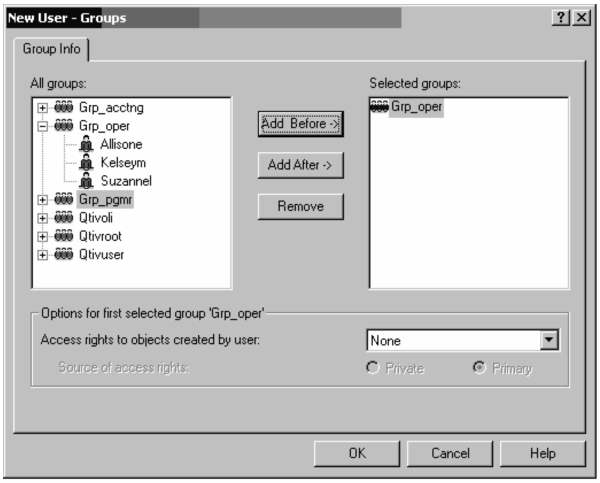


```
                   Specify Value for Parameter SPCAUT

Type choice, press Enter.


Special authority  . . . . . . .   *USRCLS

Single Values
  *USRCLS
  *NONE
Other Values
  *ALLOBJ
  *AUDIT
  *IOSYSCFG
  *JOBCTL
  *SAVSYS
  *SECADM
  *SERVICE
  *SPLCTL


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

Special Authorities (or Privileges in Ops Nav)

Special Authority	Definition
***AUDIT**	**Auditing configuration**
***IOSYSCFG**	**Communications configuration and mgmt**
***JOBCTL**	**Mgmt of any job on the system**
***SAVSYS**	**Ability to save and restore any object on the system – or the entire system regardless of authority to the object**
***SECADM**	**Create/Change/Delete user profiles**
***SERVICE**	**Ability to use Service Tools**
***SPLCTL**	**Access to every spooled file on the system regardless of authority to the outq**
***ALLOBJ**	**Access to EVERY object on the system. It is not possible to prevent an *ALLOBJ user from accessing an object!!!**

Groups – Making a user a member of a group



All groups:

- Grp_acctng
- Grp_oper
  - Allisone
  - Kelseym
  - Suzannel
- Grp_pgmr
- Qtivoli
- Qtivroot
- Qtivuser

Selected groups:

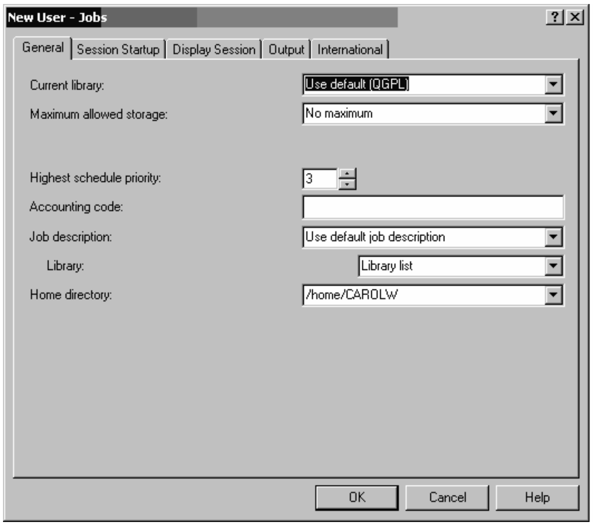
- Grp_oper

Options for first selected group 'Grp_oper'

Access rights to objects created by user: None

Source of access rights: ○ Private ● Primary

Jobs – Define a user's job attributes



Current library: Use default (QGPL)

Maximum allowed storage: No maximum

Highest schedule priority: 3

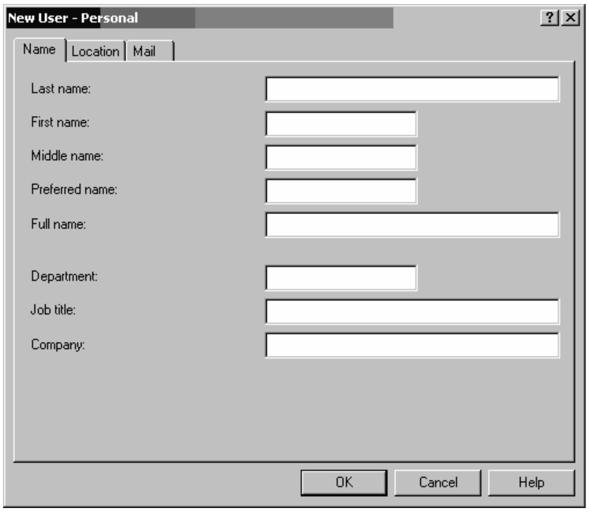
Accounting code:

Job description: Use default job description

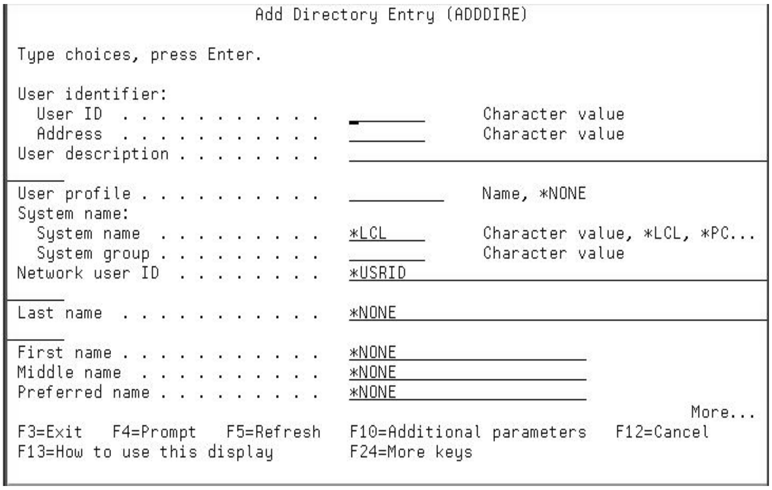
Library: Library list

Home directory: /home/CAROLW

Personal – Personal Information



ADDDIRE

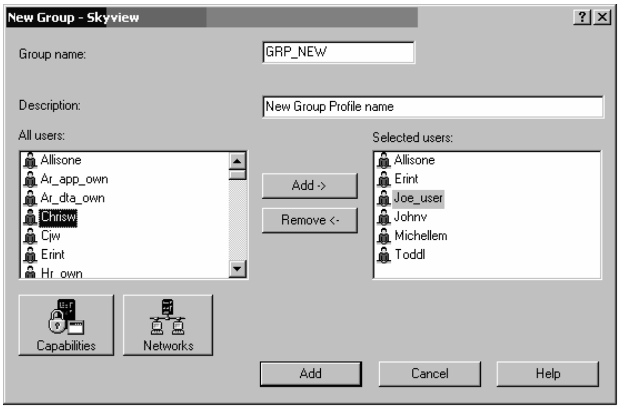


```
                        Add Directory Entry (ADDDIRE)

Type choices, press Enter.

User identifier:
  User ID  . . . . . . . . . . .   ________      Character value
  Address  . . . . . . . . . . .   ________      Character value
User description . . . . . . . .   ____________________________________________

User profile . . . . . . . . . .   __________    Name, *NONE
System name:
  System name  . . . . . . . . .   *LCL____      Character value, *LCL, *PC...
  System group . . . . . . . . .   ________      Character value
Network user ID  . . . . . . . .   *USRID______________________________________

Last name  . . . . . . . . . . .   *NONE_______________________________________

First name . . . . . . . . . . .   *NONE_________________________
Middle name  . . . . . . . . . .   *NONE_________________________
Preferred name . . . . . . . . .   *NONE_________________________
                                                                        More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

Group Profiles

- **Allows users with similar jobs to share authorities without having to share a profile**
  - Create using CRTUSRPRF or through Ops Nav
  - Choose a naming convention which makes groups easily recognizable
  - Create with PASSWORD(*NONE)
  - Should not own objects (unless you want everyone in the group to “own” the objects)
  - Users can be a member of up to 16 group profiles. Should assign profiles in order of most frequent use.
  - Special authorities are cumulative for the user and group(s).
  - Object authorities are additive at the group level.

Adding a Group



New Group - Skyview

Group name: GRP_NEW

Description: New Group Profile name

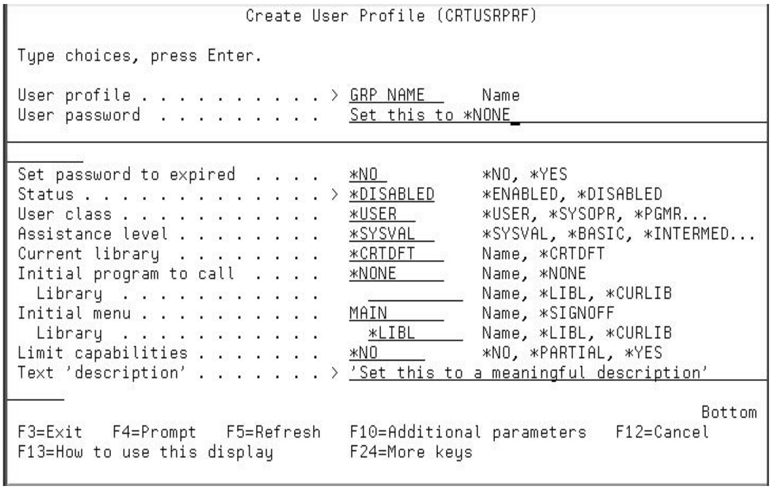
All users:
- Allisone
- Ar_app_own
- Ar_dta_own
- Chrisw
- Cjw
- Erint
- Hr_own

Selected users:
- Allisone
- Erint
- Joe_user
- Johnv
- Michellem
- Toddl

•Right click on Users and Groups

• Select New Group …

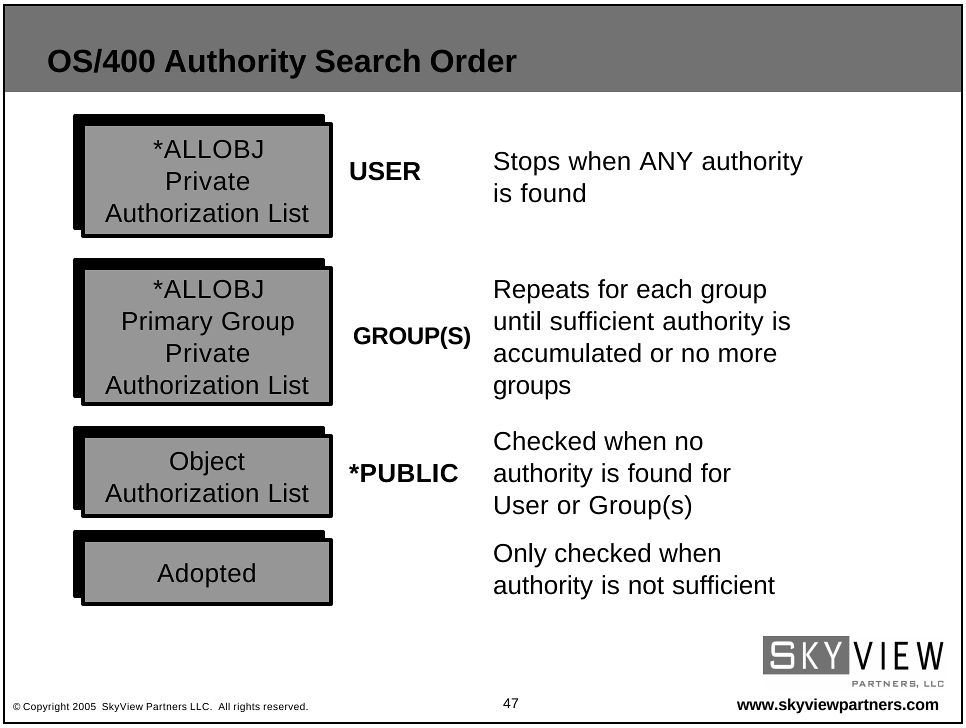
Creating or Adding a Group



```
                         Create User Profile (CRTUSRPRF)

 Type choices, press Enter.

 User profile . . . . . . . . . . > GRP NAME      Name
 User password  . . . . . . . . .   Set this to *NONE_

 Set password to expired  . . . .   *NO           *NO, *YES
 Status . . . . . . . . . . . . . > *DISABLED     *ENABLED, *DISABLED
 User class . . . . . . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
 Assistance level . . . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
 Current library  . . . . . . . .   *CRTDFT       Name, *CRTDFT
 Initial program to call  . . . .   *NONE         Name, *NONE
   Library  . . . . . . . . . . .                 Name, *LIBL, *CURLIB
 Initial menu . . . . . . . . . .   MAIN          Name, *SIGNOFF
   Library  . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
 Limit capabilities . . . . . . .   *NO           *NO, *PARTIAL, *YES
 Text 'description' . . . . . . . > 'Set this to a meaningful description'

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

How do authorization lists compare with group profiles?

Authorization Lists	Group Profiles
Associates like objects	Associates like users
Secures multiples objects	Can be authorized to multiple objects
Users can be authorized to multiple authorization lists	All users in a group have the same authority to an object
Objects can be secured by only one authorization list	Many groups can have authority to one object

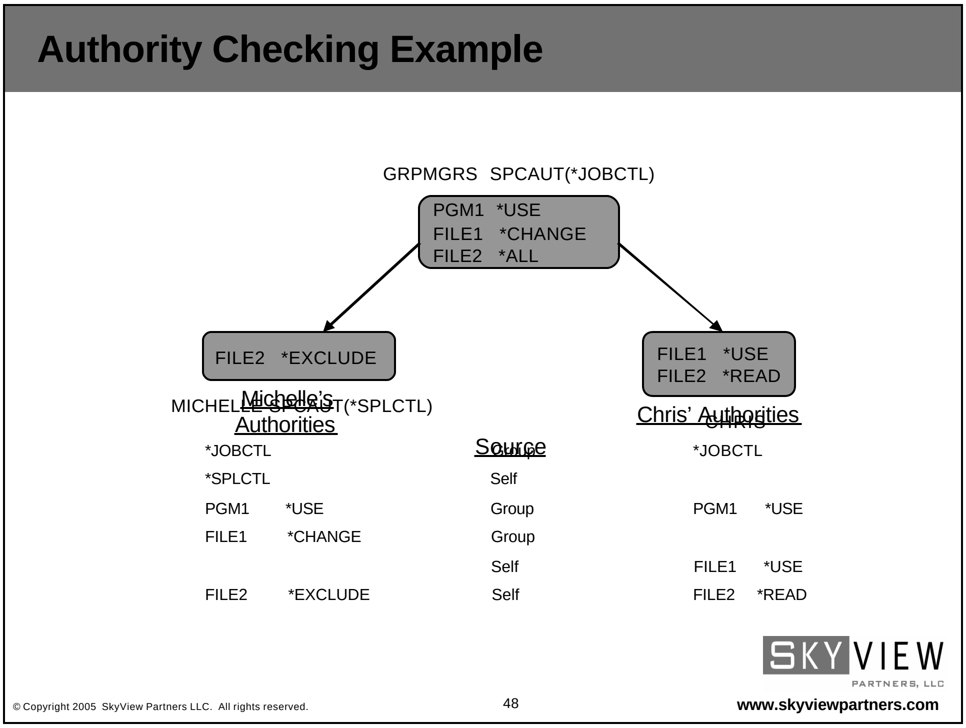


OS/400 Authority Search Order

*ALLOBJ Private Authorization List	**USER**	Stops when ANY authority is found
*ALLOBJ Primary Group Private Authorization List	**GROUP(S)**	Repeats for each group until sufficient authority is accumulated or no more groups
Object Authorization List	***PUBLIC**	Checked when no authority is found for User or Group(s)
Adopted		Only checked when authority is not sufficient

47

www.skyviewpartners.com



Authority Checking Example

GRPMGRS SPCAUT(*JOBCTL)

PGM1 *USE
FILE1 *CHANGE
FILE2 *ALL

MICHELLE SPCAUT(*SPLCTL)

FILE2 *EXCLUDE

CHRIS

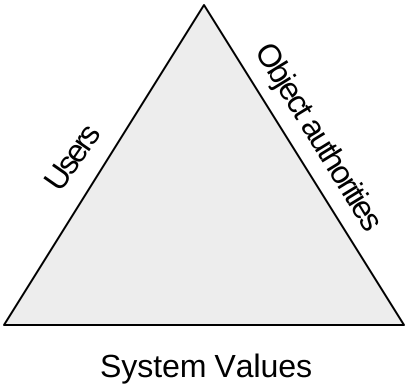
FILE1 *USE
FILE2 *READ

Michelle's Authorities		Source	Chris' Authorities	
*JOBCTL		Group	*JOBCTL	
*SPLCTL		Self		
PGM1	*USE	Group	PGM1	*USE
FILE1	*CHANGE	Group		
		Self	FILE1	*USE
FILE2	*EXCLUDE	Self	FILE2	*READ

48

www.skyviewpartners.com

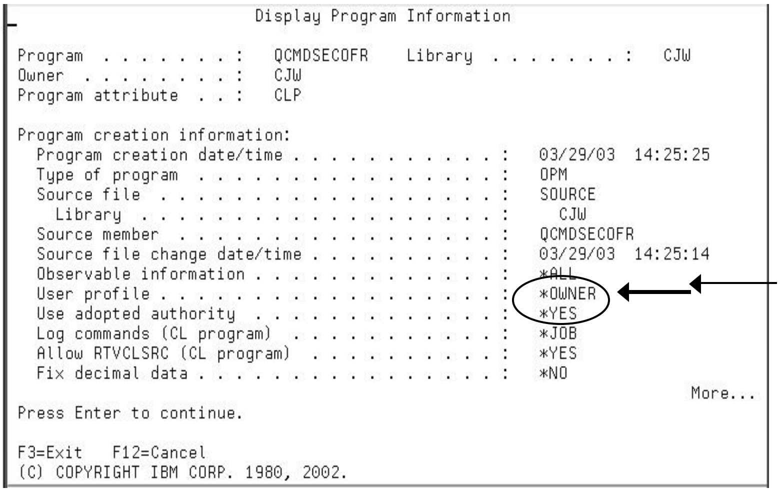
One Application Security Scheme



Adopted Authority

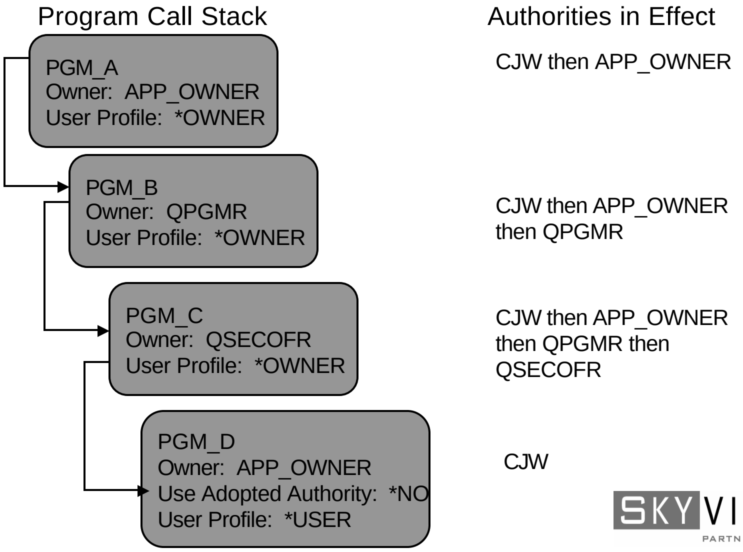
- **Used to temporarily give authority**
- **When a program with USRPRF(*OWNER) runs, the authority in effect is the user plus the owner of the program**
- **Both special authorities and private authorities are adopted (the program owner's groups are not included)**
- **Additional authority is in effect for as long as the program is in the call stack**

How can I tell whether a program adopts?



```
                        Display Program Information

Program . . . . . . . :   QCMDSECOFR    Library . . . . . . . :   CJW
Owner . . . . . . . . :   CJW
Program attribute . . :   CLP

Program creation information:
  Program creation date/time . . . . . . . . . . . :   03/29/03  14:25:25
  Type of program . . . . . . . . . . . . . . . . :   OPM
  Source file . . . . . . . . . . . . . . . . . . :   SOURCE
    Library . . . . . . . . . . . . . . . . . . . :     CJW
  Source member . . . . . . . . . . . . . . . . . :   QCMDSECOFR
  Source file change date/time . . . . . . . . . . :   03/29/03  14:25:14
  Observable information . . . . . . . . . . . . :   *ALL
  User profile . . . . . . . . . . . . . . . . . . :   *OWNER
  Use adopted authority . . . . . . . . . . . . . :   *YES
  Log commands (CL program) . . . . . . . . . . . :   *JOB
  Allow RTVCLSRC (CL program) . . . . . . . . . . :   *YES
  Fix decimal data . . . . . . . . . . . . . . . . :   *NO
                                                                      More...
Press Enter to continue.

F3=Exit   F12=Cancel
(C) COPYRIGHT IBM CORP. 1980, 2002.
```

Adopted Authority Example



Program Call Stack

Authorities in Effect

PGM_A
Owner: APP_OWNER
User Profile: *OWNER

CJW then APP_OWNER

PGM_B
Owner: QPGMR
User Profile: *OWNER

CJW then APP_OWNER then QPGMR

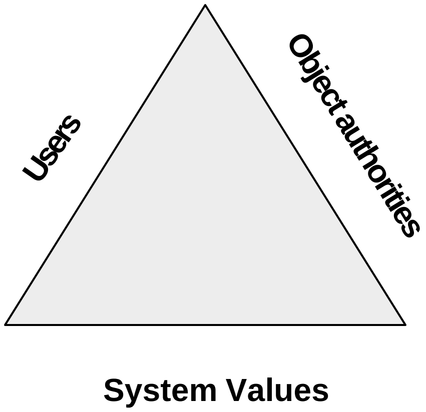
PGM_C
Owner: QSECOFR
User Profile: *OWNER

CJW then APP_OWNER then QPGMR then QSECOFR

PGM_D
Owner: APP_OWNER
Use Adopted Authority: *NO
User Profile: *USER

CJW

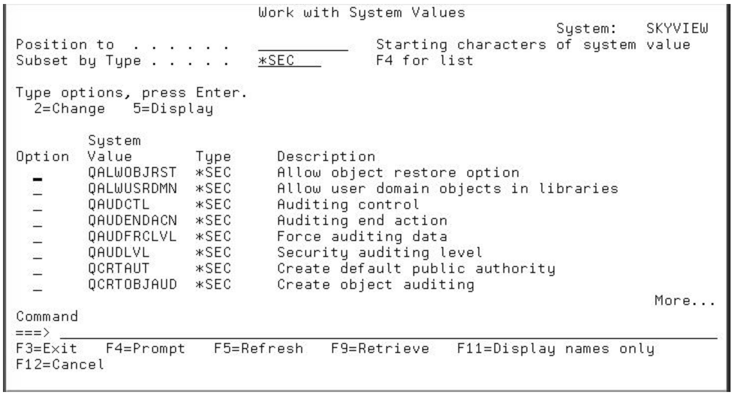
Protecting Your System



53

www.skyviewpartners.com

WRKSYSVAL *SEC

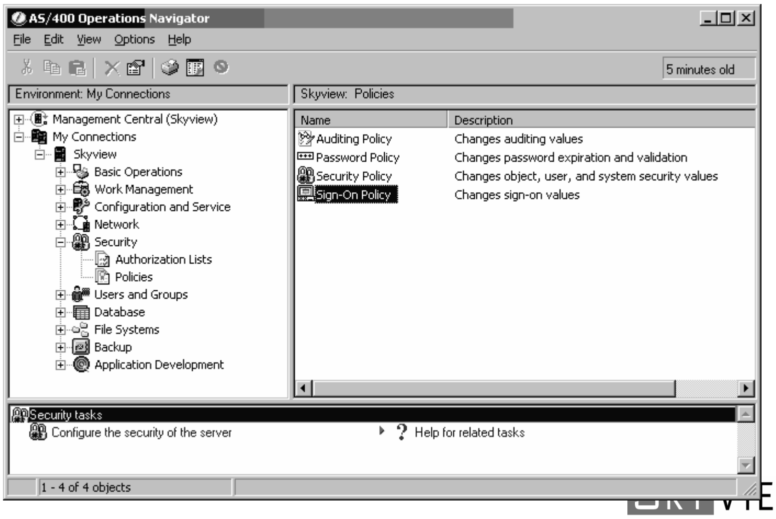


```
                           Work with System Values
                                                          System:   SKYVIEW
Position to  . . . . . .   __________   Starting characters of system value
Subset by Type . . . . .   *SEC____     F4 for list

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
  _     QAUDCTL     *SEC     Auditing control
  _     QAUDENDACN  *SEC     Auditing end action
  _     QAUDFRCLVL  *SEC     Force auditing data
  _     QAUDLVL     *SEC     Security auditing level
  _     QCRTAUT     *SEC     Create default public authority
  _     QCRTOBJAUD  *SEC     Create object auditing
                                                                   More...
Command
===> __________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display names only
F12=Cancel
```

54

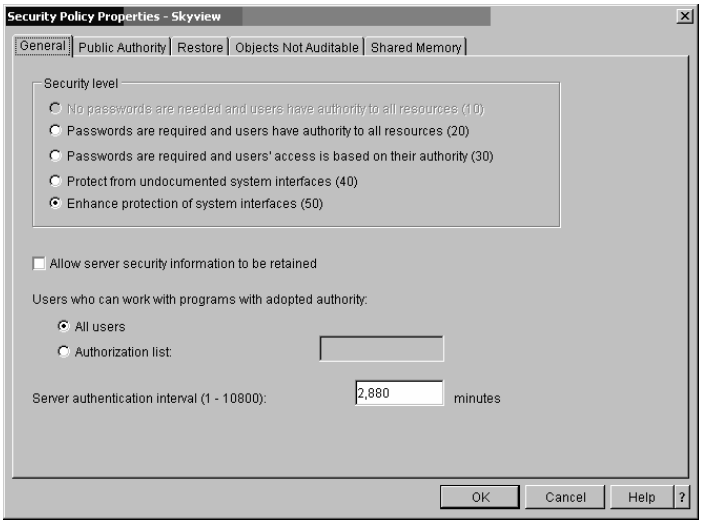
www.skyviewpartners.com

Security Policies (System Values)



Name	Description
Auditing Policy	Changes auditing values
Password Policy	Changes password expiration and validation
Security Policy	Changes object, user, and system security values
Sign-On Policy	Changes sign-on values

Security Policies - General


Security Policy Properties - Skyview
General | Public Authority | Restore | Objects Not Auditable | Shared Memory
OK
Cancel
Help
?

Security level

○ No passwords are needed and users have authority to all resources (10)

○ Passwords are required and users have authority to all resources (20)

○ Passwords are required and users' access is based on their authority (30)

○ Protect from undocumented system interfaces (40)

● Enhance protection of system interfaces (50)

□ Allow server security information to be retained

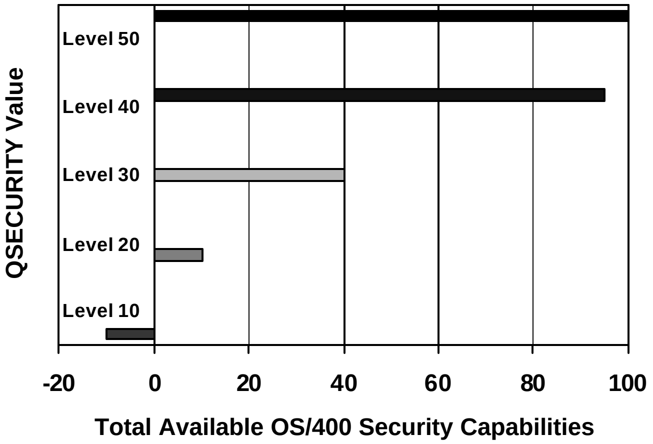
Users who can work with programs with adopted authority:

● All users

○ Authorization list:

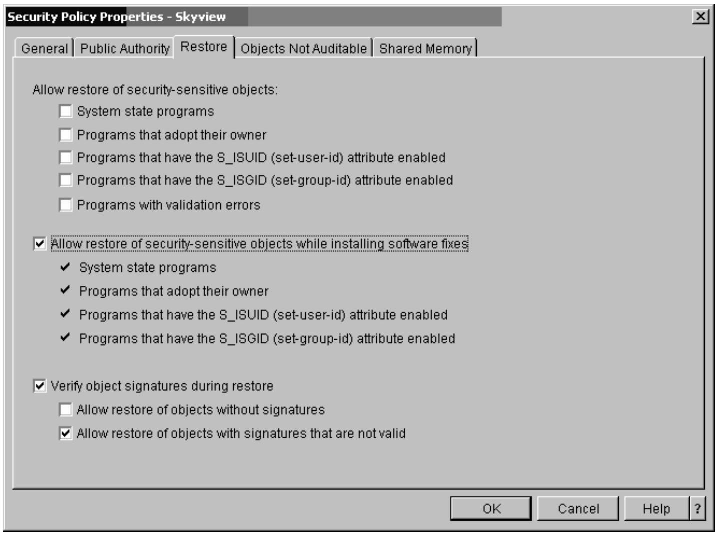
Server authentication interval (1 - 10800): 2,880 minutes

Security Level (QSECURITY)



57 www.skyviewpartners.com

Restore Policies



Allow restore of security-sensitive objects:

- □ System state programs
- □ Programs that adopt their owner
- □ Programs that have the S_ISUID (set-user-id) attribute enabled
- □ Programs that have the S_ISGID (set-group-id) attribute enabled
- □ Programs with validation errors

☑ Allow restore of security-sensitive objects while installing software fixes

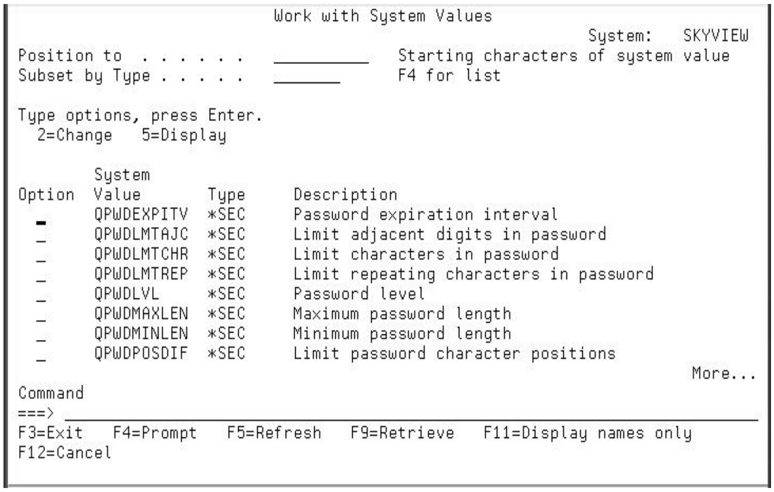
- ✓ System state programs
- ✓ Programs that adopt their owner
- ✓ Programs that have the S_ISUID (set-user-id) attribute enabled
- ✓ Programs that have the S_ISGID (set-group-id) attribute enabled

☑ Verify object signatures during restore

- □ Allow restore of objects without signatures
- ☑ Allow restore of objects with signatures that are not valid

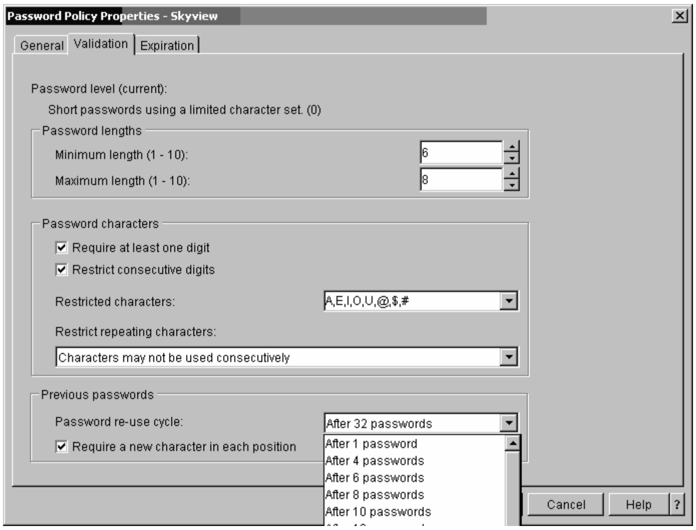
58 www.skyviewpartners.com

WRKSYSVAL QPWD*



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

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

        System
Option  Value       Type     Description
  _     QPWDEXPITV  *SEC     Password expiration interval
  _     QPWDLMTAJC  *SEC     Limit adjacent digits in password
  _     QPWDLMTCHR  *SEC     Limit characters in password
  _     QPWDLMTREP  *SEC     Limit repeating characters in password
  _     QPWDLVL     *SEC     Password level
  _     QPWDMAXLEN  *SEC     Maximum password length
  _     QPWDMINLEN  *SEC     Minimum password length
  _     QPWDPOSDIF  *SEC     Limit password character positions
                                                                      More...
Command
===> _________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display names only
F12=Cancel
```

Password System Values



Password level (current):
Short passwords using a limited character set. (0)

Password lengths
Minimum length (1 - 10): 6
Maximum length (1 - 10): 8

Password characters
☑ Require at least one digit
☑ Restrict consecutive digits
Restricted characters: A,E,I,O,U,@,$,#
Restrict repeating characters: Characters may not be used consecutively

Previous passwords
Password re-use cycle: After 32 passwords
☑ Require a new character in each position

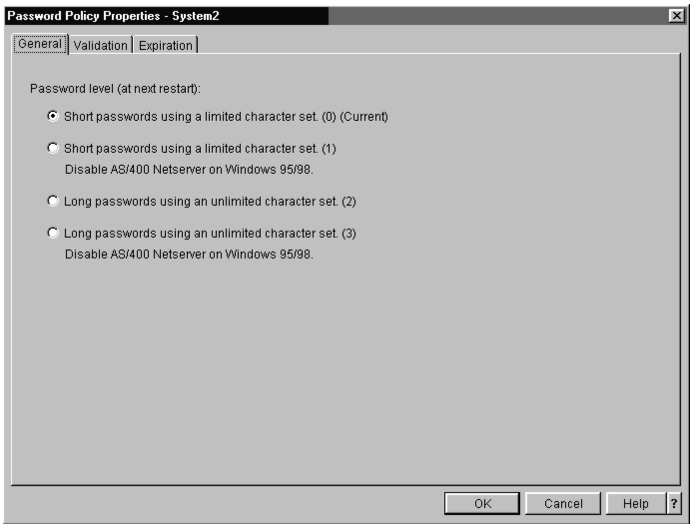
Password Recommendations

Should

- be at least seven characters long
- contain a number
- be changed regularly – more frequently for “powerful” profiles
- not be known to administrators
- not be shared

Don’t make creating a password so difficult users are forced to write them down !!!

Password Level



Password level (at next restart):

● Short passwords using a limited character set. (0) (Current)

○ Short passwords using a limited character set. (1)
Disable AS/400 Netserver on Windows 95/98.

○ Long passwords using an unlimited character set. (2)

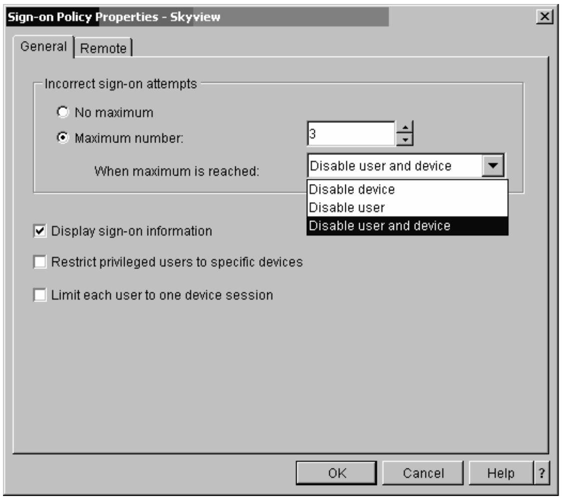
○ Long passwords using an unlimited character set. (3)
Disable AS/400 Netserver on Windows 95/98.

Password Level (QPWDLVL) – New in V5R1

Value	Effect
0	Works as it did prior to V5R1 - Default
1	Gets rid of NetServer password
2	Enables new composition rules – keeps NetServer password, encrypts with old and new algorithms
3	Enables new composition rules – gets rid of old encrypted password and NetServer password

- Requires an IPL and V5R1
- See pending value on DSPSECA

Sign on Policies - General



Incorrect sign-on attempts

○ No maximum

● Maximum number: 3

When maximum is reached: Disable user and device

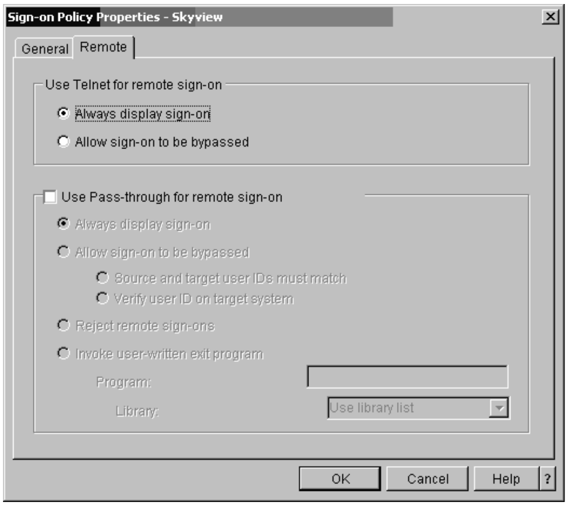
Disable device
Disable user
Disable user and device

☑ Display sign-on information

□ Restrict privileged users to specific devices

□ Limit each user to one device session

Sign on Policies - Remote



Sign-on Policy Properties - Skyview

Use Telnet for remote sign-on

● Always display sign-on

○ Allow sign-on to be bypassed

☐ Use Pass-through for remote sign-on

● Always display sign-on

○ Allow sign-on to be bypassed

○ Source and target user IDs must match

○ Verify user ID on target system

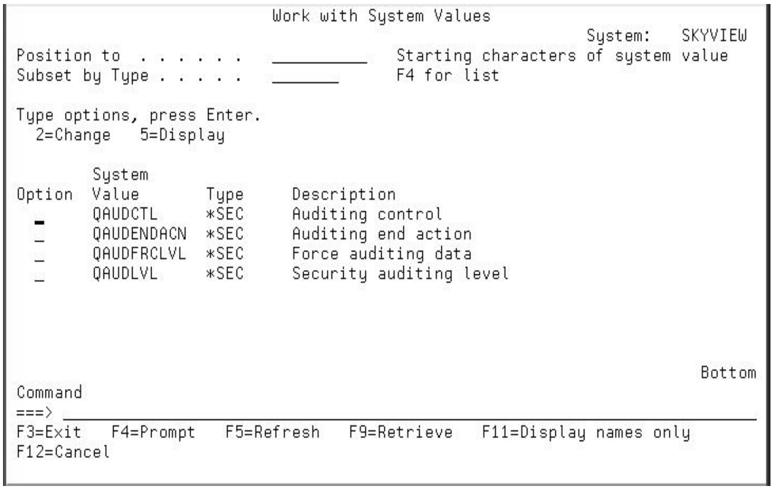
○ Reject remote sign-ons

○ Invoke user-written exit program

Program:

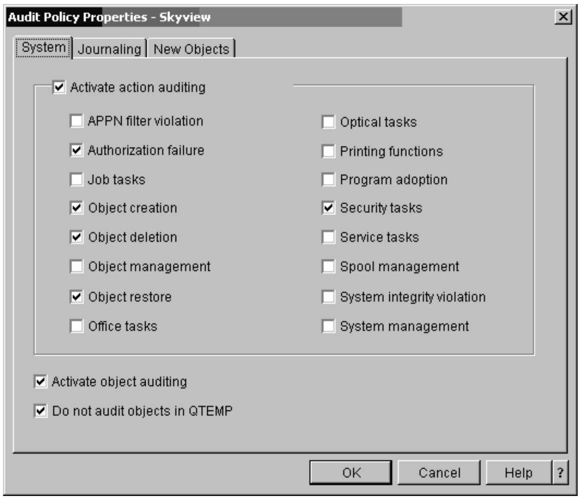
Library: Use library list

Auditing System Values



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

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

       System
Option Value       Type     Description
  _    QAUDCTL     *SEC     Auditing control
  _    QAUDENDACN  *SEC     Auditing end action
  _    QAUDFRCLVL  *SEC     Force auditing data
  _    QAUDLVL     *SEC     Security auditing level




                                                                    Bottom
Command
===> _________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F11=Display names only
F12=Cancel
```

Auditing System Values



Audit Policy Properties - Skyview

☑ Activate action auditing

- □ APPN filter violation
- ☑ Authorization failure
- □ Job tasks
- ☑ Object creation
- ☑ Object deletion
- □ Object management
- ☑ Object restore
- □ Office tasks
- □ Optical tasks
- □ Printing functions
- □ Program adoption
- ☑ Security tasks
- □ Service tasks
- □ Spool management
- □ System integrity violation
- □ System management

☑ Activate object auditing

☑ Do not audit objects in QTEMP

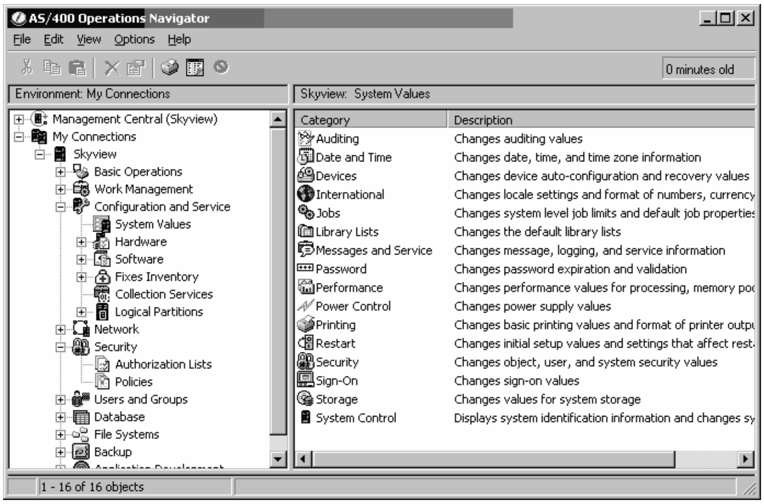
Recommended Audit Settings

- **QAUDCTL**
  - *OBJAUD
  - *AUDLVL
  - *NOQTEMP
- **QAUDLVL**
  - *AUTFAIL
  - *SECURITY
  - *CREATE
  - *DELETE
  - *SAVRST
  - *SERVICE
  - *PGMFAIL (only if running QSECURITY < 40)

New Auditing Values in V5R3

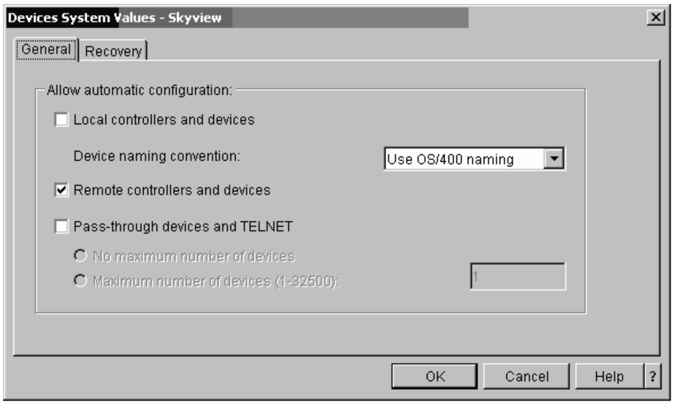
- **QAUDLVL**
  - *SECURITY is subsetted into
    - ***SECCFG – user profile, system value changes, network attributes, etc**
    - *SECDIRSRV – directory services
    - *SECIPC – interprocess communications
    - *SECNAS – network authentication ticket verification (Kerberos)
    - ***SECRUN – runtime changes of object ownership, authorization list, etc**
    - *SECSCKD – secure socket descriptors
    - *SECVFY –verification of profile handles and tokens
    - *SECVLDL - usage of validation list entries
  - *NETCMN is subsetted into
    - *NETBAS - basic network events – SSL connections, APPN "firewall" activities
    - *NETCLU – cluster resource groups
    - *NETFAIL – security-related network failures – e.g., secure socket port not available
    - *NETSCK - mail filtered, mail rejected, give and take socket descriptors
  - *AUDLVL2 (must be specified or QAUDLVL2 is ignored)
- **QAUDLVL2 (overflow for QAUDLVL)**
- **Subsetted values only available at the system value level (not user)**
- **Recommend values -- *SECCFG, *SECRUN**

Other System Values



Category	Description
Auditing	Changes auditing values
Date and Time	Changes date, time, and time zone information
Devices	Changes device auto-configuration and recovery values
International	Changes locale settings and format of numbers, currency
Jobs	Changes system level job limits and default job properties
Library Lists	Changes the default library lists
Messages and Service	Changes message, logging, and service information
Password	Changes password expiration and validation
Performance	Changes performance values for processing, memory poo
Power Control	Changes power supply values
Printing	Changes basic printing values and format of printer outpu
Restart	Changes initial setup values and settings that affect rest.
Security	Changes object, user, and system security values
Sign-On	Changes sign-on values
Storage	Changes values for system storage
System Control	Displays system identification information and changes sy

Device System Values - General



Allow automatic configuration:

☐ Local controllers and devices

Device naming convention: Use OS/400 naming

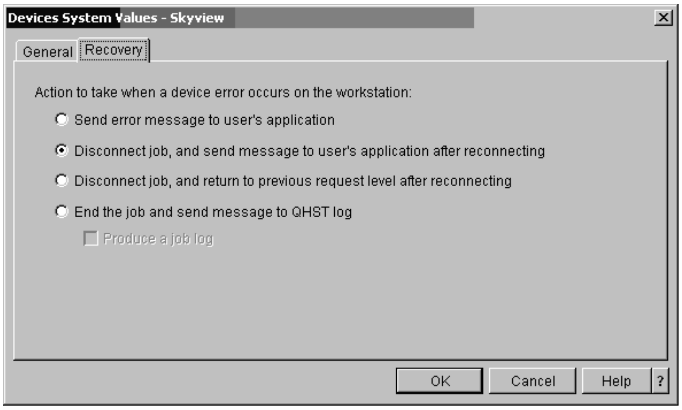
☑ Remote controllers and devices

☐ Pass-through devices and TELNET

○ No maximum number of devices

○ Maximum number of devices (1-32500): 1

Device System Values - Recovery



Action to take when a device error occurs on the workstation:

○ Send error message to user's application

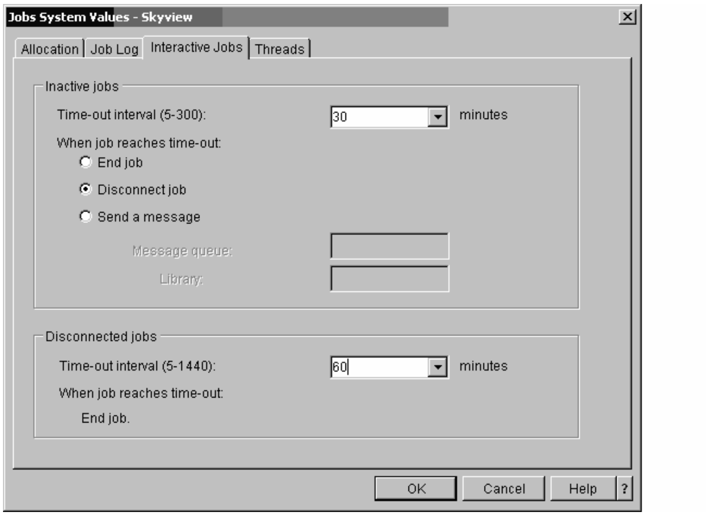
● Disconnect job, and send message to user's application after reconnecting

○ Disconnect job, and return to previous request level after reconnecting

○ End the job and send message to QHST log

☐ Produce a job log

Job System Values - Interactive



Inactive jobs

Time-out interval (5-300): 30 minutes

When job reaches time-out:

○ End job

● Disconnect job

○ Send a message

Message queue:

Library:

Disconnected jobs

Time-out interval (5-1440): 60 minutes

When job reaches time-out:

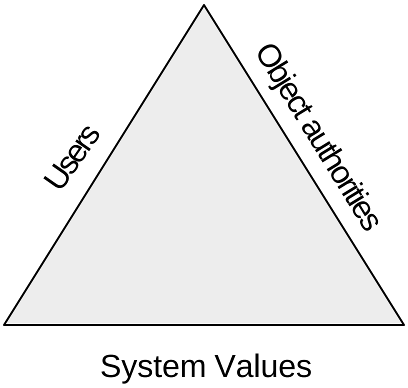
End job.

New IFS System Values and Exit Points – V5R3

- **QSCANFS – Scan file system**
  - *NONE or *ROOTUPOD – every stream file in '/', QOpenSys and user-defined file systems are scanned
  - Works together the QIBM_QP0L_SCAN_OPEN (Scan on Open) and QIBM_QP0L_SCAN_CLOSE (Scan on Close) exit points to define what program does the scanning.
    - Documented in the API section of the Info Center.
- **QSCANFSCTL – Scan file system control parameters**
  - Determines which objects and when objects within a file system are scanned (for example – scan only when the object is changed.)
  - Determines the action to take when the scan fails.
  - Works together with new attributes on *DIR (*CRTOBJSCAN) and *STMF (*SCAN)

Enable real-time virus scanning!

IFS Security Scheme



SKYVIEW PARTNERS, LLC

IFS Authorities

Authorities	*RWX	*RW	*RX	*R	*WX	*W	*X
Object							
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
*AUTLMGT							
Data							
*OBJOPR	X	X	X	X	X	X	X
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X					
*EXECUTE	X		X		X		X

*RWX = Read/Write/Execute (*CHANGE)

*RW = Read/Write

*RX = Read/Execute (*USE)

*R = Read

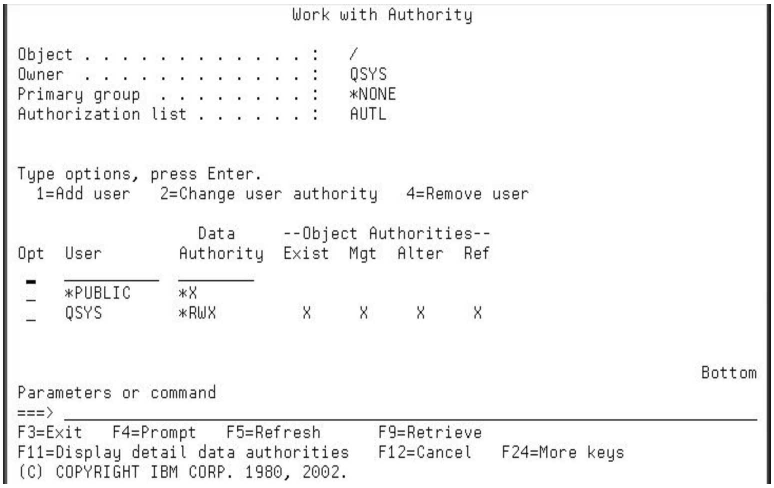
*WX = Write/Execute

*W = Write

*X = Execute

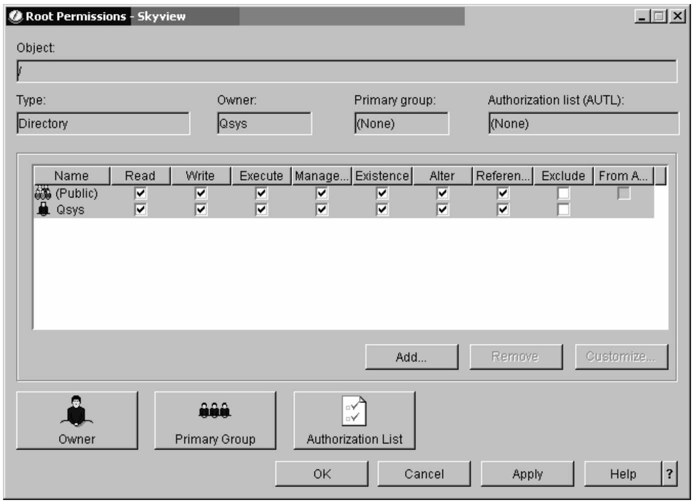
SKYVIEW PARTNERS, LLC

WRKAUT '/'



```
                              Work with Authority

Object . . . . . . . . . . . . :   /
Owner  . . . . . . . . . . . . :   QSYS
Primary group  . . . . . . . . :   *NONE
Authorization list . . . . . . :   AUTL


Type options, press Enter.
  1=Add user   2=Change user authority   4=Remove user

                  Data     --Object Authorities--
Opt  User        Authority  Exist  Mgt  Alter  Ref

 _   __________  ________
 _   *PUBLIC     *X
 _   QSYS        *RWX         X     X     X     X


                                                                    Bottom
Parameters or command
===> _________________________________________________________________________
F3=Exit   F4=Prompt   F5=Refresh      F9=Retrieve
F11=Display detail data authorities   F12=Cancel   F24=More keys
(C) COPYRIGHT IBM CORP. 1980, 2002.
```

Working with File System Permissions in Ops Nav



Root Permissions - Skyview

Object: /

Type: Directory

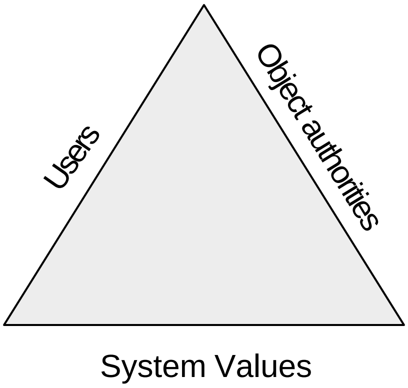
Owner: Qsys

Primary group: (None)

Authorization list (AUTL): (None)

Name	Read	Write	Execute	Manage...	Existence	Alter	Referen...	Exclude	From A...
(Public)	☑	☑	☑	☑	☑	☑	☑	□	□
Qsys	☑	☑	☑	☑	☑	☑	☑	□	

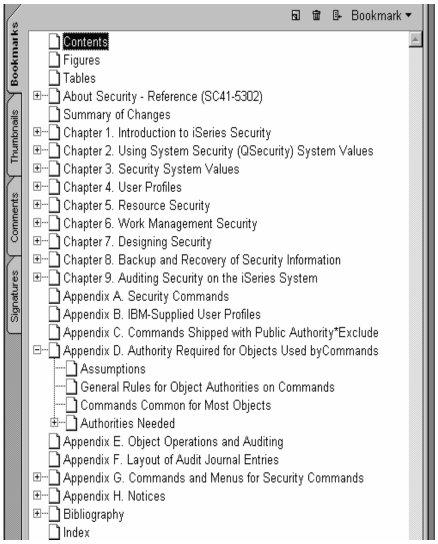
Need More Information !!!



IBM InfoCenter

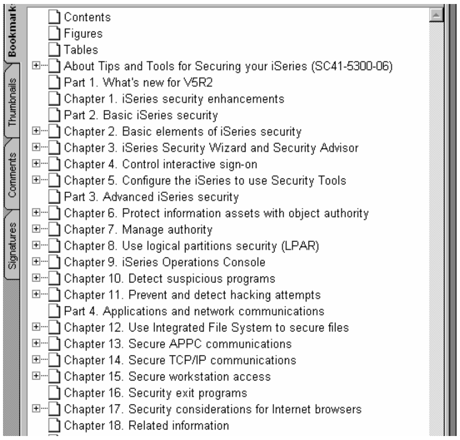
- **www.iseries.ibm.com/infocenter**
  - Basic Security - topics
  - iSeries Security Reference - PDF
    - Chapter 2 – moving between security levels
    - Chapter 6 – securing output
    - Chapter 9 – auditing
    - Appendix D – authorities required
    - Appendix F – auditing model outfiles
  - Tips and Tools for Securing your iSeries - PDF

Security Reference



Contents
Figures
Tables
About Security - Reference (SC41-5302)
Summary of Changes
Chapter 1. Introduction to iSeries Security
Chapter 2. Using System Security (QSecurity) System Values
Chapter 3. Security System Values
Chapter 4. User Profiles
Chapter 5. Resource Security
Chapter 6. Work Management Security
Chapter 7. Designing Security
Chapter 8. Backup and Recovery of Security Information
Chapter 9. Auditing Security on the iSeries System
Appendix A. Security Commands
Appendix B. IBM-Supplied User Profiles
Appendix C. Commands Shipped with Public Authority*Exclude
Appendix D. Authority Required for Objects Used byCommands
Assumptions
General Rules for Object Authorities on Commands
Commands Common for Most Objects
Authorities Needed
Appendix E. Object Operations and Auditing
Appendix F. Layout of Audit Journal Entries
Appendix G. Commands and Menus for Security Commands
Appendix H. Notices
Bibliography
Index

Tips and Tools



Contents
Figures
Tables
About Tips and Tools for Securing your iSeries (SC41-5300-06)
Part 1. What's new for V5R2
Chapter 1. iSeries security enhancements
Part 2. Basic iSeries security
Chapter 2. Basic elements of iSeries security
Chapter 3. iSeries Security Wizard and Security Advisor
Chapter 4. Control interactive sign-on
Chapter 5. Configure the iSeries to use Security Tools
Part 3. Advanced iSeries security
Chapter 6. Protect information assets with object authority
Chapter 7. Manage authority
Chapter 8. Use logical partitions security (LPAR)
Chapter 9. iSeries Operations Console
Chapter 10. Detect suspicious programs
Chapter 11. Prevent and detect hacking attempts
Part 4. Applications and network communications
Chapter 12. Use Integrated File System to secure files
Chapter 13. Secure APPC communications
Chapter 14. Secure TCP/IP communications
Chapter 15. Secure workstation access
Chapter 16. Security exit programs
Chapter 17. Security considerations for Internet browsers
Chapter 18. Related information

Want Security Information

General information

- **www.infosecuritymag.com (Security magazine and weekly alerts)**
- **www.securitypipeline.com (Security magazine and weekly alerts)**
- **www.gocsi.com (Interesting security surveys)**
- **www.sans.org (Security education)**
- **www.cert.org (Security vulnerabilities and alerts)**
- **www.cisecurity.org (Best practices – independent org)**

U.S. Government info

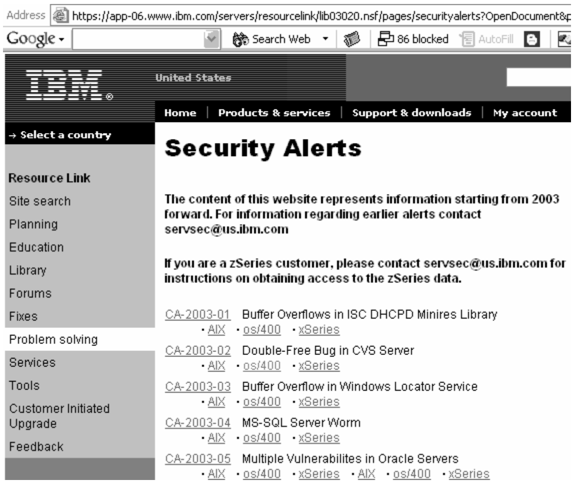
- **www.nist.gov/public_affairs/standards.htm#Information (Security standards)**
- **www.ftc.gov/ftc/news.htm (Federal Trade Commission)**
- **www.cybercrime.gov (Laws, regulations, issues)**

OS/400 information

- **www.mcpressonline.com**
  - Security Patrol
- **www.search400.com**
  - Security expert section

Checking for CERT Advisories

https://app-06.www.ibm.com/servers/resourcelink/hom03010.nsf?OpenDatabase



https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&p

Security Alerts

The content of this website represents information starting from 2003 forward. For information regarding earlier alerts contact servsec@us.ibm.com

If you are a zSeries customer, please contact servsec@us.ibm.com for instructions on obtaining access to the zSeries data.

CA-2003-01 Buffer Overflows in ISC DHCPD Minires Library
• AIX • os/400 • xSeries

CA-2003-02 Double-Free Bug in CVS Server
• AIX • os/400 • xSeries

CA-2003-03 Buffer Overflow in Windows Locator Service
• AIX • os/400 • xSeries

CA-2003-04 MS-SQL Server Worm
• AIX • os/400 • xSeries

CA-2003-05 Multiple Vulnerabilites in Oracle Servers
• AIX • os/400 • xSeries • AIX • os/400 • xSeries

- **Register**
- **Click on “Problem Solving”**
- **Click on “Security Alerts” under Alerts heading**

For More Information

- **Basic Security – iSeries Infocenter**
  - www.iseries.ibm.com/infocenter
- **iSeries Security Reference, SC41-5302**
- **Tips and Tools for Securing Your iSeries, SC41-5300**
- **Experts' Guide to OS/400 and i5/OS Security by Carol Woodbury and Patrick Botz, ISBN 1-58304-096-X, 29th Street Press 2004.**

NEW !!!

- **www.skyviewpartners.com provides**
  - SkyView Risk Assessor for OS/400 and i5/OS software and
  - On-site security assessments providing
    - An explanation of security issues
    - Roadmap for fixing top issues
  - General security consulting
  - Remediation services

Trademarks

- **iSeries, AS/400, IBM, i5/OS and OS/400 are trademarks of the IBM Corporation in the United States or other countries or both.**
- **Other company, product, and service names may be trademarks or service marks of others.**