How To Prevent Common OS/400® Security Exposures 32E

2003
iSeries and AS/400 Connection Conference

by
Wayne O. Evans

iSeries® has an excellent security implementation

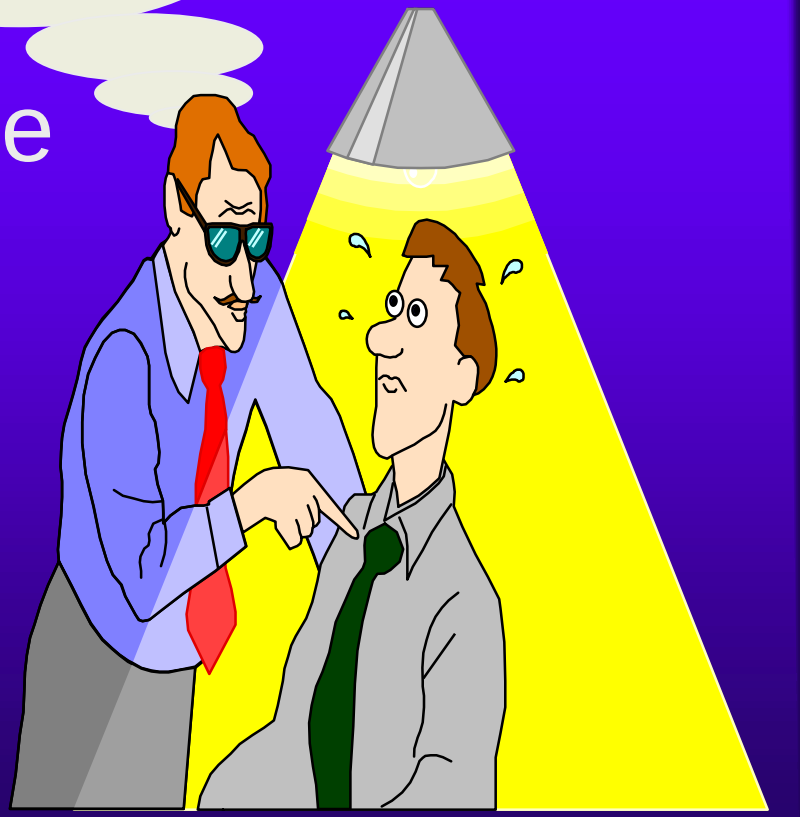
- **Machine instructions enforce access control**
- **Object architecture prevents virus**
- **Security controls integrated into OS/400**

Security is designed into OS/400

But YOU have to activate security

Is your System Secure?

- You must configure security correctly
- You must avoid common security exposures



Common Security Exposures

1. Effective written security policy
2. Security Level below 40
3. Control PC and remote system access
4. Restricting Operations Navigator
5. Excessive command line access
6. Inactive user profiles
7. Excessive special authorities
8. Elimination of trivial passwords
9. Authority to user profiles
10. Object ownership and access

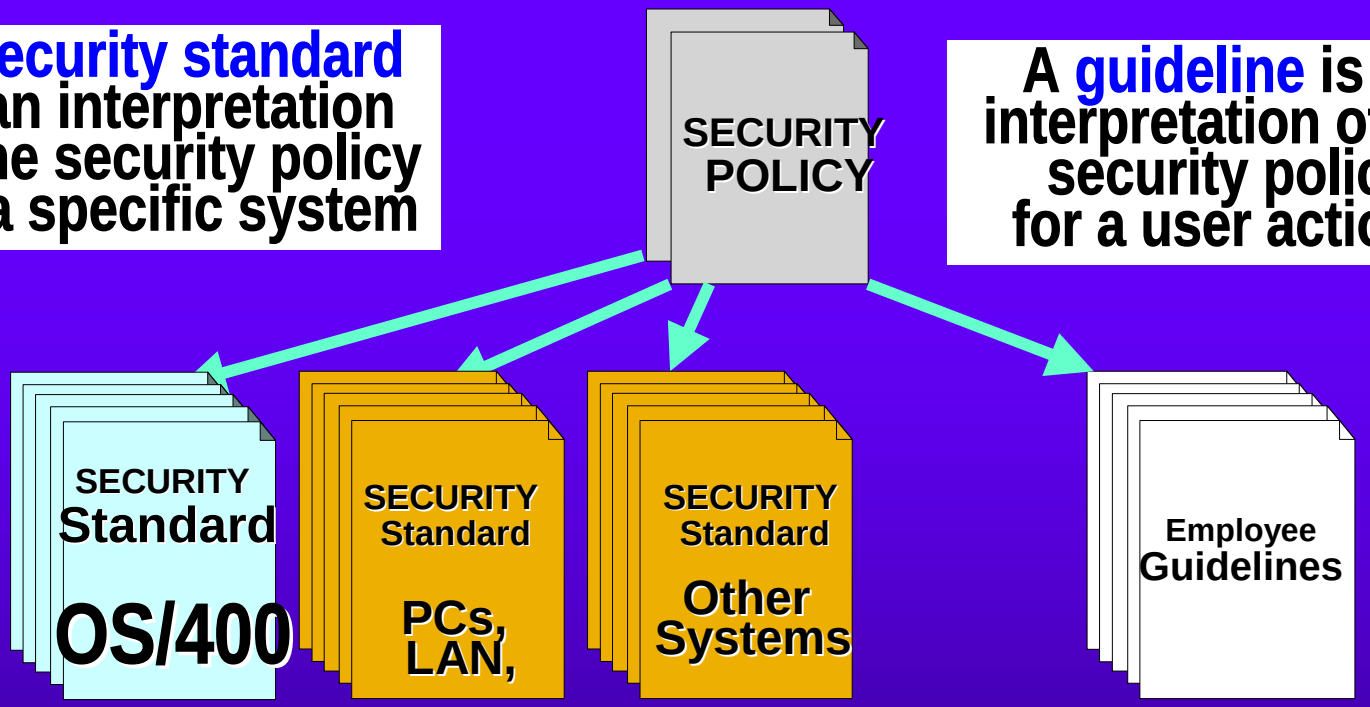
#1 –Security Policy

- **Challenge**
  - Do you have a security policy to direct security decisions?
  - Is you security policy current?
  - Are users **aware and understand** your security policy?
- **Remedy**
  - Download sample policies from WWW.WOEVANS.COM

Security Policy = Plan for Security

Levels of Documentation

A **security standard** is an interpretation of the security policy for a specific system



A **guideline** is an interpretation of the security policy for a user actions

1. Policy – High level objectives
2. Standard – System specific
3. Guideline – User instructions

#2 – System Security Level

- **Challenge**
  - System value QSECURITY sets protection level
    - Level 20 menu security only (Strongly discouraged)
    - Level 30 menu and object security (Not recommended)
    - Level 40 additional integrity protection **(RECOMMENDED)**
    - Level 50 C2 level of protection (Overkill)
- **Remedy**
  - Activate audit to determine if you can move to security level 40

#2 – System Security Level

1. Do not change system value QSECURITY immediately
2. Start up auditing and collect data thru a month-end close
3. Review audit log
4. If no problems are found, then move to level 40

More details download article "Moving to Security Level 40" from WWW.WOEVANS.com

STARTING AUDITING

1. Create journal receiver

```
CRTJRNRCV  JRNRCV(user-lib/user-name001)
           AUT(*EXCLUDE)
```

2. Create journal

```
CRTJRN  JRN(QSYS/QAUDJRN)
        JRNRCV(user-lib/user-name001)
        AUT(*EXCLUDE)
```

FIXED NAME

3. Change system values

Log level 40 failures

```
CHGSYSVAL  QAUDLVL VALUES(' *PGMFAIL ...')
```

```
CHGSYSVAL  QAUDCTL VALUES(' *AUDLVL ')
```

Turn on audit

DSPAUDJRNE ENTTYP(AF) OUTPUT(*PRINT)

Violation Type		User profile	Object name	Library name	Object type
AF	A	WOEVANS	QSYSOPR	QSYS	*MSGQ
AF	D	QSYS	S103478600	QSYS	*DEVD
AF	D	QSYS	S103478600	QSYS	*DEVD
AF	A	QUSER	ZRCRPCSPC	QTEMP	*USRSPC
AF	A	QTMHH			
AF	A	QTMHH			
AF	A	QUSER			
AF	A	WOEVA			
AF	A	QUSER			
AF	A	QUSER			

Check the violation code

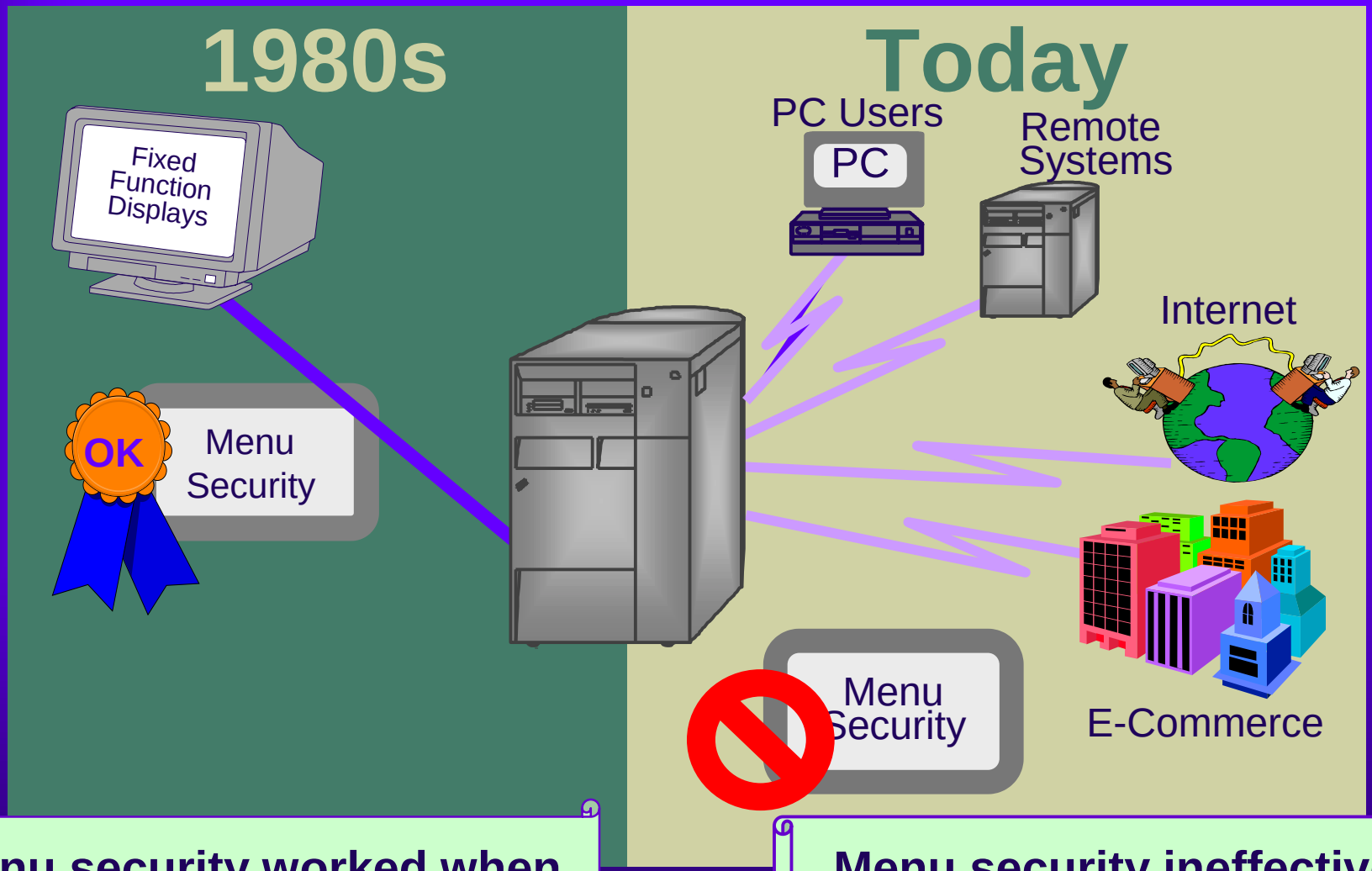
Violation code in audit AF entries

Violation Code	Description	Level 40 Problem
A	Not authorized	No
B	Blocked Instruction	Yes
C	Program Checksum	Yes
D	Domain Failure	Yes
J	Submit Job Failure	No
P	Profile Swap Failure	No
R	Restricted Interface	Yes
S	Sign-on information blank	Fix

#3 – Remote Access

- **Challenge**
  - Maintaining control over the numerous remote access points in OS/400
    - Client Access
      - File Transfer
      - Remote Commands
    - FTP
    - ODBC
- **Remedy**
  - Control object level security
  - Use exit programs to limit remote access

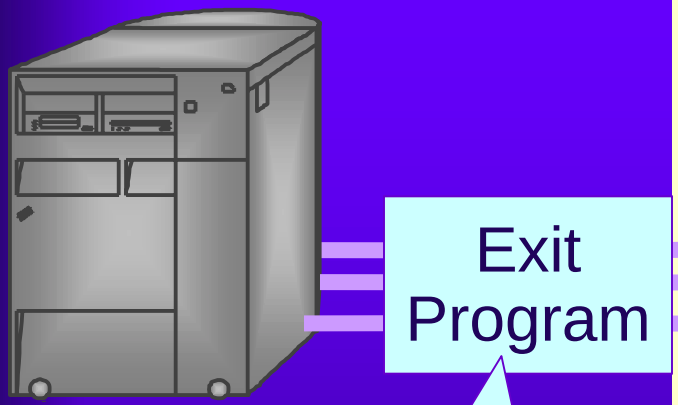
Security Has Changed



Menu security worked when users had no other access

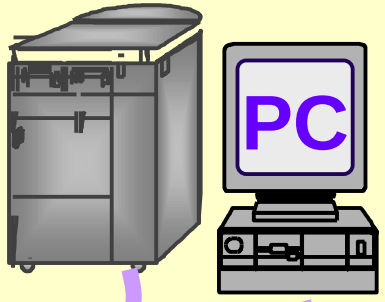
Menu security ineffective for today's environment

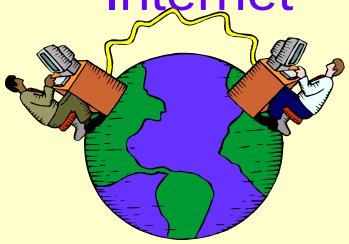
#3 Exit Programs Control Access



Exit Program

Exit Programs can restrict requests





- Client Access
  - **File Transfer**
  - **Remote Commands**
- DDM (Distributed Data Management)
  - **File Transfer**
  - **Remote Commands**
- FTP
  - **File Transfer**
  - **Remote Commands**
- ODBC
- Telnet
- IFS (Integrated File System)

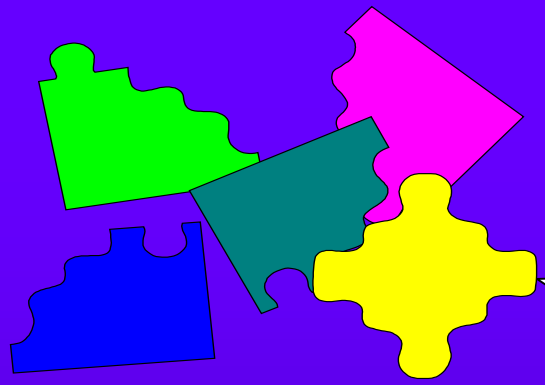
Exit Programs

- Exit programs can control actions of PC users
- Exit programs are not easy to implement
- Difficult to control Operations Navigator with exit programs

For detail go to **WWW.WOEvans.com**

- Exit program fundamentals article
- Comparison of vendor exit programs
- Download sample exit program code

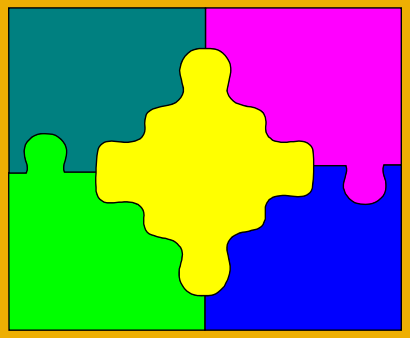
Exit Program Recommendation



- OS/400 Provides
  - Exit Points
  - Registration Facility
  - Security APIs

You must provide the programming to put the individual pieces together

Purchase exit programs

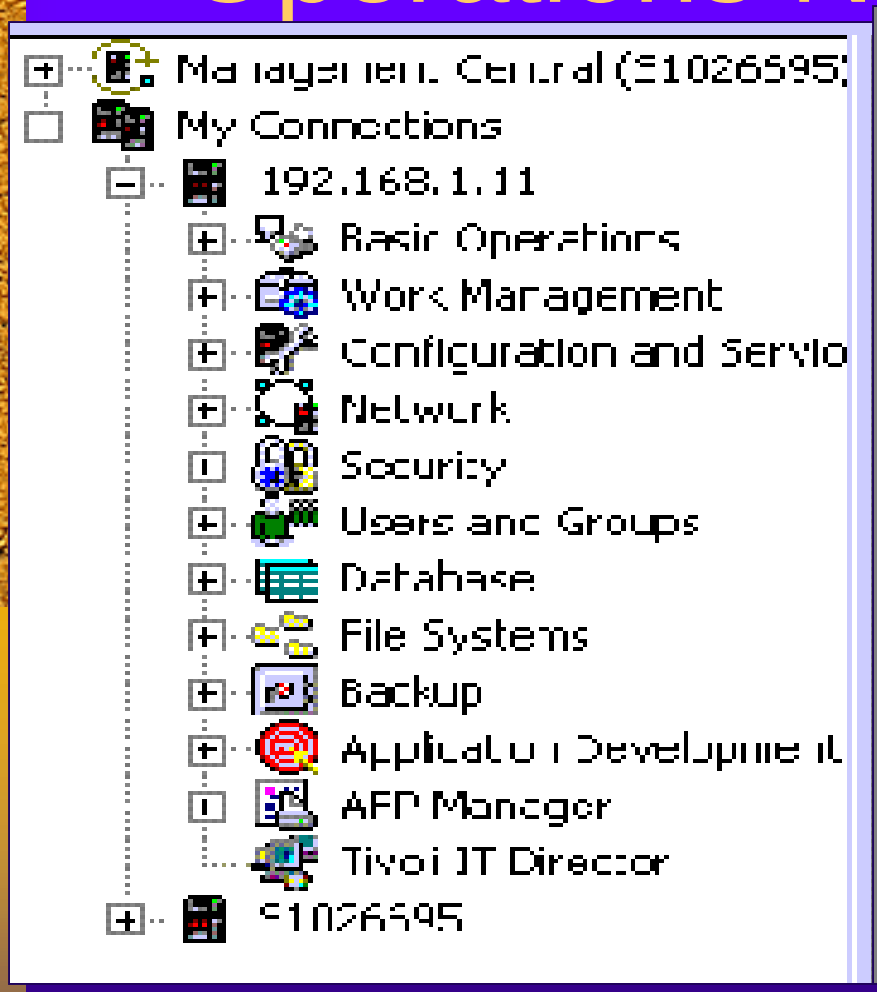


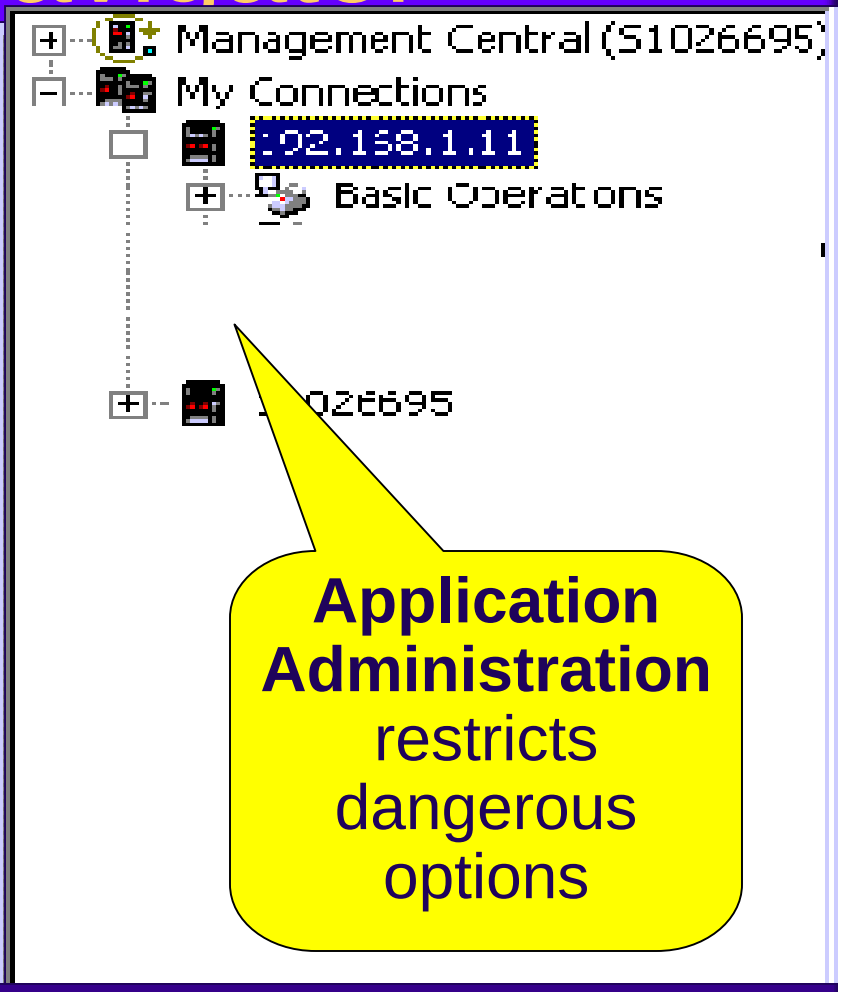
- **Software Vendors Provide**
  - Complete application that integrates IBM support into useful tool

#4 – Restricting Operations Navigator

- **Challenge**
  - Operations navigator gives users powerful functions
    - Move, Rename, and Deletion of objects (if user is authorized to object)
  - Operations navigator is not limited by command line (LMTCPB) or command authority
- Remedy
  - Application Administration to limit Operations Navigator

Operations Navigator

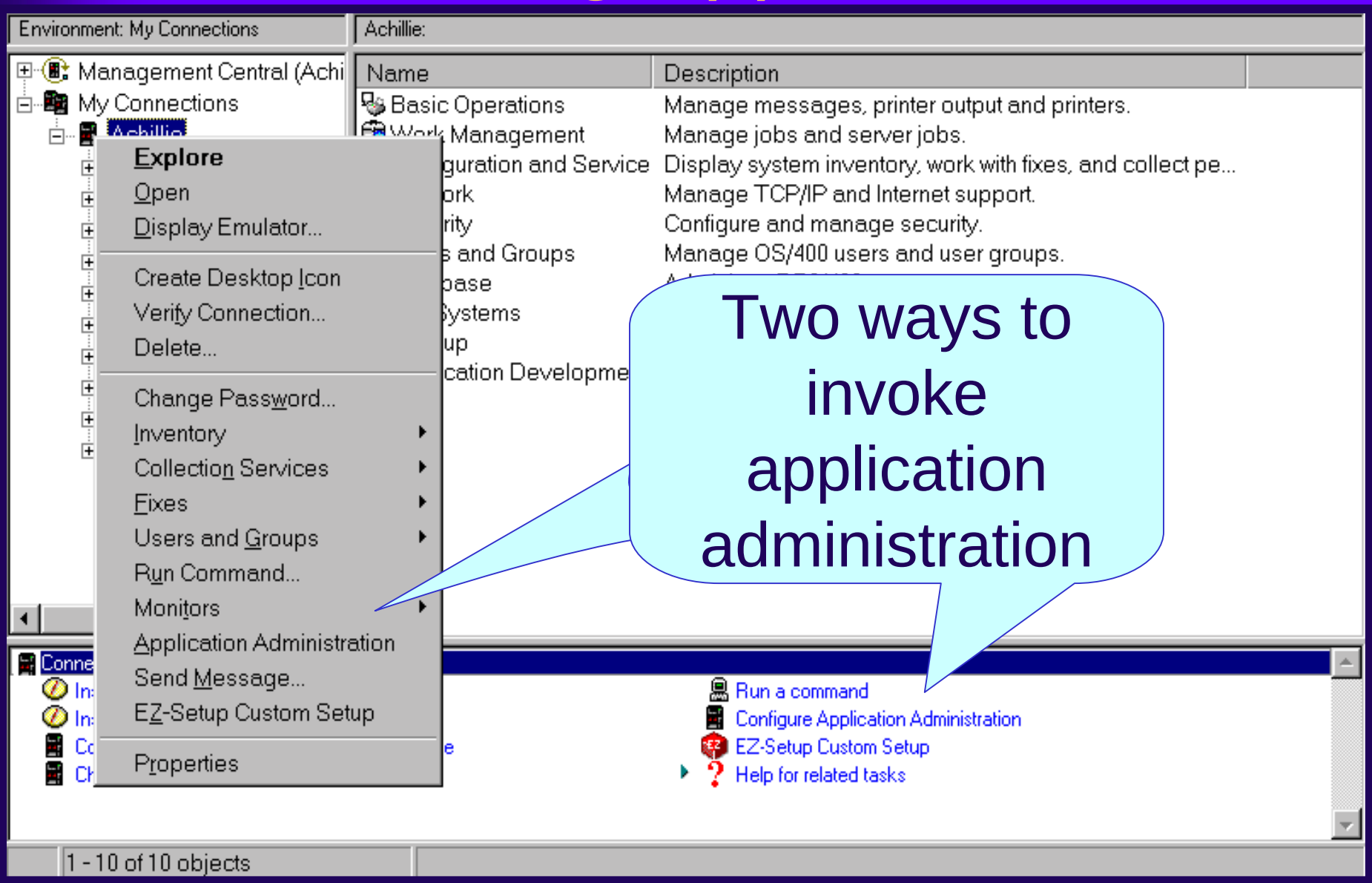




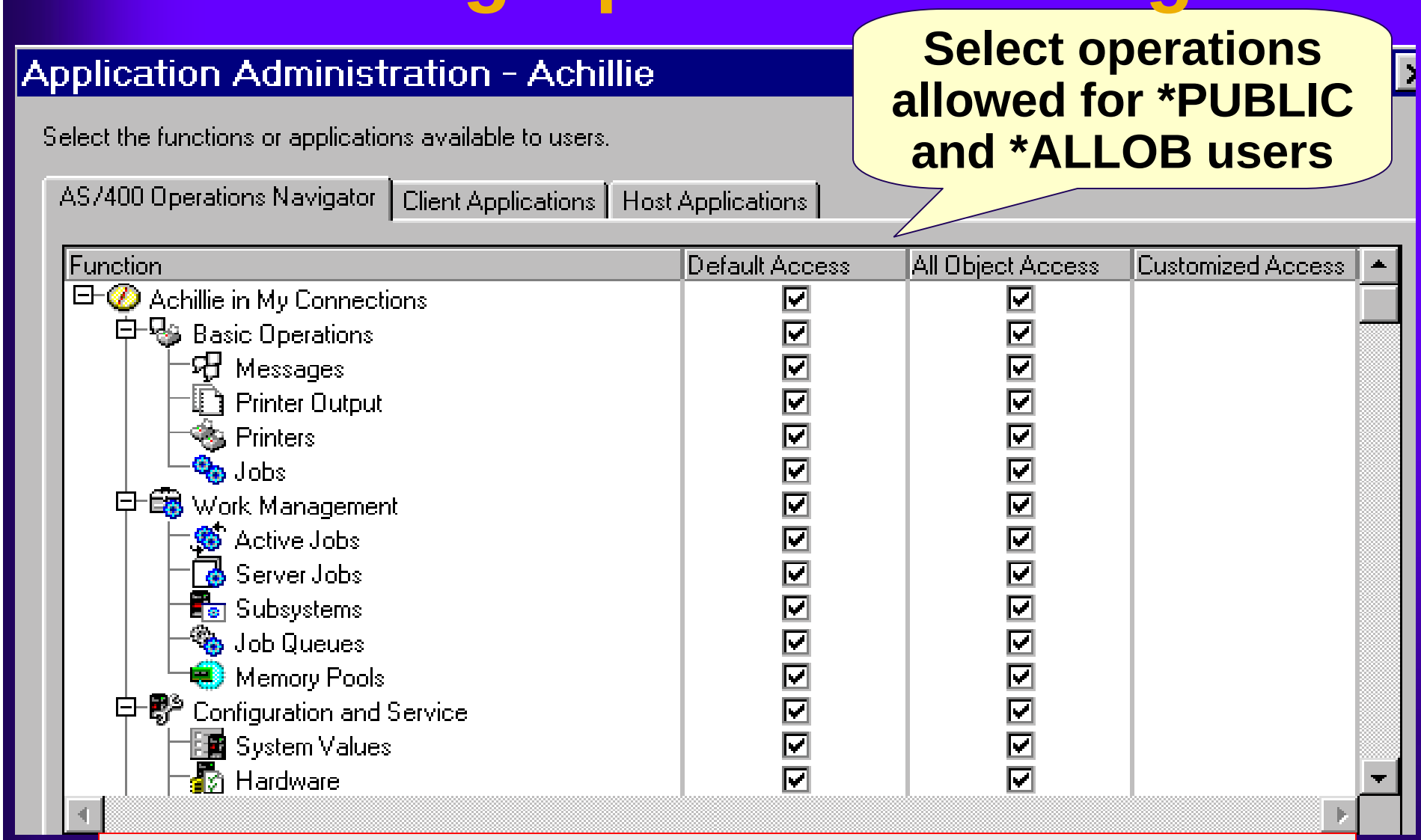
Before **After**

Application administration is used to hide Operations Navigator options

Invoking App Admin



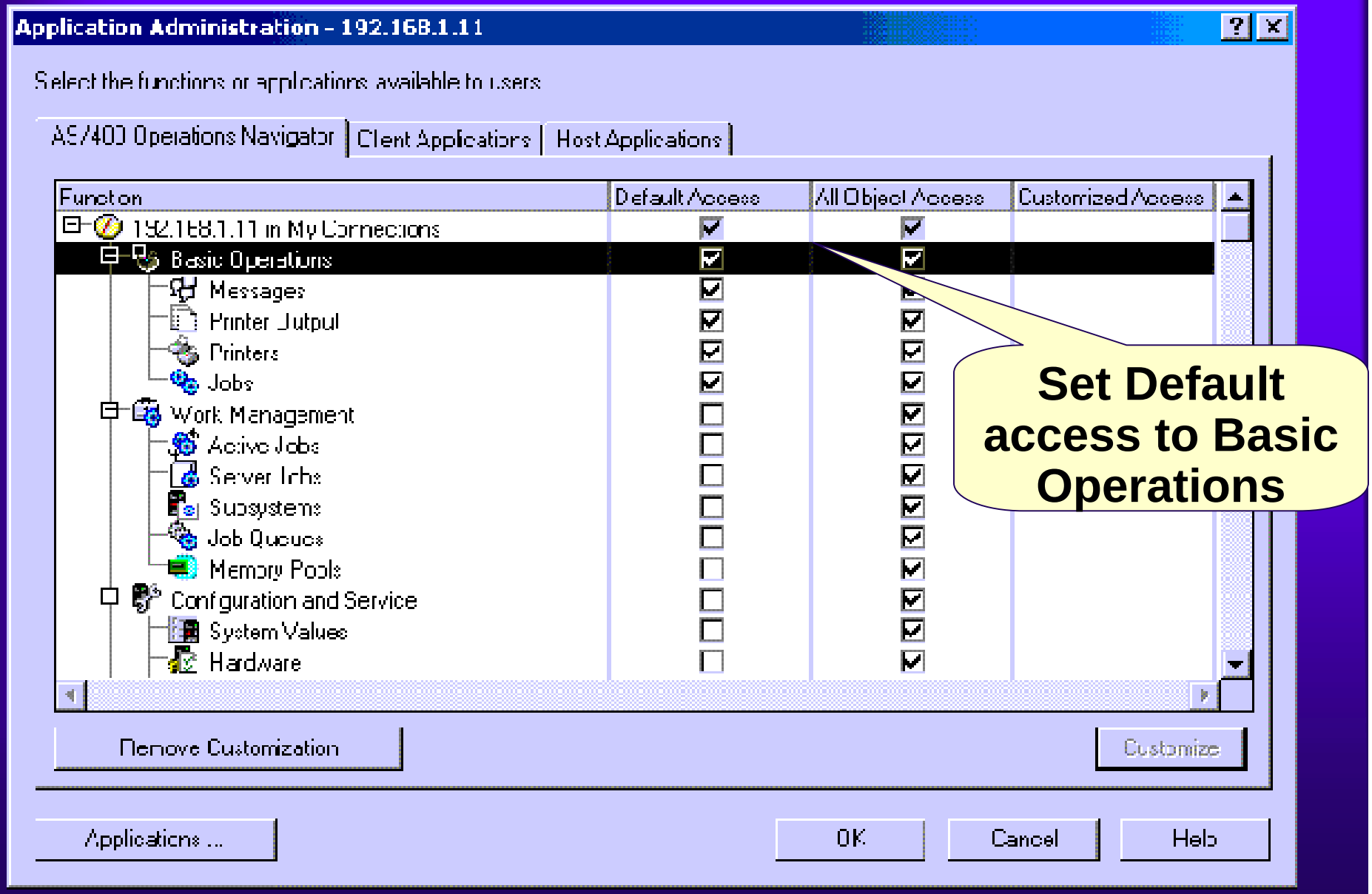
Controlling Operations Navigator



Select operations allowed for *PUBLIC and *ALLOB users

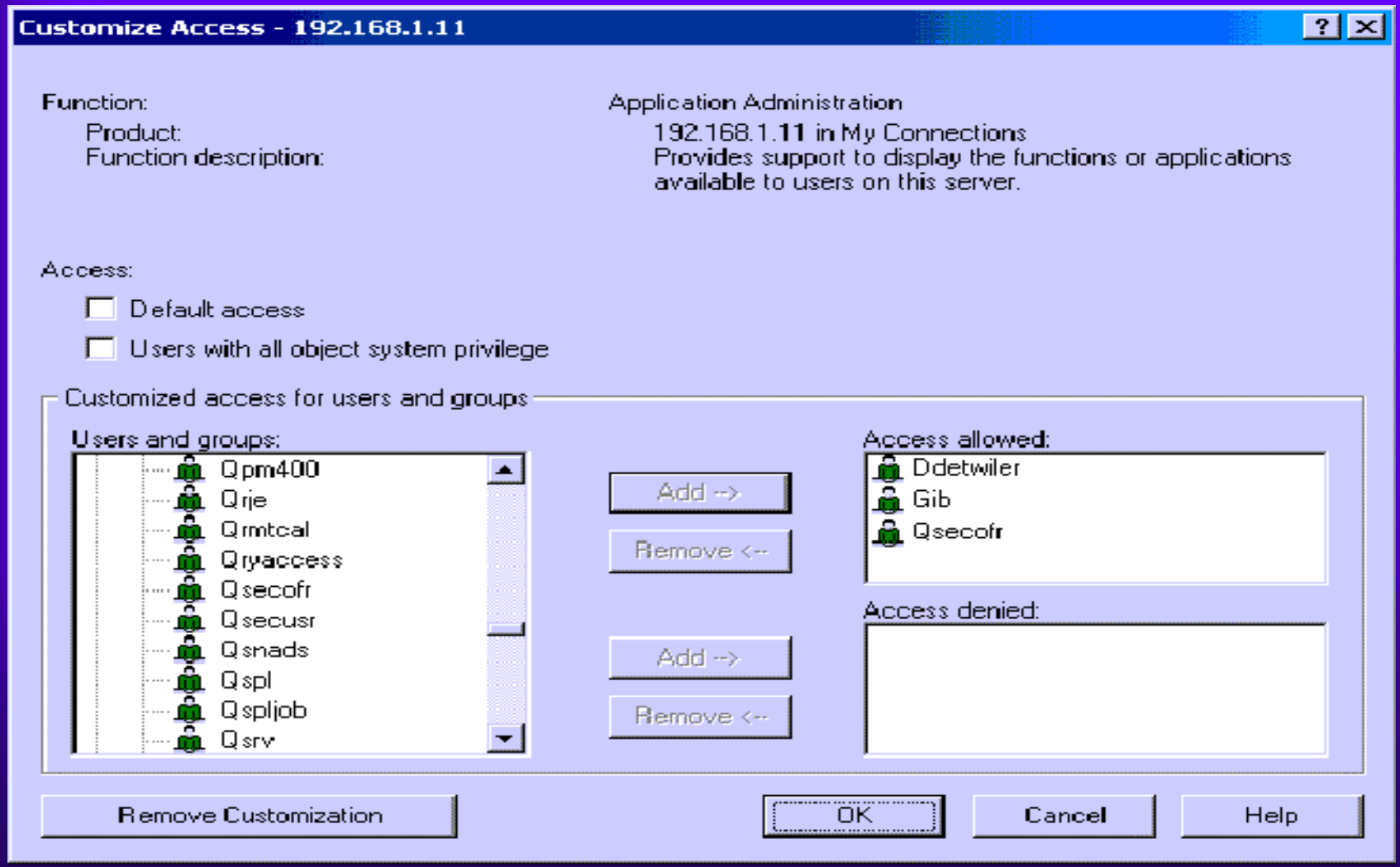
IBM Default is to allow all operations navigator functions

Restrict Options for Users



Controlling Operations Navigator

Limit users that can use Application Administration



#5 – Limiting Command Line

- **Challenge**
  - Limit users to menu options
  - End users should not be allowed to use CL Commands
- **Remedy**
  - LMTCPB(*YES) in user profile
  - Use PRTUSRPRF to find profiles with command line access

#6 – Eliminate Unused Accounts

- **Challenge**
  - Keeping up with numerous personnel changes and their user profiles can be difficult
    - User profile management is time consuming
    - Updating the system for recently terminated users is frequently overlooked
- **Remedy**
  - Security Tools option to find and disable inactive user profiles

#6 Profiles not signed on

GO SECTOOLS

```
SECTOOLS          Security Tools
   Select one of the following:
     Work with profiles
       1. Analyze default passwords

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

       5. Display activation schedule
       6. Change activation schedule entry

       7. Display expiration schedule
       8. Change expiration schedule entry

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

Inactive user profile check

#7 – Excessive special authorities

- **Challenge**

  Users are given too much special authority

  - ***ALLOBJ** -- Allows access to all data
  - ***SERVICE** – Service tools bypass security
  - ***SPLCTL** -- Access to all spool files
  - ***SECADM** – Manage user profiles

- **Remedy**
  - Use PRTUSRPRF (Print User Profile)

User Profile Information

PRTUSRPRF

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

* * * truncated output * * *

#8 – Elimination of Trivial Passwords

- **Challenge**
  - Insure that passwords are not compromised
  - Avoid trivial passwords such as password same as the user profile
- **Remedy**
  - **System values for expiration and content rules**
  - **Security tools ANZDFTPWD to check for password same as user profile name**

#8 – Eliminate of Trivial Passwords

System Value	Description	Recommendation
QPWDLVL	Type of Password	0
QPWDMINLEN	Minimum Length	10
QPWDMAXLEN	Maximum Length	>=6
QPWDLMTREP	Limit repeating char	2=no adj duplicates
QPWDRQDDIF	Limit pwd repetition	1-5 at least 10 differ
QPWDRQDDGT	Require Digit	1 = yes
QPWDLMTAJC	Prevent adjacent digits	0 = no
QPWDPOSDIF	Positional difference	0 = no restriction
QPWDVLDPGM	Validation Program	*NONE

#8 – Find Trivial Passwords

GO SECTOOLS

```
SECTOOLS          Security Tools
   Select one of the following:
     Work with profiles
       1. Analyze default passwords

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

       5. Display activation schedule
       6. Change activation schedule entry

       7. Display expiration schedule
       8. Change expiration schedule entry

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

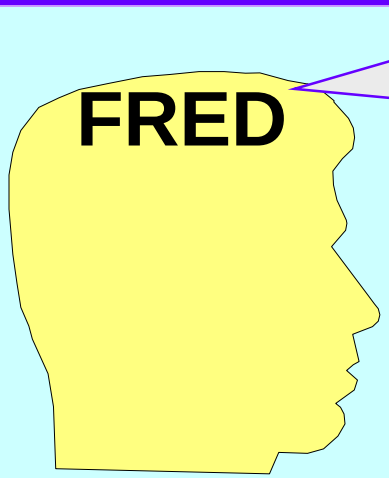
Password = Profile

New profiles that have never signed on or reset passwords

#9 – Authority to User Profile

- **Challenge**
  - The *PUBLIC authority to for user profiles should be *EXCLUDE
  - If other users have access to a user profile they can submit jobs as that user
- **Remedy**
  - Security tools PRTPUBAUT to find profiles with excessive authority

Authority to User Profiles



Object Authority
***PUBLIC *USE**

When users have *USE authority to other profiles Jobs can be submitted as other users

SBMJOB USER(FRED) CMD(CL command)

Recommend

User profiles public authority = *EXCLUDE to prevent running jobs as other users

Check Authority to User Profiles

PRTPUBAUT OBJTYPE(*USRPRF)

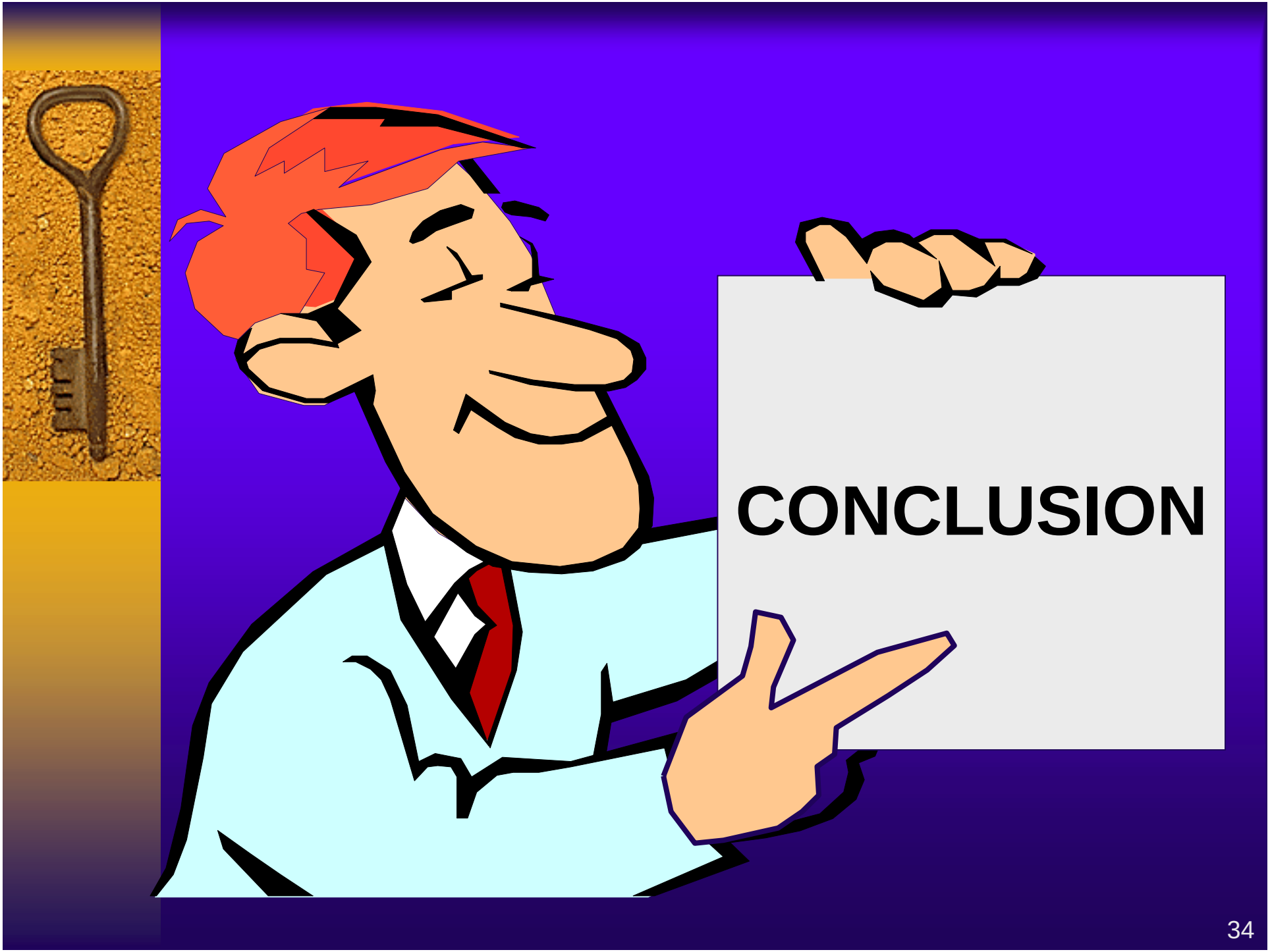
```
                          Publicly Authorized Objects (Full Report)
Object type  . . . . . . . . . :   *USRPRF
Specified library  . . . . . . :   QSYS
                        Auth                  ------Object--------- ---------Data-------
Libr  Object  Owner     List  Authority  Opr Mgt Exist Alter Ref Read Add Upd Dlt Exec
QSYS FRED       QSECOFR       *USE        X                       X
QSYS QDBSHR     QSYS          USER DEF                                X       X
QSYS QDBSHRDLO  QSYS          USER DEF                                X       X
QSYS QDPLJOB    QSYS          *USE        X                   X                   X
QSYS QTMPLPD    QSYS          USER DEF    X
                        * * * * *  E N D  O F  L I S T I N G  * * * * *
```

Profiles shown are OK

Revoke *PUBLIC authority from other profiles

#10 – Inappropriate Object Authority

- **Challenge**
  - Users may be able to view and access OS/400 libraries and objects
    - Improper permissions may be set for the “*PUBLIC” users
    - Detecting changes for PC users accessing the system via OpsNav
- **Remedy**
  - PRTPUBAUT (Print Public Authority)
  - PRTPRVAUT (Print Private Authority)


CONCLUSION

Action Plan

- ✓ Create a security policy to define security goals
- ✓ Move to security level 40
  - If audit journal indicates no application problems
- ✓ Control PC access
  - Implement exit programs to control FTP, File Transfer, Remote Commands
  - Limit Operations Navigator (Application Administration)

Action Plan

- ✓User Profiles
  - Eliminate unused accounts
  - Restrict command line for end users
  - Avoid use of trivial passwords
  - Limit powerful special authority
    *ALLOBJ *SECADM *SPLCTL *SERVICE
- ✓Verify *PUBLIC authority to user profiles is *EXCLUDE except for the profiles:
  QDBSHR QBSSHRDLO QSPLJOB QTMPLPD
- ✓Limit *PUBLIC authority to objects and libraries

QUESTIONS

If you have additional questions or want more information please contact me

Wayne O. Evans

WOEvans@AOL.com

Visit my web site

http://WWW.WOEvans.COM