

MS Office Integration Security

Berbee...putting the **e** in business™

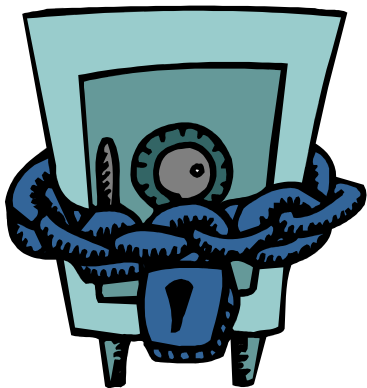
Spring 2005
Wednesday
ID# 409091

Foresight Technology Group
A Berbee Company
Frank Thomas
4092 Holland Sylvania Road
Suite C
Toledo, OH 43623
frank.thomas@berbee.com
(419) 824-9626



Security and Office Integration

How can you control who has access to your data?



Berbee...putting the **e** in business™

Foresight Technology Group
A Berbee Company
Frank Thomas
4092 Holland Sylvania Road
Suite C
Toledo, OH 43623
frank.thomas@berbee.com
(419) 824-9626





Agenda

- A quick peek at The security Wizard
- Defining the problem
- What is "normal" Security
- Security methods
- Application only access
 - Overview
 - Demonstration
 - How to set it up
- Security on the Internet
- Other Things to improve security



The Security Wizard

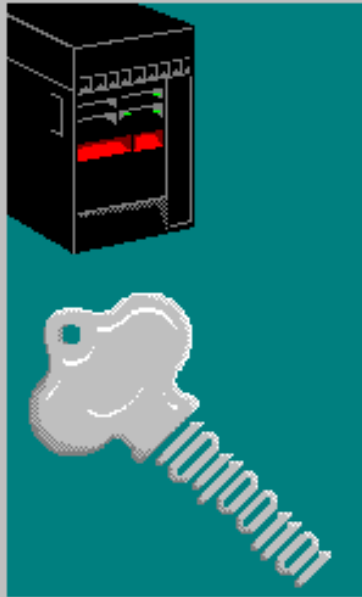
The screenshot shows the AS/400 Operations Navigator interface. The title bar reads "AS/400 Operations Navigator". Below the title bar is a menu bar with "File", "Edit", "View", "Options", and "Help". A toolbar contains icons for various functions. The main window is divided into two panes. The left pane, titled "Primary Environment", shows a tree view of "AS/400 Systems" with "S1021d1m" expanded. Under "S1021d1m", the "Security" folder is highlighted with a blue selection bar and a mouse cursor. The right pane, titled "S1021d1m: Security", displays a table with two columns: "Name" and "Description".

Name	Description
Authorization...	AS/400 Authorization Lists
Policies	AS/400 Security Policy

Right click on security then

Click on configure

AS/400 Security Wizard - S1021d1m



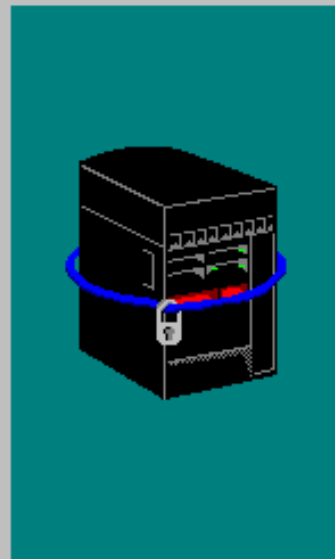
Welcome to the AS/400 Security Wizard!

Use the wizard to:

- Create a set of security recommendations for your AS/400.
- Create reports explaining the security recommendations.
- Apply the recommendations to your AS/400.

You can cancel

AS/400 Security Wizard - S1021d1m



How would you characterize the general security policy for your AS/400?

- Strict
- Average
- Relaxed

Next, Next

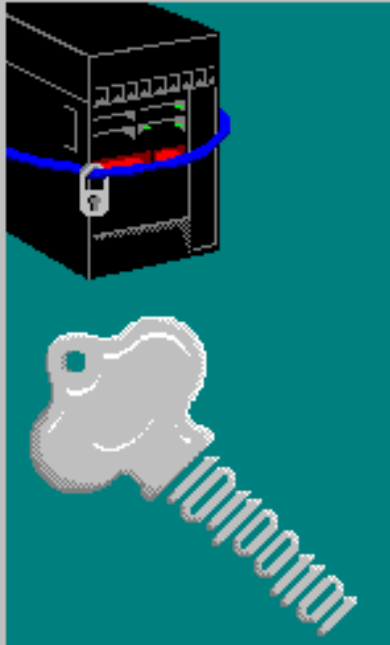
< Back

Next >

Cancel



AS/400 Security Wizard - S1021d1m



You have answered all the questions needed to create a set of security recommendations for your AS/400.

You can review the recommendations by clicking the Details button.

Details ...

All done

< Back

Next >

Cancel



Summary of Recommendations

Security Auditing Policy

Security Level

Security Journal Reports

Security Controls

Password Rules

Security Reports

To accept a recommended setting for a security control, leave its checkbox checked.

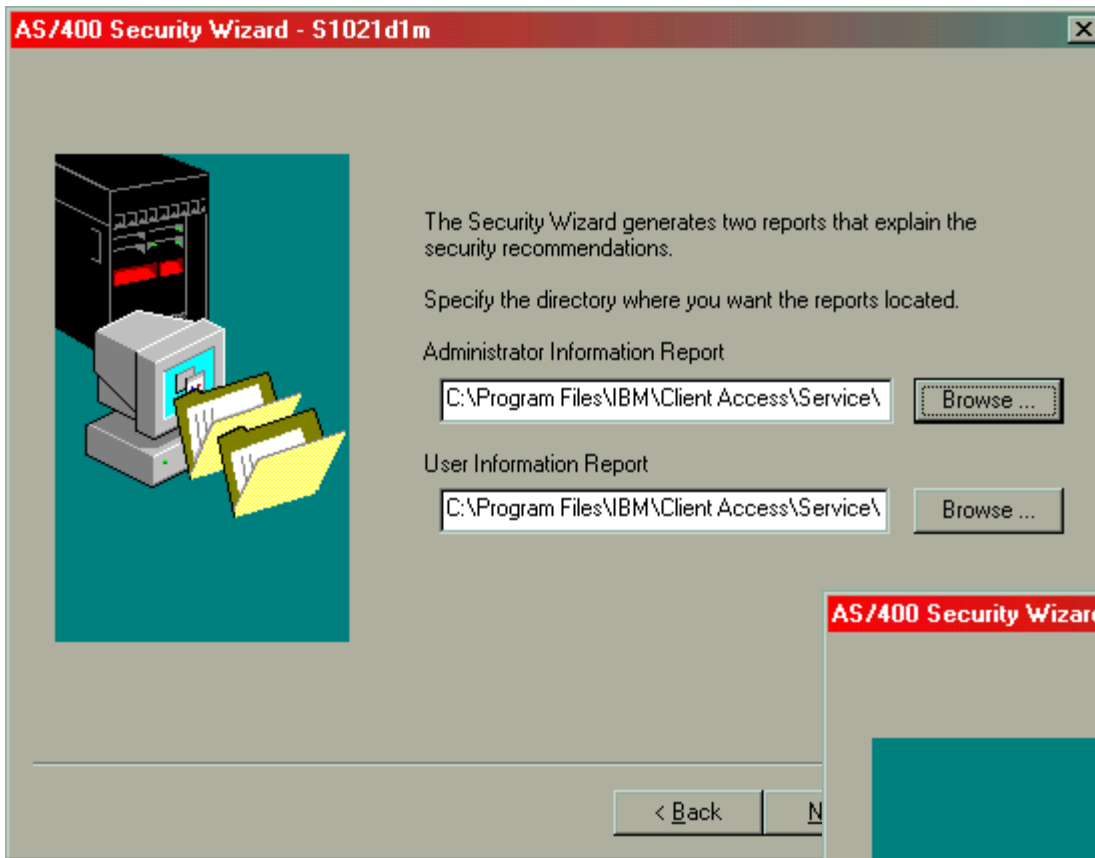
To keep the current setting for a security control, click its checkbox to remove the check.

<input type="checkbox"/>	Password Control	Current Setting	Recommended Setting
<input checked="" type="checkbox"/>	Limit characters	None	AEIOU@#\$
<input checked="" type="checkbox"/>	Required password digits	No	Yes
<input checked="" type="checkbox"/>	Duplicate password	Can be the same as old passwo	Cannot be the same as last 6
<input checked="" type="checkbox"/>	Days password valid	60	60
<input checked="" type="checkbox"/>	Limit character positions	No	Yes
<input checked="" type="checkbox"/>	Max password length	10	8
<input checked="" type="checkbox"/>	Min password length	6	6
<input checked="" type="checkbox"/>	Password validation program	None	None
<input checked="" type="checkbox"/>	Limit adjacent digits	No	Yes
<input checked="" type="checkbox"/>	Limit repeat characters	Can be repeated	Cannot be repeated consecutiv

OK

Cancel

Apply



Save the reports to print or review.

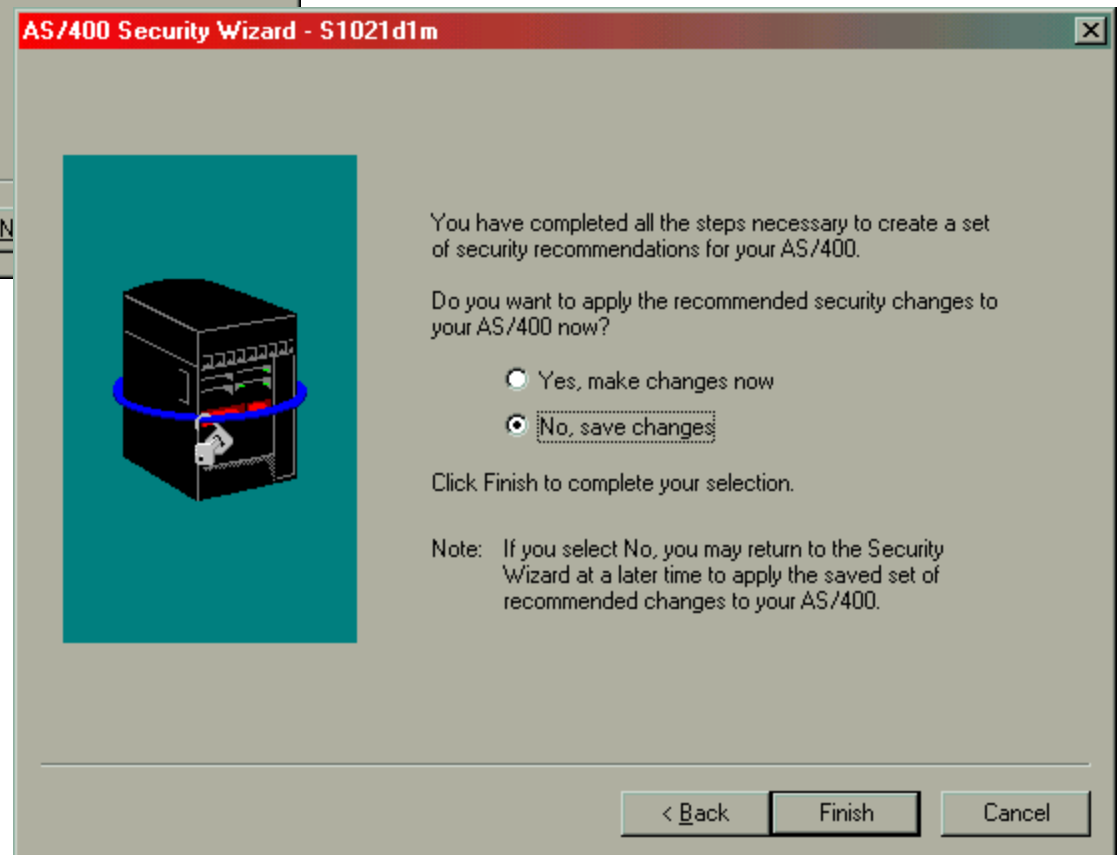


Security Wizard Administrator.TXT.lnk



Security Wizard User.TXT.lnk

DO NOT make the changes till you have carefully reviewed the reports.



What trouble can I get into today?

Berbee...putting the **e** in business™

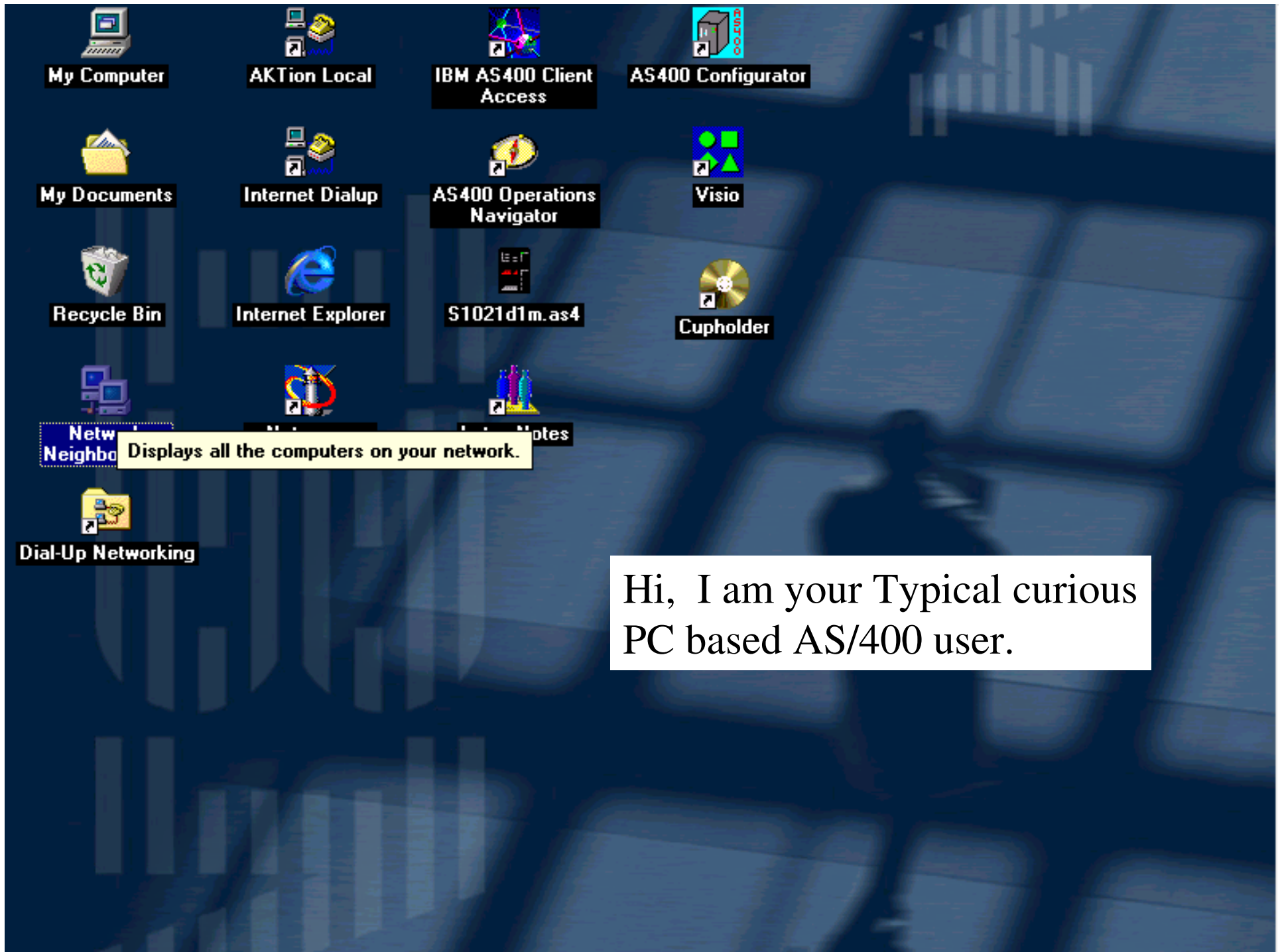
A user's favorite question

Foresight Technology Group
A Berbee Company
Frank Thomas
4092 Holland Sylvania Road
Suite C
Toledo, OH 43623
frank.thomas@berbee.com
(419) 824-9626



B E R B E E ®





My Computer

AKTion Local

IBM AS400 Client
Access

AS400 Configurator

My Documents

Internet Dialup

AS400 Operations
Navigator

Visio

Recycle Bin

Internet Explorer

S1021d1m.as4

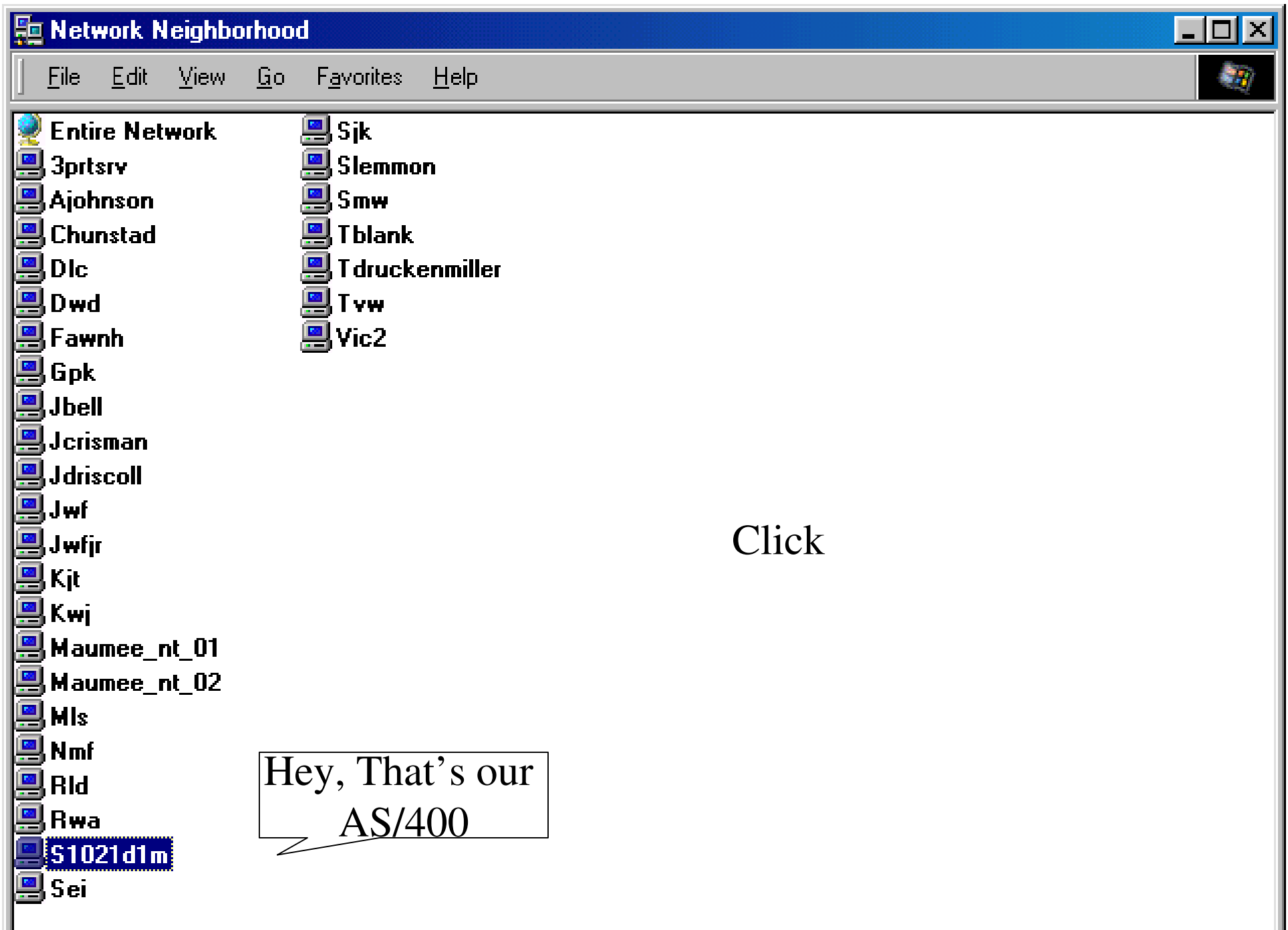
Cupholder

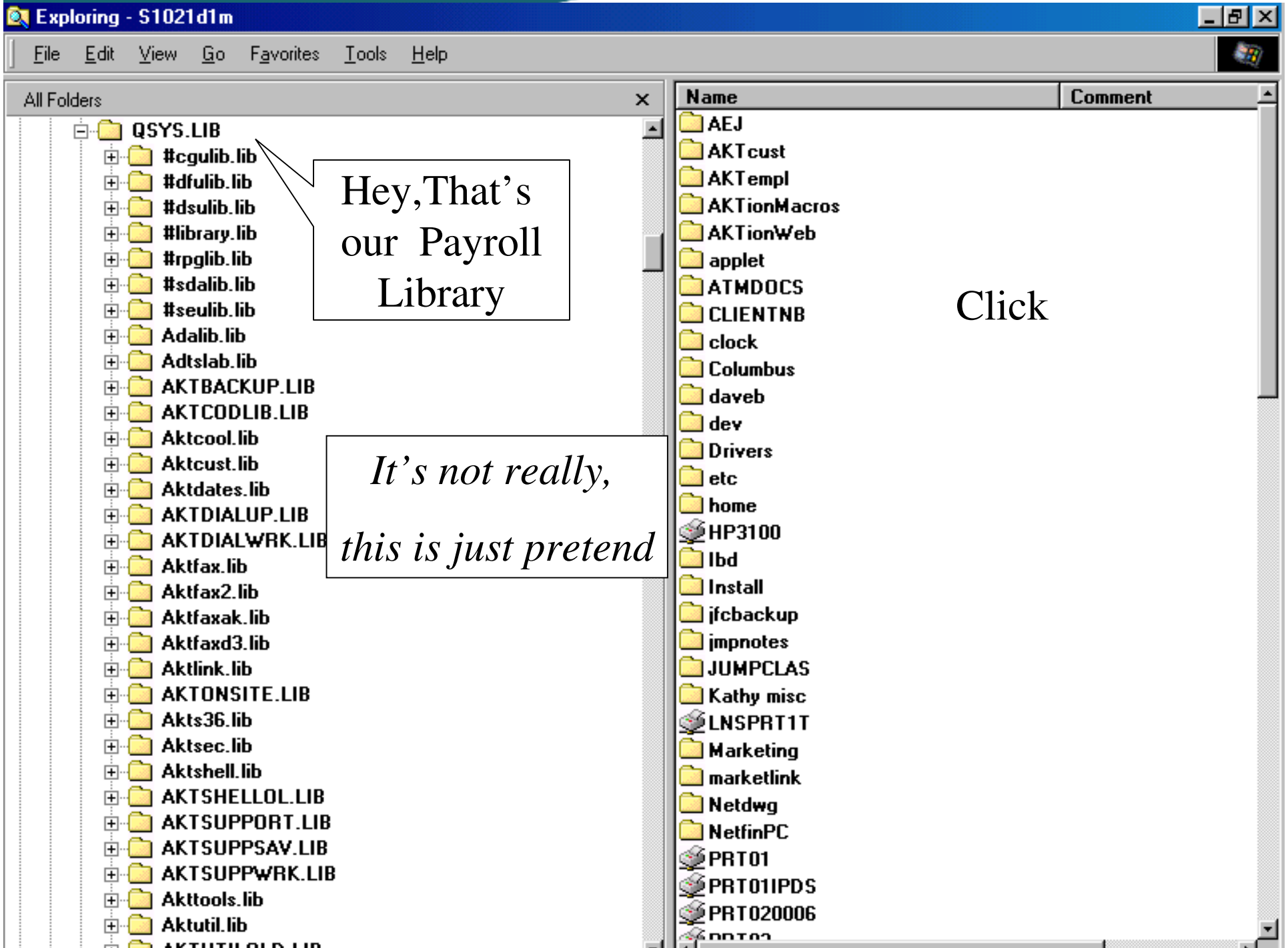
Netw
Neighb

Displays all the computers on your network.

Dial-Up Networking

Hi, I am your Typical curious
PC based AS/400 user.





S1021D1M - SYSTIME/S#EMP#(S#EMP#)

EMPCOD	EMP##	ENAME	ETYPE	ELOCAT	ESTAT
*SP	0	SUPPORT (FO...	SPRT	0	
*TC	0	TECH SERV (F...	SPRT	0	
-NO	0	**** NO EMPLO...	VEND	0	
AKT	0	ALAN K TOPE ...	ADMN	0	
BMD	10	BARBARA M D...	SPRT	6	
CJE	5	CHRIS J ELEKO...	SPRT	0	
CMS	0	CONCORD MA...	VEND	0	
DDD	16	DENNIS D DIE...	SLSA	0	
DKL	8	DEBRA K LEH...	SPRT	0	
EAJ	14	EDWARD A JU...	SLSD	0	
EEW	0	ELLIOTT E. WA...	TECH	0	
EJM	0	EDWIN J MCCL...	TECH	6	
EPS	0	ERIC P. SMITS ...	TECH	0	
FAT	7	FRANK A THO...	SLSA	0	
FLH	20	FAWN L HART...	TECH	0	
GCT	18	GARY C TROK...	TECH	0	
GTJ	0	GARY T. JUST...	TECH	0	
JCW	0	JEFF C WILLIA	TECH	6	

Retrieved record 166

- S#EMP#.FILE**
 - S#EMP#2222.FILE
 - S#EMPTMS.FILE
 - S#LINE#.A.FILE
 - S#LINE.FILE
 - S#NEW91.FILE
 - S#NEW92.FILE
 - S#ORD##.A.FILE
 - S#ORD#.FILE
 - S#ORDCUS.FILE
 - S#PRJALL.FILE
 - S#PRJATM.FILE

Cool - The employee file

Create New Data Source [?] [X]

What name do you want to give your data source?

1.

Select a driver for the type of database you want to access:

2.

Click Connect and enter any information requested by the driver:

3. S1021D1M

Select a default table for your data source (optional):

4.

Save my user ID and password

[?]

Power Word User

Query Wizard - Choose Columns [?] [X]

What columns of data do you want to include in your query?

Available tables and columns:

- S#EMP#
- S#EMP#2222
- S#EMPTMS
- S#LINE
- S#LINE#A
- S#NEW91
- S#NEW92

Columns in your query:

- EMPCOD
- EMP##
- ENAME
- ETYPE
- ELOCAT
- ESTAT
- EAP2V#
- EBUNIT

Preview of data in selected column:

[?]

Query Wizard - Finish



What would you like to do next?

Return Data to Microsoft Word

Save Query...

View data or edit query in Microsoft Query

Microsoft Query

File Edit View Format Table Criteria Records Window Help

SQL

Query 1 from time stuff

S#EMP#

- *EAP2V#
- EBUNIT
- ELOCAT
- EMP##
- EMPCOD**

- Add Column...
- Remove Column
- Edit Column...
- Sort...
- Go To...
- Allow Editing**
- Query Now
- Automatic Query

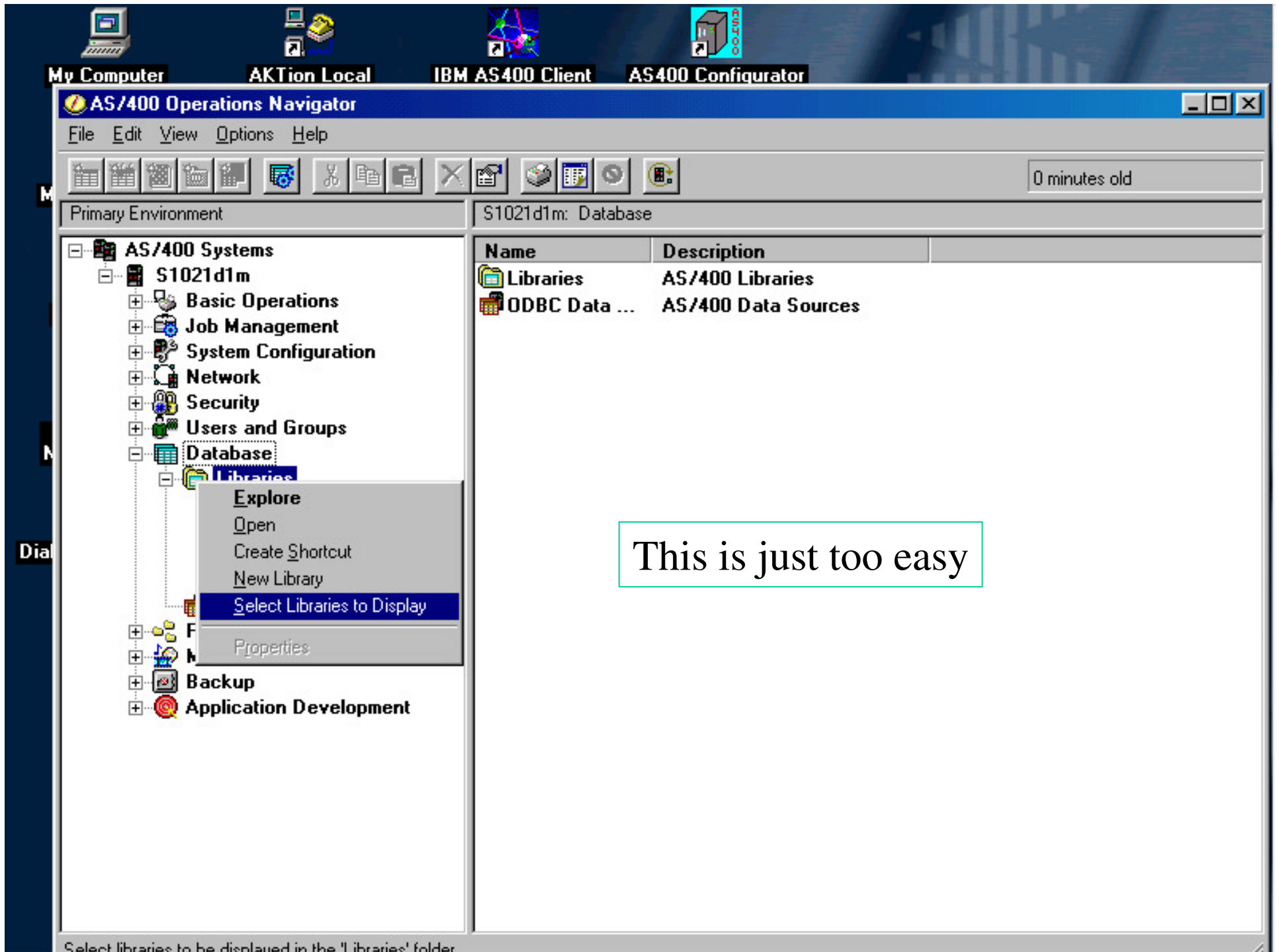
EMPCO	EMP##	ENAME	ETYPE	ELOCA	ESTA	EAP2V#	EBUNIT
*SF	0	SUPPORT (FOR SCHE	SPRT	0			
*TC	0	TECH SERV (FOR SCH	SPRT	0			
-NO	0	**** NO EMPLOYEE RE	VEND	0			
AKT	0	ALAN K TOPE	ADMN	0			ADM
BMD	10	BARBARA M DAVENPC	SPRT	6		5080	DST
CJE	5	CHRIS J ELEKONICH (S	SPRT	0		5084	CNS
CMS	0	CONCORD MANAGEME	VEND	0			
DDD	16	DENNIS D DIEBALL (S	SLSA	0		5082	DST
DKL	8	DEBRA K LEHMAN	SPRT	0		5093	
EAJ	14	EDWARD A JUSTEN	SLSD	0		5092	
EEW	0	ELLIOTT E. WAHL	TECH	0		5105	
EJM	0	EDWIN J MCCLENDON	TECH	6		5117	
EPS	0	ERIC P. SMITS	TECH	0		5097	
FAT	7	FRANK A THOMAS	SLSA	0		5099	ITG
FLH	20	FAWN L HARTMAN	TECH	0		5136	DST
GCT	18	GARY C TROKNYA	TECH	0		5102	DST
GTJ	0	GARY T. JUSTEN	TECH	0			
JCW	0	JEFF C WILLIAMS	TECH	6		5126	
JEB	0	JEFFREY E. BEAUMAN	TECH	0			
JFC	4	JOHN F CRISMAN	MNGR	0		5078	ITG
JHG	0	JACK H GOLDBERG	TECH	6		5127	
JLW	19	JONN I WAGONER	SPRT	0		5161	



- S#EMP#
- *
- EAP2V#
- EBUNIT
- ELOCAT
- EMP##
- EMPCOD

I can actually change data on the AS/400!

	EMPCO	EMP##	ENAME	ETYPE	ELOCA	ESTA1	EAP2V#	EBUNIT
✎	*SP	0	SUPPORT (FOR SCHE	SPRT	0			
	*TC	0	TECH SERV (FOR SCH	SPRT	0			
	-NO	0	**** NO EMPLOYEE RE	VEND	0			
	AKT	0	ALAN K TOPE	ADMN	0			ADM
	BMD	10	BARBARA M DAVENPC	SPRT	6		5080	DST
	CJE	5	CHRIS J ELEKONICH (S	SPRT	0		5084	CNS
	CMS	0	CONCORD MANAGEME	VEND	0			
	FLH	20	FAWN L HARTMAN	TECH	0		5136	DST
	GCT	18	GARY C TROKNYA	TECH	0		5102	DST
	GTJ	0	GARY T. JUSTEN	TECH	0			
	JCW	0	JEFF C WILLIAMS	TECH	6		5126	
	JEB	0	JEFFREY E. BEAUMAN	TECH	0			
	JFC	4	JOHN F CRISMAN	MNGR	0		5078	ITG
	JHG	0	JACK H GOLDBERG	TECH	6		5127	
	JLW	19	JODI L WAGONER	SPRT	0		5161	



This is just too easy

Select libraries to be displayed in the 'Libraries' folder

My Computer AKTior

AS/400 Operations Navigator

Primary Environment

AS/400 Systems

- S1021d1m
 - Basic Operati...
 - Job Managem...
 - System Config...
 - Network
 - Security
 - Users and Gro...
 - Database
 - Libraries
 - AKTUT
 - DBU41
 - DSMLII
 - QGGL
 - SYSTM
 - ODBC Dat...
 - File Sy...
 - Multime...
 - Backup
 - Applica...

SYSTIME.S#EMP# - S1021d1m

File Edit View Rows Help

EMPCOD	EMP##	ENAME
*SP	0	SUPPORT (FOR SCHEDULING)
*TC	0	TECH SERV (FOR SCHEDULING)
-NO	0	NO EMPLOYEE REQUIRED
AKT	0	ALAN K TOPE
BMD	10	BARBARA M DAVENPORT (BAF)
CJE	5	CHRIS J ELEKONICH (SPIKE) 53
CMS	0	CONCORD MANAGEMENT SYS
DDD	16	DENNIS D DIEBALL (SKIP) 401
DKL	8	DEBRA K LEHMAN
EAJ	14	EDWARD A JUSTEN (ED)
EEW	0	ELLIOTT E. WAHL
EJM	0	EDWIN J MCCLENDON
EPS	0	ERIC P. SMITS
FAT	7	FRANK A THOMAS 501
FLH	20	FAWN L HARTMAN
GCT	18	GARY C TROKNYA
GTJ	0	7 FRANK A THOMAS Is the man SLSA
JCW	0	JEFF C WILLIAMS

0 minutes old

PROJECT...
BILLINGS:....
DUNTING B...


Are you scared yet?

AKT Order ...
D Order Lin...
ived Time 1...
1004

D Orders ...
MMA...
FIL...
object...
cts ...
object...
R A...
Info ...
o by...

Billing & C...
omer Time f...

AS/400 Operations Navigator

 The table you are attempting to change is not being journaled, or you do not have authority to the journal. If you want to continue, you will not be able to cancel the changes you make. Do you want to continue making the change?

Yes No

KKD n IKDISTIK DORTED

S#TASK Table Task Codes Master

25 - 48 of 74 object(s)



“Normal” Security

Check your security level:

- Level 30, maybe <http://www.netiq.com/products/vsa/10point.asp>
- Passwords for sure
 - All object?
 - Command lines?
 - Week passwords?
 - Powerful profiles?
- Application security at menu level
 - No one on a green screen can get past this. (probably true unless they have a command line)



Holes in “normal” security

- With a command line I can run queries DFU, DBU or other 3rd party tools.
- I can get to any data on the AS/400 from my PC.



Exit point security

- Exit point security allows you to secure specific points in programs like Client Access and TCP to prevent accessed to the iSeries
 - The problem is you have to secure every exit point and not all 3rd party tools allow for this.



Policies

- Are "rules" that are enforced on a Client PC.
- Are Typically downloaded from a file server, but can be enter manually on an individual PC.
- Can be used to control some Client Access Functions.
 - *Restrict Number of 5250 sessions per user*
 - Restrict usage of ODBC based on DSN, AS/400, globally
 - Restrict Usage of Data Transfer
 - Restrict usage of Install and Service functions
 - *Restrict OLE DB usage*
- Can also be used to control some PC OS functions.



B E R B E E®

More on Policies

- Are created by a “Network Administrator”
- Create using Microsoft Policy Editor
 - CD from Win 98, Win NT, Office 2000
- CWBPOLUT.EXE – tells a PC to download policies
 - At <http://www.as400.ibm.com/clientaccess>



B E R B E E®

Application Administration

- Part of Operations Navigator
- Host based solution for restricting PC Programs
- Can restrict Op Nav and CA
- Must be at V4R3 or higher
- Stored on 400 by user profile
- Build in to Client Access



Appl. Admin. User Interface

AS/400 Operations Navigator

File Edit View Options Help

Environment: Primary Environment

- Management Central (S1021d1)
 - Primary Environment
 - Qs1021d1m
 - S1021d1m
 - Explore
 - Open
 - Collection Services
 - Inventory
 - Fixes
 - Run Command...
 - Event Log
 - Application Administration
 - Display Emulator...
 - Create Desktop Icon
 - Verify Connection...
 - Delete...
 - Send Message...
 - Properties

Application Administration - S1021d1m

Select the functions or applications available to users.

AS/400 Operations Navigator | Client Applications | Host Applications

Function	Default Access	All Object Access	Customized Access
AS/400 Operations Navigator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Basic Operations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Messages	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Printer Output	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Printers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Job Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Server Jobs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration and Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Hardware Inventory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Software Inventory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
IP Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Point-to-Point	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Protocols	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Remove Customization Customize

Applications ... OK Cancel Help

Right Click

Displays the functions or applications available to users on this AS/400 system.



BERBEE®

Appl. Admin. User

Application Administration - Jamaica

Select the functions or applications available to users.

AS/400 Operations Navigator Client Applications Host Applications

Function	Default Access	All Object Access	Customized Access
Jamaica in My AS/400 Connections			
Basic Operations			
Messages			
Printer Output			
Printers			
Jobs			
Work Management			
Active Jobs			
Server Jobs			
Subsystems			
Job Queues			
Memory Pools			
Configuration and Service			
System Values			
Hardware			

Customize Access - Jamaica

Function: Active Jobs
Product: Jamaica in My AS/400 Connections
Function description: Provides support to work with active jobs.

Access:

- Default access
- Users with all object system privilege

Customized access for users and groups

Users and groups	Access allowed:	Access denied:
<input checked="" type="checkbox"/> All Users		<input checked="" type="checkbox"/> Fthomas
<input checked="" type="checkbox"/> Groups		
<input checked="" type="checkbox"/> Users Not in a Group		

Buttons: Add ->, Remove <-, Add ->, Remove <-

Buttons: Remove Customization, OK, Cancel, Help

Remove Customization

Applications ...

OK

Cancel

Help

Change from Group

Qpgmr Properties - Jamaica

Group name: QPGM

Description: Program

All users:

- Cbrown
- Datalink
- Dwd
- Fat
- Flh
- Fthomas
- Gct

Capabilities | **Networks**

Qpgmr - Capabilities

Privileges | **Applications**

Access for: AS/400 Operations Navigator

Function	Qpgmr Access	Access Derived From
[-] Jamaica in My AS/400 Connections	<input checked="" type="checkbox"/>	
[-] Basic Operations	<input checked="" type="checkbox"/>	
[-] Messages	<input checked="" type="checkbox"/>	Default access
[-] Printer Output	<input checked="" type="checkbox"/>	Default access
[-] Printers	<input checked="" type="checkbox"/>	Default access
[-] Jobs	<input checked="" type="checkbox"/>	Default access
[-] Work Management	<input checked="" type="checkbox"/>	
[-] Active Jobs	<input checked="" type="checkbox"/>	Default access
[-] Server Jobs	<input checked="" type="checkbox"/>	Default access
[-] Subsystems	<input checked="" type="checkbox"/>	Default access
[-] Job Queues	<input checked="" type="checkbox"/>	Default access
[-] Memory Pools	<input checked="" type="checkbox"/>	Default access

OK Cancel Help

OK Cancel Help

Change by User

Fthomas Properties - Jamaica

User name:

Description:

Password:

Previous sign-on: 05/29/02 11:33:41
 Sign-on attempts not valid: 0

- User must change password at next sign-on
- Allow client applications to share this password
- Enable user for processing

Fthomas - Capabilities

Privileges Applications Auditing Password Certificates Unique Identifier

Access for:

Function	Fthomas Access	Access Derived From
<input checked="" type="checkbox"/> Jamaica in My AS/400 Connections	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Basic Operations	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Messages	<input checked="" type="checkbox"/>	All object system privilege
<input checked="" type="checkbox"/> Printer Output	<input checked="" type="checkbox"/>	All object system privilege
<input checked="" type="checkbox"/> Printers	<input checked="" type="checkbox"/>	All object system privilege
<input checked="" type="checkbox"/> Jobs	<input checked="" type="checkbox"/>	All object system privilege
<input type="checkbox"/> Work Management	<input type="checkbox"/>	
<input type="checkbox"/> Active Jobs	<input type="checkbox"/>	Fthomas
<input type="checkbox"/> Server Jobs	<input type="checkbox"/>	Fthomas
<input type="checkbox"/> Subsystems	<input type="checkbox"/>	Fthomas
<input type="checkbox"/> Job Queues	<input type="checkbox"/>	Fthomas
<input type="checkbox"/> Memory Pools	<input type="checkbox"/>	Fthomas



B E R B E E®

Application Admin vs Policies

- Application Admin
 - Easy to use
 - Scoped to AS/400
 - Limited to On/Off
 - Must be at V4R3
- Policies
 - Complex to use
 - PC oriented
 - More capabilities as to what can be set.
 - Any release

Both may help but neither solve problem



BERBEE®

Exit Point

- Provides a place where security can be checked when objects are accessed from outside t with he iSeries.
Programs such as iSeries TCP and iSeries Access can be secured with Exit Points
- Difficult to do yourself
- Some Vendors who offer solutions built on exit point security
 - http://www.netiq.com/products/vsa/iserie_s.asp
 - <http://powertech.com/pt-solutions.html>



Object Owner

- All Objects are changed so that they are owned by "OBJECT OWNER"

Prodownr Properties - S1021d1m

User name: PRODOWNR

Description: Production Owner

Password: Use same password

User must change password at next logon

Enable user for processing

Groups Personal Capabilities Jobs Networks

OK Cancel Help

Change the object owner

Calendar.file Permissions - 192.168.99.8(s102995c)

Object:
/QSYS.LIB/GAWCIS.LIB/CALENDAR.FILE

Type: Table Owner: Fthomas Primary group: (None) Authorization list (AUTL): (None)

Name	Use	Change	All	Exclude	From AUTL	Custom
(Public)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Fthomas	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

Basic Details Columns Add... Remove Customize...

Owner Primary Group Authorization List

OK Cancel Apply Help ?

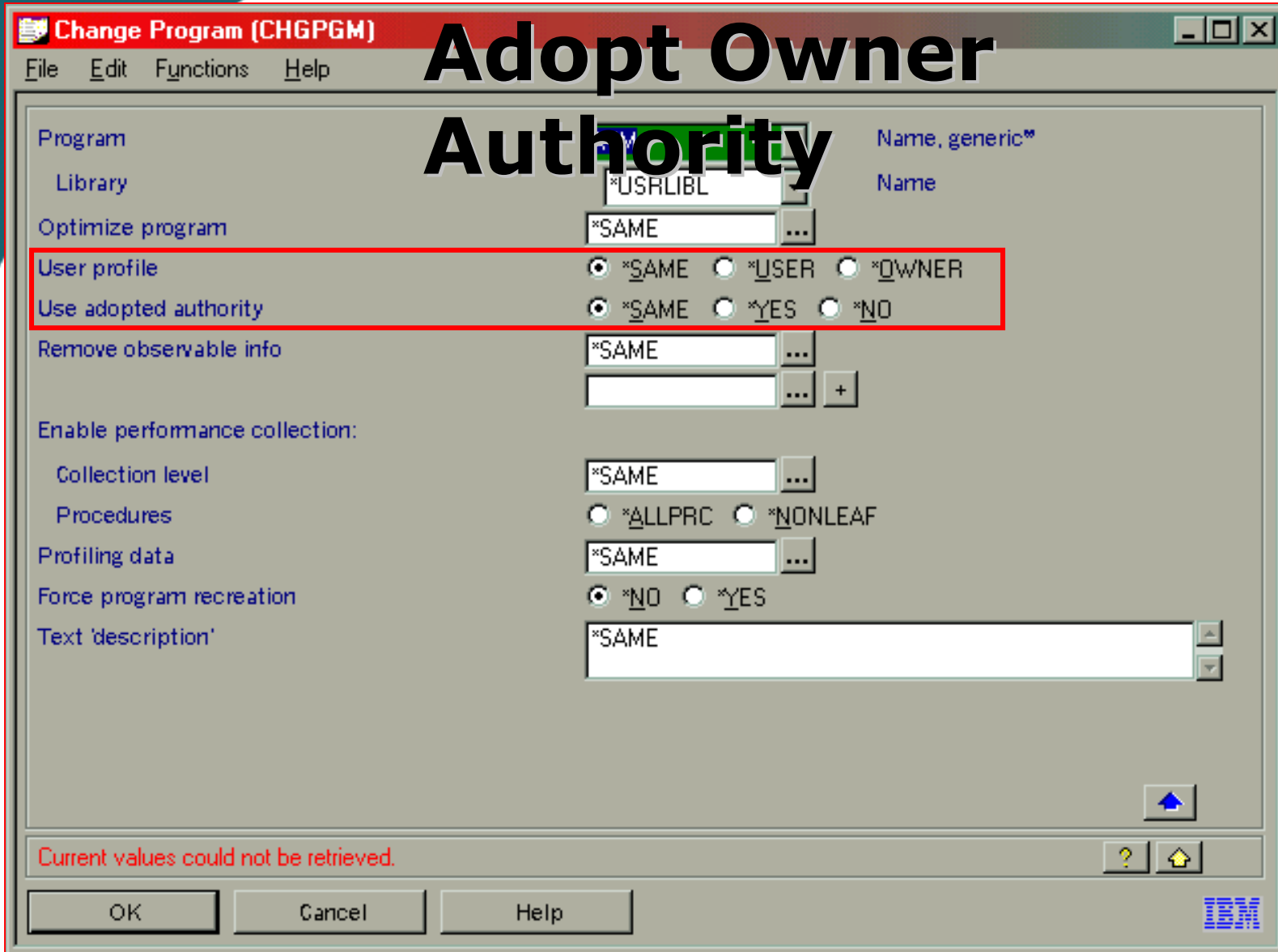


Object Owner

- Write a CL Program
 - Loop through all file and program objects in a library.
 - Use `CHGOBJOWN OBJ(MYLIB/MYFILE) OBJTYPE(*FILE) NEWOWN(PRODOWNR)` to change ownership.
- Change the create commands so that objects are owned by "prodwnr" when created.
- Use `WRKOBJOWN` (write a utility) to find any files or programs not owned



Use CHGPGM to set Adopt Owner Authority





User profile *SAME *USER *OWNER
Use adopted authority *SAME *YES *NO

This is the default, it does not add owner authority but keeps it if it is higher in the stack
Use this on all other programs

User profile *SAME *USER *OWNER
Use adopted authority *SAME *YES *NO

This adds owner authority. You use this on the initial program(s)

User profile *SAME *USER *OWNER
Use adopted authority *SAME *YES *NO

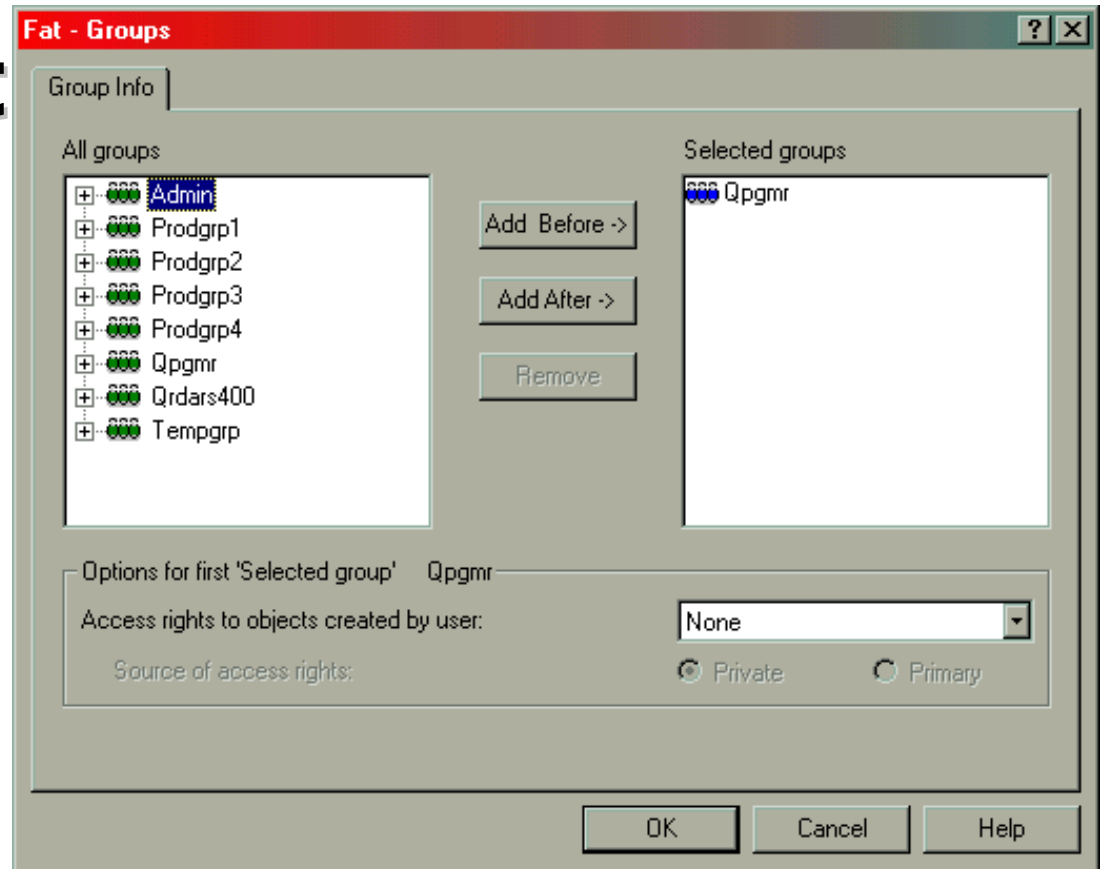
Use this if you only want owner authority on this one job step

User profile *SAME *USER *OWNER
Use adopted authority *SAME *YES *NO

Use this if you want to stop adopt authority at this level

Write a CL program to automate this process

- User1 → • Group 1
- User2 → • Group 2
- UserB → • Group 2
- User3 → • Group 3
- UserC → • Group 3
- UserD → • Group 3
- User4 → • Group 4



A user can be in more than 1 group if you have applications to secure with different users.



Authorization List

Athlist1 (Programs) *Public = Exclude

Group 2 = Use

Group 3 = Use

Group 4 = All

Athlist 2 (Data) *Public = Exclude

Group 2 = Exclude

Group 3 = Use

Group 4 = All

Object

/QSYS.LIB/PRODOWN1.AUTL

Type

Authorization list

Owner

Qpgmr

Primary group

(None)

Name	AUTL ...	Use	Change	All	Exclude	Custom
(Public)		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Qpgmr	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Prodgrp2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Prodgrp3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Prodgrp4	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	

Typical Program Authorization list

Basic Details

Add...

Remove

Customize...

Owner

Primary Group

Secured Objects

OK

Cancel

Apply

Help

Object

/QSYS.LIB/PRODOWN2.AUTL

Type

Authorization list

Owner

Qpgmr

Primary group

(None)

Name	AUTL ...	Use	Change	All	Exclude	Custom
(Public)		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Qpgmr	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
Prodgrp3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Prodgrp4	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	

Typical data
Authorization
List

Basic

Details

Add...

Remove

Customize...

Owner

Primary Group

Secured Objects

OK

Cancel

Apply

Help



AOA – is Setup

- All Objects owned by PRODOWNR
- All programs have the Adopt keyword set.
- All users are in a group
- Groups are in Authorization List
- Program objects Secured by Authorization List 1
- Data objects Secured by Authorization List 2

Tip: Once all users are assigned to groups the authorization list can be given “All” authority. To test the adopt program change the Authorization list to the final authority. If there are any issues change it back, fix the issues then reverse the change.



User in Group1

- Initial System Menu
 - Can display
- Call to System and perform allowed functions
 - Nice error message
- Access Data (read only) via Query
 - Nice error message
- Update Data via DFU/DBU
 - Nice error message
- Access Data (read only) via PC-ODBC
 - System error message (blows Up)
- Update Data via PC-ODBC
 - System error message (blows Up)



B E R B E E®

Group 1 User

- Can't run any program

```
Selection or command
```

```
===> _____
```

```
F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
```

```
F13=Information Assistant    F16=AS/400 main menu
```

```
Not authorized to program ADDSYSTIME in library MWINKLER.
```

```
MA
```

```
a
```

```
MW
```

AS/400 Operations Navigator

File Edit View Options Help



0 minutes old

Primary Environment

S1021d1m: SYSTIME

- AS/400 Systems
 - S1021d1m
 - Basic Operati
 - Job Managem
 - System Config
 - Network
 - Security
 - Users and Gr
 - Database
 - Libraries
 - AKTUT
 - DBU41
 - DSMLI
 - QGPL
 - SYSTII
 - ODBC Dat
 - File Systems
 - Multimedia
 - Backup
 - Application D

Name	Type	Description
QYTDPROJ	Table	Y-T-D CLIENT PROJECT...

AS/400 Operations Navigator Database Error



Not authorized to object S#EMP# in SYSTIME type *FILE.

AS/400 Message ID: SQL0551

Cause : An operation was attempted on object S#EMP# in SYSTIME type *FILE. This operation cannot be performed without the required authority.

Recovery : Obtain the required authority from either the security officer or the object owner. If you are not authorized to a logical file, obtain the authority to the based-on files of the logical file. Try the operation again.

OK

Job Log

Help

S#Q#TMSUM	Table	T&M WORK FILE FOR A...
S#SCHD0	Table	Requested Schedule Info ...
S#SCHD1	Table	Requested Actual Info by...
S#SLSM\$	Table	Salesman T&M Billing & C...
S#STSRPT	Table	Workfile: Customer Time f...
S#TASK	Table	Task Codes Master

25 - 48 of 74 object(s)



User in Group2

- Initial System Menu
 - Can display
- Call to System and perform allowed functions
 - Can perform
- Access Data (read only) via Query
 - Nice error message
- Update Data via DFU/DBU
 - Nice error message
- Access Data (read only) via PC-ODBC
 - System error message (blows Up)
- Update Data via PC-ODBC
 - System error message (blows Up)



B E R B E E®

Group 2 Users

- Can run programs that adopt ^{Work with Employees} SRCEMP

Position to: A

Enter options, press enter
2=Change

Opt	Code	Number	Name	Type	Loc	Unit	Stat
—	AAB	57	ALEXANDRIA A BISHOP	SPRT	6		I
—	ABA		ABACUS	VEND	0		I
—	ADA	94	ALLEN D. AUMEND	SPRT	0	ITG	
—	ADS	62	ALAN D STEINHAUSER	TECH	0		I
—	AKT		ALAN K TOPE	ADMN	0	ADM	I
—	ALA		AMY L. ALVARADO	ADMN	6	ADM	
—	ARK	89	AMY R. KRULLER	SPRT	6	CNS	
—	AWS	66	ALBERT W. SCHWALLER	SLSA	6		I
—	BAK		BETH A. KUTCHER	SPRT	0	CNS	P
—	BCK	74	BARBARA C STEWART	SPRT	6	CNS	
—	BDD	54	BRONWYN D DUPREY	SPRT	4	CNS	
—	BE	58	BERNICE ERDMANN	TECH	0		I

More...

F3=Exit F6=Add F12=Previous



B E R B E E ®

Group 2 Users

- Can't run programs that do not adopt owner authority.

Selection or command

```
==> RUNQRY QRYFILE((SYSTIME/S#EMP#))
```

F3=Exit F4=Prompt F9=Retrieve F12=Cancel

F13=Information Assistant F16=AS/400 main menu

Not allowed to use file S#EMP# in SYSTIME.



0 minutes old


Primary Environment

S1021d1m: SYSTIME

- AS/400 Systems
 - S1021d1m
 - Basic Operati
 - Job Managem
 - System Config
 - Network
 - Security
 - Users and Gr
 - Database
 - Libraries
 - AKTUT
 - DBU41
 - DSMLI
 - QGPL
 - SYSTII
 - ODBC Dat
 - File Systems
 - Multimedia
 - Backup
 - Application D

Name	Type	Description
QYTDPROJ	Table	Y-T-D CLIENT PROJECT...

AS/400 Operations Navigator Database Error



Not authorized to object S#EMP# in SYSTIME type *FILE.

AS/400 Message ID: SQL0551

Cause : An operation was attempted on object S#EMP# in SYSTIME type *FILE. This operation cannot be performed without the required authority.

Recovery : Obtain the required authority from either the security officer or the object owner. If you are not authorized to a logical file, obtain the authority to the based-on files of the logical file. Try the operation again.

OK Job Log Help

S#Q#TMSUM	Table	T&M WORK FILE FOR A...
S#SCHD0	Table	Requested Schedule Info ...
S#SCHD1	Table	Requested Actual Info by...
S#SLSM\$	Table	Salesman T&M Billing & C...
S#STSRPT	Table	Workfile: Customer Time f...
S#TASK	Table	Task Codes Master



User in Group3

- Initial System Menu
 - Can display
- Call to System and perform allowed functions
 - Can perform
- Access Data (read only) via Query
 - Can perform
- Update Data via DFU/DBU
 - Nice error message
- Access Data (read only) via PC-ODBC
 - Can perform
- Update Data via PC-ODBC
 - System error message (blows Up)



B E R B E E®

Group 3 Users

- Can run any program that does not update

display Report

Report width : 90

Position to line : _____

Shift to column : _____

Line 1 2 3 4 5 6 7

Emp Code	Emp #	Emp Name	Type	Locate #	Statu
000001	*SP	SUPPORT (FOR SCHEDULING)	SPRT	0	I
000002	*TC	TECH SERV (FOR SCHEDULING)	SPRT	0	I
000003	-NO	**** NO EMPLOYEE REQUIRED	VEND	0	I
000004	AKT	ALAN K TOPE	ADMN	0	I
000005	BMD	10 BARBARA M DAVENPORT (BARB)	521 SPRT	6	
000006	CJE	5 CHRIS J ELEKONICH (SPIKE)	531 SPRT	0	
000007	CMS	CONCORD MANAGEMENT SYSTEMS	VEND	0	I
000008	DDD	16 DENNIS D DIEBALL (SKIP)	401 SLSA	0	
000009	DKL	8 DEBRA K LEHMAN	SPRT	0	I
000010	EAJ	14 EDWARD A JUSTEN (ED)	SLSD	0	I
000011	EEW	ELLIOTT E. WAHL	TECH	0	I
000012	EJM	EDWIN J MCCLENDON	TECH	6	I
000013	EPS	ERIC P. SMITS	TECH	0	I
000014	FAT	7 FRANK A THOMAS	501 SLSA	0	
000015	FLH	20 FAWN L HARTMAN	TECH	0	

More...

F3=Exit F12=Cancel F19=Left F20=Right F21=Split



BERBEE®

Group 3 Users

- Can't update with programs that don't adopt

```

File      Format      Mode      Window      Search      Extra
File . . . : S#EMP#
Library . . : SYSTIME
Page# . . . : 1 of 1
Control . . . _____

Emp C
Em
Emp N
T
Locate #  ___
Status  I
Ap2 Vend # _____
Business Unit Code  ___

= 1. Add          ADD
  2. Change       CHG
  3. Display      DSP
  4. Delete       DLT
  5. Refresh      F5

F1=Help  F3=Exit  F12=Cancel

rd Length . . :      52
Access . . . : Keyed
rd Number . . :      1

Bottom
F1=Help          F2=Nondisplay keys  F3=Exit          F4=List fields
F5=Refresh       F6=Set key          F10=Action       F24=More keys
You are not authorized to Change records.  Select a different mode.

```

AS/400 Operations Navigator Database Error



Not authorized to object S#EMP# in SYSTIME type *FILE.

AS/400 Message ID: SQL0551

Cause : An operation was attempted on object S#EMP# in SYSTIME type *FILE. This operation cannot be performed without the required authority.

Recovery . . . : Obtain the required authority from either the security officer or the object owner. If you are not authorized to a logical file, obtain the authority to the based-on files of the logical file. Try the operation again.

OK Job Log Help

- SYSTEM
- ODBC Data Sour
- File Systems
- Multimedia
- Backup
- Application Develop

FLH	20	FAV	FRANK A THOMAS	the man
GCT	18	GAR	GARY T. JUSTEN	
GTJ	0	JCW	JEFF C WILLIAMS	
JCW	0	JEB	JEFFREY E. BEUMAN	
JEB	0	JFC	JOHN F CRISMAN	101
JFC	4	JHG	JACK H GOLDBERG	
JHG	0	JLW	JODI L WAGONER	
JLW	19	JRH	JOHN R. HARTLEY	
JRH	0	JSH	JAY S HOLSTINE	
JSH	0	JWF	JOHN W FOSTER	(JACK)
JWF	2	KKD	KDISTIK DORTER	



User in Group4

- Initial System Menu
 - Can display
- Call to System and perform allowed functions
 - Can perform
- Access Data (read only) via Query
 - Can perform
- Update Data via DFU/DBU
 - Can perform
- Access Data (read only) via PC-ODBC
 - Can perform
- Update Data via PC-ODBC
 - Can perform



BERBEE®

Group 4 users

- Can run anything

```

File      Format      Mode      Window      Search      Extra
DATA BASE UTILITY (DBU)
File . . . : S#EMP#      Member . . : S#EMP#      Record Length . :      52
Library . . : SYSTIME    Format . . . : EMP#      File Access . . : Keyed
Page# . . . : 1 of 1     Mode . . . . : Change    Record Number . :      1
Control . . . _____

      Emp Code  *SP
      Emp #    _____
      Emp Name SUPPORT (FOR SCHEDULING)
      Type    SPRT
      Locate # _____
      Status  I
      Ap2 Vend # _____
      Business Unit Code _____

Bottom
F1=Help      F2=Nondisplay keys  F3=Exit      F4=List fields
F5=Refresh   F6=Set key          F10=Action   F24=More keys

```

AS/400 Operations Navigator

File Edit View Options Help



Primary Environment

- AS/400 Systems
 - S1021d1m
 - Basic Operations
 - Job Management
 - System Configuration
 - Network
 - Security
 - Users and Groups
 - Database
 - Libraries
 - AKTUTIL
 - DBU41
 - DSMLIB
 - QGPL
 - SYSTEME**
 - ODBC Data Sour
 - File Systems
 - Multimedia
 - Backup
 - Application Develop

SYSTIME.S#EMP# - S1021d1m

File Edit View Rows Help

EMPCOD	EMP##	ENAME
*SP	0	SUPPORT (FOR SCHEDULING)
*TC	0	TECH SERV (FOR SCHEDULING)
-NO	0	NO EMPLOYEE REQUIRED
AKT	0	ALAN K TOPE
BMD	10	BARBARA M DAVENPORT (BARBARA)
CJE	5	CHRIS J ELEKONICH (SPIKE) 53
CMS	0	CONCORD MANAGEMENT SYS
DDD	16	DENNIS D DIEBALL (SKIP) 401
DKL	8	DEBRA K LEHMAN
EAJ	14	EDWARD A JUSTEN (ED)
EEW	0	ELLIOTT E WAHL
EJM	0	EDWIN J MCCLENDON
EPS	0	ERIC P. SMITS
FAT	7	FRANK A THOMAS 501
FLH	20	FRANK A THOMAS the man
GCT	18	GARY T JUSTEN
GTJ	0	GARY T. JUSTEN
JCW	0	JEFF C WILLIAMS
JEB	0	JEFFREY E. BEUMAN
JFC	4	JOHN F CRISMAN 101
JHG	0	JACK H GOLDBERG
JLW	19	JODI L WAGONER
JRH	0	JOHN R. HARTLEY
JSH	0	JAY S HOLSTINE
JWF	2	JOHN W FOSTER (JACK)
KKD	0	KRISTIK DORTCH

1 minutes old

Co... DD...

- Menus
- RP...
- SY...
- ECT...
- IGS...
- IG B...
- des ...
- employ...
- mary...
- der ...
- Lin...
- me 1...
- # (...
- s ...
- AMA...
- FIL...
- nict

Securing Other AS/400 objects

AS/400 Operations Navigator

File Edit View Options Help

Environment: Primary Environment S1021d1m: AKTempl

0 minutes old

Root

- dev
- home
- tmp
- etc
- usr
- QIBM
- QSR
- APLUS
- AKT cust
- AKTempl
- AKTionMacros
- AKTionWeb
- AS400Class
- ATMDOCS
- CLIENTNB
- Columbus
- Drivers
- lbd
- Install
- JUMPCLAS
- Marketing
- Netdwg
- NetfinPC
- QCA400
- QFFFX
- QFPNWSSTG

Name

- AAIvarado
- AAumend
- AKruller
- BDavenport
- BDuprey
- BKieroff
- BWISE
- CBardy
- CElekonich
- CGottfried
- CHenry
- DBaum
- DBlackwood
- DCornell
- DDriver
- DPavlica
- DSalazar
- FHartman
- FThomas**
- GGojcak
- GKern
- GTroknya
- GUnderdown
- GZeller
- JBell

Explore

- Open
- Create Shortcut
- Filter...
- Sharing
- Cut
- Copy
- Paste
- Permissions**
- NFS Export
- Send...
- New Folder...
- Delete
- Rename...
- Properties

Modified

Modified
6/29/99 10:32...
6/5/99 11:15 AM
6/5/99 11:18 AM
7/19/99 8:44 AM
8/21/97 10:54...
8/21/97 10:53...
5/22/99 9:42 AM
6/5/99 12:19 PM
6/5/99 12:19 PM
8/21/97 11:09...
5/22/99 9:48 AM
6/5/99 12:20 PM
4/21/98 1:53 PM
6/5/99 12:24 PM
6/7/99 8:09 AM
6/18/99 11:44...
8/21/97 11:09...
7/26/99 10:49...
6/5/99 12:35 PM
6/5/99 1:03 PM
7/23/99 4:00 AM
6/18/99 5:14 AM
6/5/99 1:04 PM
6/5/99 1:04 PM
1/27/99 9:40 AM

1 - 24 of 74 object(s)

in business®



Secure your AS/400 resident PC Files

FTthomas Permissions - S1021d1m [?] [X]

Object: /AKTempl/FTthomas

Type: Directory Owner: Lwt Primary group: (None) Authorization list (AUTL): (None)

Name	Read	Write	Exec...	Man...	Exist...	Alter	Refer...	Exclu...	From A...
Fat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
(Public)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lwt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Buttons: Add... Remove Customize...

Owner Primary Group Authorization List

OK Cancel Apply Help



BERBEE

Sharing other AS/400 objects through NetServer

AS/400 Operations Navigator

File Edit View Options Help

5 minutes old

Environment: Primary Environment S1021d1m: Root

Management Central (S1021d1m)

- Primary Environment
 - S1021d1m
 - Basic Operations
 - Job Management
 - Configuration and Service
 - Network
 - Security
 - Users and Groups
 - Database
 - File Systems
 - Integrated File System
 - Root
 - QOpenSys
 - QDLS
 - QSYS.LIB
 - QOPT
 - QFileSvr.400
 - QNTC
 - QNetWare
 - File Shares
 - Multimedia
 - Backup
 - Application Development

Name	Size	Type	Modified
dev		File Folder	5/21/99 3:07 PM
home		File Folder	5/21/99 3:07 PM
tmp		File Folder	6/5/99 3:16 PM
etc		File Folder	6/5/99 2:08 PM
usr		File Folder	5/21/99 3:07 PM
QIBM		File Folder	5/22/99 11:00...
QSR		File Folder	7/27/99 2:22 AM
APLUS		File Folder	6/5/99 1:17 PM
AKTcust		File Folder	7/27/99 5:17 AM
AKTempl		File Folder	7/23/99 7:07 AM
AKTionMacros		File Folder	6/5/99 1:16 PM
AKTionWeb		File Folder	6/5/99 1:16 PM
AS400Class		File Folder	6/5/99 1:17 PM
ATMDOCS		File Folder	6/5/99 1:17 PM
CLIENTNB		File Folder	7/22/99 7:55 AM
Columbus		File Folder	5/22/99 10:40...
Drivers		File Folder	5/22/99 10:40...
Ibd		File Folder	6/5/99 1:17 PM
Install		File Folder	6/5/99 1:17 PM
JUMPCLAS		File Folder	6/5/99 1:25 PM
Marketing		File Folder	6/16/99 5:57 AM
Netdwg		File Folder	6/5/99 1:26 PM
NetfinPC		File Folder	6/5/99 1:26 PM
QCA400		File Folder	5/22/99 10:49...
QFFEX		File Folder	5/22/99 10:51

1 - 24 of 60 object(s)



BERBEE

Adding a 400 (folder) to NetServer

The screenshot shows the AS/400 Operations Navigator interface. The main window is titled "AS/400 NetServer - S1021d1m". The left pane shows a tree view of the NetServer structure, with "AS/400 NetServer" expanded. A context menu is open over the "Sh" folder, with "New" selected, and a sub-menu showing "File" and "Printer". The right pane shows a table of shared objects.

Share	Share Type
Prt01	Printer
Prt03	Printer
Prt3rd	Printer
Qaktempl	File
Qca400	File
Qrdars	File
Txtteh	File

At the bottom, a "Properties" window is open, showing a list of folders and their creation dates. A red box highlights the "File Shares" folder in the left pane.

Folder Name	Creation Date
ibd	6/5/99 1:17 PM
Install	6/5/99 1:17 PM
JUMPCLAS	6/5/99 1:25 PM
Marketing	6/16/99 5:57 AM
Netdwg	6/5/99 1:26 PM
NetfinPC	6/5/99 1:26 PM
QCA400	5/22/99 10:49...
QFFEFAX	5/22/99 10:51



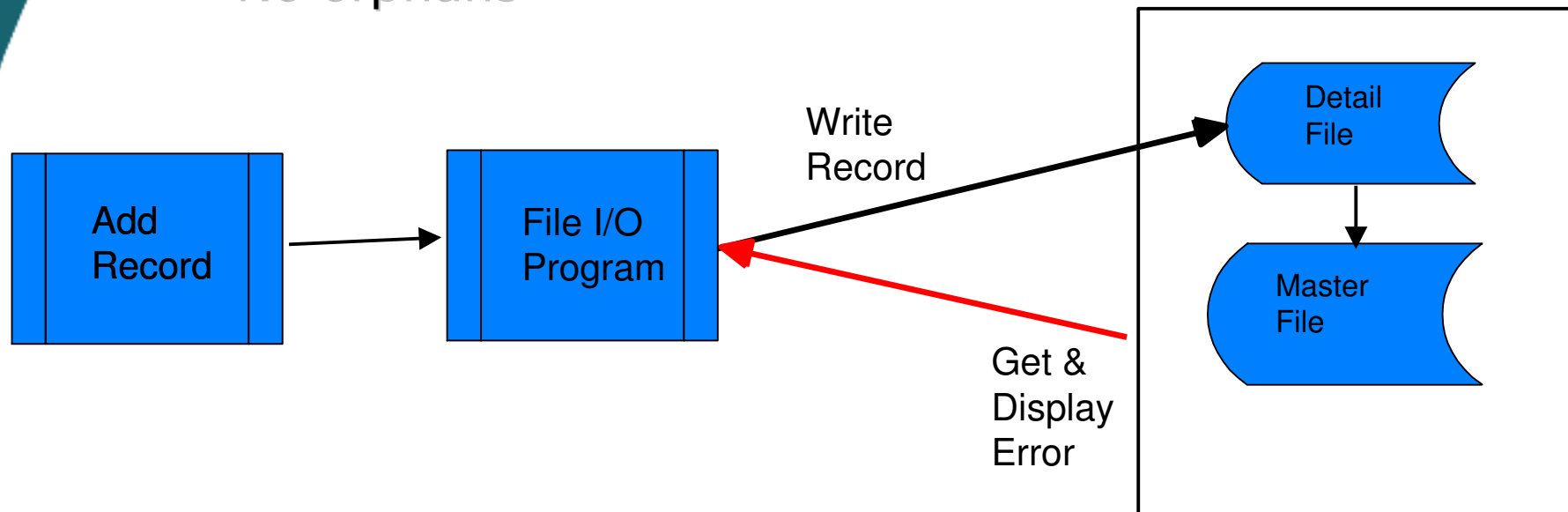
B E R B E E ®

Other Things to secure your DataBase

- Referential Integrity (RI)
- Triggers
- Stored Procedures
- Column Level Constraints

Referential Integrity (RI) Definition

- The database ensures that:
 - Data is consistent between files
 - Data is valid
 - No orphans





Referential Integrity Continued

- RI implemented at the Database Level not at the Application Level
- RI cannot be validated by anyone, not even a programmer.
 - The data is safe from the program.
- Easier application coding
- Better performance

Referential Integrity

Referential Constraint Properties

Constraint: OMML_SECLVL_OMMM

Foreign Key:

Column Name	Type	Len...	Description
ORGANIZATION_ID	CHARACTER	5	
MEMBER_ID	NUMERIC	7,0	
MEMBER_LAST_N...	CHARACTER	40	
MEMBER_FIRST_N...	CHARACTER	30	
STATUS	CHARACTER	5	

Parent table library: AKTMEMSQL

Parent table: OMML

Parent key to reference:

	Column Name	Type	Len...	Descrip
1	SECURITY_LEVEL	CHARACTER	5	
	SECURITY_LEVEL_...	CHARACTER	30	

Delete action: No action

Update action: No action

OK Cancel Help

- Constraint Name
- Dependant File
- Parent File
- Foreign Key
- Parent Key
- Delete Action
- Update Action
- Insert Action



Triggers Definition

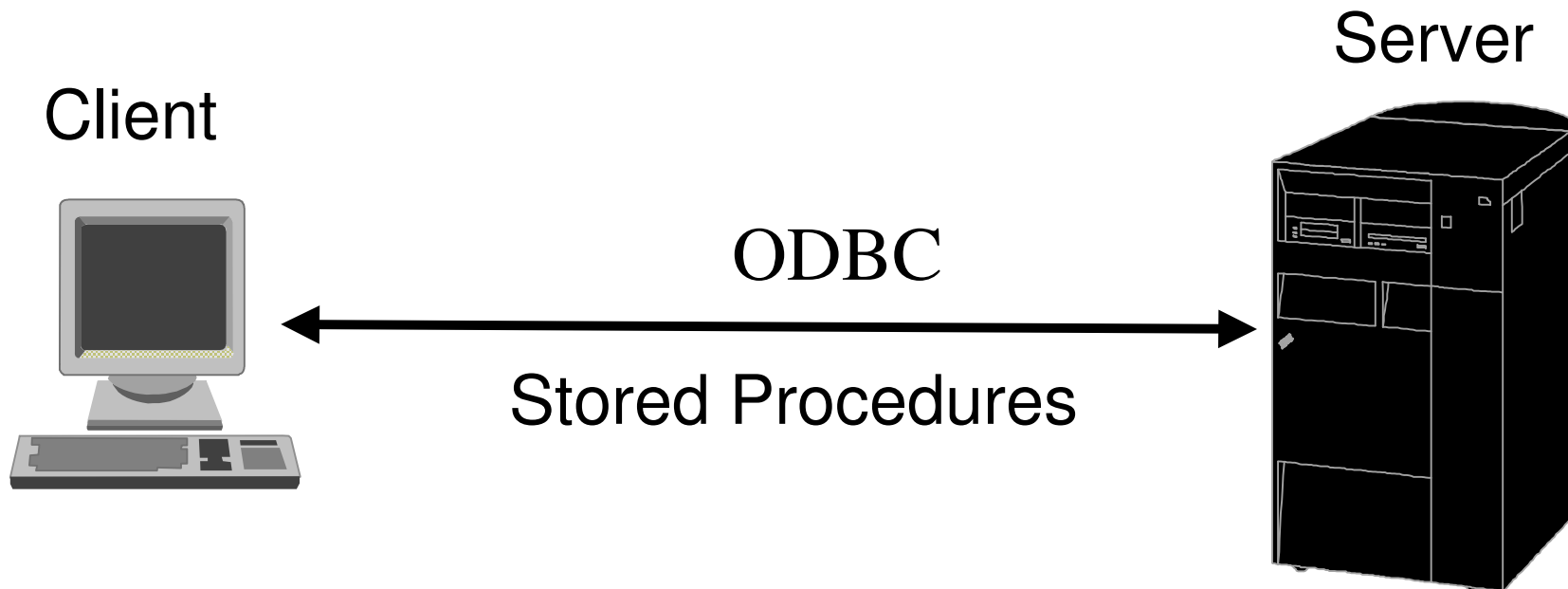
- A trigger is a program which is executed when an event occurs on a file
 - Called by the database
- Triggers can be activated either before or after:
 - Insert
 - Update *Always or *Change
 - Delete
- The data passed to the trigger program is the before and after image of the record
- Can have multiple triggers on one file



B E R B E E®

Stored Procedures Definition

- A program called by a SQL (ODBC compliant) command that receives and returns a Parameter List.





Column Level Constraints

- Allow you to Secure individual fields in a record.
- Allow you to set edit rules that can be trapped on a field in a file.
 - Ranges
 - Values
 - Logical expressions



Column Constraints

Check Constraint Search Condition [?] [X]

Constraint:

Columns	Operators	Functions
ORG_ID ORG_NAME	+ - * / < <= = > >= AND OR CONCAT	All ABS ABSVAL ACOS ANTILOG ASIN ATAN ATANH AVG CHAR CHAR LENGTH

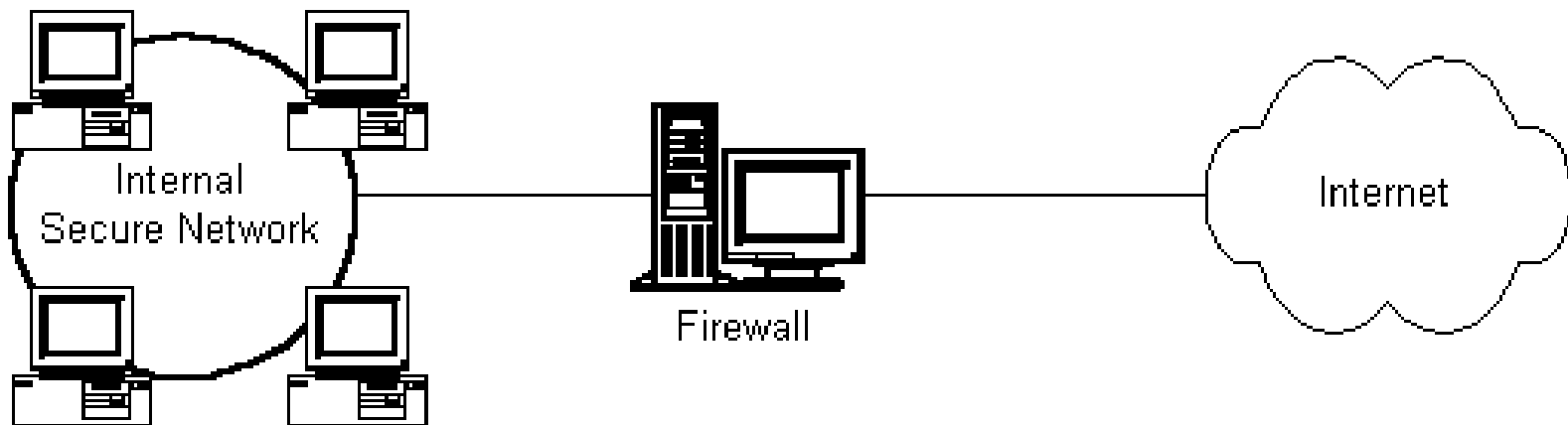
Clause

OK Cancel Help

- You can have the database enforce even more of your business rules.



A Firewall is a blockade between a secure network & an un-trusted network





B E R B E E®

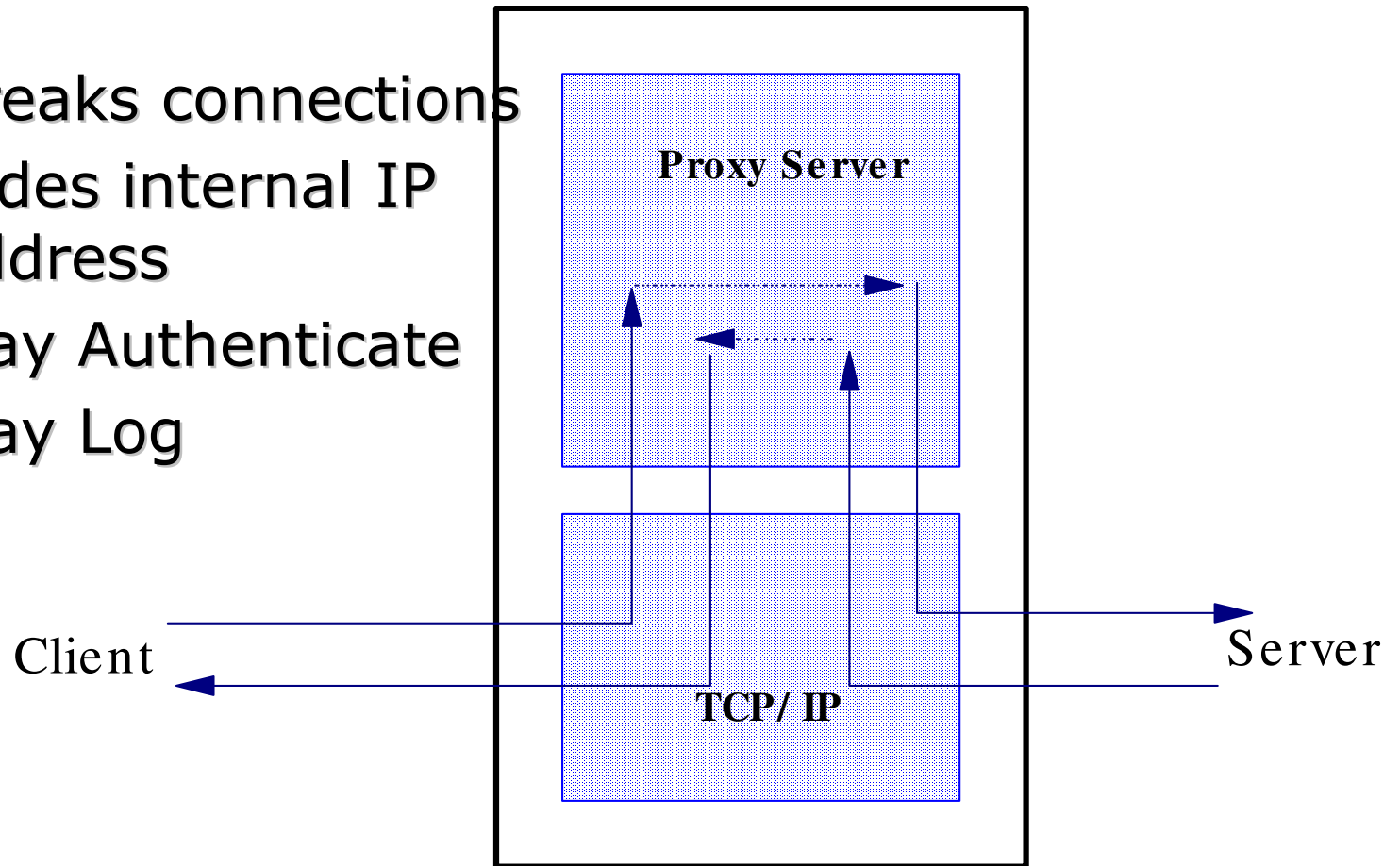
What is required for a secured Internet connection?

- Proxy,SOCKS or NAT
- Filtering
- Logging
- Reporting
- Virus Protection
- Authentication
- Encryption



Proxy Server

- Breaks connections
- Hides internal IP address
- May Authenticate
- May Log

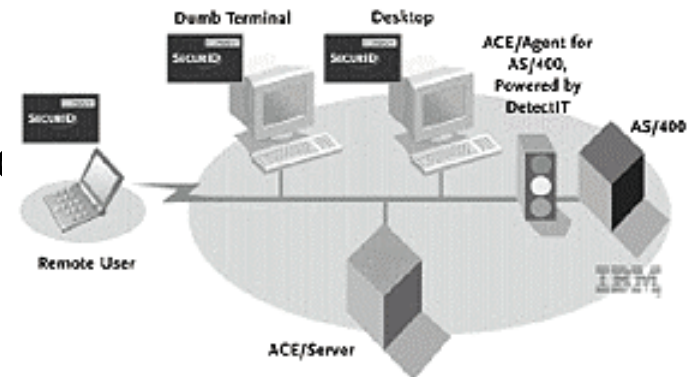




B E R B E E®

Authentication

- Who is it?
 - How can you be sure that the person signing on is the person you expect.
- Digital Certificates
 - Sounds good but?
- Authentication Server
 - Very strong if you can afford it



<http://www.securitydynamics.com/products/datasheets/as400.html>



Virus Protection

Prevent and Control Viruses

We'll give you the good news first. The good news is that AS/400 object-based architecture makes it technically unlikely that a virus will harm your AS/400. The bad news is that AS/400 object-based architecture doesn't prevent viruses from spreading among connected PCs on your network. To prevent and control viruses:

1. [Control Creation of New Objects](#)
2. [Creation Control Authority to Root Directory](#)
3. [Install and Run Virus Scan Software](#)
4. [Stage Movement of New Objects Using Temporary Folder](#)
5. [Educate Your Users about Viruses and Software](#)

For more information on controlling viruses, check out the [IBM Antivirus](#) Web site.

http://www.as400.ibm.com/tstudio/secure1/Sdex_fr.htm

http://www.symantec.com/nav/fs_nav5-95nt.html

<http://www.mcafee.com/>



Encryption

- **iSeries supports SSL, which allows all iSeries task to be encrypted.**
- **iSeries can be a VPN Server**
- **VPN be careful (At least 2 Definitions)**
 - Your firewall (IPSEC)
 - A private wide area network



B E R B E E®

Other Resources

Tips and Tools for Securing Your iSeries SC41-5300-06

Managing OS/400 with Operations Navigator V5R1 Volume 2: Security SG24-6227

iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168

AS/400 Internet Security Scenarios: A Practical Approach SG24-5954 (somewhat dated)

<http://www.woevans.com/>

Berbee...putting the  in business®