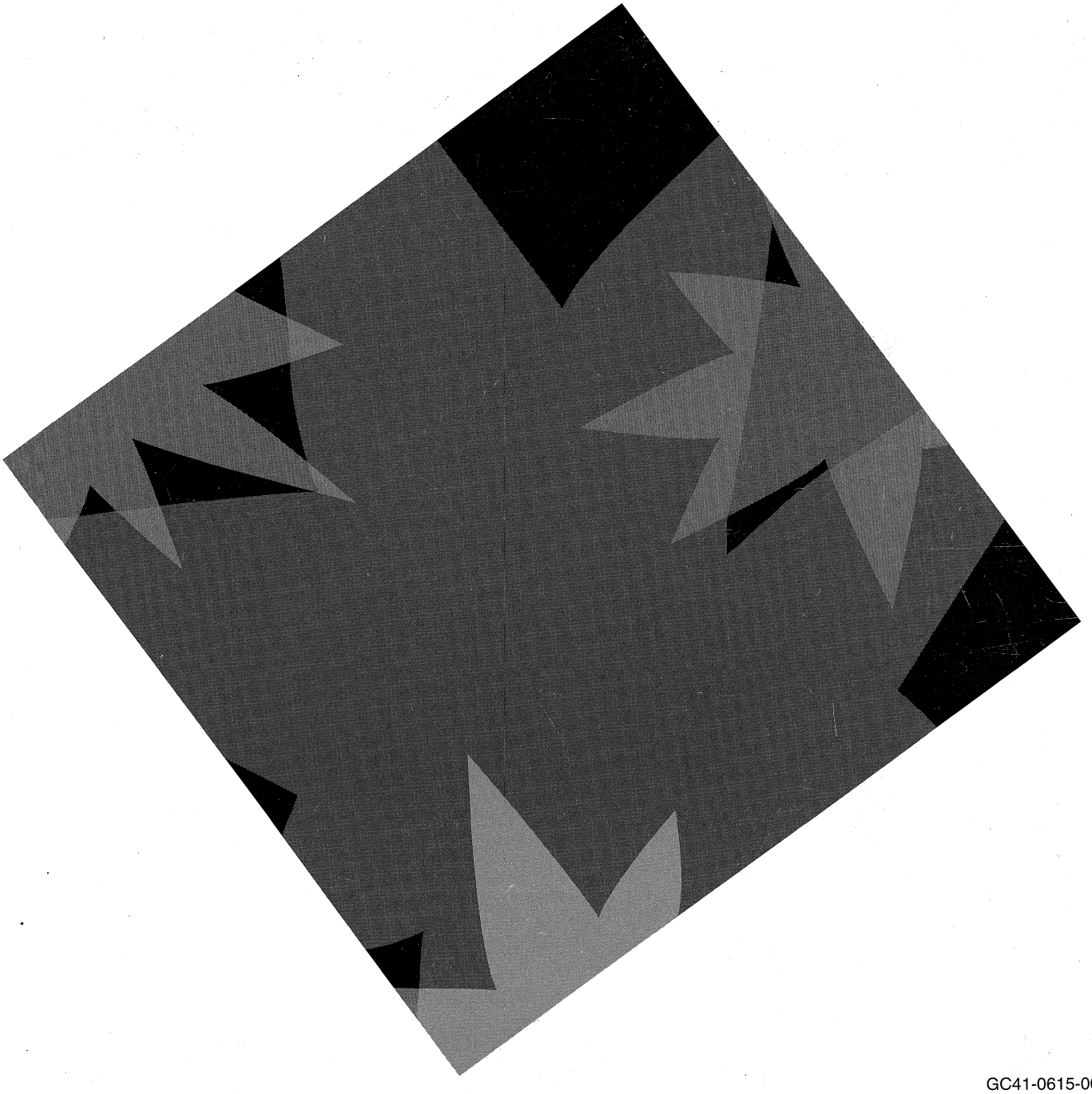
AS/400 Advanced Series

IBM

Tips and Tools for Securing Your AS/400



GC41-0615-00

AS/400 Advanced Series

Tips and Tools for Securing Your AS/400

GC41-0615-00

Take Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page xiii.

First Edition (February 1996)

This edition applies to the following licensed programs:

- IBM Operating System/400 (5738-SS1) Version 2 Release 3
- IBM Operating System/400 (5763-SS1) Version 3 Release 0 Modification 5
- IBM Operating System/400 (5763-SS1) Version 3 Release 1
- IBM Operating System/400 (5763-SS1) Version 3 Release 6
- Security ToolKit for OS/400 (5799-XDH)
- Security ToolKit for OS/400 (5799-XDJ)
- Security ToolKit for OS/400 (5799-XDK)

and to all subsequent releases and modifications until otherwise indicated in new editions. Make sure you are using the proper edition for the level of the product.

Order publications through your IBM representative or the IBM branch serving your locality. If you live in the United States, Puerto Rico, or Guam, you can order publications through the IBM Software Manufacturing Solutions at 800+879-2755. Publications are not stocked at the address given below.

A form for reader comments is provided at the back of this publication. If the form has been removed, you can mail your comments to:

Attn Department 542
IDCLERK
IBM Corporation
3605 Highway 52 N
Rochester, MN 55901-9986 USA

or you can fax your comments to:

United States and Canada: 800+937-3430
Other countries: (+1)+507+253-5192

If you have access to Internet, you can send your comments electronically to IDCLERK@RCHVMW2.VNET.IBM.COM; IBMMAIL, to IBMMAIL(USIB56RZ).

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you or restricting your use of it.

About Tips and Tools for Securing Your AS/400

The rapidly changing role of computers in organizations is causing IS managers, software providers, security administrators, and auditors to take a new look at many areas that they have taken for granted in the past. AS/400 security should be on that list.

Systems are providing many new functions that are vastly different from traditional accounting applications. Users are entering systems in new ways: LANs, switched lines (dial-up), wireless, networks of all types. Often, users never see a sign-on display. Many organizations are expanding to become an "extended enterprise," either with proprietary networks or with the Internet.

Suddenly, systems seem to have a whole new set of doors and windows. IS managers and security administrators are justifiably concerned about how to protect information assets in this rapidly changing environment.

This booklet provides a set of practical suggestions for using the security features of AS/400 and for establishing security-conscious operating procedures. It provides a set of recommendations for an installation with average security requirements and exposures. This booklet does not provide a complete description of the available AS/400 security features. If you want to read about additional options or you need more complete background information, consult the publications that are described in "Related Publications" on page H-1.

This booklet also describes how to install and use the Security ToolKit for OS/400. Many of the recommendations in this booklet assume that you have the Security ToolKit for OS/400 and the security PTF (program temporary fix) package. If you do not have them on your system, you should order and install them. Chapter 10 of this booklet describes how to order and install the Security ToolKit and the security PTF package.

What You Should Know Before You Begin

A **security officer** or **security administrator** is responsible for the security on a system. That responsibility usually includes the following tasks:

- Setting up and managing user profiles
- Setting system-wide values that affect security
- Administering the authority to objects
- Enforcing and monitoring the security policies

If you are responsible for security administration for one or more AS/400 systems, this booklet is for you. The instructions in this booklet assume the following:

- You are familiar with AS/400 basic operating procedures, such as signing on and using commands.
- You are familiar with the basic elements of AS/400 security: security levels, security system values, user profiles, and object security. Chapter 1 provides a review of these elements. But if these basic elements are new to you, you should read the *Security – Basic* book before you use this booklet.

- You have activated security on your system by setting the security level (QSECURITY) system value to at least 30.

IBM continually enhances the security capabilities of AS/400. To take advantage of these enhancements, you should regularly evaluate the cumulative PTF package that is currently available for your release to see if it contains PTFs that are relevant to security.

If you have not already done so, consider upgrading to Version 3 Release 1 or Version 3 Release 6 of the OS/400 licensed program. These releases offer several significant security enhancements that are described in Appendix B.

How to Use This booklet

If you have the Security ToolKit for OS/400 software but you have not yet installed it, do the following:

1. Start with Chapter 10 of this booklet. It describes how to install the Security ToolKit and how to get started with it.
2. Briefly review Chapter 11 to learn about the Security ToolKit commands and menus.
3. Then begin reading this booklet starting with Chapter 1. It provides many AS/400 security tips, including suggestions for using the commands and menus that are part of the Security ToolKit.

If you do not have the Security ToolKit, start reading with Chapter 1 and read the chapters that apply to your situation.

You may need to refer to other IBM books for more specific information about a particular topic. "Where to Get More Information and Assistance" on page H-1 provides information about related publications. The *Publications Reference* provides information on all the books in the AS/400 library.

If you have V3R6, the *Publications Reference* is available in the Softcopy Library. If you have V3R6, you can also use the *AS/400 Information Directory*, a unique, multimedia interface to a searchable database containing descriptions of titles available from IBM or from selected other publishers. The *AS/400 Information Directory* is shipped with your system at no charge.

Contents

Tips for Locking Your System's Doors and Windows

Tips for Protecting AS/400 from Curious or Careless Users

Tips for Protecting AS/400 from Devious or Determined Users

Security Tools

Additional Information

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594, U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact the software interoperability coordinator. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Address your questions to:

IBM Corporation
Software Interoperability Coordinator
3605 Highway 52 N
Rochester, MN 55901-9986 USA

This publication could contain technical inaccuracies or typographical errors.

This publication may refer to products that are announced but not currently available in your country. This publication may also refer to products that have not been announced in your country. IBM makes no commitment to make available any unannounced products referred to herein. The final decision to announce any product is based on IBM's business and technical judgment.

This publication contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this book softcopy, the illustrations do not appear in all environments.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

ADSM/400
Application System/400
APPN
AS/400
CT
IBM
Operating System/400
OS/2
OS/400
QMF
Ultimedia
400

Windows is a trademark of Microsoft Corporation.

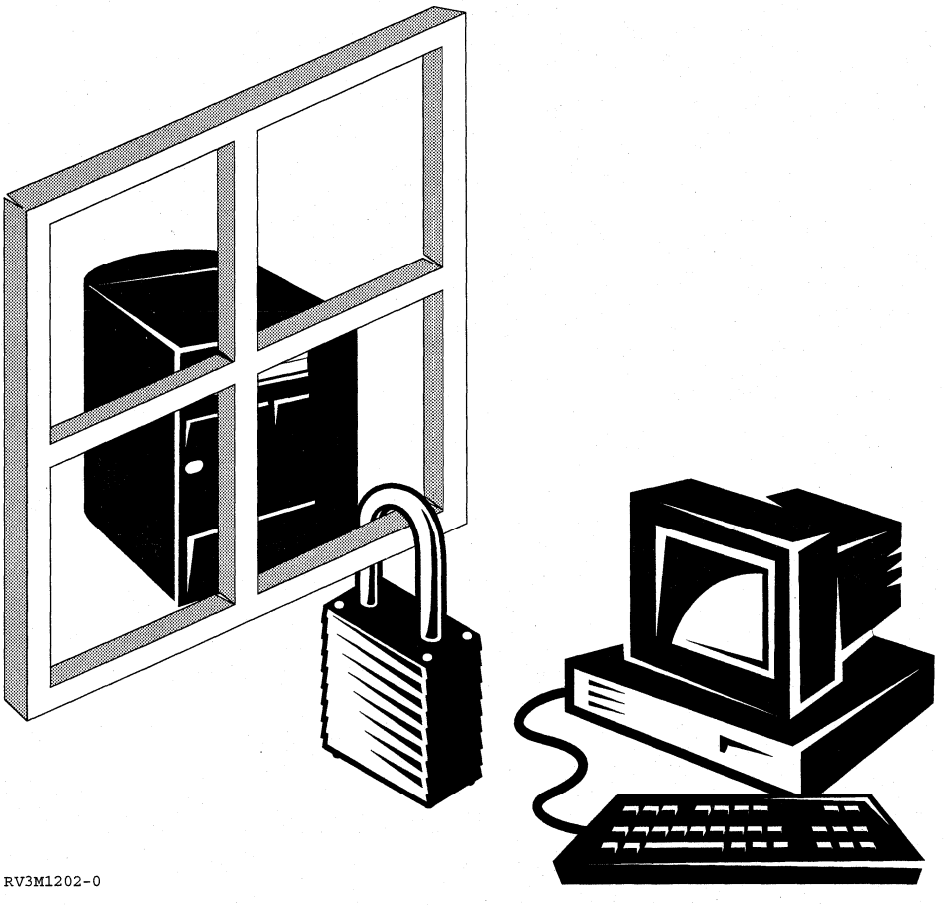
UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Tips for Locking Your System's Doors and Windows

By the pricking of my thumbs,
Something wicked this way comes.
Open, locks,
Whoever knocks!
Shakespeare: Macbeth

You probably do not want to fling open the doors of your system to anyone who comes knocking. On the contrary, your first step toward a secure system is to make sure that unauthorized people cannot enter your system. This part of the booklet provides tips for controlling who can enter your system. Some of the doors into your system may surprise you.



RV3M1202-0

Chapter 1. Basic Elements of AS/400 Security

This chapter provides a brief review of the basic elements that work together to provide AS/400 security. Each topic in this chapter tells where you can find out more information. The other chapters of this booklet go beyond the basics to provide tips for using these security elements to meet the needs of your organization.

Security Levels

You can choose how much security you want the system to enforce by setting the security level (QSECURITY) system value. The system offers five levels of security:

Level 10: The system does not enforce any security. No password is necessary. If the specified user profile does not exist on the system when someone signs on, the system creates one. Security level 10 is available primarily for compatibility with System/36. The system ships with security level 10.

Level 20: The system requires a user ID and password for signing on. Security level 20 is often referred to as **sign-on security**. By default, all users have access to all objects because all users have *ALLOBJ special authority.

Level 30: The system requires a user ID and password for signing on. Users must have authority to use objects because users do not have any authority by default. This is called **resource security**.

Level 40: The system requires a user ID and password for signing on. In addition to resource security, the system provides **integrity protection** functions. The integrity protection functions are intended to protect your system and the objects on your system from tampering by experienced system users. For most installations, level 40 is the recommended security level.

Level 50: The system requires a user ID and password for signing on. The security of resources is enforced. Level 40 integrity protection is enforced. Security level 50 adds enhanced integrity protection, such as the validation of parameters for interfaces to the operating system and the restriction of message-handling between system state programs and user state programs. Security level 50 is intended for AS/400 systems with high security requirements.

Chapter 2 of the *Security – Reference* provides more information about the security levels and how to move from one security level to another.

Global Settings

Your system has global settings that affect how work enters the system and how the system appears to system users. These settings include the following:

System values
Several topics in this booklet discuss the security implications of specific system values. Chapter 3 in the *Security – Reference* book describes all the security-relevant system values.

Network attributes
Network attributes control how your system participates (or chooses not to participate) in a network with other systems. You can read more about network attributes in the *Work Management* book.

Subsystem descriptions and other work management elements
Work management elements determine how work enters the system and what environment the work runs in. Several topics in this booklet discuss the security implications of some work management values. The *Work Management* book provides complete information.

Communications configuration
Your communications configuration also affects how work enters your system. Several topics in this booklet provide suggestions for protecting your system when it participates in a network. The topic "Related Publications" on page H-1 describes where you can read more about specific communications methods.

User Profiles

Every system user has a user profile. At security level 10, the system automatically creates a profile when a user first signs on. At higher security levels, you must create a user profile before a user can sign on.

The user profile is a powerful and flexible tool. It controls what the user can do and customizes the way the system appears to the user. Chapter 4 in the *Security – Reference* book describes all the parameters in the user profile.

Group Profiles

A group profile is a special type of user profile. You can use a group profile to define authority for a group of users, rather than giving authority to each user individually. You can also use a group profile as a pattern when you create individual user profiles by using the copy-profile function.

Chapter 5 and Chapter 7 in the *Security – Reference* book provide more information about planning and using group profiles.

Resource Security

Resource security on the system allows you to define who can use objects and how those objects can be used. The ability to access an object is called **authority**. When you set up object authority, you can specify detailed authorities, such as adding records or changing records. Or you can specify the system-defined subsets of authorities: *ALL, *CHANGE, *USE, and *EXCLUDE.

Files, programs, and libraries are the most common objects that require security protection, but you can specify authority for any object on the system.

Chapter 6, "Using Object Authority to Protect Information Assets" discusses the importance of setting up object authority on your system. Chapter 5 of the *Security – Reference* book describes the options for setting up resource security.

Security Auditing

Several functions exist on the system to help you audit the effectiveness of security. In particular, the system provides the ability to log selected security-related events in a security audit journal. Several system values, user profile values, and object values control which events are logged.

Chapter 9 of the *Security – Reference* book provides information about auditing security.

C2 Security

By using security level 50 and following the instructions in the *Guide to Enabling C2 Security* book, you can bring your AS/400 system to a C2 level of security. C2 is a security standard defined by the U.S. government in the *Department of Defense Trusted System Evaluation Criteria* (DoD 5200.28.STD).

In October, 1995, AS/400 formally received a C2 security rating from the United States Department of Defense. The C2 rating is for V2R3 of OS/400, Source Entry Utility, Query/400, SAA Structured Query Language/400, and Common Cryptographic Architecture Services/400. The C2 rating was awarded after a rigorous, multi-year period of evaluation. AS/400 is the first system to achieve a C2 rating for a system (hardware and operating system) with an integrated, full-function database. IBM is currently pursuing C2 ratings for additional hardware and releases of the operating system. Subsequent evaluations of a system are normally much faster than the first C2 evaluation.

To achieve a C2 rating, a system must meet strict criteria in the following areas:

- Discretionary access control
- User accountability
- Security auditing
- Resource isolation

Chapter 2. Tips for Controlling Interactive Sign-On

When you think about restricting entry to your system, start with the obvious, the Sign On display. Following are steps that you can take to make it difficult for an outsider to walk up (or dial up) and sign on to your system by using the Sign On display.

Setting Password Rules

Set a policy stating that passwords must not be trivial and must not be shared. Set system values to help you with enforcement. Table 2-1 shows recommended system value settings.

The combination of values in Table 2-1 is fairly restrictive and is intended to significantly reduce the likelihood of trivial passwords. However, your users may find it difficult and frustrating to select a password that meets these restrictions. Consider providing users with a list of the criteria, examples of passwords that are and are not valid, and suggestions for how to think of a good password.

If you have the Security ToolKit, you can run the Configure System Security (CFGSYSSEC) command to set these values (except the QPWDRQDDIF system value). You can use the Print System Security Attributes (PRTSYSSECA) command to print your current settings for these system values.

You can read more about these system values in Chapter 3 of the *Security – Reference*. "Values That Are Set by the Configure System Security Command" on page 11-11 provides more information about the CFGSYSSEC command.

Table 2-1 (Page 1 of 2). System Values for Passwords

System Value Name	Description	Recommended Value
QPWDEXPITV	How often the system users must change their passwords. You can specify a different value for individual users in the user profile.	60 (days)
QPWDMINLEN	The minimum number of characters in a password.	6
QPWDMAXLEN	The maximum number of characters in a password.	8
QPWDRQDDIF	How long a user must wait before using the same password again.	5 or less (expiration intervals)[1]
QPWDLMTCHR	What characters may not be used in passwords.	AEIOU#$@
QPWDLMTAJC	Whether the system prevents adjacent characters that are the same.	1 (yes)
QPWDLMTREP	Whether the system prevents the same character from appearing more than once in the password.	2 (not allowed consecutively)[2]
QPWDPOSDIF	Whether each character in a password must be different from the character in the same position on the previous password.	1 (yes)

Table 2-1 (Page 2 of 2). System Values for Passwords

System Value Name	Description	Recommended Value
QPWDRQDDGT	Whether the password must have at least one numeric character.	1 (yes)
QPWDVLDPGM	Whether an exit program is called to validate a newly assigned password.	*NONE

1 The QPWDEXPITV system value specifies how often you must change your password, such as every 60 days. This is the **expiration interval**. The QPWDRQDDIF system value specifies how many expiration intervals must pass before you can use the same password again. Chapter 3 of the *Security – Reference* book provides more information about how these system values work together.

For releases earlier than V3R1, the only valid settings for the QPWDRQDDIF system value are 0 and 1. Choose 1, which means that 32 expiration intervals must pass before you can reuse a password.

2 A value of 2 is available only for V3R1 and later versions. For earlier versions, choose 1, which means repeating characters are not allowed.

Changing Well-Known Passwords

Do the following to close some well-known entrances into AS/400 that may exist on your system.

__ **Step 1** Make sure that no user profiles still have default passwords (equal to the user profile name). If you have the Security ToolKit, you can use the Check Default Passwords (CHKDFTPWD) command. (See "Avoiding Default Passwords" on page 2-8.)

__ **Step 2** Some IBM-supplied user profiles are shipped with passwords. These passwords are published, and they are the first choice of anyone trying to break into your system. Try to sign on to your system with the user profile and password combinations that are shown in Table 2-2. If you can sign on, use the Change User Profile (CHGUSRPRF) command to change the password to the recommended value.

Table 2-2. Passwords for IBM-Supplied Profiles

User ID	Password	Recommended Value
QSECOFR	QSECOFR	A nontrivial value known only to the security administrators. **Write down the password that you have selected and store it in a safe place.**
QSYSOPR	QSYSOPR	*NONE[1]
QPGMR	QPGMR	*NONE[1]
QUSER	QUSER	*NONE[1]
QSRV	QSRV	*NONE[1]
QSRVBAS	QSRVBAS	*NONE[1]

1 The system needs these user profiles for system functions, but you should not allow users to sign on with these profiles. For new systems installed with V3R1 or later releases, this password is shipped as *NONE.

__ **Step 3** Now start Dedicated Service Tools (DST) and try to sign on with the passwords that are shown in Table 2-3 on page 2-3.

You start DST by using one of the following methods:

- Perform an IPL with the system in `Manual` mode and selecting Dedicated Service Tools from the IPL or Install the System menu.
- Place the console in DST mode by doing the following:
  a. Make sure all jobs at the console are ended.
  b. Place the system unit in manual mode.
  c. Use the system panel to select function 21.
  d. Press the enter button on the system panel.
  e. From the IPL of Install the System menu, select DST.

Table 2-3. Passwords for Dedicated Service Tools

User ID[1]	Password	Recommended Value
11111111	11111111	A nontrivial value known only to the security administrator.[2]
22222222	22222222	A nontrivial value known only to the security administrator.[2]
QSECOFR	QSECOFR	A nontrivial value known only to the security administrator.[2]

1 A user ID is only required for V3R6.

2 If your hardware service representative needs to sign on with this user ID and password, change the password to a new value after the hardware service representative leaves.

__ **Step 4** If you can sign on to DST with any of these passwords, change the passwords by doing the following:

__ **Step a** From the Dedicated Service Tools (DST) menu, select option 5 (Work with DST environment):

__ **Step b** From the Work with DST Environment menu, select option 11 (Change DST Passwords).

Note: The menu option numbers may be different on your system, depending on the release of OS/400 that you are running.

Remember the new passwords

Write down the passwords that you select and store them in a safe place. You or your hardware service representative may need these passwords to work on your system in the future.

__ **Step c** From the Change DST Passwords menu, select option 3 (Change the DST security capability password).

Note: DST full capability has the user ID of QSECOFR. You can change this user ID if you want, but be sure to write down the new user ID.

__ **Step d** On the Change DST Security Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ **Step e** Press the Enter key.

__ **Step f** From the Change DST Passwords menu, select option 2 (Change the DST full capability password).

Note: DST full capability has the user ID of 22222222. You can change this user ID if you want, but be sure to write down the new user ID.

__ **Step g** On the Change DST Full Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ **Step h** Press the Enter key.

__ **Step i** From the Change DST Passwords menu, select option 1 (Change the DST basic capability password).

Note: DST basic capability has the user ID of 11111111. You can change this user ID if you want, but be sure to write down the new user ID.

__ **Step j** On the Change DST Basic Capability Password display, type a new password. You must type the password twice for verification. The password does not display when you type it.

__ **Step k** Press the Enter key.

__ **Step l** Press F3 until you see the Dedicated Service Tools (DST) menu.

__ **Step 5** Finally, make sure that you cannot sign on just by pressing the Enter key at the Sign On display without entering a user ID and password. Try several different displays. If you can sign on without entering information on the Sign On display, do one of the following:

- Change to security level 40 or 50 (QSECURITY system value).
- Change all of the workstation entries for interactive subsystems to point to job descriptions that specify USER(*RQD).

Setting Sign-On Values

Table 2-4 shows several values that you can set to make it more difficult for an unauthorized person to sign on to your system. If you run the CFGSYSSEC command, it sets these system values to the recommended settings. You can read more about these system values in Chapter 3 of the *Security – Reference* book.

Table 2-4. Sign-On System Values

System Value Name	Description	Recommended Setting
QAUTOCFG	Whether the system automatically configures new devices.	0 (No)
QAUTOVRT	The number of virtual device descriptions that the system will automatically create if no device is available for use.	0
QDEVRCYACN[1]	What the system does when a device reconnects after an error.	*DSCMSG
QDSCJOBITV	How long the system waits before ending a disconnected job.	120
QDSPSGNINF	Whether the system displays information about previous sign-on activity when a user signs on.	1 (Yes)
QINACTITV	How long the system waits before taking action when an interactive job is inactive.	60
QINACTMSGQ	What the system does when the QINACTITV time period is reached.	*DSCJOB
QLMTDEVSSN	Whether the system prevents a user from signing on at more than one work station at the same time.	1 (Yes)
QLMTSECOFR	Whether users with *ALLOBJ or *SERVICE special authority can sign on only at specific work stations.	1 (Yes)[2]
QMAXSIGN	Maximum consecutive, incorrect sign-on attempts (user profile or password is incorrect).	3
QMAXSGNACN	What the system does when the QMAXSIGN limit is reached.	3 (Disable both user profile and device)

1 For earlier versions than V3R6, this system value is described in the *Work Management* book.

2 If you set the system value to 1 (Yes), you will need to explicitly authorize users with *ALLOBJ or *SERVICE special authority to devices. The simplest way to do this is to give the QSECOFR user profile *CHANGE authority to specific devices.

Changing Sign-On Error Messages

Hackers like to know when they are making progress toward breaking into a system. When an error message on the Sign On display says `Password not correct`, the hacker can assume that the user ID is correct. You can frustrate the hacker by using the Change Message Description (CHGMSGD) command to change the text for two sign-on error messages. Table 2-5 on page 2-6 shows the recommended text.

Table 2-5. Sign-On Error Messages

Message ID	Shipped Text	Recommended Text
CPF1107	CPF1107 – Password not correct for user profile.	Sign-on information is not correct **Note:** Do not include the message ID in the message text.
CPF1120	CPF1120 – User *XXXXX* does not exist.	Sign-on information is not correct. **Note:** Do not include the message ID in the message text.

Scheduling Availability of User Profiles

You may want some user profiles to be available for sign-on only at certain times of the day or certain days of the week. For example, if you have a profile set up for a security auditor, you may want to enable that user profile only during the hours that the auditor is scheduled to work. You might also want to disable user profiles with *ALLOBJ special authority (including the QSECOFR user profile) during off-hours.

If you have the Security ToolKit, you can use the Schedule Profile Activation (SCDPRFACT) command to set up user profiles to be enabled and disabled automatically. For each user profile that you want to schedule, you create an entry that defines the user profile's schedule.

For example, if you want the QSECOFR profile to be available only between 7 in the morning and 10 in the evening, you would type the following on the SCDPRFACT display:

```
                    Schedule Profile Activation (SCDPRFACT)

Type choices, press Enter.

User profile . . . . . > QSECOFR       Name
Enable time  . . . . . > '7:00'        Time, *NONE
Disable time . . . . . > '22:00'       Time, *NONE
Days . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                               > *TUE
                               > *WED
                               > *THU
               + for more values > *FRI
```

Figure 2-1. Schedule Profile Activation Display–Sample

You can use the Print Audit Record Report (PRTAUDRPT) command periodically to print the CP (Change Profile) audit journal entries. Use these entries to verify that the system is enabling and disabling user profiles according to your planned schedule.

Another method for checking to ensure that user profiles are being disabled on your planned schedule is to use the Print User Profile Information (PRTUSRINF) command. When you specify *PWDINFO for the report type, the report includes the status of each selected user profile. If, for example, you regularly disable all

user profiles with *ALLOBJ special authority, you can schedule the following command to run immediately after the profiles are disabled:

```
PRTUSRINF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Removing Inactive User Profiles

Your system should contain only user profiles that are necessary. If you no longer need a user profile because the user either has left or has taken a different job within the organization, remove the user profile. If someone is gone from the organization for an extended period, disable (deactivate) that user's profile. An unnecessary user profile may provide unauthorized entry to your system.

Disabling User Profiles Automatically

If you have the Security ToolKit, you can use the Process Inactive Profiles (PRCINACPRF) command to regularly disable user profiles that have been inactive for a specified number of days. When you use the PRCINACPRF command, you specify the number of inactive days that the system looks for. (The system looks at the last sign-on date for the user profile.)

Once you have specified a value for the PRCINACPRF command, the system schedules a job to run weekly at 1 minute after midnight (starting with the day after you first specified a value). The job examines all profiles and disables inactive profiles. You do not need to use the PRCINACPRF command again unless you want to change the number of inactive days.

You can use the Change Active Profile List (CHGACTPRFL) command to make some profiles exempt from PRCINACPRF processing. The CHGACTPRFL command creates a list of user profiles that the PRCINACPRF command will not disable, no matter how long those profiles have been inactive.

When the PRCINACPRF command runs, the system writes a CP entry in the audit journal for each user profile that is disabled. You can use the PRTAUDRPT command to list the user profiles that are newly disabled.

Note: The system writes audit entries only if the QAUDCTL value specifies *AUDLVL and the QAUDLVL system value specifies *SECURITY.

Another method for checking to ensure that user profiles are being disabled on your planned schedule is to use the Print User Profile Information (PRTUSRINF) command. When you specify *PWDINFO for the report type, the report includes the status of each selected user profile.

Removing User Profiles Automatically

If you have the Security ToolKit, you can use the Schedule Profile Expiration (SCDPRFEXP) command to manage the removing or disabling of user profiles. If you know that a user is leaving for an extended period, you can schedule the user profile to be removed or disabled.

The first time that you use the SCDPRFEXP command, it creates a job schedule entry that runs at 1 minute after midnight every day. The job looks at the QASECEXP file to determine whether any user profiles are scheduled for removal on that day.

With the SCDPRFEXP command, you either disable or delete a user profile. If you choose to delete a user profile, you must specify what the system will do with the objects that the user owns. Before you schedule a user profile for deletion, you need to research the objects that are owned by the user. For example, if the user owns programs that adopt authority, do you want those programs to adopt the ownership of the new owner? Or does the new owner have too much authority?

You also need to research whether deleting the user profile will cause any problems with applications. For example, is the user profile specified as the default user in any job descriptions?

You can use the Display Expiration Schedule (DSPEXPSCD) command to display the list of profiles that are scheduled to be disabled or removed.

If you do not have the Security ToolKit, you can use the Display Authorized Users (DSPAUTUSR) command to list all of the user profiles on your system. Use the Delete User Profile (DLTUSRPRF) command to delete outdated profiles.

Security Note

You disable a user profile by setting its status to *DISABLED. When you disable a user profile, you make it unavailable for interactive use. You cannot sign on with or change your job to a disabled user profile. Batch jobs can run under a user profile that is disabled.

Avoiding Default Passwords

When you create a new user profile, the default is to set the password equal to the user profile name. This provides an opportunity for someone to enter your system, if someone knows your policy for assigning profile names and knows that a new person is joining your organization.

When you create new user profiles, consider assigning a unique, non-trivial password instead of using the default password. Tell the new user the password confidentially, such as in a "Welcome to the System" letter that outlines your security policies. Require the user to change the password the first time that the user signs on by setting the user profile to PWDEXP(*YES).

If you have the Security ToolKit, you can use the Check Default Passwords (CHKDFTPWD) command to check all the user profiles on your system for default passwords. When you print the report, you have the option of specifying that the system should take action (such as disabling the user profile) if the password is the same as the user profile name. The CHKDFTPWD command prints a list of the profiles that it found and any action that it took.

Note: Passwords are stored on your system in one-way encrypted form. They cannot be decrypted. The system checks for a default password by encrypting the user profile name and comparing it to the password, just as it would check a password when you sign on the system.

Monitoring Sign-On and Password Activity

If you are concerned about unauthorized attempts to enter your system, you can use the PRTUSRINF command to help you monitor sign-on and password activity. Figure 2-2 shows an example of the report:

```
                                   User Profile Information
5799XDJ V3R1M0  960115                                                        SYSTEM4
 Report type  . . . . . . . . . . :  *PWDINFO
 Select by  . . . . . . . . . . . :  *SPCAUT
 Special authorities  . . . . . . :  *ALLOBJ     *SERVICE
 QPWDEXPITV system value  . . . . :       60
 User                          Not Valid         No       Previous     Password     Expiration     Password
 Profile        Status         Sign-ons        Password    Sign-on      Changed       Interval      Expired
 USERA          *DISABLED             1                   07/19/95     05/25/95      *SYSVAL         *YES
 USERB          *ENABLED              2                   06/30/95     03/02/95      *SYSVAL         *YES
 USERX          *DISABLED             0          X          / /        11/28/95      *SYSVAL         *NO
 USERY          *ENABLED              0                   04/25/95     04/25/95      120             *YES
```

Figure 2-2. User Information Report–Password Information Example

Following are several suggestions for using this report:

- Determine whether the password expiration interval for some user profiles is longer than the system value and whether the longer expiration interval is justified. For example, in the report, USERY has a password expiration interval of 120 days.
- Run this report regularly to monitor unsuccessful sign-on attempts. Someone who is trying to break into your system may be aware that your system takes action after a certain number of unsuccessful attempts. Each night, the would-be intruder might try fewer times than your QMAXSIGN value to avoid alerting you to the attempts. However, if you run this report early each morning and notice that certain profiles often have unsuccessful sign-on attempts, you might suspect that you have a problem.
- Identify user profiles that have not been used for a long time or whose passwords have not been changed for a long time.

Chapter 3. Tips for Securing APPC Communications

When your system participates in a network with other systems, a new set of doors and windows to your system becomes available. As security administrator, you should be aware of the options that you can use to control the entrances to your system in an APPC environment.

APPC is a common way that computers, including personal computers, communicate with each other. Display station pass-through, distributed data management, and Client Access for OS/400 all use APPC communications.

The topics that follow provide some basic information about how APPC communications works and how you can set up appropriate security. These topics concentrate primarily on the security-relevant elements of an APPC configuration. To adapt this example to your situation, you will need to work with the people who manage your communications network and perhaps your application providers. Use this information as a foundation to help you understand the security issues and the options that are available for APPC.

Security is never "free." Some suggestions for making network security easier may make network administration more difficult. For example, this booklet does not emphasize APPN, because security is easier to understand and manage without APPN. However, without APPN, the network administrator must manually create configuration information that APPN creates automatically.

APPC Terminology

APPC provides the ability for a user on one system to perform work on another system. The system from which the request initiates is called any of the following:

Source system
Local system
Client

The system that receives the request is called any of the following:

Target system
Remote system
Server

Basic Elements of APPC Communications

From the perspective of a security administrator, the following must happen before a user on one system (SYSTEMA) can perform meaningful work on another system (SYSTEMB):

- The source system (SYSTEMA) must provide a path to the target system (SYSTEMB). This path is called an **APPC session**.
- The target system must identify the user and associate the user with a user profile.
- The target system must start a job for the user with an appropriate environment (work management values).

The topics that follow discuss these elements and how they relate to security. The security administrator on the target system has primary responsibility for ensuring that APPC users do not violate security. However, when the security administrators on both systems work together, the job of managing APPC security is much easier.

The Basics of an APPC Session

In an APPC environment, when a user or application on one system (such as SYSTEMA in Figure 3-1) requests access to another system (SYSTEMB), the two systems set up a session. To establish the session, the systems must link two matching APPC device descriptions. The remote location name (RMTLOCNAME) parameter in the SYSTEMA device description must match the local location name (LCLLOCNAME) parameter in the SYSTEMB device description and vice versa

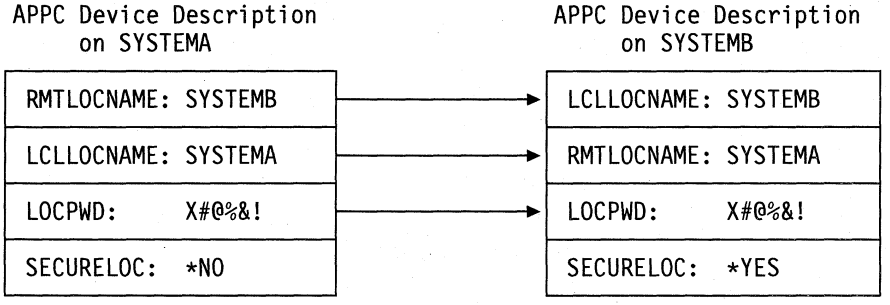


Figure 3-1. APPC Device Description Parameters

For the two systems to establish an APPC session, the location passwords in the APPC device descriptions on SYSTEMA and SYSTEMB must be identical. Both must specify *NONE, or both must specify the same value.

If the passwords are a value other than *NONE, they are stored and transmitted in encrypted format. If the passwords match, the systems establish a session. If the passwords do not match, the user's request is rejected. When systems specify location passwords to establish a session, this is called a **secure bind**.

Note: Not all computer systems provide support for the secure bind function.

Tips for Restricting APPC Sessions

As security administrator on a source system, you can use authority to APPC devices to control who can attempt to access other systems. Set the public authority for APPC device descriptions to *EXCLUDE and give *CHANGE authority to specific users. Use the QLMTSECOFR to prevent users with *ALLOBJ special authority from using APPC communications.

As security administrator on a target system, you can also use authority to APPC devices to prevent users from starting an APPC session on your system. However, you need to understand what user ID will be attempting access. "How an APPC User Gains Entrance to the Target System" on page 3-3 describes how AS/400 associates a user ID with a request for an APPC session.

Note: If you have the Security ToolKit, you can use the Print Publicly Authorized Objects (PRTPUBAUT *DEVD) command and the Print Private Authorities (PRTPVTAUT *DEVD) command to find out who has authority to device descriptions on your system.

When your system uses APPN, it automatically creates a new APPC device when no existing device is available for the route that the system has chosen. One method for restricting access to APPC devices on a system that is using APPN is to create an authorization list. The authorization list contains the list of users who should be authorization to APPC devices. You then use the Change Command Default (CHGCMDDFT) command to change the CRTDEVAPPC command. For the authority (AUT) parameter on the CRTDEVAPPC command, set the default value to the authorization list that you created.

Note: If your system has a language other than English, you need to change the command default in the QSYSxxxx library for each national language that is on your system.

You use the location password (LOCPWD) parameter in the APPC device description to validate the identity of another system that is requesting a session on your system (on behalf of a user or an application). The location password can help you detect an imposter system.

When you use location passwords, you must coordinate with security administrators for other systems in the network. You must also control who can create or change APPC device descriptions and configuration lists. For systems with V3R1 or later, you must have *IOSYSCFG special authority to use the commands that work with APPC devices and configuration lists. For earlier releases, the system sets the public authority for the commands to *EXCLUDE when you install the security PTF package.

Notes:

1. Security for APPC device description commands and configuration list commands is part of the security PTF package. Beginning with V3R1, your system enforces the requirements for *IOSYSCFG only if you have installed the security PTF package.
2. When you use APPN, the location passwords are stored in the QAPPNRMT configuration list rather than in device descriptions.

How an APPC User Gains Entrance to the Target System

When the systems establish the APPC session, they create a path for the requesting user to get to the door of the other system. Several other elements determine what the user must do to gain entrance to the other system.

The topics that follow describe the elements that determine how an APPC user gains entrance to the target system.

Methods That the System Uses to Send Information about a User

APPC architecture provides three methods for sending security information about a user from the source system to the target system. These methods are referred to as the **architected security values**. Table 3-1 on page 3-4 shows these methods:

Note: The *APPC Programming* book provides more information about the architected security values.

Table 3-1. Security Values in the APPC Architecture

Architected Security Value	User ID Sent to Target System	Password Sent to Target System
None	No	No
Same	Yes[1]	No[2]
Program	Yes	Yes[3]

1 The source system sends the user ID if the target system specifies SECURELOC(*YES).

2 The password is already verified by the source system.

3 On V3R1 and later versions, the system sends the password in encrypted form if both the source and target systems support password encryption. Otherwise, the password is not encrypted.

The application that the user requests determines the architected security value. For example, SNADS always uses SECURITY(NONE). DDM uses SECURITY(SAME). With display station pass-through, the user specifies the security value by using parameters on the STRPASTHR command.

In all cases, the target system chooses whether to accept a request with the security value that is specified on the source system. In some situations, the target system may reject the request completely. In other situations, the target system may force a different security value. For example, when a user specifies both a user ID and a password on the STRPASTHR command, the request uses SECURITY(PGM). However, if the QRMTSIGN system value is *FRCSIGNON on the target system, the user still sees a Sign On display. With the *FRCSIGNON setting, the systems always use SECURITY(NONE), which is the equivalent of the user entering no user ID and password on the STRPASTHR command.

Note: The source and target systems negotiate the security value before data is sent. In the situation where the target system specifies SECURELOC(*NO) and the request is SECURITY(SAME), for example, the target system tells the source system to use SECURITY(NONE). The source system does not send the user ID.

Options for Dividing Security Responsibility in a Network

When your system participates in a network with other systems, you must decide whether to trust the other systems to validate the identity of a user who is trying to enter your system. Will you trust SYSTEMA to ensure that USERA is really USERA (or QSECOFR is really QSECOFR)? Or will you require a user to provide a user ID and password again?

The secure location (SECURELOC) parameter on the APPC device description on the target system specifies whether the source system is a secure (trusted) location. For example, in Figure 3-1 on page 3-2, SYSTEMB trusts SYSTEMA to validate user identities (the SECURELOC parameter in the device description on SYSTEMB is *YES). SYSTEMA does not trust SYSTEMB to validate user identities.

Table 3-2 on page 3-5 shows how the architected security value and the SECURELOC value work together:

Table 3-2. How the APPC Security Value and the SECURELOC Value Work Together		
Source System	**Target System**	
Architected Security Value	**SECURELOC Value**	**User Profile for Job**
None	*NO	Default user[1]
	*YES	
Same	*NO	Default user[1]
Same	*YES	Same user profile name as requester from source system
Program	*NO	The user profile that is specified on the request from the source system.
	*YES	
1 The default user is determined by the communications entry in the subsystem description. "How the Target System Assigns a User Profile for the Job" describes this.		

How the Target System Assigns a User Profile for the Job

When a user requests an APPC job on another system, the request has a mode name associated with it. The mode name may come from the user's request or it may be a default value from the network attributes of the source system.

The target system uses the mode name and the APPC device name to determine how the job will run. It searches the active subsystems for a communications entry that is the best match for the APPC device name and the mode name.

The communications entry specifies what user profile the system will use for SECURITY(NONE) requests. Following is an example of a communications entry in a subsystem description:

```
                        Display Communications Entries

Subsystem description:   QCMN            Status:   ACTIVE

                              Job                          Default        Max
Device        Mode        Description    Library          User          Active
*ALL          *ANY        *USRPRF                         *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                         *NONE         *NOMAX
```

Table 3-3 on page 3-6 shows the possible values for the default user parameter in a communications entry:

Table 3-3. Possible Values for the Default User Parameter

Value	Result
***NONE**	No default user is available. If the source system does not supply a user ID on the request, the job will not run.
***SYS**	Only IBM-supplied programs (system jobs) will run. No user applications will run.
user-name	If the source system does not send a user ID, the job runs under this user profile.

If you have the Security ToolKit, you can use the Print Subsystem Description (PRTSBSDAUT) command to print a list of all subsystems that have communications entries with a default user profile.

Options for Display Station Pass-Through

Display station pass-through is an example of an application that uses APPC communications. You can use display station pass-through to sign on to another system that is connected to your system through a network.

Table 3-4 on page 3-7 shows examples of pass-through requests (STRPASTHR command) and how the target system handles them. For display station pass-through, the system uses the basic elements of APPC communications and the remote sign-on (QRMTSIGN) system value.

Table 3-4. Sample Pass-Through Sign-On Requests

Values on STRPASTHR Command		Target System		
User ID	**Password**	**SECURELOC Value**	**QRMTSIGN Value**	**Result**
*NONE	*NONE	Any	Any	The user must sign on the target system.
*CURRENT or a user profile name	Not entered	*NO	Any	The user must sign on the target system
		*YES	*SAMEPRF	An interactive job starts with the same user profile name as the user profile on the source system. No password is passed to the remote system. The user profile name must exist on the target system.
			*VERIFY	The user must sign on the target system.
			*FRCSIGNON	
*CURRENT or a user profile name	Entered	*NO	Any	The user must sign on the target system
		*YES	*SAMEPRF	An interactive job starts with the same user profile name as the user profile on the source system. The password is not sent to the remote system. The user profile name must exist on the target system.
			*VERIFY	An interactive job starts with the same user profile name as the user profile on the source system. The password is sent to the remote system. The user profile name must exist on the target system, and the password must be correct.
			*FRCSIGNON	The user must sign on the target system.

Tips for Avoiding Unexpected Device Assignments

When a failure occurs on an active device, the system attempts to recover. In some circumstances, when the connection is broken, another user can unintentionally reestablish the session that had the failure. For example, assume that USERA powered off a workstation without signing off. USERB could power on the workstation and restart USERA's session without signing on.

To prevent this possibility, set the Device I/O Error Action (QDEVRCYACN) system value to *DSCJOB. When a device fails, the system will end the user's job.

Tips for Controlling Remote Commands and Batch Jobs

Several options are available to help you control what remote commands and jobs can run on your system, including the following:

- If your system uses DDM, you can restrict access to DDM files to prevent users from using the Submit Remote Command (SBMRMTCMD) command from another system. To use the SBMRMTCMD, the user must be able to open a DDM file. You also need to restrict the ability to create DDM files.
- You can specify an exit program for the DDM request access (DDMACC) system value. In the exit program, you can evaluate all DDM requests before allowing them.
- You can use the network job action (JOBACN) network attribute to prevent network jobs from being submitted or to prevent them from running automatically.
- You can specify explicitly which program requests can run in a communications environment by removing the PGMEVOKE routing entry from subsystem descriptions. The PGMEVOKE routing entry allows the requester to specify the program that runs. When you remove this routing entry from subsystem descriptions, such as the QCMN subsystem description, you must add routing entries for the communications requests that need to run successfully.

  Table A-2 on page A-3 lists the program names for the communications requests by IBM-supplied applications. For each request that you want to allow, you can add a routing entry with the compare value and the program name both equal to the program name.

  When you use this method, you need to understand the work management environment on your system and the types of communications requests that occur on your system. If possible, you should test all types of communications requests to ensure that they work properly after changing the routing entries. When a communications request does not find an available routing entry, you receive a CPF1269 message. If you have the following PTF on your system, the text of the message indicates the name of the program start request:

OS/400 Release	PTF Number
V2R3	SF23809
V3R0M5	SF23808
V3R1	SF23807

  Notes:

  1. You do not need a PTF with V3R6.
  2. The *Work Management* book provides more information about routing entries and how the system handles program-start requests.

Security Tips for Evaluating Your APPC Configuration

If you have the Security ToolKit, you can use the Print Communications Information (PRTCMNINF) command or menu options to print the security-relevant values in your APPC configuration. The topics that follow describe the information on the reports.

Security-Relevant Parameters for APPC Devices

Figure 3-2 shows an example of the Communications Information Report for device descriptions. Figure 3-3 shows an example of the report for configuration lists. Following the reports are explanations of fields on the reports.

```
                          Communications Information (Full Report)
                                                                                SYSTEM4
Object type  . . . . . . . . . :  *DEVD

                                                                                  Pre          SNUF
Object        Object      Device        Secure      Location     APPN      Single     Establish    Program
Name          Type        Category      Location    Password     Capable   Session    Session      Start

CDMDEV1       *DEVD       *APPC         *NO         *NO          *NO       *YES       *NO
CDMDEV2       *DEVD       *APPC         *NO         *NO          *NO       *YES       *NO
```

Figure 3-2. APPC Device Descriptions–Sample Report

```
                    Display Configuration List                              Page     1
5763SS1 V3R1M0  940909                                  SYSTEM4  12/17/95  07:24:36
 Configuration list . . . . . . . . :   QAPPNRMT
 Configuration list type  . . . . . :   *APPNRMT
 Text . . . . . . . . . . . . . . . :
 ----------------APPN Remote Locations------------------
           Remote                Remote    Control
 Remote    Network   Local       Control   Point      Secure
 Location  ID        Location    Point     Net ID      Loc
 SYSTEM36  APPN      SYSTEM4     SYSTEM36  APPN        *NO
 SYSTEM32  APPN      SYSTEM4     SYSTEM32  APPN        *NO
 SYSTEMU   APPN      SYSTEM4     SYSTEM33  APPN        *YES
 SYSTEMJ   APPN      SYSTEM4     SYSTEMJ   APPN        *NO
 SYSTEMR2  APPN      SYSTEM4     SYSTEM1   APPN        *NO
 -------------------------APPN Remote Locations--------------------------
           Remote                                            Local       Pre-
 Remote    Network   Local       Single      Number of       Control   established
 Location  ID        Location    Session   Conversations     Point      Session
 SYSTEM36  APPN      SYSTEM4      *NO             10          *NO         *NO
 SYSTEM32  APPN      SYSTEM4      *NO             10          *NO         *NO
```

Figure 3-3. Configuration List Report–Example

Secure Location Field

The secure location (SECURELOC) field specifies whether the local system trusts the remote system to do password verification on its behalf. The SECURELOC field applies only to applications that use the SECURITY(SAME) value, such as DDM and applications that use the CPI-Communications API.

SECURELOC(*YES) makes the local system vulnerable to possible weaknesses in the remote system. Any user that exists on both systems can call programs on the local system. This is particularly dangerous because the QSECOFR (security officer) user profile exists on all AS/400 systems and has *ALLOBJ special authority. If a system in the network does not do a good job of protecting the QSECOFR password, other systems that treat that system as a secure location are at risk.

If a system specifies SECURELOC(*NO), applications that use SECURITY(SAME) will need a default user to run programs. The default user depends on both the

device description and the mode that are associated with the request. (See "How the Target System Assigns a User Profile for the Job" on page 3-5.)

Location Password Field

The location password field determines whether the two systems will exchange passwords to verify that the requesting system is not an imposter system. "The Basics of an APPC Session" on page 3-2 provides more information about location passwords.

APPN-Capable Field

The APPN-capable (APPN) field specifies whether the remote system can support advanced networking functions or is limited to single-hop connections. APPN(*YES) means the following:

- If the remote system is a network node, the remote system may be capable of connecting the local system to other systems. This is called **intermediate node routing**. It means that users on your system may be able to use the remote system as a route to a larger network.
- If the local system is a network node, the remote system can use the local system to connect to other systems. Users on the remote system may be able to use your system as a route to a larger network.

  Note: You can use the DSPNETA command to determine whether a system is a network node or an end node.

Single Session Field

The single session (SNGSSN) field specifies whether the remote system can run more than one session at a time by using the same APPC device description. SNGSSN(*NO) is commonly used because it eliminates the need to create multiple device descriptions for a remote system. For example, a PC user often wants more than one 5250-emulation session and sessions for file-server and print-server functions. With SNGSSN(*NO), you can provide this function with one device description for the PC on the AS/400 system.

SNGSSN(*NO) means you must rely on the security-conscious operating procedures of PC users and other APPC users. Your system is vulnerable to someone on the remote system starting an unauthorized session that uses the same device description as an existing session. (This practice is sometimes referred to as **piggy-backing**.)

Pre-Establish Session Field

The pre-establish (PREESTSSN) session field for a single-session device controls whether the local system starts a session with the remote system when the remote system first contacts the local system. PREESTSSN(*NO) means that the local system waits to start a session until an application requests a session with the system. PREESTSSN(*YES) is useful for minimizing how long it takes for an application program to complete the connection.

PREESTSSN(*YES) prevents the system from disconnecting a switched (dial-up) line that is no longer being used. The application or user must explicitly vary off the line. This may lengthen the time that the local system is vulnerable to piggy-backing on the session.

SNUF Program Start Field

The SNUF program start field specifies whether the remote system is allowed to start programs on the local system. *YES means the object authority scheme on the local system must be adequate to protect objects when users on the remote system start jobs and run programs on the local system.

Security-Relevant Parameters for APPC Controllers

Figure 3-4 shows an example of the Communications Information Report for controller descriptions. Following the report are explanations of fields on the report.

```
                          Communications Information (Full Report)
                                                                                SYSTEM4
Object type . . . . . . . . . . :   *CTLD

Object    Object    Controller   Auto     Switched     Call       APPN      CP        Disconnect   Delete    Device
Name      Type      Category     Create   Controller   Direction  Capable   Sessions  Timer        Seconds   Name
CTL01     *CTLD     *APPC        *YES     *YES         *DIAL      *YES      *YES            0        1440    AARON
CTL02     *CTLD     *APPC        *YES     *YES         *DIAL      *YES      *YES            0        1440    BASIC
CTL03     *CTLD     *APPC        *YES     *YES         *DIAL      *YES      *YES            0        1440    *NONE
```

Figure 3-4. APPC Controller Descriptions–Sample Report

Auto-Create Field

On a line description, the auto-create (AUTOCRTCTL) field specifies whether the local system automatically creates a controller description when an incoming request cannot find a matching controller description. On a controller description, the auto-create (AUTOCRTDEV) field specifies whether the local system automatically creates a device description when an incoming request cannot find a matching device description.

For controllers that are APPN-capable, the auto-create field has no effect. The system automatically creates device descriptions when necessary, regardless of how you have set the auto-create field.

When you specify *YES for a line description, anyone with access to the line can connect to your system. This includes sites connected by bridges and routers.

Control Point Sessions Field

For APPN-capable controllers, the control point sessions (CPSSN) field controls whether the system establishes an APPC connection with the remote system automatically. The system uses the CP session to exchange network information and status with the remote system. Exchanging up-to-date information is particularly important between APPN network nodes so that your network functions smoothly.

When you specify *YES, an idle switched line does not disconnect automatically. This makes your system more vulnerable to a piggy-back session.

Disconnect Timer Field

For an APPC controller, the disconnect timer field specifies how long a controller must be unused (no active sessions) before the system disconnects the line to the remote system. This field has two values. The first value specifies how long the controller will stay active from the time it is initially contacted. The second value determines how long the system waits after the last session has ended on the controller before dropping the line.

The system uses the disconnect timer only when the switched disconnect (SWTDSC) field is *YES.

If you make these values large, your system is more vulnerable to piggy-back sessions.

Security-Relevant Parameters for Line Descriptions

Figure 3-5 shows an example of the Communications Information Report for line descriptions. Following the report are explanations of fields on the report.

```
                        Communications Information (Full Report)

Object type  . . . . . . . . . :   *LIND

                                                          Auto
 Object         Object         Line           Auto      Delete       Auto      Auto
 Name           Type           Category       Create    Seconds      Answer    Dial
 LINE01          *LIND          *SDLC          *NO             0      *NO       *NO
 LINE02          *LIND          *SDLC          *NO             0      *YES      *NO
 LINE03          *LIND          *SDLC          *NO             0      *NO       *NO
 LINE04          *LIND          *SDLC          *NO             0      *YES      *NO
```

Figure 3-5. APPC Line Descriptions–Sample Report

Auto Answer Field

The auto answer (AUTOANS) field specifies whether the switched line will accept incoming calls without operator intervention.

When you specify *YES, your system is less secure because it can be accessed more easily. To minimize the security exposure when you specify *YES, you should vary off the line when you do not need it.

Auto Dial Field

The auto dial (AUTODIAL) field specifies whether the switched line can make outgoing calls without operator intervention.

When you specify *YES, you allow local users who do not have physical access to communications lines and modems to connect to other systems.

Chapter 4. Tips for Securing TCP/IP Communications

TCP/IP (Transmission Control Protocol/Internet Protocol) is a common way that computers of all types communicate with each other. TCP/IP applications are well-known and widely used throughout the "information highway."

Are you using Version 3?

AS/400 TCP/IP was enhanced significantly in V3R1. This includes performance and security enhancements. If you use TCP/IP on your system, consider upgrading to V3R1 or V3R6 to take advantage of these enhancements.

Following are descriptions of several commonly used TCP/IP servers that are part of the AS/400 TCP/IP function. Other servers are available for use by other applications.

- TELNET provides an interactive session on your system. Your system presents the Sign On display to anyone who attempts to enter your system by using TELNET. TELNET requires a password if your system is running security level 20 or higher.
- FTP (file transfer protocol) provides the capability of transferring files between the client (a user on another system) and the server (your system). You can also use the remote command capability of FTP to submit commands to the server system. FTP requires a user ID and a password.
- SMTP (simple mail transfer protocol) provides the capability to distribute documents to your system. The system does not perform any sign-on processing for SMTP.
- LPD (line printer daemon) provides the capability to distribute printer output to your system. The system does not perform any sign-on processing for LPD.
- A user application that is associated with a TCP/IP port can provide "back-door" entry to your system without a user ID or a password. Someone with sufficient authority on your system can associate an application with a TCP or UDP port.
- AS/400 can act as an agent in a simple network management protocol (SNMP) network. SNMP provides a means for managing the gateways, routers, and hosts in an internet environment. An SNMP agent gathers information about the system and performs functions that are requested by remote SNMP network managers.

This chapter provides tips either for preventing TCP/IP applications from running on your system on your system or for protecting system resources when you allow TCP/IP applications to run on your system.

Tips for Preventing Any TCP/IP Processing

If you do not want your system to be a server for any TCP/IP applications, you can do the following:

- For systems that run V3R0M5 and earlier versions, do not start the QTCP subsystem, which runs TCP/IP and TCP/IP applications. If the QTCP subsystem is not active, no TCP/IP activity can occur on your system.

You must make sure that the subsystem does not start automatically when your system performs an IPL.

You must also make sure that the public authority to the QTCP subsystem description is set to *EXCLUDE to prevent unauthorized users from starting the subsystem with the STRSBS command.

- For systems that are running V3R1 or a later version, TCP/IP runs in the QSYSWRK subsystem. You use the Start TCP/IP (STRTCP) command to start TCP/IP on your system. If you do not want any TCP/IP processing or applications to run, do not use the STRTCP command. Your system ships with the public authority for the STRTCP command set to *EXCLUDE.

  If you suspect that someone with access to the command is starting TCP/IP (during off-hours, for example), you can set up object auditing on the STRTCP command. The system will write an audit journal entry whenever a user runs the command.

Tips for Controlling TCP/IP Applications

On many systems, you want TCP/IP to run but you want to control which TCP/IP applications can run. The topics that follow provide tips for controlling and securing specific TCP/IP applications.

Security Tips for TELNET

If your system runs V3R1 or a later release and you do not want TELNET to run on your system, do the following:

__ **Step 1** To prevent TELNET server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGTELNA AUTOSTART(*NO)
```

__ **Step 2** Make sure that the public authority for the Start TCP/IP Server (STRTCPSVR) command is *EXCLUDE, which is the shipped value. You might also want to use CHGCMDDFT command to change the default value for the STRTCPSVR command. Set the default for the server (SERVER) parameter to include the specific server types that you normally want to start (instead of *ALL).

__ **Step 3** To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for TELNET, do the following:

__ **Step a.** Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ **Step b.** Select option 4 (Work with TCP/IP port restrictions).

__ **Step c.** On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ **Step d.** For the lower port range, specify `23`.

__ **Step e.** For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) The *TCP/IP Configuration and Reference* book lists the well-known TCP/IP ports. RFC1700 provides the latest information about assigned port numbers. The *TCP/IP Configuration and Reference* book describes how to obtain RFCs (Requests for Comment).

__ **Step f.** For the protocol, specify `*TCP`.

__ **Step g.** For the user profile field, specify a user profile name that is protected on your system (not shared or adopted). By restricting the port to a specific user, you automatically exclude all other users.

If your system is running V2R3 and you do not want to allow TELNET, do the following:

__ **Step 1** Make sure that no virtual devices are configured on your system. (This may affect other applications in addition to TELNET, such as display station pass-through.)

__ **Step 2** Make sure that the QAUTOVRT system value is set to 0.

If you want to allow TELNET on your system, be aware of the following security issues:

- TELNET passwords are not encrypted when they are sent between the client and the server. Depending on your connection methods, your system may be vulnerable to password theft through line sniffing.

  Note: Monitoring a line by using electronic equipment is often referred to as **sniffing**.

- Although the QMAXSIGN system value applies to TELNET, you reduce the effectiveness of this system value if you set up your system to configure virtual devices automatically. When the QAUTOVRT system value has a value greater than 0, the unsuccessful TELNET user can reconnect and attach to a newly-created virtual device. This can continue until one of the following occurs:

  - All virtual device are disabled and the system has exceeded the limit for creating new virtual devices.
  - All user profiles are disabled.
  - The hacker succeeds in signing on to your system.

  Automatically configuring virtual devices multiplies the number of TELNET attempts that are available.

  Note: To make it easier to control virtual devices, you might want to set the QAUTOVRT system value to a value that is greater than 0 for a short period of time. Either use TELNET yourself to force the system to create devices or wait until other users have caused the system to

create sufficient virtual devices. Then set the QAUTOVRT system value to 0.

- You can use the QLMTSECOFR system value to restrict users with *ALLOBJ or *SERVICE special authority. The user or QSECOFR must be explicitly authorized to a device to sign on. Thus, you can prevent anyone with *ALLOBJ special authority from using TELNET to access your system by ensuring that QSECOFR does not have authority to any virtual devices.

Security Tips for File Transfer Protocol

If your system runs V3R1 or a later release and you do not want FTP to run on your system, do the following:

__ **Step 1** To prevent FTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGFTPA AUTOSTART(*NO)
```

__ **Step 2** Make sure that the public authority for the Start TCP/IP Server (STRTCPSVR) command is *EXCLUDE, which is the shipped value. You might also want to use CHGCMDDFT command to change the default value for the STRTCPSVR command. Set the default for the server (SERVER) parameter to include the specific server types that you normally want to start (instead of *ALL).

__ **Step 3** To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for FTP, do the following:

__ **Step a.** Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ **Step b.** Select option 4 (Work with TCP/IP port restrictions).

__ **Step c.** On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ **Step d.** For the lower port range, specify `20`.

__ **Step e.** For the upper port range, specify `21`.

Notes:

1) The ability to restrict a range of ports is available beginning with V3R1. For earlier releases, you must specify ports individually.

2) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

3) The *TCP/IP Configuration and Reference* book lists the well-known TCP/IP ports. RFC1700 provides the latest information about assigned port numbers. The *TCP/IP Configuration and Reference* book describes how to obtain RFCs (Requests for Comment).

__ **Step f.** For the protocol, specify `*TCP`.

__ **Step g.** For the user profile field, specify a user profile name that is protected on your system (not shared or adopted). By restricting the port to a specific user, you automatically exclude all other users.

__ **Step h.** Repeat steps 3c through 3g for the *UPD protocol.

Note: This method works only for completely restricting an application such as the FTP server. It does not work for restricting specific users. When a user connects to the FTP server, the request uses the QTCP profile initially. The system changes to the individual user profile after the connection is successful. Every user of the FTP server uses QTCP's authority to the port.

If your system is running V2R3 and you do not want to allow FTP, do the following:

__ **Step 1** After you start the QTCP subsystem, use the End Job (ENDJOB) command to end the FTP server jobs.

If you want to allow FTP on your system, be aware of the following security issues:

- FTP passwords are not encrypted when they are sent between the client system and the server system. Depending on your connection methods, your system may be vulnerable to password theft through line sniffing.
- The QMAXSIGN system value applies to TELNET but not to FTP. With FTP, the system breaks the connection after 5 unsuccessful sign-on attempts, but the user can simply establish a new connection. Theoretically, an FTP user has unlimited attempts to break into your system.

  For each unsuccessful attempt, the system writes message CPF2234 to the QHST log. You can write a program to monitor the QHST log for the message. If the program detects repeated attempts, it can end the FTP servers.
- The *TCP/IP Configuration and Reference* book describes how to use FTP batch support, for example, to send files between systems at night. When you use FTP batch support, the program must send both the user ID and the password to the server system. Either the user ID and password must be coded in the program, or the program must retrieve them from a file.

  Both these options for storing passwords and user IDs represent a potential security exposure. If you use FTP batch, you must ensure that the user ID and password information are protected with object security. You should also use a single user ID that has very limited authority on the target system. It should have only enough authority to perform the function that that you want, such as file transfer.
- FTP provides remote-command capability, just as APPC and Client Access for OS/400 do. The RCMD (Remote Command) FTP-server subcommand is the equivalent of having a command line on the system. Before you allow FTP, you must ensure that your object security scheme is adequate.

Security Tips for Simple Mail Transfer Protocol

If your system runs V3R1 or a later release and you do not want SMTP to run on your system, do the following:

__ **Step 1** If you do not plan to use SMTP at all, do not configure it on your system (or allow anyone else to configure it). If you need SMTP occasionally, but you normally do not want it to run, continue with the next steps.

__ **Step 2** To prevent SMTP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGSMTPA AUTOSTART(*NO)
```

__ **Step 3** Make sure that the public authority for the Start TCP/IP Server (STRTCPSVR) command is *EXCLUDE, which is the shipped value. You might also want to use CHGCMDDFT command to change the default value for the STRTCPSVR command. Set the default for the server (SERVER) parameter to include the specific server types that you normally want to start (instead of *ALL).

__ **Step 4** To prevent SMTP from starting and to prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for SMTP, do the following:

__ **Step a.** Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ **Step b.** Select option 4 (Work with TCP/IP port restrictions).

__ **Step c.** On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ **Step d.** For the lower port range, specify `25`.

__ **Step e.** For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) The *TCP/IP Configuration and Reference* book lists the well-known TCP/IP ports. RFC1700 provides the latest information about assigned port numbers. The *TCP/IP Configuration and Reference* book describes how to obtain RFCs (Requests for Comment).

__ **Step f.** For the protocol, specify `*TCP`.

__ **Step g.** For the user profile field, specify a user profile name that is protected on your system (not shared or adopted). By restricting the port to a specific user, you automatically exclude all other users.

__ **Step h.** Repeat steps 4c through 4g for the *UDP protocol.

__ **Step 5** As extra protection, hold the SNADS distribution queues that the SMTP application uses by typing the following commands:

```
HLDDSTQ DSTQ(QSMTPQ) PTY(*NORMAL)
HLDDSTQ DSTQ(QSMTPQ) PTY(*HIGH)
```

If your system is running V2R3 and you do not want to allow SMTP, do the following:

__ **Step 1** Do not configure SMTP. It is not automatically configured on your system.

If you want to allow SMTP on your system, be aware of the following security issues:

- If possible, avoid using an *ANY *ANY entry in the system distribution directory. When your system does not have an *ANY *ANY entry, it is more difficult for someone to attempt to use SMTP to flood your system with unwanted mail that is being routed through your system to another system.
- To prevent a user from swamping your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST). The *Backup and Recovery – Advanced* book provides more information about ASP thresholds.

Security Tips for Line Printer Daemon

If your system runs V3R1 or a later release and you do not want LPD to run on your system, do the following:

__ **Step 1** To prevent LPD server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGLPDA AUTOSTART(*NO)
```

__ **Step 2** Make sure that the public authority for the Start TCP/IP Server (STRTCPSVR) command is *EXCLUDE, which is the shipped value. You might also want to use CHGCMDDFT command to change the default value for the STRTCPSVR command. Set the default for the server (SERVER) parameter to include the specific server types that you normally want to start (instead of *ALL).

__ **Step 3** To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for LPD, do the following:

- __ **Step a.** Type `GO CFGTCP` to display the Configure TCP/IP menu.
- __ **Step b.** Select option 4 (Work with TCP/IP port restrictions).
- __ **Step c.** On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).
- __ **Step d.** For the lower port range, specify `515`.
- __ **Step e.** For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) The *TCP/IP Configuration and Reference* book lists the well-known TCP/IP ports. RFC1700 provides the latest information about assigned port numbers. The *TCP/IP Configuration and Reference* book describes how to obtain RFCs (Requests for Comment).

__ **Step f.** For the protocol, specify `*TCP`.

__ **Step g.** For the user profile field, specify a user profile name that is protected on your system (not shared or adopted). By restricting the port to a specific user, you automatically exclude all other users.

__ **Step h.** Repeat steps 3c through 3g for the *UDP protocol.

If your system is running V2R3 and you do not want to allow LPD, do the following:

__ **Step 1** After you start the QTCP subsystem, use the End Job (ENDJOB) command to end the LPD server jobs.

If you want to allow LPD on your system, be aware of the following security issues:

- To prevent a user from swamping your system with unwanted objects, be sure that you have set adequate threshold limits for your auxiliary storage pools (ASPs). You can display and set the thresholds for ASPs by using either system service tools (SST) or dedicated service tools (DST). The *Backup and Recovery – Advanced* book provides more information about ASP thresholds.
- You can use the authority to output queues to restrict who can send spooled files to your system. LPD users without an AS/400 user ID use the QTMPLPD user profile. You can give this user profile access to only a few output queues.

Security Tips for Simple Network Management Protocol

If your system runs V3R1 or a later release and you do not want SNMP to run on your system, do the following:

__ **Step 1** To prevent SNMP server jobs from starting automatically when you start TCP/IP, type the following:

```
CHGSNMPA AUTOSTART(*NO)
```

__ **Step 2** Make sure that the public authority for the Start TCP/IP Server (STRTCPSVR) command is *EXCLUDE, which is the shipped value. You might also want to use CHGCMDDFT command to change the default value for the STRTCPSVR command. Set the default for the server (SERVER) parameter to include the specific server types that you normally want to start (instead of *ALL).

__ **Step 3** To prevent someone from associating a user application, such as a socket application, with the port that the system normally uses for SNMP, do the following:

__ **Step a.** Type `GO CFGTCP` to display the Configure TCP/IP menu.

__ **Step b.** Select option 4 (Work with TCP/IP port restrictions).

__ **Step c.** On the Work with TCP/IP Port Restrictions display, specify option 1 (Add).

__ **Step d.** For the lower port range, specify `161`.

__ **Step e.** For the upper port range, specify `*ONLY`.

Notes:

1) The port restriction takes effect the next time that you start TCP/IP. If TCP/IP is active when you set the port restrictions, you should end TCP/IP and start it again.

2) The *TCP/IP Configuration and Reference* book lists the well-known TCP/IP ports. RFC1700 provides the latest information about assigned port numbers. The *TCP/IP Configuration and Reference* book describes how to obtain RFCs (Requests for Comment).

__ **Step f.** For the protocol, specify `*TCP`.

__ **Step g.** For the user profile field, specify a user profile name that is protected on your system (not shared or adopted). By restricting the port to a specific user, you automatically exclude all other users.

__ **Step h.** Repeat steps 3c through 3g for the *UDP protocol.

If you want to allow SNMP on your system, be aware of the following security issues:

- Change the default for the Add Community for SNMP (ADDCOMSNMP) command to set the manager internet address (INTNETADR) parameter to *NONE instead of *ANY.

Tips for Limiting TCP/IP Roaming

If your system is connected to a network, you may want to limit your users' ability to roam the network with TCP/IP applications. One way to do this is to restrict access to the following client TCP/IP commands:

STRTCPFTP
FTP
STRTCPTELN
TELNET
LPR
SNDTCPSPLF

Your users' possible destinations are determined by the following:

- Entries in your TCP/IP host table.

- *DFTROUTE entry in the TCP/IP route table. This allows users to enter the IP address of the next-hop system when their destination is an unknown network. A user can reach or contact a remote network by using the default route.
- Remote name server configuration. This support allows another server in the network to locate host names for your users.
- Remote system table.

You need to control who can add entries to these tables and change your configuration. You also need to understand the implications of your table entries and your configuration.

Be aware that a knowledgeable user with access to an ILE C compiler can create a socket program that can attach to a TCP or UDP port. You can make this more difficult by restricting access to the following sockets interface files in the QSYSINC library:

SYS
NETINET
H
ARPA

However, equivalent files are also available in many other environments. A determined programmer could upload the necessary files to the AS/400 from a PC. If you have an ILE C compiler, you probably need to restrict access to TCP and UDP ports if you want to prevent network roaming.

General Tips for Securing Your TCP/IP Environment

Following are additional suggestions for steps that you can take to reduce the security exposures in the TCP/IP environment on your system. These tips apply to your entire TCP/IP environment rather than to the specific applications that are discussed in earlier topics.

- Take full advantage of the AS/400 functions that are available. For example, run your system at security level 40 or 50. Set up a good object authority scheme. Use system values, such as QMAXSIGN and QLMTSECOFR.
- When you write an application for a TCP/IP port, make sure that the application is properly secure. You should assume that an outsider might try to access that application through that port. A knowledgeable outsider may attempt to TELNET to that application.
- Set the public authority to *EXCLUDE for the files that hold TCP/IP configuration information. The file names begin with QATOC for V3R1 and later versions and QATM for earlier versions than V3R1. The files are in the QUSRSYS library.
- As a security administrator, you should be aware of a technique called *IP spoofing* that is used by hackers. Every system in a TCP/IP network has an IP address. Someone who uses IP spoofing sets up a system (usually a PC) to pretend to be an existing IP address or a trusted IP address. Thus, the imposter can establish a connection with your system by pretending to be a system that you normally connect with.

  If you run TCP/IP on your system and your system participates in a network that is not physically protected (all nonswitched lines and pre-defined links), you are vulnerable to IP spoofing. Many of the suggestions in this chapter will help

to protect your system from damage by a "spoofer," starting with sign-on protection and object security. You should also ensure that your system has reasonable auxiliary storage limits set. This prevents a spoofer from flooding your system with mail or spooled files to the point that your system becomes inoperable.

In addition, you should regularly monitor TCP/IP activity on your system. If you detect IP spoofing, you can try to discover the weak points in your TCP/IP setup and make adjustments.

- The *TCP/IP Configuration and Reference* book has an appendix that provides security information about TCP/IP. Review the information in the appendix.

Tips for Securing the TCP/IP File Server Support for OS/400 Licensed Program

When you have the TCP/IP File Server Support for OS/400 licensed program, your AS/400 system can act as a network file server for other systems in a TCP/IP network. A client system can "mount" an AS/400 directory as if it is a local directory. The QSYS library, which includes all libraries on the AS/400 system, can look like a directory and subdirectories on the client system.

To a great extent, the File Server Support product relies on the security capabilities of the client system to control access to AS/400 resources. If you are a AS/400 security administrator and you have this product installed on your system, you should review the product documentation to understand the functions that it provides and the security implications. With the shipped configuration for File Server Support, your system resources are vulnerable to unintended use by File Server Support users.

Following are some suggestions for protecting your AS/400 system when TCP/IP File Server Support for OS/400 is installed:

- Remove all root-level user profile entries from the export table and from the authorized users table. Do not allow the shipped profile, Q7FSOWN, to have root authority. On other systems that can be client systems for File Server Support, it is possible to set up a user that pretends to have root authority. You need to protect your system from this.
- For the configuration database files for File Server Support, set the database capabilities value to *NO for all attributes except *READ. This protects the contents of File Server Support database files from unauthorized changes outside the command and menu interfaces that are part of the product.
- Set up your system to reject any requests that do not have a user identification (uid) specified explicitly. Do not allow such requests to use a default user.
- Review all the entries in the export table to ensure that they meet your security requirements. Consider removing all of the default entries that are provided with the product and setting up only entries that you know will not cause a security exposure.
- For the CL commands that start and stop the File Server Support function, set the public authority to *EXCLUDE. This allows you to control when the File Server Support environment is active and who can activate it. Grant authority only to trusted administrators on your system.

- When you add entries to the export table, in most cases you should set the write permission and the root access to *NO. Use other values cautiously. You can change the default values for the command to *NO to help you avoid oversights.
- Potentially serious security exposures exist when your AS/400 system is a server for a client that does not protect the ROOT uid with a non-trivial password.

Chapter 5. Tips for Securing PC Access

Many of your system users have personal computers on their desks as their workstations. They use tools that run on the PC, and they use the PC to connect to AS/400.

Most methods of connecting a PC to AS/400 provide more function than workstation emulation. The PC may look like a display to AS/400 and provide the user with interactive sign-on sessions. In addition, the PC may look to AS/400 like another computer and provide functions such as file transfer and remote procedure call.

As an AS/400 security administrator, you need to be aware of the functions that are available to PC users who are connected to your system and of the AS/400 resources that PC users can access. You may want to prevent advanced PC functions (such as file transfer and remote procedure call) if your AS/400 security scheme is not yet prepared for those functions. Probably, your long-range goal is to allow advanced PC functions while you still protect the information on your system. The topics that follow discuss some of the security issues that are associated with PC access.

Tips for Securing PC Data Access

For releases earlier than V3R1, PCs use shared folders to store information on AS/400. To access AS/400 database files, the PC user has a limited, well-defined set of interfaces. With the file transfer capability that is part of most client/server software, the PC user can copy files between the AS/400 system and the PC. With database access capability; such as a DDM file, remote SQL, or an ODBC driver; the PC user can access data on the AS/400 system.

In this environment, you can create programs to intercept and evaluate PC-user requests to access AS/400 resources. When the requests use a DDM file, you specify the exit program in the distributed data management access (DDMACC) network attribute. For some methods of PC file transfer, you specify the exit program in the client request access (PCSACC) network attribute, or you can specify PCSACC(*REGFAC) to use the registration function. When the requests use other server functions to access data, you can use the WRKREGINF command to register exit programs for those server functions.

Exit programs, however, can be difficult to design, and they are rarely foolproof. They are not a replacement for object authority, which is designed to protect your objects from unauthorized access no matter what the source of the request.

With the introduction of the integrated file system in V3R1 and V3R6, object authority becomes even more essential. With the integrated file system, the entire AS/400 becomes more easily available to PC users. Through the integrated file system, a user with sufficient authority can view an AS/400 library as if it is a PC directory. Simple move and copy commands can instantly move data from an AS/400 library to a PC directory or vice versa. The system automatically makes the appropriate changes to the format of the data.

Note: If you have PTF SF23879 installed on your system, you can use an authorization list to control the use of objects in the QSYS.LIB file system.

The strength of the integrated file system is its simplicity for users and developers. With a single interface, the user can work with objects in multiple environments. The PC user does not need special software or APIs to access objects. Instead, the PC user can use OS/400 commands to work with objects directly.

For all systems with PCs attached, but particularly for systems that are running V3R1 or later releases, a good object authority scheme is critical. Because security is integrated into OS/400, any request to access data, no matter what the source or method, must go through the authority checking process.

Object Authority with PC Access

When you set up authority for objects, you need to evaluate what that authority provides for the PC user. For example, when a user has *USE authority to a file, the user can view or print data in the file. The user cannot change information in the file or delete the file. For the PC user, viewing is equivalent to "reading," which provides sufficient authority for the user to make a copy of a file on the PC. This may not be what you intend.

For some critical files, you may need to set the public authority to *EXCLUDE to prevent downloading. You can then provide another method to "view" the file on AS/400, such as using a menu and programs that adopt authority.

Another option to prevent downloading is to use an exit program that runs whenever a PC user starts an AS/400 function (other than interactive sign-on). You can specify an exit program in the PCSACC network attribute, or you can register exit programs by using the Work with Registration Information (WRKREGINF) command. The method that you use depends on how PCs will be accessing data on your system.

PC software typically provides upload capability also, so that a user can copy data from the PC to an AS/400 database file. If your authority scheme is not set up correctly, a PC user might overlay all of the data in a file with data from a PC. You need to assign *OBJMGT authority and *OBJEXIST authority carefully and review Appendix D in the *Security – Reference* book to understand what authority is required for file operations.

The *OS/400 Server Concepts and Administration* book provides more information about the authority for PC functions and about using exit programs.

Security Considerations for PC Session Passwords

Typically, when a PC user starts the connection software, such as Client Access for OS/400, the user types the user ID and password for the server once. The password is encrypted and stored in PC memory. Whenever the user establishes a new session to the same server, the PC sends the user ID and password automatically.

Some client/server software also provides the option of bypassing the Sign On display for interactive sessions. The software will send the user ID and encrypted password when the user starts an interactive (5250 emulation) session. To support this option, the QRMTSIGN system value on the AS/400 server must be set to *VERIFY.

When you choose to allow bypassing the Sign On display, you need to consider the security trade-offs.

Security Exposure When You Require the Sign On Display: For 5250 emulation or any other type of interactive session, the Sign On display is the same as any other display. Although the password is not displayed on the screen when it is typed, the password is sent over the link in unencrypted form just like any other data field. For some types of links, this may provide the opportunity for a would-be intruder to monitor the link and detect a user ID and password from the link. Monitoring a link by using electronic equipment is often referred to as **sniffing**.

Security Exposure When You Bypass the Sign On Display: When you choose the option to bypass the Sign On display, the PC encrypts the password before it is sent, which avoids the possibility of having a password stolen by sniffing. However, you must ensure that your PC users practice operational security. An unattended PC with an active session to the AS/400 system provides the opportunity for someone to start another session without knowing a user ID and password. PCs should be set up to lock when the system is inactive for an extended period, and they should require a password to resume the session.

Even if you do not choose to bypass the Sign On display, an unattended PC with an active session represents a security exposure. Someone can start a server session and access data using PC software, again without knowing a user ID and a password. The exposure with 5250 emulation is somewhat greater because it requires less knowledge to start a session and begin accessing data.

Tips for Protecting AS/400 from Remote Commands and Procedures

A knowledgeable PC user with software such as Client Access for OS/400 can run commands on an AS/400 system without going through the Sign On display. With some client/server software, a user can open a DDM file and use the remote command function to run a command. Other client/server software, such as Client Access for OS/400 optimized clients, provides the remote command function through Distributed Program Call APIs, with the use of DDM.

For client/server software that uses DDM for remote command support, you can use the DDMACC network attribute to prevent remote commands completely. For client/server software that uses other server support, you can register exit programs for the server. If you want to allow remote commands, you must make sure that your object authority scheme protects your data adequately. Remote command capability is equivalent to giving a user a command line.

Tips for Protecting PCs from Remote Commands and Procedures

The Client Access Optimized for OS/2 client software provides the capability of receiving remote commands on the PC. You can use the Run Remote Command (RUNRMTCMD) command on AS/400 to run a procedure on an attached PC. The RUNRMTCMD capability is a valuable tool for system administrators and help-desk personnel. However, it also provides the opportunity for damaging PC data, either deliberately or by accident.

PCs do not have the same object authority functions as AS/400. Your best protection against problems with the RUNRMTCMD command is to carefully restrict

the AS/400 users who have access to the command. The OS/2 optimized client software provides the capability to register the users who can run remote commands on a specific PC. However, the default is to allow remote commands. After you have registered specific users on the PC, all nonregistered users are prevented from running remote commands on that PC.

Tips for Gateway Servers

Your system may participate in a network with an intermediate or gateway server between the AS/400 system and the PCs. For example, your AS/400 system might be attached to a LAN with a PC server that has PCs attached to it. The security issues in this situation depend on the capabilities of the software that is running on the gateway server. Figure 5-1 shows an example of a gateway-server configuration:

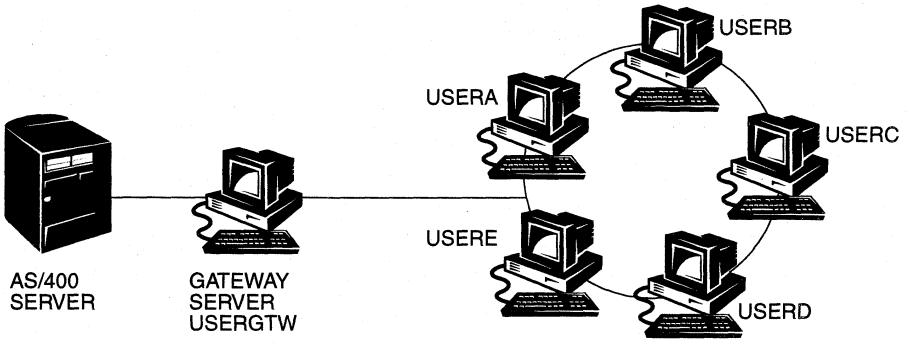


Figure 5-1. AS/400 with a Gateway Server–Example

With some software, your AS/400 system will not know about any users (such as USERA or USERC) who are downstream from the gateway server. The server will sign on to AS/400 as a single user (USERGTW). It will use the USERGTW user ID to handle all requests from downstream users. A request from USERA will look to AS/400 like a request from user USERGTW.

If this is the case, you must rely on the gateway server for security enforcement, and you must understand and manage the security capabilities of the gateway server. From an AS/400 perspective, every user has the same authority as the user ID that the gateway server uses to start the session. You might think of this as equivalent to running a program that adopts authority and provides a command line.

With other software, the gateway server passes requests from individual users to AS/400. AS/400 knows that USERA is requesting access to a particular object. The gateway is almost transparent to AS/400.

If your system is in a network that has gateway servers, you need to evaluate how much authority to provide to the user IDs that are used by the gateway servers. You also need to understand what security mechanisms are enforced by the gateway servers and how downstream users will appear to your AS/400 system.

Tips for Protecting AS/400 from Curious or Careless Users

Curiosity is one of the permanent and certain characteristics of a vigorous mind.
Samuel Johnson: The Rambler

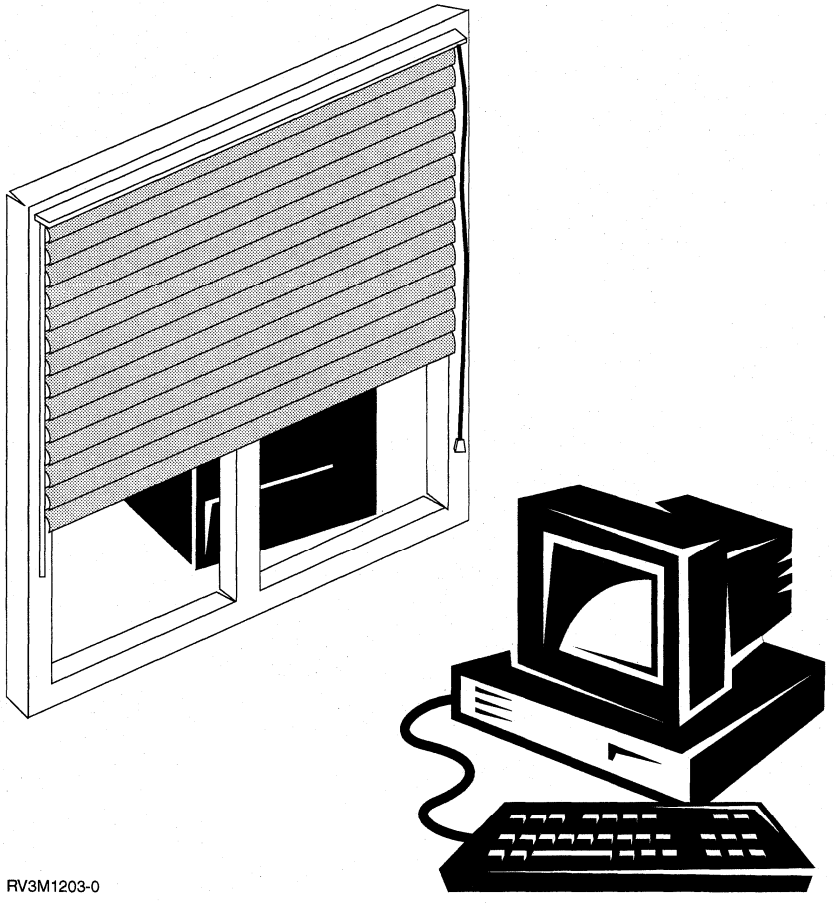
While we stop to think, we often miss our opportunity.
Publilius Syrus: Maxim 185

Two noted thinkers from many years ago commented on basic human characteristics that are relevant to your job as security administrator:

- People (system users) are naturally curious. Given the opportunity, they will explore and try new things.
- People often act (or type) before they think.

Undoubtedly, your system has some areas that are confidential. You also have information (confidential or not) that is critical to your organization. One of your jobs as security administrator is to protect your organization's assets by restricting system users.

Authorized system users (those who are entitled to sign on) should be able to use selected information, but they should not be allowed to roam through every corridor of your system. Nor should they be able to accidentally damage or destroy information. This part of the booklet describes techniques for protecting your system from average users who decide to explore or experiment.



RV3M1203-0

Chapter 6. Using Object Authority to Protect Information Assets

Your challenge as security administrator is to protect your organization's information assets without frustrating the users on your system. You need to make sure that users have enough authority to do their jobs without giving them the authority to browse throughout the system and to make unauthorized changes.

Security Tip

Authority that is too tight can backfire. Users sometimes react to authority restrictions that are too tight by sharing passwords with each other.

The OS/400 operating system provides integrated object security. Users must use the interfaces that the system provides to access objects. For example, if you want to access a database file, you must use commands or programs that are intended for accessing database files. You cannot use a command that is intended for accessing a message queue or a job log.

Whenever you use a system interface to access an object, the system verifies that you have the authority to the object that is required by that interface. Object authority is a powerful and flexible tool for protecting the assets on your system. Your challenge as a security administrator is to set up an effective object security scheme that you can manage and maintain.

Does the System Always Enforce Object Authority?

The answer is yes and no. Whenever you try to access an object, the operating system checks your authority to that object. However, if the security level on your system (QSECURITY system value) is set to 10 or 20, every user automatically has authority to access every object because every user profile has *ALLOBJ special authority.

Object Authority Tip

If you are not sure whether you are using object security, check the QSECURITY (security level) system value. If it is 10 or 20, you are not using object security.

You must plan and prepare before you change to security level 30 or higher. Otherwise, your users may not be able to access the information that they need.

The *Security – Basic* book provides a method for analyzing your applications and deciding how you should set up object security. If you are not yet using object security or if your object security scheme is outdated and convoluted, read this chapter to help you get started.

The Legacy of Menu Security

AS/400 was originally designed as a follow-on product for S/36 and S/38. Many AS/400 installations were, at one time, S/36 installations or S/38 installations. With those earlier systems, security administrators often used a technique referred to as **menu security** or **menu access control** to control what users could do.

Menu access control means that when a user signs on, the user gets a menu such as the following:

```
OEMENU      Order Entry Menu

1. Work with customer records
2. Work with orders
3. Work with order history
4. Work with prices
5. Work with contracts

Select option number:  ___
```

Figure 6-1. Sample Order Entry Menu

The user can perform only the functions that are on the menu. The user cannot get to a command line on the system to perform any functions that are not on the menu. In theory, the security administrator does not have to worry about authority to objects because menus and programs control what users can do.

AS/400 provides several user profile options to assist with menu access control:

- You can use the initial menu (INLMNU) parameter to control what menu the user first sees after signing on.
- You can use the initial program (INLPGM) parameter to run a setup program before the user sees a menu or to restrict a user to running a single program.
- You can use the limit capabilities (LMTCPB) parameter to restrict a user to a limited set of commands. It also prevents the user from specifying a different initial program or menu on the Sign On display. (The LMTCPB parameter only limits commands that are entered from the command line.)

Limitations of Menu Access Control

Computers and computer users have changed a great deal in the past few years. Many tools, such as query programs and spreadsheets, are available so that users can do some of their own programming to off-load IS departments. Some tools, such as SQL or ODBC, provide the capability to view information and to change information. To enable these tools within a menu structure is very difficult.

Fixed-function ("green-screen") workstations are rapidly being replaced by personal computers and computer-to-computer networks. If your system participates in a network, users may enter your system without ever seeing a sign-on display or a menu.

As a security administrator who is trying to enforce menu access control, you have two basic problems:

- If you are successful in limiting users to menus, your users will probably be unhappy because their ability to use modern tools is limited.
- If you are not successful, you could jeopardize critical, confidential information that menu access control is supposed to protect. When your system participates in a network, your ability to enforce menu access control decreases. For example, the LMTCPB parameter applies only to commands that are entered from a command line in an interactive session. The LMTCPB parameter has no affect on requests from communications sessions, such as PC file transfer, FTP, or remote commands.

Tips for Enhancing Menu Access Control with Object Security

With the many new options that are available to connect to systems, a viable AS/400 security scheme for the future cannot rely solely on menu access control. This topic provides suggestions for moving toward an object security environment to complement your menu access control.

The *Security – Basic* book describes a technique for analyzing the authority that users must have to objects to run your current applications. You then assign users to groups and give the groups appropriate authority. This approach is reasonable and logical. However, if your system has been operational for many years and has many applications, the task of analyzing applications and setting up object authority probably seems overwhelming.

Object Authority Tip

Your current menus combined with programs that adopt the authority of the program owners may provide a transition beyond menu access control. Be sure to protect the programs that adopt authority and the user profiles that own them.

You may be able to use your current menus to help you set up a transition environment while you gradually analyze your applications and objects. Following is an example that uses the Order Entry (OEMENU) menu (Figure 6-1 on page 6-2) and its associated files and programs.

Setting Up a Transition Environment–Example

This example starts with the following assumptions and requirements:

- All of the files are in the library ORDERLIB.
- You do not know the names of all the files. You also do not know what authority the menu options require to different files.
- The menu and all the programs that it calls are in a library called ORDERPGM.
- You want everyone who can sign on to your system to be able to view information in all the order files, customer files, and item files (with queries or spreadsheets, for example).
- Only users whose current sign-on menu is the OEMENU should be able to change the files, and they must use the programs on the menu to do this.
- System users other than the security administrators do not have *ALLOBJ or *SECADM special authority.

Do the following to change this menu-access-control environment to accommodate the need for queries:

__ **Step 1** Make a list of the users whose initial menu is the OEMENU. If you have the Security ToolKit, you can use the Print User Profile Information (PRTUSRINF (*ENVINFO) command to list the environment for every user profile on your system. The report includes the initial menu, initial program, and current library. Figure 7-8 on page 7-7 shows an example of the report.

__ **Step 2** Make sure that the OEMENU object (it may be a *PGM object or a *MENU object) is owned by a user profile that is not used for sign on. The user profile should be disabled or have a password of *NONE. For this example, assume that OEOWNER owns the OEMENU program object.

__ **Step 3** Make sure that the user profile that owns the OEMENU program object is not a group profile. You can use the following command:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ **Step 4** Change the OEMENU program to adopt the authority of the OEOWNER user profile. (Use the CHGPGM command to change the USRPRF parameter to *OWNER.)

Note: *MENU objects cannot adopt authority. IF OEMENU is a *MENU object, you can adapt this example by doing one of the following:

- Create a program to display the menu.
- Use adopted authority for the programs that run when the user selects options from the OEMENU menu.

__ **Step 5** Set the public authority to all of the files in ORDERLIB to *USE by typing the following two commands:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
    AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
    AUT(*USE)
```

Remember that if you select *USE authority, users can copy the file by using PC file transfer or FTP.

__ **Step 6** Give the profile that owns the menu program *ALL authority to the files by typing the following:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
    AUT(*ALL)
```

For most applications, *CHANGE authority to files is sufficient. However, your applications may perform functions, such as clearing physical file members, that require more authority than *CHANGE. Eventually, you should analyze your applications and provide only the minimum authority that is necessary for the application. However, during the transition period, by adopting *ALL authority, you avoid applications failures that may be caused by insufficient authority.

__ **Step 7** Restrict authority to the programs in the order library by typing the following:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
    AUT(*EXCLUDE)
```

__ **Step 8** Give the OEOWNER profile authority to the programs in the library by typing the following:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
    AUT(*USE)
```

__ **Step 9** Give the users that you identified in step 1 authority to the menu program by typing the following for each user:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
    USER(user-profile-name) AUT(*USE)
```

When you have completed these steps, all system users who are not explicitly excluded will be able to access (but not change) the files in the ORDERLIB library. Users who have authority to the OEMENU program will be able to use the menu and the programs that it calls to update files in the ORDERLIB library. The files in this library can now be changed only by users who have authority to the OEMENU program. The files are protected by a combination of object security and menu access control.

When you complete similar steps for all the libraries that contain user data, you have created a simple scheme to prevent system users from updating database files except when they use the approved menus and programs. At the same time, you have made database files available for viewing, analyzing, and copying by users with decision-support tools or with links from another system or from a PC.

Object Authority Tip

When your system participates in a network, *USE authority may provide more authority than you expect. For example, with FTP, you can make a copy of a file to another system (including a PC) if you have *USE authority to the file.

Using Library Security to Complement Menu Security

To access an object in a library, you must have authority both to the object and to the library. For systems that are running V3R0M5 or an earlier version, most operations require either *READ authority or *USE authority to the library that contains the object. For later versions, most operations require either *EXECUTE authority or *USE authority to the library.

Depending on your situation, you may be able to use library authority as a simple means for securing objects. For example, assume that for the Order-Entry menu example, everyone who has authority to the Order Entry menu can use all of the programs in the ORDERPGM library. Rather than securing individual programs, you can set the public authority to the ORDERPGM library to *EXCLUDE. You can then grant *USE authority to the library to specific user profiles, which will allow them to use the programs in the library. (This assumes that public authority to the programs is *USE or greater.)

Library authority can be a simple, efficient method for administering object authority. However, you must ensure that you are familiar with the contents of the libraries that you are securing so that you do not provide unintended access to objects.

Tips for Setting Up Object Ownership

The ownership of objects on your system is an important part of your object authority scheme. By default, the owner of an object has *ALL authority to the object. Chapter 5 in the *Security – Reference* book provides recommendations and examples for planning object ownership. Following are a few tips:

- In general, group profiles should not own objects. If a group profile owns an object, all group members have *ALL authority to the object unless the group member is explicitly excluded.
- If you use adopted authority, consider whether the user profiles that own programs should also own application objects, such as files. You may not want the users who run the programs that adopt authority to have *ALL authority to files.

Tips for Object Authority to System Commands and Programs

Following are several suggestions when you restrict authority to IBM-supplied objects:

- When you have more than one national language on your system, your system has more than one system (QSYS) library. Your system has a QSYSxxxx library for each national language on your system. If you are using object authority to control access to system commands, remember to secure the command in the QSYS library and in every QSYSxxx library on your system.
- The System/38 library sometimes provides a command with function that is equivalent to the commands that you want to restrict. Be sure you restrict the equivalent command in the QSYS38 library.
- If you have the System/36 environment, you may need to restrict additional programs. For example, the QY2FTML program provides System/36 file transfer.

Chapter 7. Tips for Managing and Monitoring Authority

The Security ToolKit provides a set of reports that can help you keep track of how the authority is set up on your system. When you run these reports initially, you can print everything (authority for all the files or for all the programs, for example).

After you have established your base of information, you can run the changed versions of reports regularly. The changed versions help you identify security-relevant changes on your system that require your attention. For example, you can run the report that shows the public authority for files every week. You can request only the changed version of the report. It will show you new files on the system that are available to everyone and existing files whose public authority has changed since the last report.

The Security ToolKit provides two menus:

- Use the SECTOOLS menu for running programs interactively. "Options on the Security Tools Menu" on page 11-1 provides more information about the menu.
- Use the SECBATCH menu for running programs in batch. The SECBATCH menu has two parts: one for submitting jobs to the job queue immediately, and the other for placing jobs on the job scheduler. "Options on the Security Batch Menu" on page 11-5 provides more information about the menu.

This chapter provides examples of how you can monitor the authority on your system. The examples in this chapter use reports from V3R1. If your system is running an earlier version, your report formats will differ because some authorities and the primary group are available only with V3R1 or later versions of OS/400.

Monitoring Public Authority to Objects

For both simplicity and performance, most systems are set up so that most objects are available to most users. Users are explicitly denied access to certain confidential, security-sensitive objects rather than having to be explicitly authorized to use every object. A few systems with high security requirements take the opposite approach and authorize objects on a need-to-know basis. On those systems, most objects are created with the public authority set to *EXCLUDE.

AS/400 is an object-based system with many different types of objects. Most object types do not contain sensitive information or perform security-relevant functions. As a security administrator on an AS/400 system with typical security needs, you probably want to focus your attention on objects that require protection, such as database files and programs. For other object types, you can just set public authority that is sufficient for your applications, which for most object types is *USE authority.

If you have the Security ToolKit, you can use the Print Public Authority (PRTPUBAUT) command to print information about objects that public users can access. (A **public user** is anyone with sign-on authority who is not explicitly denied access to an object.) When you use the PRTPUBAUT command, you can specify the object types (and libraries) that you want to examine. Options are available on the SECBATCH and SECTOOLS menus to print the Publicly Authorized Objects Report for the object types that most commonly have security implications.

Figure 7-1 on page 7-2 shows an example of the Publicly Authorized Objects Report for the *FILE objects in the CUSTLIB library:

```
                          Publicly Authorized Objects (Full Report)
                                                                                SYSTEM4
Object type . . . . . :   *FILE
Specified library . . . . . :   CUSTLIB
                          Authorization          ----------Object----------  ------------Data------------
Library     Object      Owner       List         Authority  Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
CUSTLIB     CUSTMAST    AROWNER     *NONE        *USE       X                             X                        X
CUSTLIB     ORDERS      AROWNER     *NONE        *CHANGE    X                             X     X    X    X     X
CUSTLIB     PRICES      AROWNER     *NONE        *USE       X                             X                        X
CUSTLIB     TAXES       AROWNER     *NONE        *CHANGE    X                             X     X    X    X     X
```

Figure 7-1. Publicly Authorized Objects Report–Sample

You can print the changed version of this report regularly to see what objects might require your attention.

Managing Authority for New Objects

OS/400 provides functions to help you manage the authority and ownership for new objects on your system. When a user creates a new object, the system determines the following:

- Who will own the object
- What the public authority for the object is
- Whether the object has any private authorities
- Where to put the object (what library or directory)
- Whether access to the object will be audited

The system uses system values, library parameters, and user profile parameters to make these decisions. "Assigning Authority and Ownership to New Objects" in chapter 5 of the *Security – Reference* provides several examples of the options that are available.

If you have the Security ToolKit, you can use the PRTUSRINF command to print the user profile parameters that affect ownership and authority for new objects. Figure 7-6 on page 7-5 shows an example of this report.

Monitoring Authorization Lists

SECBATCH menu options:
3 *to submit immediately*
32 *to use the job scheduler*

You can group objects with similar security requirements by using an authorization list. Conceptually, an authorization list contains a list of users and the authority that the users have to the objects that are secured by the list. Authorization lists provide an efficient way to manage the authority to similar objects on the system. However, in some cases, they make it difficult to keep track of authorities to objects.

You can use the Print Private Authority (PRTPVTAUT) command to print information about authorization list authorities. Figure 7-2 on page 7-3 shows a sample of the report.

```
                                Private Authorities (Full Report)
                                                                                                    SYSTEM4
Authorization                    Primary                                  List  ----------Object----------  ------------Data------------
    List          Owner          Group          User          Authority   Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
 LIST1            QSECOFR        *NONE          *PUBLIC       *EXCLUDE
 LIST2            BUDNIKR        *NONE          BUDNIKR       *ALL        X     X    X    X      X      X    X     X    X    X    X
                                                *PUBLIC       *CHANGE           X                             X     X    X    X    X
 LIST3            QSECOFR        *NONE          *PUBLIC       *EXCLUDE
 LIST4            CJWLDR         *NONE          CJWLDR        *ALL        X     X    X    X      X      X    X     X    X    X    X
                                                GROUP1        *ALL              X    X    X      X      X    X     X    X    X    X
                                                *PUBLIC       *EXCLUDE
```

Figure 7-2. Private Authorities Report for Authorization Lists

This report shows the same information that you see on the Edit Authorization List (EDTAUTL) display. The advantage of the report is that it provides information about all authorization lists in one place. If you are setting up security for a new group of objects, for example, you can quickly scan the report to see if an existing authorization list meets your needs for those objects.

You can print a changed version of the report to see new authorization lists or authorization lists with authority changes since you last printed the report. You also have the option of printing a list of the objects that are secured by each authorization list. Figure 7-3 shows an example of the report for one authorization list:

```
                          Display Authorization List Objects
5763SS1 V3R1M0  940909
 Authorization list . . . . . :   CUSTAUTL
   Library  . . . . . . . . . :     QSYS
 Owner  . . . . . . . . . . . :   AROWNER
 Primary group  . . . . . . . :   *NONE
                                                                Primary
 Object          Library         Type          Owner            group          Text
 CUSTMAS         CUSTLIB         *FILE         AROWNER          *NONE
 CUSTORD         CUSTORD         *FILE         OEOWNER          *NONE
```

Figure 7-3. Display Authorization List Objects Report

You can use this report, for example, to understand the effect of adding a new user to an authorization list (what authorities that user will receive).

Monitoring Private Authority to Objects

SECBATCH menu options:
12 *to submit immediately*
41 *to use the job scheduler*

If you have the Security ToolKit, you can use the Print Private Authority (PRTPVTAUT) command to print a list of all the private authorities for objects of a specified type in a specified library.

You can use this report to help you detect new authorities to objects. It can also help you keep your private authority scheme from becoming convoluted and unmanageable. Figure 7-4 on page 7-4 shows an example of the report:

```
                              Private Authorities (Full Report)
5799XDH V2R3M0  960115                                                    SYSTEM8
 Library . . . . . . . . . . . :   JCMGR
   *PUBLIC authority . . . . . :     *CHANGE
 Object type . . . . . . . . . :   *PGM
                        Authorization                          ------Object-------   ----------Data-----------
 Object       Owner     List          User        Authority    Opr   Mgt   Exist    Read   Add   Upd   Dlt
 CLNOBJOWN    JCMGR     *NONE         JCMGR       *ALL         X     X     X        X      X     X     X
                                      *PUBLIC     *CHANGE      X                    X      X     X     X
 CLNUSRPRF    JCMGR     *NONE         JCMGR       *ALL         X     X     X        X      X     X     X
                                      BASMLYRY    *USE         X                    X
                                      CJWX        *ALL         X     X     X        X      X     X     X
                                      *PUBLIC     *CHANGE      X                    X      X     X     X
```

Figure 7-4. Private Authorities Report–Sample

Monitoring Access to Output Queues and Job Queues

Sometimes a security administrator does a great job of protecting access to files and then forgets about what happens when the contents of a file are printed. AS/400 provides functions for you to protect sensitive output queues and job queues. You protect an output queue so that unauthorized users cannot, for example, view or copy confidential spooled files that are waiting to print. You protect job queues so that an unauthorized user cannot either redirect a confidential job to a nonconfidential output queue or cancel the job entirely.

SECBATCH menu options:
15 *to submit immediately*
44 *to use the job scheduler*

The *Security – Basic* and *Security – Reference* books describe how to protect your output queues and job queues.

You can use the Print Queue Authority (PRTQAUT) command to print the security settings for the job queues and output queues on your system. You can then evaluate printing jobs that print confidential information and ensure that they are going to output queues and job queues that are protected. Figure 7-5 shows an example of the PRTQAUT report:

```
                                Queue Authority (Full Report)
                                                                                SYSTEM4
 Specified library . . . . . :   *ALL
 Library      Object       Type         Owner        Authority    DSPDTA       OPRCTL       AUTCHK
 BASQLIB      OUTQ1        *OUTQ        BASMLYR      *USE         *NO          *YES         *OWNER
 BASQLIB      OUTQ2        *OUTQ        BASMLYR      *ALL         *YES         *YES         *OWNER
 BASQLIB      OUTQ3        *OUTQ        BASMLYR      *CHANGE      *OWNER       *YES         *OWNER
 BASQLIB      OUTQ4        *OUTQ        BASMLYR      *EXCLUDE     *NO          *NO          *OWNER
 BASQLIB      OUTQ5        *OUTQ        BASMLYR      *EXCLUDE     *NO          *NO          *DTAAUT
 BASQLIB      JOBQ2        *JOBQ        BASMLYR      *CHANGE      *NONE        *NO          *OWNER
 BASQLIB      JOBQ3        *JOBQ        BASMLYR      *EXCLUDE     *NONE        *NO          *DTAAUT
```

Figure 7-5. Queue Authority Report–Sample

For output queues and job queues that you consider to be security-sensitive, you can compare your security settings to the information in Appendix D of the *Security – Reference* book. The tables in Appendix D tell what settings are required to perform different output queue and job queue functions.

Monitoring Special Authorities

When users on your system have unnecessary special authorities, your efforts to develop a good object authority scheme may be wasted. Object authority is meaningless when a user profile has *ALLOBJ special authority. A user with *SPLCTL special authority can see any spooled file on the system, no matter what efforts you make to secure your output queues. A user with *JOBCTL special authority can affect system operations and redirect jobs. A user with *SERVICE special authority may be able to use service tools to access data without going through the operating system.

SECBATCH menu options:
20 *to submit immediately*
49 *to use the job scheduler*

If you have the Security ToolKit, you can use the Print User Profile Information (PRTUSRINF) command to print information about the special authorities and user classes for user profiles on your system. When you run the report, you have several options:

- All user profiles
- User profiles with specific special authorities
- User profiles that have specific user classes
- User profiles with a mismatch between user class and special authorities.

Figure 7-6 shows an example of the report that shows the special authorities for all user profiles:

```
                                    User Profile Information
5799XDJ V3R1M0  960115                                                                  SYSTEM4
 Report type  . . . . . . . . . :   *AUTINFO
 Select by  . . . . . . . . . . :   *SPCAUT
 Special authorities  . . . . . :   *ALL
                      -------------Special Authorities-------------
                                    *IO                                                 Group
 User       Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User                      Group      Authority  Limited
 Profile    Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner          Authority  Type       Capability
 USERA      *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF        *NONE      *PRIVATE   *NO
 USERB      *NONE                      X     X                       *PGMR      *USRPRF        *NONE      *PRIVATE   *NO
 USERC      *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF        *NONE      *PRIVATE   *NO
 USERD      *NONE                                                    *USER      *USRPRF        *NONE      *PRIVATE   *NO
```

Figure 7-6. User Information Report–Example 1

In addition to the special authorities, the report shows the following:

- Whether the user profile has limited capability.
- Whether the user or the user's group owns new objects that the user creates.
- What authority the user's group automatically receives to new objects that the user creates.

Figure 7-7 on page 7-6 shows an example of the report for mismatched special authorities and user classes:

```
                                    User Profile Information
5799XDJ V3R1M0  960115                                                          SYSTEM4
 Report type  . . . . . :   *AUTINFO
 Select by  . . . . . :   *MISMATCH
                      ------------Special Authorities-------------
                                  *IO                                                  Group
 User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User                 Group      Authority  Limited
 Profile   Profiles  OBJ   IT    CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner     Authority  Type       Capability
 USERX     *NONE     X                 X     X                  X   *SYSOPR    *USRPRF   *NONE      *PRIVATE   *NO
 USERY     *NONE                                      X             *USER      *USRPRF   *NONE      *PRIVATE   *NO
 USERZ                                                X             *USER      *USRPRF   *NONE      *PRIVATE   *NO
         QPGMR                       X     X
```

Figure 7-7. User Information Report–Example 2

In Figure 7-7, notice the following:

- USERX has a system operator (*SYSOPR) user class but has *ALLOBJ and *SPLCTL special authorities.
- USERY has a user (*USER) user class but has *SECADM special authority.
- USERZ also has a user (*USER) class and *SECADM special authority. You can also see that USERZ is a member of the QPGMR group, which has *JOBCTL and *SAVSYS special authorities.

You can run these reports regularly to help you monitor the administration of user profiles.

Monitoring User Environments

One role of the user profile is to define the environment for the user, including the output queue, the initial menu, and the job description. The user's environment affects how the user sees the system and, to some extent, what the user is allowed to do. The user must have authority to the objects that are specified in the user profile. However, if your authority scheme is still in progress or is not very restrictive, the user environment that is defined in a user profile may produce results that you do not intend. Following are several examples:

SECBATCH menu options:
20 *to submit immediately*
49 *to use the job scheduler*

- The user's job description may specify a user profile that has more authority than the user.
- The user may have an initial menu that does not have a command line. However, the user's attention-key-handling program may provide a command line.
- The user may be authorized to run confidential reports. However, the user's output may be directed to an output queue that is available to users who should not see the reports.

If you have the Security ToolKit, you can use the *ENVINFO option of the Print User Profile Information (PRTUSRINF) command to help you monitor the environments that are defined for system users. Figure 7-8 on page 7-7 shows an example of the report:

```
                                User Profile Information
5799XDJ V3R1M0  960115                                                    SYSTEM4
 Report type  . . . . . :   *ENVINFO
 Select by  . . . . . :   *USRCLS
                          Initial       Initial          Job          Message      Output       Attention
 User                     Menu/         Program/     Description/     Queue/       Queue/       Program/
 Profile       Current    Library       Library        Library        Library      Library      Library
 AUDSECOFR     AUDITOR    MAIN          *NONE          QDFTJOBD       QSYSOPR      *WRKSTN      *SYSVAL
                          *LIBL                        QGPL           QSYS
 USERA         *CRTDFT    OEMENU        *NONE          QDFTJOBD       USERA        *WRKSTN      *SYSVAL
                          *LIBL                        QGPL           QUSRSYS
 USERB         *CRTDFT    INVMENU       *NONE          QDFTJOBD       USERB        *WRKSTN      *SYSVAL
                          *LIBL                        QGPL           QUSRSYS
 USERC         *CRTDFT    PAYROLL       *NONE          QDFTJOBD       USERC        PAYROLL      *SYSVAL
                          *LIBL                        QGPL           QUSRSYS      PRPGMLIB
```

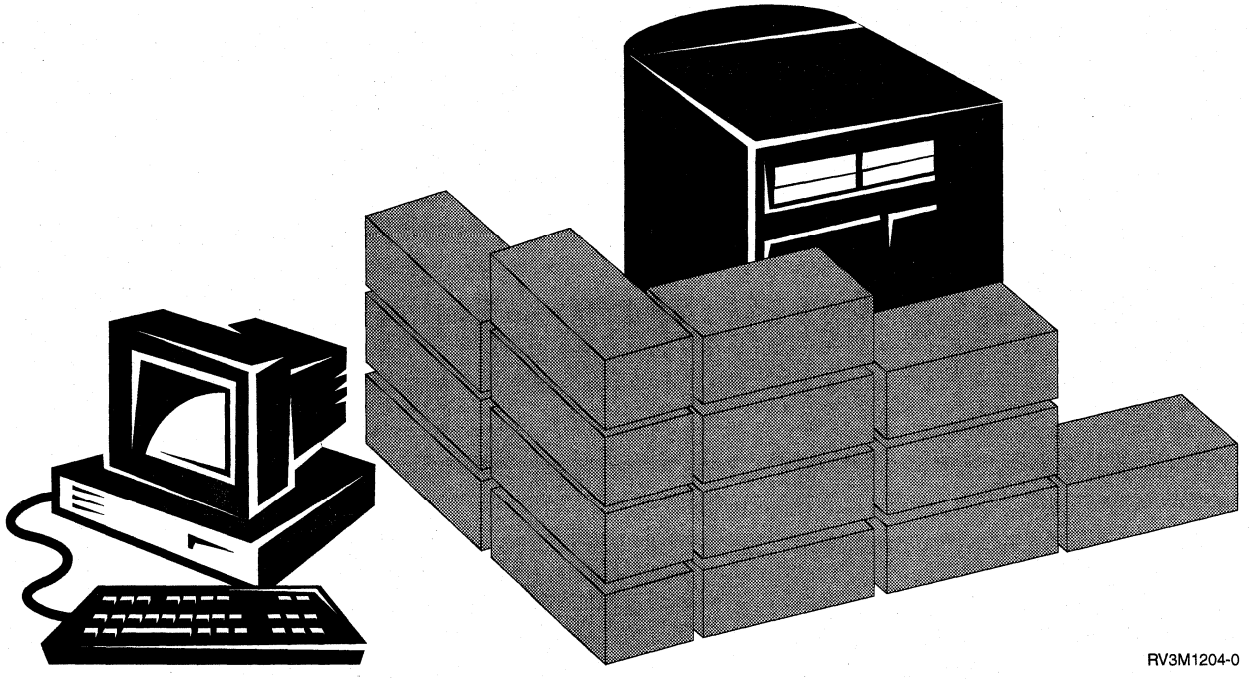
Figure 7-8. Print User Profile Information–User Environment Example

Tips for Protecting AS/400 from Devious or Determined Users

If all the good people were clever,
And all clever people were good,
The world would be a nicer place than ever
We thought that it possibly could.
Elizabeth Wordsworth

The 1990 printing of *Webster's Dictionary* defines a hacker as "an expert at programming and solving problems with a computer." Anyone who is associated with computer security knows that hackers do not always apply their formidable expertise in appropriate ways. (The clever are not always good.) For the hacker, the "problem" may simply be proving that a system can be entered or compromised.

This part of the booklet provides tips for protecting your system from expert users who try to circumvent your security.



RV3M1204-0

Chapter 8. Tips for Detecting Suspicious Programs

Recent trends in computer usage have increased the likelihood that your system may have programs from untrusted sources or programs that perform unknown functions. Following are examples:

- A personal computer user sometimes obtains programs from other PC users. If the PC is attached to your AS/400 system, that program can affect your AS/400.
- Users who are connected to networks can also obtain programs, for example from bulletin boards.
- Hackers have become more active and renowned. They often publish their methods and their results. This can lead to copycat activity by normally law-abiding programmers.

These trends have led to a new problem in computer security called a **computer virus**. A virus is a program that can change other programs to include a copy of itself. The other programs are then said to be infected by the virus. Additionally, the virus can perform other operations that can take up system resources or destroy data.

The architecture of AS/400 provides some protection from the infectious characteristics of a computer virus. "Protecting Against Computer Viruses" describes this. An AS/400 security administrator needs to be more concerned about programs that perform unauthorized functions. The remaining topics in this chapter describe some ways that programs with ill intentions might be set up to run on your system. The topics provide tips for preventing programs from performing unauthorized functions.

Security Tip

Object authority is always your first line of defense. If you do not have a good plan for protecting your objects, your system is defenseless. This chapter discusses ways that an authorized user might try to take advantage of loop-holes in your object authority scheme.

Protecting Against Computer Viruses

A computer that has a virus infection has a program that can change other programs. The object-based architecture of AS/400 makes this type of virus more difficult to produce and spread than it is with other computer architectures. On AS/400, you use specific commands and instructions to work on each type of object. You cannot use a file instruction to change an operable program object (which is what most virus-creators do). Nor can you easily create a program that changes another program object. To do so requires considerable time, effort, and expertise, and it requires access to tools and documentation that are not generally available.

However, as new AS/400 functions become available to participate in the open-systems environment, some of the object-based protection functions of AS/400 no longer apply. For example, with the integrated file system function that became

available with V3R1, users can directly manipulate some objects in directories, such as stream files.

Also, although AS/400 architecture makes it difficult for a virus to spread among AS/400 programs, it does not prevent AS/400 from being a virus-carrier. As a file server, AS/400 auxiliary storage can hold programs that are shared by many PC users. Any one of these programs might contain a virus that is not detected by AS/400. To prevent this type of virus from infecting the PCs that are attached to your AS/400 server, you must use PC virus-scan software.

Several functions exist on AS/400 to prevent someone from using a low-level language with pointer capability to alter an operable object program:

- If your system runs at security level 40 or higher, the integrity protection includes protections against changing program objects. For example, you cannot successfully run a program that contains blocked (protected) machine instructions.
- On systems that run an earlier version than Version 1 Release 3, you can create a program that contains blocked machine instructions. On later versions, you cannot create a program with blocked instructions.

  At security level 40 or higher, the program validation value is intended to protect you when you restore a program that was created on a system that runs an earlier version than V1R3. You can specify that the system should re-create a program that was saved on a version earlier than V1R3.
- At security level 40 or higher, the program validation value is also intended to protect you when you restore a program that was saved (and potentially changed) on another system. Chapter 2 in the *Security – Reference* book describes the integrity protection functions for security level 40 and higher, including program validation values.

  Note: The program validation value is not foolproof, and it is not a replacement for vigilance in evaluating programs that are restored to your system. Some hackers have attempted to duplicate the algorithm that is used to produce the program validation value.
- If you are running V3R6, you can use the force object conversion (FRCOBJCVN) parameter on the restore commands to automatically re-create every program that is restored to your system. When you force object conversion, the system uses the program template to re-create the object program. You can set the FRCOBJCVN parameter so that the system will not restore a program that does not have a program template (called observability).

Several tools are also available to help you detect the introduction of an altered program into your system:

- You can use the Check Object Integrity (CHKOBJITG) command to scan objects (operable objects) that meet your selection criteria to ensure that those objects have not been altered. This is similar to a virus-scan function.
- You can use the security auditing function to monitor programs that are changed or restored. The *PGMFAIL, *SAVRST, and *SECURITY values for the authority level system value provide audit records that can help you detect attempts to introduce a virus-type program into your system. Chapter 9 and Appendix F in the *Security – Reference* book provide more information about audit values and the audit journal entries.

- You can use the force create (FRCCRT) parameter of the Change Program (CHGPGM) command to re-create any program that has been restored to your system. The system uses the program template (observable information) to re-create the program. If the program object has been changed after being compiled, the re-creation replaces that program object. If the program template contains blocked (protected instructions) and you are running security level 40 or higher, the system will not re-create the program successfully.

Monitoring the Use of Adopted Authority

On AS/400, you can create a program that adopts the authority of the owner of the program. This means that any user who runs the program has the same authorities (private authorities and special authorities) as the user profile that owns the program.

Adopted authority is a valuable security tool when it is used correctly. "Tips for Enhancing Menu Access Control with Object Security" on page 6-3, for example, describes how to combine adopted authority and menus to help you expand beyond menu access control. You can use adopted authority to protect your important files from being changed outside of your approved application programs while you still allow queries against the files.

As security administrator, you should make sure that adopted authority is used properly:

- Programs should adopt the authority of a user profile that has only enough authority to do the necessary functions, not excessive authority. You should be particularly cautious of programs that adopt the authority of a user profile that either has *ALLOBJ special authority or owns important objects.
- Programs that adopt authority should have a specific, limited function and should not provide command-entry capability.
- Programs that adopt authority should be secured properly.
- Excessive use of adopted authority may have a negative impact on your system performance. To help you avoid performance problems, review the authority-checking flowcharts and the suggestions for using adopted authority in Chapter 5 of the *Security – Reference* book

SECBATCH menu options:
1 *to submit immediately*
30 *to use the job scheduler*

If you have the Security ToolKit, you can use the Print Adopted Information (PRTADPINF) command (option 20 on the SECTOOLS menu) to help you monitor the use of adopted authority on your system.

Figure 8-1 on page 8-4 shows an example of the output from this command:

```
                    Adopted Objects by User Profile (Full Report)

User profile . . . . . :   CJWLDR
Special authorities  . . . . . :   *ALLOBJ  *AUDIT   *IOSYSCFG  *JOBCTL
                                   *SAVSYS  *SECADM  *SERVICE   *SPLCTL
----------Object------------     ------Library--------
                    Public                    Public        Private
Name      Type      Authority    Name         Authority     Authorities
PGM1      *PGM      *USE         LIB1         *USE               Y
PGM2      *PGM      *CHANGE      LIB2         *USE               N
```

Figure 8-1. Adopted Objects by User Profile Report–Full Report

Figure 8-1 shows information for one user profile, CJWLDR. It shows the special authorities that CJWLDR has and the programs that adopt CJWLDR's authority. In this example, anyone who has access to a command line can run the programs that adopt CJWLDR's authority because the programs have public authority of *USE. This example demonstrates a potentially serious security exposure because of CJWLDR's special authorities.

After you have established a base of information, you can print the changed version of the adopted objects report regularly. It lists new programs that adopt authority and programs that have been changed to adopt authority since you last ran the report. Figure 8-2 shows an example of the changed report:

```
                      Adopted Objects by User Profile (Changed Report)
5799XDJ V3R1M0  960115
 User profile . . . . . :   CJWLDR
 Special authorities  . . . . . :   *ALLOBJ  *AUDIT   *IOSYSCFG  *JOBCTL
                                    *SAVSYS  *SECADM  *SERVICE   *SPLCTL
 Last changed report  . . . . . :   01/21/96  14:23:53
 ----------Object------------     --------Library---------
                     Public                    Public        Private
 Name      Type      Authority    Name         Authority     Authorities
 PGMX      *PGM      *CHANGE      LIB3         *CHANGE            Y
 PGMY      *PGM      *USE         LIB4         *USE               N
```

Figure 8-2. Adopted Objects by User Profile Report–Changed Report

If you suspect that adopted authority is being misused on your system, you can set the QAUDLVL system value to include *PGMADP. When this value is active, the system creates an audit journal entry whenever someone starts or ends a program that adopts authority. The entry includes the name of the user who started the program and the name of the program.

Monitoring the Use of Trigger Programs

Beginning with V3R1, DB2 for OS/400 provides the capability to associate trigger programs with database files. Trigger-program capability is common across the industry for high-function database managers.

When you associate a trigger program with a database file, you specify when the trigger program runs. For example, you can set up the customer order file to run a trigger program whenever a new record is added to the file. When the customer's

outstanding balance exceeds the credit limit, the trigger program can print a warning letter to the customer and send a message to the credit manager.

Trigger programs provide a productive way to provide application functions and manage information. They also provide the ability for someone with devious intentions to create a "Trojan horse" on your system. A destructive program may be sitting and waiting to run when a certain event occurs in a database file on your system.

Note: In history, the Trojan horse was a large hollow wooden horse that was filled with Greek soldiers. After the horse was introduced within the walls of Troy, the soldiers climbed out of the horse and fought the Trojans. In the computer world, a program that hides destructive functions is often called a Trojan horse.

SECBATCH menu options:
18 *to submit immediately*
37 *to use the job scheduler*

When your system ships, the ability to add a trigger program to a database file is restricted. If you are managing object authority carefully, the typical user will not have sufficient authority to add a trigger program to a database file. (Appendix D in the *Security – Reference* book tells the authority that is required for all commands, including the Add Physical File Trigger (ADDPFTRG) command.)

If you have the Security ToolKit, you can use the Print Trigger Programs (PRTTRGPGM) command to print a list of all the trigger programs in a specific library or in all libraries. Figure 8-3 shows an example of the report:

```
                                Trigger Programs (Full Report)

Specified library . . . . . :   CUSTLIB
                                Trigger      Trigger      Trigger      Trigger      Trigger
Library      File               Library      Program      Time         Event        Condition
CUSTLIB      MB106              ARPGMLIB     INITADDR     Before       Update       Always
CUSTLIB      MB107              ARPGMLIB     INITNAME     Before       Update       Always
```

Figure 8-3. Print Trigger Programs Report–Full Report Example

You can use the initial report as a base to evaluate any trigger programs that already exist on your system. Then, you can print the changed report regularly to see whether new trigger programs have been added to your system.

When you evaluate trigger programs, consider the following:

- Who created the trigger program? You can use the Display Object Description (DSPOBJD) command to determine this.
- What does the program do? You will have to look at the source program or talk to the program creator to determine this. For example, does the trigger program check to see who the user is? Perhaps the trigger program is waiting for a particular user (QSECOFR) in order to gain access to system resources.

After you have established a base of information, you can print the changed report regularly to monitor new trigger programs that have been added to your system. Figure 8-4 on page 8-6 shows an example of the changed report:

```
                              Trigger Programs (Changed Report)
5799XDJ V3R1M0  960115                                                    SYSTEM4
 Specified library . . . . . :  JCHEIDEL
 Last changed report . . . . :  96/01/21  14:33:37
                          Trigger       Trigger       Trigger       Trigger       Trigger
 Library       File       Library       Program       Time          Event         Condition
 INVLIB        MB108      INVPGM        NEWPRICE      After         Delete        Always
 INVLIB        MB110      INVPGM        NEWDSCNT      After         Delete        Always
```

Figure 8-4. Print Trigger Programs Report–Changed Report Example

The *DB2 for OS/400 Database Programming* book has more information about the security issues that are associated with using trigger programs.

Checking for Hidden Programs

Trigger programs are not the only possible way to introduce a Trojan horse into your system. Trigger programs are an example of an **exit program**. When a certain event occurs, such as a file update in the case of a trigger program, the system runs the exit program that is associated with that event.

Table 8-1 describes other examples of exit programs that might be on your system. You should use the same methods for evaluating the use and content of these exit programs that you use for trigger programs.

Note: Table 8-1 is not a complete list of possible exit programs.

Table 8-1 (Page 1 of 2). System-Provided Exit Programs

Program Name	When the Program Runs
User-specified name on the DDMACC network attribute.	When a user attempts to open a DDM file on your system.
User-specified name on the PCSACC network attribute.	When a user attempts to use Client Access for OS/400 functions to access objects on your system.
User-specified name on the QPWDVLDPGM system value.	When a user runs the Change Password function.
User-specified name on the QRMTSIGN system value.	When a user attempts to sign on interactively from a remote system.
QSYS/QEZUSRCLNP	When the automatic cleanup function runs.
User-specified name on the EXITPGM parameter of the CHGBCKUP command.	When you use the Operation Assistant backup function.
User-specified names on the CRTPRDLOD command.	Before and after you save, restore, or delete the product that was created with the command.

Table 8-1 (Page 2 of 2). System-Provided Exit Programs	
Program Name	**When the Program Runs**
User-specified name on the DFTPGM parameter of the CHGMSGD command.	If a default program is specified for a message, the system runs the program when the message is issued. Because of the large number of message descriptions on a typical system, the use of default programs is difficult to monitor. To prevent public users from adding default programs for messages, consider setting the public authority for message files (*MSGF objects) to *USE.
User-specified name on the FKEYPGM parameter of the STREML3270 command.	When the user presses a function key during the 3270 device emulation session. The system returns control to the 3270 device emulation session when the exit program ends.
User-specified name on the EXITPGM parameter of the performance monitor commands.	To process data that is collected by the following commands: STRPFRMON, ENDPFRMON, ADDPFRCOL, and CHGPFRCOL. The program runs when data collection ends.
User-specified name on the EXITPGM parameter of the RCVJRNE command.	For each journal entry that it reads from the specified journal receiver.
User-specified name on the QTNADDCR API.	During a COMMIT or ROLLBACK operation.
User-specified names on the QHFRGFS API.	To perform the file system functions.
User-specified name on the SEPPGM parameter of a printer device description.	To determine what to print on the separator page before or after a spooled file or a print job.
QGPL/QUSCLSXT	When a database file is closed to allow the capture of file usage information.
User-specified name on the FMTSLR parameter of a logical file.	When a record is written to the database file and a record format name is not included in the high-level language program. The selector program receives the record as input, determines the record format used, and returns it to the database.
User-specified name that is specified in the QATNPGM system value, the ATNPGM parameter in a user profile, or the PGM parameter of the SETATNPGM command.	When a user presses the Attention key.
User-specified name on the EXITPGM parameter of the TRCJOB command.	Before starting the Trace Job procedure.

For commands that allow you to specify an exit program, you should ensure that the command default has not been changed to specify an exit program. You should also ensure that the public authority for these commands is not sufficient to change the command default. The CHGCMDDFT command requires *OBJMGT

authority to the command. You do not need *OBJMGT authority to run a command.

Evaluating Registered Exit Programs

Beginning with V3R1, you can use the system registration function to register exit programs that should be run when certain events occur. To list the registration information on your system, type `WRKREGINF OUTPUT(*PRINT)`. Figure 8-5 shows an example of the report:

```
                Work with Registration Information
5763SS1 V3R1M0  940909                              SYSTEM4  01/15/96
 Exit point . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
 Exit point format  . . . . . . . . . . . :   NJE00100
 Exit point registered  . . . . . . . . . :   *YES
 Allow deregister . . . . . . . . . . . . :   *YES
 Maximum number of exit programs  . . . . :   *NOMAX
 Current number of exit programs  . . . . :   0
 Preprocessing for add  . . . . . . . . . :   *NONE
   Library  . . . . . . . . . . . . . . . :
   Format . . . . . . . . . . . . . . . . :
 Preprocessing for remove . . . . . . . . :   *NONE
   Library  . . . . . . . . . . . . . . . :
   Format . . . . . . . . . . . . . . . . :
 Preprocessing for retrieve . . . . . . . :   *NONE
   Library  . . . . . . . . . . . . . . . :
```

Figure 8-5. Work with Registration Information–Example

For each exit point on the system, the report shows whether any exit programs are currently registered. When an exit point has programs that are currently registered, you can select option 8 (Display programs) from the display version of WRKREGINF to display information about the programs:

```
                        Work with Registration Information

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

                           Exit
     Exit                  Point
Opt  Point                 Format    Registered  Text
     QIBM_QGW_NJEOUTBOUND  NJE00100     *YES     Network Job Entry outbound ex
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     Original Data Queue Server
     QIBM_QLZP_LICENSE     LICM0100     *YES     Original License Mgmt Server
     QIBM_QMF_MESSAGE      MESS0100     *YES     Original Message Server
     QIBM_QNPS_ENTRY       ENTR0100     *YES     Network Print Server - entry
     QIBM_QNPS_SPLF        SPLF0100     *YES     Network Print Server - spool
     QIBM_QNS_CRADDACT     ADDA0100     *YES     Add CRQ description activity
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     Change CRQ description activi
```

Use the same method for evaluating these exit programs that you use for other exit programs and trigger programs.

Checking Scheduled Programs

AS/400 provides several methods for scheduling jobs to run at a later time, including the job scheduler and the OfficeVision for OS/400 calendar. Normally, these methods do not represent a security exposure because the user who schedules the job must have the same authority that is required to submit the job to batch.

However, you should periodically check for jobs scheduled in the future. A disgruntled user who is no longer in the organization may use this method to schedule a disaster.

Restricting Save and Restore Capability

Most users do not need to save and restore objects on your system. The save commands provide the possibility of copying important assets of your organization to media or to another system. Most save commands support save files that can be sent to another system (by using the SNDNETF file command) without having access to media or a save/restore device.

Restore commands provide the opportunity to restore unauthorized objects, such as programs, commands, and files, to your system. You can also restore information without access to media or to a save/restore device by using save files. Save files can be sent from another system by using the SNDNETF command or by using the FTP function.

Following are suggestions for restricting save and restore operations on your system:

- Control which users have *SAVSYS special authority. *SAVSYS special authority allows the user to save and restore objects even when the user does not have the necessary authority to the objects.
- Control physical access to save and restore devices (tape units).
- Restrict access to the save and restore commands. These commands ship with the public authority set to *USE. Consider changing the public authority to *EXCLUDE.
- Use the QALWOBJRST system value to restrict restoration of system-state programs and programs that adopt authority.
- Use security auditing to monitor restore operations. Include *SAVRST in the QAUDLVL system value, and periodically print audit records that are created by restore operations. (Chapter 9 and Appendix F of the *Security – Reference* book provide more information about the audit entries operations.)

Checking for User Objects in Protected Libraries

Every AS/400 job has a library list. The library list determines the sequence in which the system searches for an object if a library name is not specified with the object name. For example, when you call a program without specifying where the program is, the system searches your library list in order and runs the first copy of the program that it finds.

The *Security – Reference* provides more information about the security exposures of library lists and calling programs without a library name (called an **unqualified call**). It also provides suggestions for controlling the content of library lists and the ability to change the system library lists.

For your system to run properly, certain system libraries, such as QSYS and QGPL, must be in the library list for every job. You should use object authority to control who can add programs to these libraries. This helps to prevent someone from placing an imposter program in one of these libraries with the same name as a program that appears in a library later in the library list.

You should also evaluate who has authority to the CHGSYSLIBL command and monitor SV records in the security audit journal. A devious user could place a library ahead of QSYS in the library list and cause other users to run unauthorized commands with the same names as IBM-supplied commands.

SECBATCH menu options:
19 *to submit immediately*
38 *to use the job scheduler*

If you have the Security ToolKit, you can use the Print User Objects (PRTUSROBJ) command to print a list of user objects (objects not created by IBM) that are in a specified library. You can then evaluate the programs on the list to determine who created them and what function they perform.

User objects other than programs can also represent a security exposure when they are in system libraries. For example, if a program writes confidential data to a file whose name is not qualified, that program might be fooled into opening an imposter version of that file in a system library.

Figure 8-6 shows an example of the report:

User Objects (Full Report)

Library	Object	Type	Attribute	Owner	Description
QSYS	PRTCUSTL	*PGM	RPG	GEORGE	
QSYS	CHGLMT	*PGM	RPG	GEORGE	
QSYS	TESTINV	*PGM	CLP	ROSE	

Figure 8-6. Print User Objects Report–Sample

Note: This report includes objects that the system places in the library either when you install a licensed program or when a PTF exit program creates objects.

Chapter 9. More Tips for Preventing and Detecting Mischief

This chapter is a collection of miscellaneous tips to help you to detect potential security exposures and mischief-makers.

Tips for Physical Security

Your system unit represents an important business asset and a potential door into your system. Some system components inside the system are both small and valuable. You should place the system unit in a controlled location to prevent someone from removing valuable system components.

The system unit has a control panel that provides the ability to perform basic functions without a workstation. For example, you can use the control panel to do the following:

- Stop the system.
- Start the system.
- Load the operating system.
- Start service functions.

All of these activities can disrupt your system users. They also represent a potential security exposure to your system. You can use the keylock that comes with your system to control when these activities are allowed. To prevent the use of the control panel, place the keylock in the Secure position, remove the key, and store it in a safe place.

Notes:

1. If you need to perform remote IPLs or perform remote diagnostics on your system, you may need to choose another setting for the keylock. The *System Startup and Problem Handling* book provides more information about the keylock settings.
2. Not all system models come with a keylock as a standard feature.

Tips for Monitoring Subsystem Descriptions

When you start a subsystem on AS/400, the system creates an environment for work to enter the system and run. A subsystem description defines what that environment looks like. Subsystem descriptions, therefore, can provide an opportunity for devious users. A mischief-maker might use a subsystem description to start a program automatically or to make it possible to sign on without a user profile.

When you run the Revoke Public Authority (RVKPUBAUT) command that is part of the Security ToolKit, the system sets public authority to subsystem description commands to *EXCLUDE. This prevents users who are not specifically authorized (and who do not have *ALLOBJ special authority) from changing or creating subsystem descriptions.

The topics that follow provide suggestions for reviewing the subsystem descriptions that currently exist on your system. You can use the Work with Subsystem Descriptions (WRKSBSD) command to create a list of all the subsystem

descriptions. When you select 5 (Display) from the list, you see a menu like the one shown in Figure 9-1 for the system description that you selected. It shows a list of the parts of a subsystem environment.

```
                        Display Subsystem Description

Subsystem description:   QINTER         Library:   QSYS
Status:   ACTIVE

Select one of the following:

     1. Operational attributes
     2. Pool definitions
     3. Autostart job entries
     4. Work station name entries
     5. Work station type entries
     6. Job queue entries
     7. Routing entries
     8. Communications entries
     9. Remote location name entries
    10. Prestart job entries
```

Figure 9-1. Display Subsystem Description Display

You select options to see details about the parts. Use the Change Subsystem Description (CHGSBSD) command to change the first two items on the menu. To change other items, use the appropriate add, remove, or change command for the entry type. For example, to change a workstation entry, use the Change Workstation Entry (CHGWSE) command.

The *Work Management* book provides more information about working with subsystem descriptions. It also lists the shipped values for IBM-supplied subsystem descriptions.

Tips for Autostart Job Entries

An autostart job entry contains the name of a job description. The job description may contain request data (RQSDTA) that causes a program or a command to run. For example, the RQSDTA might be `CALL LIB1/PROGRAM1`. Whenever the subsystem starts, the system will run the program PROGRAM1 in library LIB1.

Look at your autostart job entries and the associated job descriptions. Ensure that you understand the function of any program that runs automatically when a subsystem starts.

Tips for Workstation Names and Workstation Types

When a subsystem starts, it allocates all unallocated workstations that are listed (specifically or generically) in its entries for workstation names and workstations types. When a user signs on, the user is signing on to the subsystem that has allocated the workstation.

The workstation entry tells what job description will be used when a job starts at that workstation. The job description may contain request data that causes a program or a command to run. For example, the RQSDTA parameter might be `CALL LIB1/PROGRAM1`. Whenever a user signs on to a workstation in that subsystem, the system will run PROGRAM1 in LIB1.

Look at your workstation entries and the associated job descriptions. Ensure that no one has added or updated any entries to run programs that you are not aware of.

A workstation entry might also specify a default user profile. For certain subsystem configurations, this allows someone to sign on simply by pressing the Enter key. If the security level (QSECURITY system value) on your system is less than 40, you should review your workstation entries for default users.

Tips for Job Queue Entries

When a subsystem starts, it allocates any unallocated job queues that are listed in the subsystem description. Job queue entries do not provide any direct security exposure. However, they do provide an opportunity for someone to tamper with system performance by causing jobs to run in unintended environments.

You should periodically review the job queue entries in your subsystem descriptions to ensure that batch jobs are running where you expect them to run.

Tips for Routing Entries

A routing entry defines what a job does once it enters the subsystem. The subsystem uses routing entries for all job types: batch, interactive, and communications jobs. A routing entry specifies the following:

- The class for the job. Like job queue entries, the class that is associated with a job can affect its performance but does not represent a security exposure.
- The program that runs when the job starts. Look at the routing entries and ensure that no one has added or updated any entries to run programs that you are not aware of.

Tips for Communications Entries and Remote Location Names

When a communications job enters your system, the system uses the communications entries and the remote location name entries in the active subsystem to determine how the communications job will run. Look at the following for these entries:

- All subsystems are capable of running communications jobs. If a subsystem that you intend for communications is not active, a job that is trying to enter your system might find an entry in another subsystem description that meets its needs. You need to look at the entries in all subsystem descriptions.
- A communications entry contains a job description. The job description may contain request data that runs a command or program. Look at your communications entries and their associated job descriptions to ensure that you understand how jobs will start.
- A communications entry also specifies a default user profile that the system uses in some situations. Make sure that you understand the role of default profiles. If your system contains default profiles, you should ensure that they are profiles with minimal authority. See Chapter 3, "Tips for Securing APPC Communications" for more information about default user profiles.

  If you have the Security ToolKit, you can use the Print Subsystem Description (PRTSBSDAUT) command to identify communications entries that specify a user profile name.

Tips for Prestart Job Entries

You can use prestart job entries to make a subsystem ready for certain kinds of jobs so that the jobs start more quickly. Prestart jobs may start when the subsystem starts or when they are needed. A prestart job entry specifies the following:

A program to run
A default user profile
A job description

All of these provide the potential for security exposures. You should make sure that prestart job entries perform only authorized, intended functions.

Tips for Jobs and Job Descriptions

Job descriptions contain request data and routing data that can cause a specific program to run when that job description is used. When the job description specifies a program in the request data parameter, the system runs the program. When the job description specifies routing data, the system runs the program that is specified in the routing entry that matches the routing data.

The system uses job descriptions for both interactive and batch jobs. For interactive jobs, the workstation entry specifies the job description. Typically, the workstation entry value is *USRPRF, so the system uses the job description that is specified in the user profile. For batch jobs, you specify the job description when you submit the job.

You should periodically review job descriptions to make sure that they do not run unintended programs. You should also use object authority to prevent changes to job descriptions. *USE authority is sufficient to run a job with a job description. A typical user does not need *CHANGE authority to job descriptions.

SECBATCH menu options:
9 *to submit immediately*
38 *to use the job scheduler*

Job descriptions can also specify what user profile the job should run under. With security level 40 and higher, you must have *USE authority to the job description and to the user profile that is specified in the job description. With security levels lower than 40, you need *USE authority only to the job description.

If you have the Security ToolKit, you can use the Print Job Description Authority (PRTJOBDAUT) command to print a list of job descriptions that specify user profiles and have public authority of *USE. Figure 9-2 shows an example of the report:

```
                        Job Descriptions with Excess Authority (Full Report)
5799XDJ V3R1M0  960115                                                                  SYSTEM4
 Specified library . . . . . :   QGPL
                                                    -------------------Special Authorities----------------------
                Job                     User        *ALL   *AUD    *IOSYS    *JOB    *SAV    *SEC    *SER    *SPL
 Library        Description     Owner   Profile      OBJ    IT       CFG      CTL     SYS     ADM     VICE     CTL
 QGPL           JOBD1           QSECOFR USERA
 QGPL           JOBD2           QSECOFR USERB        X      X        X        X       X       X       X        X
```

Figure 9-2. Job Descriptions with Excess Authority Report–Example

The report shows the special authorities of the user profile that is specified in the job description. The report includes the special authorities of any group profiles that the user profile has. You can use the following command to to display the user profile's private authorities:

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

The job description specifies the library list that the job uses when it runs. If someone can change a user's library list, that user might run an unintended version of a program in a different library. You should periodically review the library lists that are specified in the job descriptions on your system.

Finally, you should ensure that the default values for the Submit Job (SBMJOB) command and the Create User Profile (CRTUSRPRF) command have not been changed to point to unintended job descriptions.

Tips for Architected Transaction Program Names

Some communications requests send a specific type of signal to your system. This request is called an **architected transaction program name (TPN)** because the name of the transaction program is part of the APPC architecture for the system. A request for display station pass-through request is an example of an architected TPN. Architected TPNs are a normal way for communications to function and do not necessarily represent a security exposure. However, architected TPNs may provide an unexpected entrance into your system.

Some TPNs do not pass a profile on the request. If the request becomes associated with a communications entry whose default user is *SYS, the request may be initiated on your system. However, the *SYS profile can run system functions only, not user applications.

If you do not want architected TPNs to run with a default profile, you can change the default user from *SYS to *NONE in communications entries. Table A-2 on page A-3 lists the architected TPNs and the associated user profiles.

If you do not want a specific TPN to run on your system at all, do the following:

1. Create a CL program that accepts several parameters. The program should perform no function. It should simply have the Declare (DCL) statements for parameters and then end.
2. Add a routing entry for the TPN to each subsystem that has communications entries or remote location name entries. The routing entry should specify the following:
   - A *Compare value* (CMPVAL) value equal to the program name for the TPN (see Table A-2) with a starting position of 37.
   - A *Program to call* (PGM) value equal to the name of the program that you created in step 1. This prevents the TPN from locating another routing entry, such as *ANY.

Several TPNs already have their own routing entry in the QCMN subsystem. These have been added for performance reasons.

Methods for Monitoring Security Events

Setting up security is not a one-time effort. You need to constantly evaluate both the changes on your system and your security failures. Then make adjustments to your security environment to respond to what you have discovered.

The reports that are part of the Security ToolKit help you monitor changes that occur on your system that are relevant to security. Following are other system functions that you can use to help you to detect security failures or exposures:

- Security auditing is a powerful tool that you can use to observe many different types of security-relevant events that occur on your system. For example, you can set up the system to write an audit record every time a user opens a particular database file for updating. You can audit all changes to system values. You can audit actions that happen when objects are restored.

  Chapter 9 in the *Security – Reference* book provides complete information about the security auditing function. If you have the Security ToolKit, you can use the Change Security Auditing (CHGSECAUD) command to set up security auditing on your system. You can also use the Print Audit Record Report (PRTAUDRPT) command to print selected information from the security audit journal.

- You can create the QSYSMSG message queue to capture critical system-operator messages. The QSYSOPR message queue receives many messages of varying importance throughout a typical business day. Critical, security-relevant messages may be overlooked because of the sheer volume of messages in the QSYSOPR message queue.

  If you create a QSYSMSG message queue in the QSYS library on your system, the system automatically directs certain critical messages to the QSYSMSG message queue instead of to the QSYSOPR message queue.

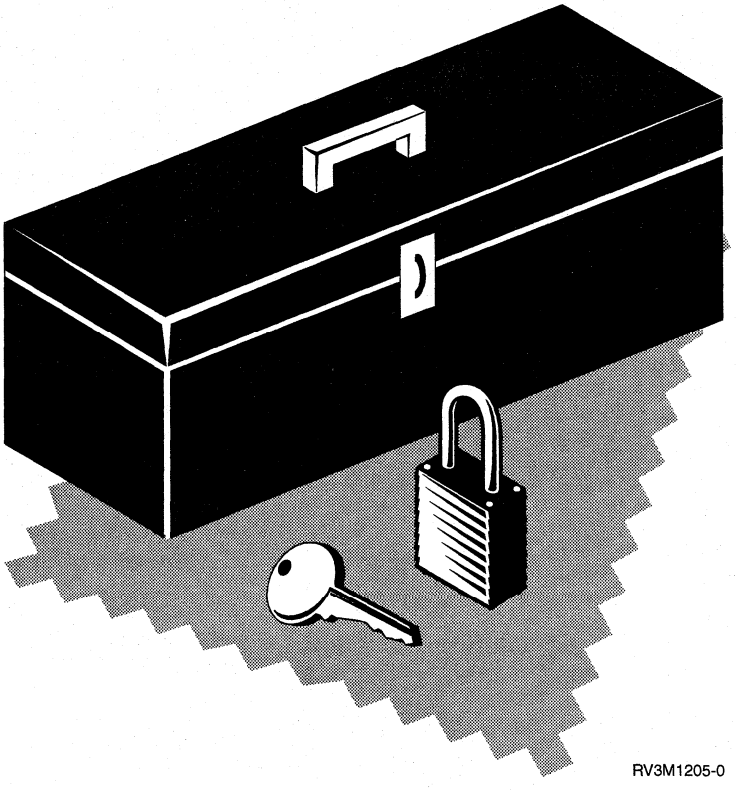
  Either you can create a program to monitor the QSYSMSG message queue, or you can assign it in break mode to yourself or to another trusted user.

Security Tools

Man is a tool-using animal... Without tools he is nothing,
with tools he is all.
Thomas Carlyle

OS/400 provides an integrated set of security functions. Security ToolKit for OS/400 provides additional commands and programs to help you use AS/400 security functions more effectively.

You will find examples of how to use the tools throughout this booklet. This part of the booklet describes how to order and install the Security ToolKit and the security PTF package.



RV3M1205-0

Chapter 10. How to Order and Install the Tools and PTFs

This chapter describes how to order and install Security ToolKit for OS/400 and the security program temporary fix (PTF) package. Many of the recommendations in this booklet assume that you have the Security ToolKit for OS/400 and the security PTF (program temporary fix) package.

Ordering the Security ToolKit and Security PTFs

Table 10-1 provides ordering information. Security ToolKit for OS/400 is a PRPQ. Contact your IBM representative for information about ordering. Before you install the Security ToolKit, you should install the prerequisite PTFs for your release. These PTFs are required for some of the new Security ToolKit commands to run properly.

The security PTF package is included as part of the latest PTF package for all supported releases of OS/400. You can order the security PTF package separately by using your normal method for ordering PTFs. The first PTF number listed in Table 10-1 for each version is the main or umbrella PTF number. When you order the umbrella PTF, you receive other corequisite PTFs. You do not need the security PTF package for the Security ToolKit commands to run, but you should install the PTF package because it provides additional protection for your system.

Table 10-1 (Page 1 of 2). Ordering Information for Security Tools and PTFs

Release	Security ToolKit Program Number	Prerequisite PTFs for the Security ToolKit	Security PTF Package
V2R2	Not available	Not available	SF24390[1] SF24430 SF24424 SF24429 SF24438 SF24452
V2R3	5799-XDH	SF27682 MF10999	SF23874[1] SF24431 SF24425 SF24233 SF24229 SF24453
V3R0M5	5799-XDH	SF27683 MF11000	SF23873[1] SF24432 SF24426 SF24232 SF24230 SF24455
V3R1	5799-XDJ	SF27685 MF11001	SF23871[1] SF24433 SF24427 SF24228 SF24231 SF24456

Table 10-1 (Page 2 of 2). Ordering Information for Security Tools and PTFs			
Release	**Security ToolKit Program Number**	**Prerequisite PTFs for the Security ToolKit**	**Security PTF Package**
V3R6	5799-XDK	SF27681 MF11019	See note 2

1 When you order this PTF, you will receive all the other security PTFs that are listed for that release. However, you must install each of the PTFs individually. See the *PTF Shipping Information Letter* for installation instructions.

2 The content of the security PTF package is included in V3R6 of OS/400.

Installing the Security PTF Package

If you are installing the PTFs as part of a cumulative PTF package, use the normal procedures for installing PTFs. If you are installing the security PTFs individually, you must install all the associated PTFs, not just the umbrella PTF that you ordered. The cover letter that arrived with the PTFs lists all of the corequisite PTFs that you should install.

When you apply the PTFs, the system makes changes to the public authority to objects that may affect your system operations. Following are the changes:

- Public authority for the following commands is changed from *USE to *EXCLUDE. For systems that are running V3R1 or a later version, these commands are also changed to require *IOSYSCFG special authority.

  CRTDEVAPPC (Create Device Description (APPC))
  CHGDEVAPPC (Change Device Description (APPC))
  ADDCFGLE (Add Configuration List Entry)
  CHGCFGLE (Change Configuration List Entry)
  RMVCFGLE (Remove Configuration List Entry)
  CRTCFGL (Create Configuration List)
  CHGCFGL (Change Configuration List)
  CPYCFGL (Copy Configuration List)
  DLTCFGL (Delete Configuration List)
  WRKCFGL (Work with Configuration List)

- Public authority for the QCPFMSG message file is changed from *CHANGE to *USE.
- *OBJMGT and *CHANGE authority are required to change a device description. Before installing the security PTF package, only *CHANGE authority is required.

Installing Security ToolKit for OS/400

To install the Security ToolKit, do the following:

__ **Step 1** Mount the media (tape or CD-ROM) that contains the Security ToolKit program in the appropriate device.

__ **Step 2** Sign on the system as QSECOFR.

__ **Step 3** Type `RSTLICPGM` and press F4 (Prompt). You see the Restore Licensed Program (RSTLICPGM) display:

```
                    Restore Licensed Program (RSTLICPGM)

Type choices, press Enter.

Product  . . . . . . . . . . . . LICPGM
Device . . . . . . . . . . . . . DEV
                          + for more values
Optional part to be restored . . OPTION         *BASE
Type of object to be restored  . RSTOBJ         *ALL
Language for licensed program  . LNG            *PRIMARY
Output . . . . . . . . . . . . . OUTPUT         *NONE
Release  . . . . . . . . . . . . RLS            *FIRST
Replace release  . . . . . . . . REPLACERLS     *ONLY
```

__ **Step 4** For the product (LICPGM) field, type the program number for your release of the operating system. (See Table 10-1 on page 10-1 or the label on your media.)

__ **Step 5** For the device (DEV) field, type the name of your tape or CD-ROM device.

__ **Step 6** For the *Language for licensed program* (LNG) field, type one of the following values:

Language Feature	Description
2924	English uppercase and lowercase
2950	English uppercase
2938	English uppercase support for (double-byte character set (DBCS)
2984	English uppercase and lowercase support for DBCS

__ **Step 7** Press the Enter key. When the RSTLICPGM command completes, you should receive a confirmation message that the program installed successfully. If the program does not install correctly, follow the procedure in "Resolving Installation Problems" on page 10-4.

Security ToolKit Objects

When you install the Security ToolKit for OS/400 product, the following occurs:

- The system creates the QSECUSR user profile.
- The system installs the QSECLIB product library.
- The system creates the QSECOUTQ output queue in the QSECLIB library.
- If the primary language on your system is different from the language that you select when you install the Security ToolKit, the system places the online information for the Security ToolKit in the QSYS29xx library. For example, if you select language feature 2924 (English uppercase and lowercase), the system places the online information in the QSYS2924 library.

Resolving Installation Problems

If you receive a message from the RSTLICPGM command that the program did not install correctly, use normal procedures to diagnose and resolve the problem that caused the failure. Review the job log for the installation job and contact software support for assistance, if necessary.

When you have resolved the problem, do the following:

__ **Step 1** Delete any parts of the Security ToolKit that are on the system by doing the following:

- __ **Step a.** Type `DLTLICPGM` and press F4 (Prompt).
- __ **Step b.** On the Delete Licensed Program (DLTLICPGM) display, type the PRPQ number for the *Product* parameter. (See Table 10-1 on page 10-1 or the label on your media.)
- __ **Step c.** For the *Option* parameter, type `*ALL`.
- __ **Step d.** Press the Enter key and wait for the confirmation message.

__ **Step 2** Delete the QSECLIB library (if it still exists), by typing `DLTLIB QSECLIB` and pressing the Enter key. The system will delete the Security ToolKit library.

Note: If you receive the message `QSECLIB not found`, ignore the message. Either the system did not get far enough in the installation procedure to create the library, or the DLTLICPGM command deleted the library already.

__ **Step 3** Repeat the installation procedures in the topic "Installing Security ToolKit for OS/400" on page 10-2.

Getting Started with the Security ToolKit

The Security ToolKit is ready to use immediately after you install it. The topics that follow provide suggestions for operating procedures with the Security ToolKit.

Securing the Security ToolKit

When the system installs the Security ToolKit, the objects that are associated with the Security ToolKit are secure. To operate the Security ToolKit securely, avoid making authority changes to any Security ToolKit objects.

Following are the security settings and requirements for Security ToolKit objects:

- The Security ToolKit programs and commands are in the QSECLIB product library. The commands, the programs, and the QSECLIB library itself ship with the public authority of *EXCLUDE. Many of the Security ToolKit reporting commands create files in the QSECLIB library. These files might contain confidential information about your system. Therefore, you should not change the public authority to the QSECLIB library.
- The Security ToolKit commands create the following files in the QUSRSYS library:

  QASECACT

QASECEXP
QASECIDL

The public authority for these files is set to *EXCLUDE. Because these files affect how your system manages user profiles, you should not change the public authority for these files.

- The Security ToolKit commands use the QSECOUTQ output queue in the QSECLIB library. The public authority for the output queue is *EXCLUDE. Users with *JOBCTL special authority are not permitted to view or manipulate any spooled files on the output queue. You should not change the security settings for this output queue.
- Because of their security functions and because they access many objects on the system, the Security ToolKit commands require *ALLOBJ special authority. Some of the commands also require *SECADM, *AUDIT, or *IOSYSCFG special authority. To ensure that the commands run successfully, you should sign on as a security officer when you use the Security ToolKit. Therefore, you should not need to grant private authority to any commands in the library.

Accessing the Security ToolKit

To ensure that the Security ToolKit commands run properly and find the objects that they need, you must have the QSECLIB library in your library list when you run the commands or use the menus. You can either create a special job description or use the Add Library List Entry (ADDLIBLE) command.

Using a Job Description: The easiest way to access the Security ToolKit is to create a job description for yourself that includes the QSECLIB library in the initial library list (INLLIBL) parameter. Make sure that the public authority for the job description is *EXCLUDE.

Note: If the primary language on your system is not one of the Security ToolKit language features, you also need to add the QSYS29xx library that contains the online information to your library list. (See "Security ToolKit Objects" on page 10-3.)

Change the job description (JOBD) parameter in your user profile to use the new job description. Then sign off and sign on again to associate the new job description with your job.

To access the Security ToolKit, type `GO SECTOOLS` or `GO SECBATCH`. (Chapter 11 describes these menus.)

Using the ADDLIBLE Command: If you use the Security ToolKit only occasionally, you can use the Add Library List Entry (ADDLIBLE) command rather than create a special job description. To access Security ToolKit, type the following:

```
ADDLIBLE QSECLIB
GO SECTOOLS or
GO SECBATCH
```

Note: If the primary language on your system is not one of the Security ToolKit language features, you also need to add the QSYS29xx library that contains the online information to your library list. For example, if you selected feature 2924, type `ADDLIBLE QSYS2924`. (See "Security ToolKit Objects" on page 10-3.)

Avoiding File Conflicts

Many of the Security ToolKit report commands create a database file that you can use to print a changed version of the report. (Chapter 11 tells the file name for each command.) To avoid unpredictable results in your reports, only one job should run a specific command at a time.

Many print jobs are long-running jobs. You need to be careful to avoid file conflicts when you submit reports to batch or add them to the job scheduler. For example, you might want to print two versions of the PRTUSRINF report with different selection criteria. If you are submitting reports to batch, you should use a job queue that runs only one job at a time to ensure that the report jobs run sequentially.

If you are using the job scheduler, you need to schedule the two jobs far enough apart that the first version completes before the second job starts.

Saving the Security ToolKit

You can use the Save Licensed Program (SAVLICPGM) command to save your initial copy of the Security ToolKit after you install it. After installation, you should save the Security ToolKit as part of your regular operating procedures.

The QSECLIB library is an IBM-supplied library. It contains your Security ToolKit programs and commands. It also contains the QSECOUTQ output queue and the files to produce changed versions of the printed reports.

The system saves the QSECLIB library when you use any of the following:

- The SAVLIB *NONSYS command.
- The SAVLIB *IBM command.
- Any option from the Save menu that saves IBM-supplied libraries, such as option 21 (Entire system) or option 22 (System data only).

The following files that are in the QUSRSYS library help you manage user profiles:

QASECACT
QASECEXP
QASECIDL

You should already be saving the QUSRSYS library regularly by using one of the following:

- The SAVLIB *ALLUSR command.
- The SAVLIB LIB(QUSRSYS) command.
- Any option from the Save menu that saves the QUSRSYS library, such as option 21 (Entire system) or option 23 (All user data).

Chapter 11. Security ToolKit for OS/400 Commands and Menus

This chapter describes the Security ToolKit commands and menus. Examples of how to use the commands are included throughout this booklet.

Security ToolKit provides two menus:

- The SECTOOLS (Security Tools) menu to run Security ToolKit commands interactively.
- The SECBATCH (Submit or Schedule Security Reports to Batch) menu to run the Security ToolKit report commands in batch. The SECBATCH menu has two parts. The first part of the menu uses the Submit Job (SBMJOB) command to submit reports for immediate processing in batch.

  The second part of the menu uses the Add Job Schedule Entry (ADDJOBSCDE) command. You use it to schedule security reports to be run regularly at a specified day and time.

Options on the Security Tools Menu

Following is the part of the SECTOOLS menu that relates to user profiles. To access this menu, type `GO SECTOOLS`

Note: You must have the QSECLIB library in your library list. If the primary language on your system is not one of the Security ToolKit languages, you must also have the appropriate QSYS29xx libraries in your library list.

```
SECTOOLS                          Security Tools

Select one of the following:

  Work with profiles
     1. Check profiles for default passwords

     2. Display active profile list
     3. Change active profile list
     4. Process inactive profiles

     5. Display activation schedule
     6. Schedule profile activation

     7. Display expiration schedule
     8. Schedule profile expirations
```

Table 11-1 describes these menu options and the associated commands:

Table 11-1 (Page 1 of 2). Security ToolKit Commands for User Profiles

Option on the SECTOOLS Menu	Command Name	Description	Database File Used
1	CHKDFTPWD	Use the Check Default Passwords command to report on and take action on user profiles that have a password equal to the user profile name.	QSECPWDF[1]
2	DSPACTPRFL	Use the Display Active Profile List command to display or print the list of user profiles that are exempt from PRCINACTPRF processing.	QASECIDL[2]
3	CHGACTPRFL	Use the Change Active Profile List command to add and remove user profiles from the exemption list for the PRCINACPRF command. A user profile that is on the active profile list is permanently active (until you remove the profile from the list). The PRCINACPRF command does not disable a profile that is on the active profile list, no matter how long the profile has been inactive.	QASECIDL[2]
4	PRCINACPRF	Use the Process Inactive Profiles command to disable user profiles that have not been used for a specified number of days. After you use the PRCINACPRF command to specify the number of days, the system runs the PRCINACPRF job once per week during the night. You can use the CHGACTPRFL command to exempt user profiles from being disabled.	QASECIDL[2]
5	DSPACTSCD	Use the Display Profile Activation Schedule command to display or print information about the schedule for enabling and disabling specific user profiles. You create the schedule with the SCDPRFACT command.	QASECDIS[2]
6	SCDPRFACT	Use the Schedule Profile Activation command to make a user profile available for sign on only at certain times of the day or week. For each user profile that you schedule, the system creates job schedule entries for the enable and disable times.	QASECDIS[2]
7	DSPEXPSCD	Use the Display Expiration Schedule command to display or print the list of user profiles that are scheduled to be disabled or removed from the system in the future. You use the SCDPRFEXP command to set up user profiles to expire.	QASECEXP[2]

Table 11-1 (Page 2 of 2). Security ToolKit Commands for User Profiles

Option on the SECTOOLS Menu	Command Name	Description	Database File Used
8	SCDPRFEXP	Use the Schedule Profile Expiration command to schedule a user profile for removal. You can remove it temporarily (by disabling it) or you can delete it from the system. This command uses a job schedule entry that runs every day at 00:01 (1 minute after midnight). The job looks at the QASECEXP file to determine whether any user profiles are set up to expire on that day. Use the DSPEXPSCD command to display the user profiles that are scheduled to expire.	QASECEXP[2]

[1] This file is in the QSECLIB library.

[2] This file is in the QUSRSYS library.

You can page down on the menu to see additional options. Table 11-2 describes the menu options and associated commands for security auditing:

Table 11-2. Security ToolKit Commands for Security Auditing

Option on the SECTOOLS Menu	Command Name	Description	Database File Used
10	CHGSECAUD	Use the Change Security Auditing command to set up security auditing and to change the system values that control security auditing. When you run the CHGSECAUD command, the system creates the security audit (QAUDJRN) journal if it does not exist. The CHGSECAUD command provides options that make it simpler to set the QAUDLVL (audit level) system value. You can specify *ALL to activate all of the possible audit level settings. Or, you can specify *DFTSET to activate the most commonly used settings (*AUTFAIL, *CREATE, *DELETE, *SECURITY, and *SAVRST).	
11	DSPSECAUD	Use Display Security Auditing command to display information about the security audit journal and the system values that control security auditing.	

How to Use the Security Batch Menu

Following is the first part of the SECBATCH menu:

```
SECBATCH          Submit or Schedule Security Reports To Batch
                                                          System:
Select one of the following:

  Submit Reports to Batch
     1. Adopted object information
     2. Audit record report
     3. Authorization list authorities
     4. Command authority
     5. Communications information
     6. Document authority
     7. File authority
     8. Folder authority
     9. Job description authority
    10. Library authority
    11. Object authority
    12. Private authority
    13. Program authority
```

When you select an option from this menu, you see the Submit Job (SBMJOB) display, such as the following:

```
                              Submit Job (SBMJOB)

Type choices, press Enter.

Command to run . . . . . > PRTADPINF USRPRF(*ALL)
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
                                                                          ...
Job name . . . . . *JOBD          Name, *JOBD
Job description  . . . . . *USRPRF      Name, *USRPRF
  Library  . . . . . .                  Name, *LIBL, *CURLIB
Job queue  . . . . . *JOBD        Name, *JOBD
  Library  . . . . . .                  Name, *LIBL, *CURLIB
Job priority (on JOBQ) . . . . *JOBD      1-9, *JOBD
Output priority (on OUTQ)  . . *JOBD      1-9, *JOBD
Print device . . . . . *CURRENT   Name, *CURRENT, *USRPRF...
```

If you want to change the default options for the command, you can press F4 (Prompt) on the *Command to run* line.

You can page down to see the Schedule Batch Reports part of the menu. By using the options on this part of the menu, you can, for example, set up your system to run changed versions of reports regularly.

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                          System:
Select one of the following:

    14. Profile authority
    15. Queue authority
    16. Subsystem authority
    17. System security attributes
    18. Trigger programs
    19. User objects
    20. User profile information

    21. Check object integrity

  Schedule Batch Reports
    30. Adopted object information
    31. Audit record report
    32. Authorization list authorities
```

You can page down for additional menu options. When you select an option from this part of the menu, you see the Add Job Schedule Entry (ADDJOBSCDE) display:

```
                    Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . .                    Name, *JOBD
Command to run . . . . . > PRTADPINF USRPRF(*ALL)
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
                                                                  ...
Frequency . . . . . .                   *ONCE, *WEEKLY, *MONTHLY
Schedule date, or . . . . . *CURRENT    Date, *CURRENT, *MONTHST
Schedule day . . . . . *NONE            *NONE, *ALL, *MON, *TUE.
             + for more values
Schedule time . . . . . *CURRENT        Time, *CURRENT
```

You can position your cursor on the *Command to run* line and press F4 (Prompt) to choose different settings for the report. You should assign a meaningful job name so that you can recognize the entry when you display the job schedule entries.

Options on the Security Batch Menu

Table 11-3 on page 11-6 describes the menu options and associated commands for security reports. The menu options on your system may differ slightly because some menu options are not available on every version of OS/400.

When you run security reports, the system prints only information that meets the selection criteria and is relevant to security. For example, job descriptions are relevant to security if they specify a user profile name. Therefore, the job description (PRTJOBDAUT) report prints job descriptions in the specified library only if the public authority for the job description is not *EXCLUDE and if the job description specifies a user profile name in the USER parameter.

Similarly, when you print subsystem information (PRTSBSDAUT command), the system prints information about a subsystem only when the subsystem description has a communications entry that specifies a user profile.

If a particular report prints less information than you expect, consult the online help information to find out the selection criteria for the report.

Table 11-3 (Page 1 of 5). Security ToolKit Commands for Security Reports

Option on the SECBATCH Menu	Command Name	Description	Database File Used
1, 30	PRTADPINF	Use the Print Adopted Object Information command to print a list of objects that adopt the authority of the specified user profile. You can specify a single profile, a generic profile name (such as all profiles that begin with Q), or all user profiles on the system. This report has two versions. The full report lists all adopted objects that meet the selection criteria. The changed report lists differences between adopted objects that are currently on the system and adopted objects that were on the system the last time that you ran the report.	QSECADPOLD[1]
2, 31	PRTAUDRPT	Use the Print Audit Record Report command to display or print information about entries in the security audit journal. You can select specific entry types, specific users, and a time period.	QASYxxJE[2]
3, 32	PRTPVTAUT *AUTL	When you use the Print Private Authorities command for *AUTL objects, you receive a list of all the authorization lists on the system. The report includes the users who are authorized to each list and what authority the users have to the list. Use this information to help you analyze sources of object authority on your system. This report has three versions. The full report lists all authorization lists on the system. The changed report lists additions and changes to authorization since you last ran the report. The deleted report lists users whose authority to the authorization list has been deleted since you last ran the report. When you print the full report, you have the option to print a list of objects that each authorization list secures. The system will create a separate report for each authorization list.	QSECATLOLD[1]

Table 11-3 (Page 2 of 5). Security ToolKit Commands for Security Reports

Option on the SECBATCH Menu	Command Name	Description	Database File Used
5, 34	PRTCMNINF	Use the Print Communications Information command to print the security-relevant settings for objects that affect communications on your system. These settings affect how users and jobs can enter your system. This command produces two reports: a report that displays the settings for configuration lists on the system and a report that lists security-relevant parameters for line descriptions, controllers, and device descriptions. Each of these reports has a full version and a changed version.	QSECCMNOLD[1]
9, 38	PRTJOBDAUT	Use the Print Job Description Authority command to print a list of job descriptions that specify a user profile and have public authority that is not *EXCLUDE. The report shows the special authorities for the user profile that is specified in the job description. This report has two versions. The full report lists all job description objects that meet the selection criteria. The changed report lists differences between job description objects that are currently on the system and job description objects that were on the system the last time that you ran the report.	QSECJBDOLD[1]
See note 3	PRTPUBAUT	Use the Print Publicly Authorized Objects command to print a list of objects whose public authority is not *EXCLUDE. When you run the command, you specify the type of object and the library or libraries for the report. Use the PRTPUBAUT command to print information about objects that every user on the system can access. This report has two versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report.	QPBxxxxxx[4]

Table 11-3 (Page 3 of 5). Security ToolKit Commands for Security Reports

Option on the SECBATCH Menu	Command Name	Description	Database File Used
12, 41	PRTPVTAUT	Use the Print Private Authorities command to print a list of the private authorities to objects of the specified type in the specified library. Use this report to help you determine the sources of authority to objects. This report has three versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report. The deleted report lists users whose authority to an object has been deleted since you last printed the report.	QPVxxxxxx[4]
15, 44	PRTQAUT	Use the Print Queue Report to print the security settings for output queues and job queues on your system. These settings control who can view and change entries in the output queue or job queue. This report has two versions. The full report lists all output queue and print queue objects that meet the selection criteria. The changed report lists differences between output queue and print queue objects that are currently on the system and output queue and print queue objects that were on the system the last time that you ran the report.	QSECQOLD[1]
16, 45	PRTSBSDAUT	Use the Print Subsystem Description command to print the security-relevant communications entries for subsystem descriptions on your system. These settings control how work can enter your system and how jobs run. The report prints a subsystem description only if it has communications entries that specify a user profile name. This report has two versions. The full report lists all subsystem description objects that meet the selection criteria. The changed report lists differences between subsystem description objects that are currently on the system and subsystem description objects that were on the system the last time that you ran the report.	QSECSBDOLD[1]

Table 11-3 (Page 4 of 5). Security ToolKit Commands for Security Reports

Option on the SECBATCH Menu	Command Name	Description	Database File Used
17, 46	PRTSYSSECA	Use the Print System Security Attributes command to print a list of security-relevant system values and network attributes. The report shows the current value and the recommended value.	
18, 47	PRTTRGPGM[5]	Use the Print Trigger Programs command to print a list of trigger programs that are associated with database files on your system. This report has two versions. The full report lists every trigger program that is assigned and meets your selection criteria. The changed report lists trigger programs that have been assigned since the last time that you ran the report.	QSECTRGOLD[1]
19, 48	PRTUSROBJ	Use the Print User Objects report to print a list of the user objects (objects not supplied by IBM) that are in a library. You might use this report to print a list of user objects that are in a library (such as QSYS) that is in the system portion of the library list.	
20, 49	PRTUSRINF	Use the Print User Profile Information command to analyze user profiles that meet specified criteria. You can select user profiles based on special authorities, user class, or a mismatch between special authorities and user class. You can print authority information, environment information, or password information.	
21, 50	CHKOBJITG	Use the Check Object Integrity command to determine whether operable objects (such as programs) have been changed without using a compiler. This command can help you to detect attempts to introduce a virus program on your system or to change a program to perform unauthorized instructions. The *Security – Reference* book provides more information about the CHKOBJITG command.	

Table 11-3 (Page 5 of 5). Security ToolKit Commands for Security Reports

Option on the SECBATCH Menu	Command Name	Description	Database File Used

1 This file is in the QSECLIB library.

2 xx is the two-character journal entry type. For example, the model output file for AE journal entries is QSYS/QASYAEJE. The model output files are described in Appendix F of the *Security – Reference* book.

3 The SECTOOLS menu contains options for the object types that are typically of concern to security administrators. For example, options 7 and 36 run the PRTPUBAUT command for *FILE objects. Use the general options (11 and 30) to specify the object type.

4 The xxxxxxx in the name of the file is the object type. For example, the file for program objects is called QPBPGM for public authorities and QPVPGM for private authorities. The files are in the QSECLIB library.

The file contains a member for each library for which you have printed the report. The member name is the same as the library name.

5 This command is available only for V3R1 and later releases.

Security ToolKit Options for Customizing Security

Table 11-4 describes the Security ToolKit commands that you can use to customize the security on your system. These commands are on the SECTOOLS menu:

Table 11-4. Security ToolKit Commands for Customizing Your System

Option on the SECTOOLS Menu	Command Name	Description	Database File Used
50	CFGSYSSEC	Use the Configure System Security command to set security-relevant system values to their recommended settings. The command also sets up security auditing on your system."Values That Are Set by the Configure System Security Command" describes what the command does.	
51	RVKPUBAUT	Use the Revoke Public Authority command to set the public authority to *EXCLUDE for a set of security-sensitive commands on your system. "What the Revoke Public Authority Command Does" on page 11-13 lists the actions that the RVKPUBAUT command performs.	

Values That Are Set by the Configure System Security Command

Table 11-5 lists the system values that are set when you run the CFGSYSSEC command. The CFGSYSSEC command runs a program that is called QSECLIB/QSECCFGS.

Table 11-5 (Page 1 of 2). Values Set by the CFGSYSSEC Command

System Value Name	Setting	System Value Description
QAUTOCFG	0 (No)	Automatic configuration of new devices
QAUTOVRT	0	The number of virtual device descriptions that the system will automatically create if no device is available for use.
QDEVRCYACN	*DSCMSG (Disconnect with message)	System action when communications is re-established
QDSCJOBITV	120	Time period before the system takes action on a disconnected job
QDSPSGNINF	1 (Yes)	Whether users see the sign-on information display
QINACTITV	60	Time period before the system takes action on an inactive job

Table 11-5 (Page 2 of 2). Values Set by the CFGSYSSEC Command

System Value Name	Setting	System Value Description
QINACTMSGQ	*ENDJOB	Action that the system takes for an inactive job
QLMTDEVSSN	1 (Yes)	Whether users are limited to signing on at one device at a time
QLMTSECOFR	1 (Yes)	Whether *ALLOBJ and *SERVICE users are limited to specific devices
QMAXSIGN	3	How many consecutive, unsuccessful sign-on attempts are allowed
QMAXSGNACN	3 (Both)	Whether the system disables the workstation or the user profile when the QMAXSIGN limit is reached.
QRMTSIGN	*FRCSIGNON	How the system handles a remote (pass-through) sign-on attempt
QSECURITY	50	The level of security that is enforced
QPWDEXPITV	60	How often users must change their passwords
QPWDMINLEN	6	Minimum length for passwords
QPWDMAXLEN	8	Maximum length for passwords
QPWDPOSDIF	1 (Yes)	Whether every position in a new password must differ from the same position in the last password
QPWDLMTCHR	See note 1	Characters that are not allowed in passwords
QPWDLMTAJC	1 (Yes)	Whether adjacent numbers are prohibited in passwords
QPWDLMTREP	1 (Yes)	Whether repeating characters in are prohibited in passwords
QPWDRQDDGT	1 (Yes)	Whether passwords must have at least one number
QPWDVLDPGM	*NONE	The user exit program that the system calls to validate passwords

1 The restricted characters are stored in message ID SEC1DAB in the message file QSECLIB/QSECMSGF. They are shipped as `AEIOU@$#`. You can use the Change Message Description (CHGMSGD) command to change the restricted characters.

The CFGSYSSEC command also sets the password to *NONE for the following IBM-supplied user profiles:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

Finally, the CFGSYSSEC command sets up security auditing according to the values that you have specified by using the Change Security Auditing (CHGSECAUD) command.

Changing the Program: If some of these settings are not appropriate for your installation, you can create your own version of the program that processes the command. Do the following:

__ **Step 1** Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the CFGSYSSEC command. The program to retrieve is QSECLIB/QSECCFGS. When you retrieve it, give it a different name.

__ **Step 2** Edit the program to make your changes. Then compile it. When you compile it, make sure that you do not replace the IBM-supplied QSECLIB/QSECCFGS program. Your program should have a different name.

__ **Step 3** Use the Change Command (CHGCMD) command to change the program to process command (PGM) parameter for the CFGSYSSEC command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYSECCFG, you would type the following:

```
CHGCMD CMD(QSECLIB/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

Note: If you change the QSECLIB/QSECCFGS program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.

What the Revoke Public Authority Command Does

You can use the Revoke Public Authority (RVKPUBAUT) command to set the public authority to *EXCLUDE for a set of commands and programs. The RVKPUBAUT command runs a program that is called QSECLIB/QSECRVKP. As it is shipped, the QSECRVKP revokes public authority (by setting public authority to *EXCLUDE) for the commands that are listed in Table 11-6 on page 11-14 and the application programming interfaces (APIs) that are listed in Table 11-7 on page 11-14. When your system arrives, these commands and APIs have their public authority set to *USE.

The commands that are listed in Table 11-6 on page 11-14 and the APIs that are listed in Table 11-7 on page 11-14 all perform functions on your system that may provide an opportunity for mischief. As security administrator, you should explicitly authorize users to run these commands and programs rather than make them available to all system users.

When you run the RVKPUBAUT command, you specify the library that contains the commands. The default is the QSYS library. If you have more than one national language on your system, you need to run the command for each QSYSxxx library.

Table 11-6. Commands Whose Public Authority Is Set by the RVKPUBAUT Command

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

The APIs in Table 11-7 are all in the QSYS library:

Table 11-7. Programs Whose Public Authority Is Set by the RVKPUBAUT Command

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR

Changing the Program: If some of these settings are not appropriate for your installation, you can create your own version of the program that processes the command. Do the following:

__ **Step 1** Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the RVKPUBAUT command. The program to retrieve is QSECLIB/QSECRVKP. When you retrieve it, give it a different name.

__ **Step 2** Edit the program to make your changes. Then compile it. When you compile it, make sure that you do not replace the IBM-supplied QSECLIB/QSECRVKP program. Your program should have a different name.

__ **Step 3** Use the Change Command (CHGCMD) command to change the program to process command (PGM) parameter for the RVKPUBAUT command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYRVKPGM, you would type the following:

```
CHGCMD CMD(QSECLIB/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

Note: If you change the QSECLIB/QSECRVKP program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.

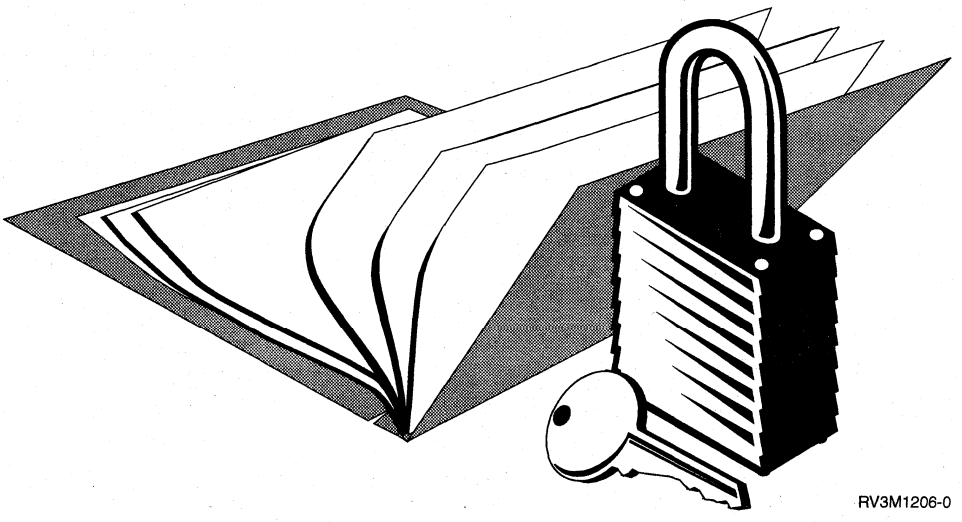
Additional Information

But the desire of knowledge, like the thirst of riches,
increases ever with the acquisition.
Laurence Sterne: Tristram Shandy

The only fence against the world is a thorough knowledge
of it.
John Locke: Some Thoughts Concerning Education

This booklet is only the beginning. Hackers are relentless in their pursuit of knowledge and information about potential loopholes in system security. As a AS/400 security administrator, you also need to pursue knowledge about your system. You need to increase your technical depth to match your potential opponents.

This booklet and the Security ToolKit point out many possible weaknesses and provide tips for strengthening your security. But don't stop there. Browse through some of the publications that are described in this part of the book. Find the topics that discuss security. Continue to build your knowledge of how someone might enter or compromise your system and how you can protect against it.



RV3M1206-0

Appendix A. Examples of Reports and Programs

This appendix provides additional information and examples.

System Security Attributes Report–Sample

Figure A-1 shows an example of the output from the Print System Security Attributes (PRTSYSSECA) command. The report shows the settings for security-relevant system values and network attributes that are recommended for systems with normal security requirements. It also shows the current settings on your system.

Note: The report shows that the recommended value for the QPWDRQDDIF system value is 1 because only values of 0 and 1 are available before V3R1. If your system is running V3R1 or a later release, the recommended setting is a number from 1 to 5.

```
                    System Security Attributes

System Value
Name                Current value          Recommended value
   QALWUSRDMN       *ALL                   QTEMP
   QATNPGM          QEZMAIN   QSYS         *NONE
   QAUDENDACN       *NOTIFY                *NOTIFY
   QAUDFRCLVL       *SYS                   *SYS
   QAUDCTL          *AUDLVL                *AUDLVL   *OBJAUD
   QAUDLVL          *SECURITY              *AUTFAIL  *CREATE
                                           *DELETE   *SECURITY
                                           *SAVRST

   QAUTOCFG         0                      0
   QAUTOVRT         9999                   0
   QCMNRCYLMT       0 0                    0 0
   QCRTAUT          *CHANGE                Control at library level.
   QCRTOBJAUD       *NONE                  Control at library level.
   QDEVRCYACN       *DSCMSG                *DSCMSG
   QDSCJOBITV       120                    120
   QDSPSGNINF       1                      1
   QINACTITV        60                     60
   QINACTMSGQ       *ENDJOB                *ENDJOB
   QLMTDEVSSN       0                      1
   QLMTSECOFR       0                      1
   QMAXSGNACN       2                      3
   QMAXSIGN         3                      3
```

Figure A-1 (Part 1 of 2). System Security Attributes Report–Sample

```
QPWDEXPITV      60                  60
QPWDLMTAJC      1                   1
QPWDLMTCHR      *NONE               AEIOU@$#
QPWDLMTREP      1                   1
QPWDMAXLEN      8                   8
QPWDMINLEN      6                   6
QPWDPOSDIF      1                   1
QPWDRQDDGT      1                   1
QPWDRQDDIF      0                   1
QPWDVLDPGM      *NONE               *NONE
QRMTIPL         0                   0
QRMTSIGN        *FRCSIGNON          *FRCSIGNON
QSECURITY       50                  50
QSRVDMP         *DMPUSRJOB          *NONE

                System Security Attributes

Network Attribute
Name            Current value       Recommended value
   DDMACC       *OBJAUT             *REJECT
   JOBACN       *FILE               *REJECT
   PCSACC       *OBJAUT             *REJECT
```

Figure A-1 (Part 2 of 2). System Security Attributes Report–Sample

Security Exit Programs

Some AS/400 functions provide an exit so that your system can run a user-created program to perform additional checking and validation. For example, you can set up your system to run an exit program every time that someone attempts to open a DDM (distributed data management) file on your system. Beginning with V3R1, you can use the registration function to specify exit programs that run under certain conditions.

Several AS/400 publications contain examples of exit programs that perform security functions. Table A-1 provides a list of these exit programs and where you can find the examples.

Table A-1 (Page 1 of 2). Sources of Sample Exit Programs

Type of Exit Program	Purpose	Where to Find an Example
Password validation	You specify this program name in the QPWDVLDPGM system value to check a new password for additional requirements that are not handled by the QPWDxxx system values. The use of this program should be carefully monitored because it receives unencrypted passwords. This program should not store passwords in a file or pass them to another program.	• *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200 • *Security – Reference*, SC41-4302

Table A-1 (Page 2 of 2). Sources of Sample Exit Programs

Type of Exit Program	Purpose	Where to Find an Example
PC Support/400 or Client Access for OS/400 access	You can specify this program name in the Client request access (PCSACC) parameter of the network attributes to control the following functions: • Virtual printer function • File transfer function • Shared folders Type 2 function • Client access message function • Data queues • Remote SQL function	• *An Implementation Guide for AS/400 Security and Auditing* • *Client Access/400 for DOS and OS/2 Technical Reference*, SC41-3563 • *OS/400 Server Concepts and Administration*, SC41-4740
Distributed Data Management (DDM) access	You can specify this program name in the DDM request access (DDMACC) parameter of the network attributes to control the following functions: • Shared folders Type 0 and 1 function • Submit Remote Command function	• *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200
Remote sign on	You can specify a program in the QRMTSIGN system value to control what users can be automatically signed on from which locations (pass-through.)	• *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200
Open Database Connectivity (ODBC) with Client Access for OS/400	Control the following functions of ODBC: • Whether ODBC is allowed at all. • What functions are allowed for AS/400 database files. • What SQL statements are allowed. • What information can be retrieved about database server objects. • What SQL catalog functions are allowed.	• *OS/400 Server Concepts and Administration*, SC41-4740
QSYSMSG break handling problem	You can create a program to monitor the QSYSMSG message queue and take appropriate action (such as notifying the security administrator) depending on the type of message.	• *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200

Architected TPN Requests

Table A-2 (Page 1 of 3). Programs and Users for Architected TPN Requests

TPN Request	Program	User Profile	Description
'30F0F8F1'X	AMQCRC6A	*NONE	Message queuing
'06F3F0F1'X	QACSOTP	QSYS	APPC sign-on transaction program
'30F0F2D1'X	QANRTP	QADSM	ADSM/400 APPC configuration
'30F0F1F9'X	QCNPCSUP	*NONE	Shared folders
'07F0F0F1'X	QCNTEDDM	QUSER	DDM

Table A-2 (Page 2 of 3). Programs and Users for Architected TPN Requests

TPN Request	Program	User Profile	Description
'07F6C4C2'X	QCNTEDDM	QUSER	Remote SQL–DRDA1
'30F0F1F4'X	QDXPRCV	QUSER	DSNX–PC receiver
'30F0F1F3'X	QDXPSEND	QUSER	DSNX–PC sender
'30F0F2C4'X	QEVYMAIN	QUSER	ENVY**/400 Server
'30F0F6F0'X	QHQTRGT	*NONE	PC data queue
'30F0F8F0'X	QLZPSERV	*NONE	Client Access for OS/400 license manager
'30F0F1F7'X	QMFRCVR	*NONE	PC message receiver
'30F0F1F8'X	QMFSNDR	*NONE	PC message sender
'30F0F6F6'X	QND5MAIN	QUSER	APPN 5394 workstation controller
APINGD	QNMAPINGD	QUSER	APINGD
'30F0F5F4'X	QNMEVK	QUSER	System management utilities
'30F0F2C1'X	QNPSERVR	*NONE	PWS-I network print server
'30F0F7F9'X	QOCEVOKE	*NONE	Cross-system calendar
'30F0F6F1'X	QOKCSUP	QDOC	Directory shadowing
'20F0F0F7'X	QOQSESRV	QUSER	DIA Version 2
'20F0F0F8'X	QOQSESRV	QUSER	DIA Version 2
'30F0F5F1'X	QOQSESRV	QUSER	DIA Version 2
'20F0F0F0'X	QOSAPPC	QUSER	DIA Version 1
'30F0F0F5'X	QPAPAST2	QUSER	S/36—S/38 pass-through
'30F0F0F9'X	QPAPAST2	QUSER	Printer pass-through
'30F0F4F6'X	QPWFSTP0	*NONE	Shared Folders Type 2
'30F0F2C8'X	QPWFSTP1	*NONE	Client Access file server
'30F0F2C9'X	QPWFSTP2	*NONE	Windows** Client Access file server
'30F0F6F9'X	QRQSRVX	*NONE	Remote SQL–converged server
'30F0F6F5'X	QRQSRV0	*NONE	Remote SQL without commit
'30F0F6F4'X	QRQSRV1	*NONE	Remote SQL without commit
'30F0F2D2'X	QSVRCI	QUSER	SOC/CT
'21F0F0F8'X	QS2RCVR	QGATE	SNADS FS2 receiver
'21F0F0F7'X	QS2STSND	QGATE	SNADS FS2 sender
'30F0F1F6'X	QTFDWNLD	*NONE	PC transfer function
'30F0F2F4'X	QTIHNPCS	QUSER	TIE function
'30F0F1F5'X	QVPPRINT	*NONE	PC virtual print
'30F0F2D3'X	QWGMTP	QWGM	Ultimedia Mail/400 Server
'30F0F8F3'X	QZDAINIT	QUSER	PWS-I data access server
'21F0F0F2'X	QZDRCVR	QSNADS	SNADS receiver
'21F0F0F1'X	QZDSTSND	QSNADS	SNADS sender
'30F0F2C5'X	QZHQTRG	*NONE	PWS-I data queue server
'30F0F2C6'X	QZRCSRVR	*NONE	PWS-I remote command server

Table A-2 (Page 3 of 3). Programs and Users for Architected TPN Requests

TPN Request	Program	User Profile	Description
'30F0F2C7'X	QZSCSRVR	*NONE	PWS-I central server

Appendix B. Security Enhancements for V3R1 and V3R6

This appendix provides an overview of the changes that been made to security for V3R1 and V3R6 to support enhanced functions in the AS/400 system:

- Increased system openness
- An integrated file system
- Advanced database functions
- Enhanced system integrity

For more information about these changes, beyond what is covered in this appendix, consult the *Security – Reference* book, SC41-3302.

Note: The security capabilities of V3R1 and V3R6 are the same.

Multiple Group Support: Beginning with V3R1, a user can be a member of up to 16 group profiles. This provides more flexibility in organizing groups and may reduce the number of private authorities needed. A user's first group is specified in the group profile parameter of the group profile. Additional groups are specified by using a user profile parameter called supplemental groups.

User and Group Identification Numbers: Many network and client/server systems require that users be identified by a unique number. Two user profile parameters provide this support:

User Identification Number (*uid*)
Group Identification Number (*gid*)

When you upgrade to V3R1 or V3R6 from an earlier version of the OS/400 licensed program, the system generates a unique *uid* for each user profile on your system. It also generates a unique *gid* for each group profile.

New Special Authority: A special authority, *IOSYSCFG, is available to control which users can make changes to your system configuration.

New Object and Data Authorities: Three additional authorities are available beginning with V3R1:

*OBJALTER — Object alter authority is required to change the attributes of an object. For example, you need *OBJALTER to add or remove a trigger for a database file.

*OBJREF — Object reference authority is required to define a relationship for referential integrity.

*EXECUTE — Execute authority allows you to run a program or search a library for an object. In versions earlier than V3R1, most operations require *READ authority to the library containing an object. Starting with V3R1, *EXECUTE authority for the object library is required. When you upgrade to V3R1 or V3R6, the system converts the authority for the objects on your system.

Support for Primary Group: Beginning with V3R1, you can specify a primary group for any object on the system. The name of the primary group and the primary group's authority to the object are stored with the object. You might improve the performance of the authority checking process if you use primary group authority instead of granting private authority to a group profile.

The primary group appears on object authority displays. The following commands and parameters are available to work with primary groups:

- Change Object Primary Group (CHGOBJPGP)
- Work with Objects by Primary Group (WRKOBJPGP)
- Display User Profile (DSPUSRPRF) with *OBJPGP option

Integrated File System Support: The **integrated file system** is a part of OS/400 that provides storage management similar to personal computer and UNIX** operating systems, while providing an integrating structure over all information stored in the AS/400 system. A set of integrated file system commands is available to work with security:

Change Auditing (CHGAUD)
Change Authority (CHGAUT)
Change Owner (CHGOWN)
Change Primary Group (CHGPGP)
Display Authority (DSPAUT)
Work with Authority (WRKAUT)

The integrated file system security commands support these system-defined authority subsets that are new with V3R1:

*RWX	Read/write/execute
*RW	Read/write
*RX	Read/execute
*R	Read
*WX	Write/execute
*W	Write
*X	Execute

Some object authority displays have been enhanced to support full path names for objects. F22 can be used on these displays to see the absolute path name.

A user profile parameter, home directory (homedir), can be used to designate the default directory for a user in the integrated file system.

Additional System Integrity Support: Protecting system integrity is an important part of security. V3R1 and V3R6 include several enhancements in this area:

- The use of enhanced hardware storage protection has been expanded.
- The QALWOBJRST system value controls whether you allow security-sensitive objects to be restored to your system. You can prevent the restoring of adopted authority programs and system state programs.
- The Check Object Integrity (CHKOBJITG) command scans objects on your system. You can look for compiled programs or modules that have been altered or objects whose domain has been changed.
- Action auditing has been expanded to include many network and server activities.

Data Authority to Logical Files: The flexibility of logical files as a security tool has been enhanced. Starting with V3R1, you specify data authority for both physical and logical files. You can have different data authorities for different logical files that are associated with the same physical file.

When you upgrade to V3R1 or V3R6, the data authorities to physical files and associated logical files are adjusted the first time that you open each file.

Changes to Password System Values: Two of the system values that control password composition have been enhanced to give you more flexibility:

QPWDRQDDIF	This system value controls whether users can repeat previous passwords. The options have been expanded to give more flexibility in the number of unique passwords required.
QPWDLMTREP	The system value that controls repeating characters in a password has a new option. You can now choose to restrict only adjacent repeating characters.

IBM-Supplied Profiles Shipped without Passwords: Shipping IBM-supplied profiles with passwords represented a security exposure. These passwords were the same for all systems and were commonly known. Starting with V3R1, all IBM-supplied profiles, except QSECOFR, will be shipped with a password of *NONE. QSECOFR must be shipped with a password to allow you to install your system.

Passwords for IBM-supplied profiles are not changed when you upgrade an existing system to V3R1 or V3R6.

Where to Get More Information and Assistance

Many resources are available if you need more information about security or if you need assistance.

Security Service Offerings

Security Review services are available from IBM Availability Services. The review includes the following:

- Use of the Security ToolKit.
- A customer questionnaire.
- An interview to gather information about security practices.

The result of the review is a report that summarizes your potential security exposures and makes preliminary recommendations for corrective action.

Security planning, implementation, and consulting services are also available from IBM Availability Services.

For more information, please contact your IBM representative. In the U.S., you can contact your local Express Services marketing office, or you can call 1-800-IBM-4YOU.

Related Publications

Following are publications that provide more information about AS/400 security:

- *APPC Programming* describes the advanced program-to-program communications (APPC) support for the AS/400 system. This book guides in developing application programs that use APPC and defining the communications environment for APPC communications. It includes application program considerations, configuration requirements and commands, problem management for APPC, and general networking considerations.

  Version 3 Order Number: SC41-3443
  Version 2 Order Number: SC41-8189

- *System/36 Environment Programming* provides information identifying the differences in the applications process in the System/36 environment on the AS/400 system. It helps the user understand the functional and operational differences (from a System/36 perspective) when processing in the System/36 environment on the AS/400 system. This includes an environment functional overview, considerations for migration, programming, communications, security, and coexistence.

  Version 3 Order Number: SC41-3730
  Version 2 Order Number: SC41-9663

- *Backup and Recovery – Advanced* provides information about setting up and managing:
  - Journaling, access path protection, and commitment control
  - User auxiliary storage pools (ASPs)
  - Disk protection (device parity, mirrored, and checksum)

  Version 3 Order Number: SC41-3305
  Version 2 Order Number: SC41-8079

- *Backup and Recovery – Basic* describes how to do the following:
  - Plan a save strategy for your system.
  - Perform basic save operations.
  - Select which availability options are appropriate for you system.
  - Recover your system if a failure occurs.

  Version 3 Order Number: SC41-3304
  Version 2 Order Number: SC41-0036

- *Client Access Windows 3.1 Client for OS/400 ODBC User's Guide* describes how to install, configure, and use the Microsoft ODBC driver with Client Access for OS/400 for Windows 3.1. This publication includes example displays that show how to set up the ODBC driver for various PC database programs.

  Order Number: SC41-3533

- *DB2 for OS/400 Database Programming* Provides a detailed discussion of the AS/400 database organization, including information on how to create, describe, and update database files on the system. It also describes how to define files to the system using OS/400 data description specifications (DDS) keywords.

  Version 3 Order Number: SC41-3701
  Version 2 Order Number: SC41-9659

- *DDS Reference* provides detailed descriptions for coding the data description specifications (DDS) for files that can be described externally. These files are physical, logical, display, print, and intersystem communication function (ICF) files.

  Version 3 Order Number: SC41-3712
  Version 2 Order Number: SC41-9620

- *Distributed Database Programming* provides information on preparing and managing an AS/400 system in a distributed relational database using the Distributed Relational Database Architecture (DRDA). The publication describes planning, setting up, programming, administering, and operating a distributed relational database on more than one AS/400 system in a like-system environment.

Version 3 Order Number: SC41-3702
Version 2 Order Number: SC41-0025

- *Guide to Enabling C2 Security* describes how to customize your system to meet the requirements for C2 Security, as described in the *Department of Defense Trusted Computer Evaluation Criteria*.

  Order Number: SC41-0103

- *An Implementation Guide for AS/400 Security and Auditing: Including C2, Cryptography, Communications, and PC Connectivity* provides practical suggestions and examples for many areas of AS/400 security.

  Order Number: GG24-4200

- *Implementing AS/400 Security* by Wayne Madden. Loveland, Colorado: Duke Press, a division of Duke Communications International, 1995. Provides guidance and practical suggestions for planning, setting up, and managing AS/400 security.

  ISBN Order Number: 1-882419-20-0

- *Managing OfficeVision/400* provides information about how to manage the day-to-day activities of OfficeVision for OS/400. The book includes information on maintaining office enrollment and creating and managing office objects.

  Version 3 Order Number: SH21-0699
  Version 2 Order Number: SC41-9627

- *OS/400 Server Concepts and Administration* provides information for the system administrator working with AS/400 server functions. The book includes server concepts, server functions, and exit program information.

  Order Number: SC41-3470

- *Planning for and Setting Up OfficeVision/400* provides information about planning for and setting up OfficeVision for OS/400. The book includes information on planning for enrolling users, word processing, mail and calendar processing, using OfficeVision for OS/400 with IBM personal computers, and using OfficeVision for OS/400 in a communications network. The planning activities include filling out planning work sheets that are used to do the setup tasks.

  Version 3 Order Number: SH21-0695
  Version 2 Order Number: SC41-9626

- *Publications Reference* identifies and describes the printed and online information in the AS/400 library, and also lists other publications about the AS/400 system. It includes cross-reference information between the current library and the previous version library.

  Version 3 Order Number: SC41-3003
  Version 2 Order Number: GC41-9678

- *Security – Basic* explains why security is necessary, defines major concepts, and provides information on planning, setting up, and monitoring basic security on the AS/400 system.

  Version 3 Order Number: SC41-3301
  Version 2 Order Number: SC41-0047

- *Security – Reference* provides complete information about security system values, user profiles, resource security, and security auditing. This manual does not describe security for specific licensed programs, languages, and utilities.

  Version 3 Order Number: SC41-3302
  Version 2 Order Number: SC41-8083

- *System Startup and Problem Handling* provides information about the system unit control panel, starting and stopping the system, using tapes and diskettes, working with program temporary fixes, as well as handling problems.

  Version 3 Order Number: SC41-3206
  Version 2 Order Number: SC41-8082

- *TCP/IP Configuration and Reference* provides information for configuring and using AS/400 TCP/IP support. The applications included are Network Status (NETSTAT), Packet Internet Groper (PING), TELNET, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), line printer requester (LPR), and line printer daemon (LPD). The TCP and UDP Pascal application program interface (API) is also discussed.

  Version 3 Order Number: SC41-3420
  Version 2 Order Number: SC41-9875

- *TCP/IP File Server Support for OS/400 Installation and User's Guide* provides introductory information, installation instructions, and setup procedures for the File Server Support licensed program offering. It explains the functions available with the product and includes examples and hints for using it with other systems.

  Order Number: SC41-0125

- *Trusted Computer Systems Evaluation Criteria*, DoD 5200.28.STD, describes the criteria for levels of trust for computer systems. The TCSEC is a publication of the United States government. Copies may be obtained from:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards

- *Work Management* provides programmers with information about how to effectively manage their system work load by changing work management objects to meet their needs. The publication provides guidelines for performance tuning; descriptions of system values; and information on

collecting performance data, gathering system use data, using work entries, and scheduling batch jobs.	Version 3 Order Number: SC41-3306 Version 2 Order Number: SC41-8078

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Reader Comments—We'd Like to Hear from You!

AS/400 Advanced Series
Tips and Tools
for Securing Your AS/400

Publication No. GC41-0615-00

Overall, how would you rate this manual?

	Very Satisfied	Satisfied	Dissatis-fied	Very Dissatis-fied
Overall satisfaction				

How satisfied are you that the information in this manual is:

Accurate				
Complete				
Easy to find				
Easy to understand				
Well organized				
Applicable to your tasks				

THANK YOU!

Please tell us how we can improve this manual:

_____

_____

_____

_____

_____

May we contact you to discuss your responses? __ Yes __ No
Phone: (____) _____ Fax: (____) _____ Internet: _____

To return this form:

- Mail it
- Fax it
  United States and Canada: **800+937-3430**
  Other countries: **(+1)+507+253-5192**
- Hand it to your IBM representative.

Note that IBM may use or distribute the responses to this form without obligation.

Name _____ Address _____

Company or Organization _____ _____

Phone No. _____ _____

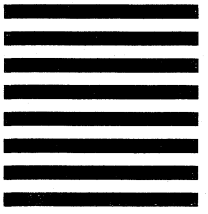
Reader Comments—We'd Like to Hear from You!
GC41-0615-00

IBM®

Cut
Alon

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

ATTN DEPT 542 IDCLERK
IBM CORPORATION
3605 HWY 52 N
ROCHESTER MN 55901-9986

Fold and Tape | **Please do not staple** | Fold and Tape

Cut c
Along

Printed in Denmark by Kodak FM Services A/S

GC41-0615-00