IBM

eserver

iSeries

Configure Your System For Common Criteria Security

Version 5 Release 3

SC41-5336-00

IBM

@server

iSeries

Configure Your System For Common Criteria Security

Version 5 Release 3

SC41-5336-00

me.

Notes

Before using this information and the product it supports, be sure to read the Appendix G, "Notices," on page 301.

First Edition (October 2004)

This edition applies to version 5, release 3, modification 0 of IBM Operating System/400 (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

About this information

This information explains how to plan, install, set up, and manage your iSeries™ system to comply with the IBM® OS/400® V5R3 security target based on the Common Criteria Controlled Access Protection Profile (CAPP).

See the following URLs for related information:

- http://csrc.nist.gov/cc/index.html (Common Criteria information)
- http://niap.nist.gov/cc-scheme/vpl_type.html (The IBM OS/400 V5R3 security target)
- http://niap.nist.gov/cc-scheme/PP_CAPP_V1.d.pdf (the definition of the Controlled Access Protection Profile)

The CAPP is published by:

Information Systems Security Organization
National Security Agency
9800 Savage Road
Fort Meade, Maryland 20755-6000 U.S.A.

The IBM server and the Operating System/400® (OS/400) licensed program (Version 5 Release 3 or later) have been designed to exceed the Common Criteria requirements as specified in the Controlled Access Protection Profile (CAPP) and represented in the IBM OS/400 V5R3 security target. In particular, OS/400 has been design to offer the following security functions: audit, discretionary access control, identification and authentication, security management, and self protection. Furthermore, OS/400 has been developed and evaluated in accordance with the Common Criteria EAL4 (Evaluation Assurance Level) assurance requirements as characterized below:

- **Objectives**
  - EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
  - EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity targets of evaluation (TOE) and are prepared to incur additional security-specific engineering costs.
- **Assurance components**
  - EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behavior. Assurance is additionally gained through an informal model of the TOE security policy. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.
  - EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.
  - This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

Common Criteria security requires the following documentation:

- *Administrator Guidance*, which describes the tasks that a security administrator must perform to install and manage a Common Criteria evaluated system.
- *User Guidance*, which describes user responsibilities for security. See Appendix D, "User responsibilities for security," on page 141.

This information is designed to meet the Common Criteria requirement for both administrator guidance and user guidance, when used in conjunction with the following supplemental information:

- *iSeries Security Reference*, SC41-5302-08
- *Install, Upgrade, or Delete i5/OS™ and Related Software*, SC41-5120-07
- *Backup and Recovery*, SC41-5304-07
- Application Programming Interfaces (APIs), located in the V5R3 iSeries Information Center.
- *Tips and Tools for Securing Your iSeries*, SC41-5300-07.

This guide should be read first and should be considered the primary source of information for setting up your system to meet Common Criteria security requirements on OS/400. Appendix D, "User responsibilities for security," on page 141 of this information is designed to meet the Common Criteria requirement for user guidance documentation. The introduction to Appendix D, "User responsibilities for security," on page 141 explains how to customize it for your installation.

Who should read this information

This information is intended for system administrators or security administrators that want to customize an iSeries system to meet the requirements for Common Criteria security. This information details the unique requirements of Common Criteria security and is intended as a supplement to other manuals that describe how to install and set up your system.

You need the following special authorities in your user profile to perform the tasks in this guide:

*ALLOBJ (all object) special authority
*AUDIT (audit) special authority
*IOSYSCFG (system configuration) special authority
*SAVSYS (save system) special authority
*SECADM (security administrator) special authority
*SERVICE (service) special authority

You also need to know how to perform the following tasks:

- Operate display stations and installation devices.
- Sign on and sign off the system.
- Use function keys on your workstation keyboard.
- Use displays and menus.
- Use commands.

If you are changing OS/400 to meet Common Criteria security requirements, familiarize yourself with the following information before attempting to perform the tasks in this guide:

- Backup and recovery procedures (see **Back up your server** in the iSeries Information Center).
- Procedures for defining security (see the *iSeries Security Reference*).
- The security auditing function (see the *iSeries Security Reference*).
- Procedures for configuring disk mirroring and auxiliary storage pools, if these capabilities are used by your installation (see **Back up your server** in the iSeries Information Center).

You may need to refer to other IBM information for more specific information about a particular topic. The iSeries Information Center provides detailed information on a variety of OS/400 topics.

Contents

Part 1. The OS/400 implementation of Common Criteria security

This chapter provides an overview of the requirements for Common Criteria security and relates these requirements to the OS/400 operating system. The United States Department of Defense (DoD) defines Common Criteria security.

Chapter 1. Basic Common Criteria security requirements

The Controlled Access Protection Profile (CAPP) has replaced the *Trusted Computing Systems Evaluation Criteria (TCSEC)* C2 evaluation requirements, for which previous versions and releases of OS/400 qualified. CAPP specifies a set of security functional and assurance requirements for Information Technology (IT) products. Products that conform to CAPP, such as OS/400, support access controls that are capable of enforcing access limitations on individual users and data objects. These products also provide an audit capability that records the security-relevant events occurring within the system. In summary, OS/400 meets the all of the following CAPP requirements:

Discretionary access control

Object reuse

Identification and authentication

Auditability of security-relevant events

Discretionary access control

Common Criteria security requires the ability to restrict access to objects on a system. This is based on the identity of a user or a user's group. The Common Criteria term for this is *discretionary access control*. The OS/400 term is *object authority*. Authority can be defined for any object on the iSeries system.

Appendix F, "Authority required for objects used by commands," on page 155 explains what authority is required for the objects that are used by commands on the system. For information about what constitutes the discretionary access control (DAC) policy on the system, see the following resources:

- The System API Programming information, located in the iSeries Information Center, describes what authority is required for the objects that are used by Application Programming Interfaces (APIs).
- The **DB2 Universal Database™ for iSeries SQL Reference** topic in the iSeries Information Center describes what authority is required for objects that are used by Structured Query Language (SQL) statements.

Object authority is designed to prevent unauthorized access to objects. Normally, permission to access an object is granted by the object's owner. An administrator can also grant it. On the system, a privilege is called a *special authority*. An administrator is a user with one or more special authorities.

Object reuse

Common Criteria security requires the management of internal storage on the system so that storage is cleared before it is reused. This prevents a user who creates a new object on the system from accessing any information that formerly resided in the same location in physical storage. Common Criteria security also requires that when a new object is created, it does not receive any authorities that are associated with a previously deleted object.

The system controls object reuse in several ways:

- Management of virtual addresses and single-level storage on the system ensures that two objects never share the same address space. It also ensures that an object's boundaries are not crossed when manipulating that object.
- When an object is deleted, all authority information for that object is deleted with it. If an object with the same name and type is later restored from backup media, the system performs several security checks. These security checks are used to determine how public authority and ownership for the restored object should be set. If a user's authorities to objects are restored on the system, the system also performs checks to ensure that the objects match.

- A page of memory is cleared before a new page is moved in. This ensures that a program does not access data that is left in memory by another program.
- The program does not permit direct manipulation of any storage objects, except user spaces, indexes, and queues. On a Common Criteria system running OS/400, user objects can exist only in the temporary library assigned to a user's job (QTEMP). Each job on the system has a unique QTEMP library. The QTEMP library for a job cannot be accessed by any other job on the system. The QTEMP library for a job is cleared when the job ends.

Identification and authentication

Common Criteria security requires that individuals who use the system are personally accountable for the actions they perform. Everyone who signs on the system must be uniquely identified, and that identity must be confirmed. The system must be able to associate every security-relevant action with a specific person.

On the iSeries system, each user is uniquely identified by a user profile. The user profile name is entered on the sign on display. The password confirms or authenticates the identity of the user. The user's password is also entered on the sign on display. The user profile name and password are verified before the user is allowed to sign on the system.

Note: FTP specifies the user identity as part of the USER subcommand and the password is specified as part of the PASS subcommand. An FTP user cannot access any OS/400 objects until he has specified a user identity and password. REXEC specifies the user identity and password on every request sent to the system. The user identity and password must be verified before the command is executed.

Batch jobs are also associated with a specific user profile. If a user wants to run a batch job under a different user profile, the submitting user must have authority to the user profile.

Auditability of security-related events

Common Criteria security requires that the system be capable of auditing any security-relevant event that is performed by any system user. A **security-relevant** event is anything that occurs on the system that affects the safety and integrity of the system processes and data.

The facts recorded for a security-relevant event must include:

- The time and date of the event
- The name of the event
- The name of the objects
- The name of the user who performed the action

On the system, you use a combination of system values, user profile parameters, and object parameters to determine which events you want to audit. To work with the auditing characteristics of the system, you must have *AUDIT special authority. For more information about object types and the events that can be audited on the system, See "Appendix E: Object Operations and Auditing" in the *iSeries Security Reference*.

Chapter 2. Target of Evaluation (TOE)

The **Target of Evaluation** (TOE) is the combination of hardware and software that provides security protection within a computer system.

On the OS/400 operating system, the TOE includes:

- Most currently available hardware (see "Hardware for the Target of Evaluation").
- Feature code 1930 (see "Software for the Target of Evaluation" on page 6).
  - The base operating system (the OS/400 licensed program)
  - Some optional features of the operating system
  - Some additional licensed programs

Products that are included in the TOE have been evaluated and tested for Common Criteria security compliance. Products that are not included in the TOE have not been evaluated for Common Criteria security compliance. Because the TOE is a general building block, many installations require changes or additions to the evaluated configuration. For U.S. Government installations, any changes or additions to the TOE should be approved by your Designated Approving Authority (DAA). For other installations, your security administrator should assess the security risk of any changes or additions to the TOE configuration.

Hardware for the Target of Evaluation

The following table lists the hardware that has been evaluated for Common Criteria security. You can install any items on this list on a Common Criteria OS/400 system.

Table 1. Hardware Included in the Target of Evaluation

Machine type	Model	Features	Processor type
9406	520	0900, 0901, 0902, 0903, 0904, 0905	Power5
9406	550	0914, 0915	Power5
9406	570	0920, 0921, 0922, 0923, 0924, 0925, 0926, 0927	Power5

A set of peripheral devices may be attached to system as needed. The following table lists the peripheral devices that are included in the TOE.

Table 2. Peripheral hardware devices that are included in the Target of Evaluation

Type	Feature Code	Description	520	550	570	590
Disk	4317/7501 6617	8.58GB 10K RPM Disk Unit	X	X	X	X
Disk	4318/7502 6618	17.54GB 10K RPM Disk Unit	X	X	X	X
Disk	4319/7504 6619	35.16GB 10K RPM Disk Unit	X	X	X	X
Disk	4326/7508	35.16GB 15K RPM Disk Unit	X	X	X	X
Disk	4327/7509	70.56GB 15K RPM Disk Unit	X	X	X	X
Disk	4328/7510	146.8GB ULTRA320 15K RPM U320	X	X	X	X
IOP	2843	PCI IOP	X	X	X	X
IOP	2844	PCI IOP	X	X	X	X
LAN	2743	PCI 1Gbps Ethernet IOA		X	X	X
LAN	2744	PCI 4/16/100Mbps Token-Ring IOA		X	X	X

Table 2. Peripheral hardware devices that are included in the Target of Evaluation (continued)

Type	Feature Code	Description	520	550	570	590
LAN	4723	PCI 10Mbps Ethernet IOA	X	X	X	X
LAN	5707	PCI 1Gbps Ethernet Fiber 2–port	X	X	X	X
LAN	5706	PCI 10/100/1000 Mpbs Ethernet UTP 2–port	X	X	X	X
LAN	5701	PCI 1Gbps Ethernet UTP IOA	X	X	X	X
LAN	5700	PCI 1Gbps Ethernet IOA	X	X	X	X
LAN	4838 2838	PCI 100/10Mbps Ethernet IOA	X	X	X	X
LAN	2849	PCI 100/10Mbps Ethernet IOA	X	X	X	X
LAN	2760	PCI IGbps Ethernet UTP IOA	X	X	X	X
RemMed	1889	80GB VXA-2 Tape (bolt-in)	X	X	X	X
RemMed	2640	DVD ROM Slimline	X	X	X	X
RemMed	5751	DVD RAM Slimline	X	X	X	X
RemMed	5753	30GB 1/4–inch Cartridge Tape (bolt-in)	X	X	X	X
RemMed	5754	50GB 1/4–inch Cartridge Tape (bolt-in)	X	X	X	X
Encryption	4801	4758–023 PCI Encryption Tamper Proof FIPS 3	X	X	X	X
Encryption	4764	5733-CY1 Cryptographic Device Manager	X	X	X	X
WS	4746 2746	PCI Twinax Workstation IOA	X	X	X	X

Note: To meet Common Criteria security requirements, your system unit must have a keylock. For OS/400 Advanced Series models, you must order a keylock for the system unit.

Software for the Target of Evaluation

Version 5, Release 3 (V5R3) of the OS/400 licensed program has been designed to meet the Common Criteria security requirements. Earlier versions of the OS/400 program do not meet all Common Criteria security requirements. The following tables list the software options and licensed programs that have been evaluated for Common Criteria compliance.

These options for the OS/400 licensed program may be installed on a Common Criteria OS/400 system:

Table 3. OS/400 Options Included in the Target of Evaluation

Description	Libraries
General purpose library	QGPL[1]
User library	QUSRSYS[1]
Extended Base Support	QQALIB, QSYS2
Online Information	QHLPSYS
Extended Base Directory Support	QSYSDIR, QSYSCGI
Example Tools library	QUSRTOOL
AFP™ Compatibility Fonts	QFNTCPL
*PRV CL Compiler Support	QSYSVxRyMz
OS/400 GDDM®	QGDDM
System Openness Includes	QSYSINC
Extended NLS Support	QSYSLOCALE
Cryptographic Service Provider	QCCA

Table 3. OS/400 Options Included in the Target of Evaluation (continued)

Description	Libraries
[1] You must install the QGPL and QUSRSYS libraries on your system.	

The licensed programs listed in the following table run in system state. These licensed programs have been evaluated for Common Criteria security. No other programs that run in system state have been evaluated, nor should they be installed on a Common Criteria evaluated system. If you install system state programs that have not been evaluated, you will not be running an evaluated configuration. Your system will not meet Common Criteria security requirements.

Note: The Common Criteria configuration sets the system value QALWOBJRST to *NONE. Programs that are in system state or programs that adopt the profile of the owner **cannot be restored** to the system.

Table 4. Licensed Programs Included in the Target of Evaluation. You can install these licensed programs on a Common Criteria OS/400 system.

Product number	Option	Description	Version
5722SS1	—	The OS/400 Operating system with options:	V5R3M0
	1	OS/400 Extended Base Support	V5R3M0
	2	OS/400 Online Information	V5R3M0
	3	OS/400 Extended Base Directory Support	V5R3M0
	7	OS/400 Example Tools Library	V5R3M0
	8	OS/400 AFP Compatibility Fonts	V5R3M0
	9	OS/400 *PRV CL Compiler Support	V5R3M0
	12	OS/400 Host Servers	V5R3M0
	13	OS/400 System Openness Includes	V5R3M0
	14	OS/400 GDDM	V5R3M0
	21	OS/400 Extended NLS support	V5R3M0
	26	OS/400 DB2® Symmetric Multiprocessing	V5R3M0
	27	OS/400 DB2 Multisystem	V5R3M0
	35	OS/400 CCA Cryptographic Service Provider	V5R3M0
	36	OS/400 PSF/400 1–45 IPM Printer Support	V5R3M0
	37	OS/400 PSF/400 1–100 IPM Printer Support	V5R3M0
	38	OS/400 PSF/400 Any Speed Printer Support	V5R3M0
	39	OS/400 International Components for Unicode	V5R3M0
	43	OS/400 Additional Fonts	V5R3M0
5722AC3	—	IBM Cryptographic Acess Provider 128-bit for iSeries [1]	V5R3M0
5769FNT	—	IBM Advanced Function Printing™ Fonts for AS/400® with all available options:	V4R2M0
	1	AFP Fonts — Sonoran Serif	V4R2M0
	2	AFP Fonts — Sonoran Serif Headliner	V4R2M0
	3	AFP Fonts — Sonoran Sans Serif	V4R2M0
	4	AFP Fonts — Sonoran Sans Serif Headliner	V4R2M0
	5	AFP Fonts — Sonoran Sans Serif Condensed	V4R2M0
	6	AFP Fonts — Sonoran Sans Serif Expanded	V4R2M0
	7	AFP Fonts — Monotype Garamond	V4R2M0
	8	AFP Fonts — Century Schoolbook	V4R2M0
	9	AFP Fonts — Pi and Specials	V4R2M0
	10	AFP Fonts — ITC Souvenir	V4R2M0
	11	AFP Fonts — ITC Avant Garde Gothic	V4R2M0
	12	AFP Fonts — Math and Science	V4R2M0

Table 4. Licensed Programs Included in the Target of Evaluation (continued). You can install these licensed programs on a Common Criteria OS/400 system.

Product number	Option	Description	Version
	13	AFP Fonts — DATA1	V4R2M0
	14	AFP Fonts — APL2	V4R2M0
	15	AFP Fonts — OCR A and OCR B	V4R2M0
5769FN1	—	Advanced Function Printing DBCS Fonts/400 with all available options:	V4R2M0
	1	AFP DBCS Fonts — Japanese	V4R2M0
	2	AFP DBCS Fonts — Korean	V4R2M0
	3	AFP DBCS Fonts — Traditional Chinese	V4R2M0
	4	AFP DBCS Fonts — Simplified Chinese	V4R2M0
	5	AFP DBCS Fonts — Thai	V4R2M0
5722QU1	—	IBM Query for iSeries	V5R3M0
5722ST1	—	IBM DB2 Query Manager and SQL Development Kit for iSeries	V5R3M0
5722TC1	—	IBM TCP/IP Connectivity Utilities for OS/400	V5R3M0
5722XE1	—	IBM eServer™ iSeries Access for Windows®	V5R3M0
5722XW1	—	IBM eServer iSeries Access Family	V5R3M0
	1	iSeries Access Enablement Support	V5R3M0

[1] This licensed program is included in the Common Criteria Target of Evaluation; however, cryptographic algorithms are not included in the Common Criteria evaluation.

Chapter 3. Plan an OS/400 operating system that meets Common Criteria security requirements

It is important to develop a plan for your OS/400 operating system which meets the Common Criteria security requirements. A successful plan can make your system implementation go smoothly. Planning security on your system consists of the following activities:

Planning physical security

Planning overall security (system values)

Planning group profiles

Planning user profiles

Planning resource security

See the Security topic in the iSeries Information Center for guidance on planning your security strategy.

Requirements for system hardware

Review your system hardware to determine if you are using any hardware that has not been evaluated. See "Hardware for the Target of Evaluation" on page 5 for a list of the evaluated hardware which can be used as part of a Common Criteria evaluated system. If your system contains hardware that has not been evaluated, you must remove it, or you must have the use of the hardware approved by your Designated Approving Authority.

Requirements for system values

System values determine the security rules that apply to all users on your system. Common Criteria security requires specific settings for some system values. The customization program that is provided for setting up your system sets these system values. See Table 16 on page 134 for these settings.

Notes:

1. The integrated security tools include the CFGSYSSEC command for setting security-relevant system values. The CFGSYSSEC command uses settings that are less restrictive than Common Criteria security requirements.
2. Do not use the CFGSYSSEC command to set system values on your system.
3. Do not use the PRTSYSSECA command because the recommended values on the report do not match Common Criteria security requirements for system values.

Compare the Common Criteria system value recommendations to your own requirements and decide whether you need to make changes to the recommended settings. For all other security system values, choose values that are appropriate for the security requirements of your installation.

Security level 50

To meet the requirements of Common Criteria security, you must set the security level (QSECURITY) system value to 50. Security level 50 provides signon security, resource security, and enhanced integrity protection.

Most application software that runs at security level 40 will run at security level 50. However, you should check with your programmer or application provider to ensure that your applications will run properly. You may need to make changes to your applications before you bring your system to security level 50.

Note: If your current system is running at security level 10 and you change it to security level 50, you will no longer be able to change it back to security level 10. Security level 10 is only supported on systems that currently use it. Once you change from security level 10 to another security level, you cannot go back to security level 10.

Plan explicit authority

Common Criteria security requires that authority to objects be explicitly given to users on a need-to-know basis and not provided automatically.

Before you enable Common Criteria security on your system, do the following to plan how to meet the requirement for explicit authority:

1. Determine whether to use library security or individual object security to exclude unauthorized users from the application objects. Use the Edit Object Authority (EDTOBJAUT) command to ensure that one of the following occurs for every library:
   - The public authority to the library is *EXCLUDE.
   - The public authority to each security-relevant object in the library is *EXCLUDE.

   Setting the public authority of each user library to *EXCLUDE is the simplest method for providing explicit authority. The customization program changes the default for the Create Library (CRTLIB) command so that new libraries are automatically created with public authority that is set to *EXCLUDE.
2. Choose the default authority for new objects. The create authority (CRTAUT) parameter controls this.

   The default when you create a library is to set the value of CRTAUT to *SYSVAL. This means that new objects in the library have their public authority set to the value of the QCRTAUT (create authority) system value. The customization program sets the QCRTAUT system value to *EXCLUDE.
3. Prepare a Library Description Form (located in the system security and planning information topic in the iSeries Information Center) for each user library on your system.
4. Evaluate the owner and group authority values for user profiles:
   - If the owner value in a user profile specifies *GRPPRF, the user's group profile owns any new objects that are created by the user. All members of the user's group receive authority to new objects. This may not meet the requirement for explicit authority.
   - If the group authority (GRPAUT) value in a user profile is a value other than *NONE or *EXCLUDE, the members of a user's group are given some authority to any new objects the user creates. This may not meet the requirement for explicit authority.
   - The best way to ensure that you meet the requirement for explicit authority is to set the OWNER value to *USRPRF. Also, set the GRPAUT value in user profiles to *NONE.

Plan explicit authority for the integrated file system

OS/400 provides multiple ways to view and store information. The integrated file system is a part of the OS/400 operating system that supports stream file input and output operation. It provides storage management methods that are similar to (and compatible with) personal computer operating systems and UNIX® operating systems.

With the integrated file system, all objects on the system can be viewed from the hierarchical directory structure. Additionally, new objects called directories and stream files are available. These object types more closely match the semantics available on personal computer and UNIX operating systems than library and folder objects do.

The ″root″ (/) file system acts as an umbrella (or foundation) for all other file systems on the server. At a high level, it provides an integrated view of all objects on the system. The ″root″ (/) file system, QOpenSys file system, and user-defined file systems blend the security capabilities of the QSYS.LIB file system with UNIX and personal computer operating systems. The system enforces all of the security settings for an object regardless of the interface that is used to access the object.

Note: The QOpenSys file system provides capabilities similar to those of the ″root″ (/) file system. The QOpenSys file system is case-sensitive. The ″root″ (/) file system is not case-sensitive.

OS/400 underlying security provides more detailed authorizations than either PCs or UNIX-like operating systems. OS/400 provides object authorities (*OBJEXIST, *OBJMGT, *OBJALTER, and *OBJREF) that do not have equivalents in the other environments. Therefore, to ensure that UNIX-like applications work as expected, the public has all object authorities to the root directory when the system ships. The default when creating a new object is to inherit object authorities from the direct parent directory.

On a Common Criteria evaluated system, the default values for the ″root″ (/) file system do not meet the requirements for explicit (need-to-know) authority. Therefore, you will need to make changes to the default authorities. In addition, you will need to set up operational procedures for creating new directories. The typical user will not have sufficient authority to create a new directory because creating an object requires *W authority to the parent directory. Also, if your applications use UNIX-like APIs, the authority checking might not behave according to UNIX-like rules after you make the changes described. You will need to review the authority requirements for your UNIX-like applications. All existing directories except for ″/tmp″ will be changed by the setup programs to have no more than *RX public data authority and *NONE public object authority.

When a user needs a private directory, an administrator should use the CRTDIR command to create the directory in the /home subdirectory. On the CRTDIR command, specify DTAAUT(*EXCLUDE) and OBJECT(*NONE). Also, use the CHGOWN command to transfer ownership from the administrator to the user who needs the directory. When you transfer ownership, the system automatically gives the new owner all authorities to the directory.

When an application needs to create a new object (stream file) in the /tmp directory, the stream file should be opened with an option that allows non-shared use of the file. This creates the stream file. Immediately after opening the stream file, delete or unlink the stream file. This removes it from the /tmp directory. When the application is finished with the stream file, close it. This removes it from the system and makes the disk space available for other use.

Prevent the use of authority holders

The ability to create and use authority holders is an option of the OS/400 licensed program. Authority holders are commonly used by applications that have been migrated from the System/36™. They allow you to hold the authority information for program-defined physical files that are deleted and created again.

Authority holders do not meet the Common Criteria security requirement for explicit authority. A user may create a physical file that becomes associated with an authority holder. Users who are authorized to the authority holder then have access to the physical file without being explicitly authorized. Authority holders must not be used on a system that is enabled for Common Criteria security.

To determine whether any authority holders exist on your system, use the Display Authority Holder (DSPAUTHLR) command. If your applications use authority holders, you must find another method, such as using authorization lists, to provide the same function.

Restrict administration

An administrator for a Common Criteria evaluated system is a user with one or more special authorities.

To meet Common Criteria security requirements, special authorities should be used only for specific purposes in a controlled environment. For example, a user who has *SAVSYS (save system) special authority should use that special authority only when saving and restoring objects on the system. *SAVSYS special authority should not be used when running other functions that do not require the authority.

Set up multiple user profiles

One way to restrict administrators is to create two or more profiles for users who need special authorities.

For example, if a user, Rita Hogan, is responsible for backing up the system, she might have two profiles: HOGANR and HOGANRS. She signs on as HOGANR to perform normal application activities. The HOGANR profile does not have any special authorities. She signs on as HOGANRS to perform save or restore activities. The HOGANRS profile has the necessary authorities to back up the system:

*SAVSYS special authority

*JOBCTL special authority

*CHANGE authority to the system operator (QSYSOPR) message queue

Use menus

Another way to restrict administrators is to create menus or CL (control language) programs to perform system functions.

For example, use a CL program that is called MYSAVE to display the system menu for save operations:

```
PGM
GO SAVE
ENDPGM
```

The MYSAVE program is owned by the user profile HOGANRS, which has the necessary authorities to perform save operations. The MYSAVE program adopts owner authority. Public authority to the MYSAVE program is *EXCLUDE. The user profile HOGANR has *USE authority to the MYSAVE program.

For her normal work, Rita Hogan signs on as HOGANR. When she needs to perform save operations, she calls the MYSAVE program, which adopts the authority of HOGANRS and gives her the necessary authorities. When she has completed the save operations, she ends the MYSAVE program and returns to her normal work.

Attention!

Your Designated Approving Authority (DAA), auditor, or security administrator must evaluate the security risk when you create any program that adopts authority. In particular, you should evaluate programs that adopt a user profile with special authorities. You should also ensure that programs with adopted authority adopt only as much authority as the program requires to function properly. When you create a program that adopts authority, you are extending the TOE of your system beyond what has been evaluated for Common Criteria security.

You can use the QUSEADPAUT system value to identify an authorization list that is used to control which users can create programs that inherit adopted authority from previous programs in the program stack.

iSeries Security Reference discusses all the special authorities available on the system, the risks that are associated with them, and recommendations for their use. Carefully review the need for special authorities on your system and develop a method for restricting them.

Restrict application development tools

Data File Utility (DFU), which is commonly used by application software, has not been evaluated for Common Criteria security. DFU should not be installed on a Common Criteria evaluated system. Before you enable Common Criteria security on your system, determine whether your applications use DFU. If they do, you need to provide the function in another way, such as developing high-level language programs.

Restrict Java programs

Java™ programs have not been evaluated for Common Criteria security. Java should not be used on a Common Criteria evaluated system. Before you enable Common Criteria security on your system, determine whether your applications use Java. If they do, you need to provide the function in another way, such as using different high-level language programs.

The QSYLMTJAVA authorization list is set to public *EXCLUDE authority on systems configured for Common Criteria to prevent Java programs from being used.

Optional features and licensed programs

Review your applications to determine whether they use optional features of the OS/400 licensed program or additional licensed programs. “Software for the Target of Evaluation” on page 6 lists all OS/400 options and licensed programs that have been evaluated as part of the Target of Evaluation (TOE). If your applications use features and licensed programs that are not part of the TOE and run in system state, you must find other ways to provide the functions.

Note: You can use the Allow Object Restore (QALWOBJRST) system value to prevent installation of system state programs on your system.

Use exit programs

OS/400 uses exits as a method for communicating between user programs and system functions. In some cases, you have the capability of creating an exit program that is called by the system to provide a specific function. For example, if you use database journaling, you can create an exit program that the system calls when you use the Receive Journal Entry (RCVJRNE) command. Some exits from the operating system have been evaluated as part of the TOE. Other exits should not be used. You and your security administrator should evaluate the use of exit programs using the information that is provided in Chapter 21, “Restrict the use of exit programs,” on page 79.

Part 2. Configure OS/400 to meet Common Criteria security requirements

After you have completed the planning phase for your Common Criteria evaluated system, you can begin taking the steps required by the Common Criteria security evaluation to configure your system. These steps are explained in detail in this guide. Ensure that you have access to the V5R3 iSeries Information Center during the configuration process. The iSeries Information Center provides detailed information on a variety of topics regarding OS/400 and the iSeries server. Familiarize yourself with the following iSeries information topics, prior to configuring your system to comply with the Common Criteria security requirements:

The software installation process

How to back up your server

Device configuration

Work management

Chapter 4. Prepare the OS/400 operating system for Common Criteria security

Before you can configure your Common Criteria evaluated system, you will need to plan the installation procedure and your installation tasks, to ensure that you do not miss any important steps. Use the following sections to guide you through this part of the process.

Installation tasks

To meet the requirements for Common Criteria security, you must use the installation procedures that are presented in this information. You cannot use the automatic installation procedure for your Licensed Internal Code (LIC) and operating system. The following list shows the sequence of tasks required to install your system and customize it to meet Common Criteria security requirements. Use this list to check off each task as you complete it.

__ • "Plan the installation."
__ • "Reinitialize the server by installing feature code 1930" on page 18:
  __ – "Install the licensed internal code" on page 18.
  __ – "Install the OS/400 operating system" on page 20.
  __ – "Set the system values" on page 20.
  __ – "Install licensed programs" on page 22.
__ • "Install a secondary language" on page 23 (optional).
__ • "Install a PTF package" on page 23.
__ • Chapter 6, "Customize the OS/400 system for Common Criteria security," on page 31.

Plan the installation

The *Install, upgrade, or delete OS/400 and related software* (SC41-5120-07) information describes planning activities you should perform before starting the installation process. Many of these activities apply only when you are installing a new release of the operating system on an existing system. Some that are required for the installation and preventing installation problems, apply to all systems. Perform the planning tasks that apply to your situation. These are described in Part 1 of the *Install, upgrade, or delete OS/400 and related software* (SC41-5120-07) guide.

It is a good idea to place the CD-ROMs in order before beginning the following tasks. Labels on the distribution media that is used for installation have unique identifiers. Media type identifiers are located on the center of the left-hand side of the CD-ROM label. These identifiers help you determine when to use each volume. You should order your CD-ROMs as follows:

1. I_1930_01 (Licensed Internal Code for OS/400)
2. B_1930_01 (Operating System/400)
3. B_1930_02 (OS/400 no-charge options and licensed programs)
4. B29MM_03 (OS/400 no-charge options)
5. B29MM_04 (OS/400 no-charge options)
6. D_1930_01 (OS/400 no-charge options)
7. D_1930_02 (OS/400 no-charge options)
8. D_1930_03 (OS/400 no-charge options)
9. D_1930_04 (no-charge licensed programs)
10. D_1930_05 (no-charge licensed programs)
11. L_1930_01 (Priced licensed programs)

12. L_1930_02 (Priced licensed programs)
13. L_1930_03 (Priced licensed programs)
14. F29xx_01 (Other feature 1930 licensed programs)
15. N29xx (Secondary Language Media if ordered)
16. C4272530_01 (Cumulative PTF Package if ordered)
17. C4272530_02 (Cumulative PTF Package)
18. C4272530_03 (Cumulative PTF Package if ordered)
19. C4272530_04 (Cumulative PTF Package if ordered)
20. C_1930_01 (Cumulative PTF Package)

Keep the following installation media available for later use:

- N29xx (Secondary Language Media if ordered)
- C4272530_01 (Cumulative PTF Package if ordered)
- C4272530_02 (Cumulative PTF Package)
- C4272530_03 (Cumulative PTF Package if ordered)
- C4272530_04 (Cumulative PTF Package if ordered)
- C_1930_01 (Cumulative PTF Package)
- SK3T-4091 iSeries Information Center

The 29xx number is different depending on the primary language that you ordered. For example, the number is 2924 for English.

You can see what is on each CD-ROM by consulting the Media Distribution Report that accompanied your software, or you can verify the contents of your software order according to the information located in the V5R3 iSeries Information Center, for the contents of the B29xx and L29xx CD-ROMs.

Reinitialize the server by installing feature code 1930

Once you have planned adequately for your installation and Common Criteria security customization, you can begin the process of rebuilding your system from the licensed internal code all the way through the process of applying a PTF package. The following information guides you through the process.

Install the licensed internal code

Before you Begin

1. Ensure the following for the server:
   - If you are using twinaxial console, verify that the device description for the console is specified in the **QCONSOLE** system value. Also verify that the console is powered on.
   - If you are using Operations Console, you need a valid connection configuration for the server after you have run the Operations Console wizard. The console for the server needs to be at Connecting console.
2. For all servers, verify that the console mode value is set correctly for your console. To verify the console mode value, follow these steps:
   a. Access Dedicated Service Tools (DST).
   b. Select Work with DST environment (Option 5).
   c. Select System Devices (Option 2).
   d. Select Console mode. The value of the current console mode is present in the input field. Verify that this is the correct setting. The console mode value must be one of the following values:
      - 1 Twinaxial console
      - 2 Operations Console (directly attached)

Installation process

Your system may arrive with the Licensed Internal Code and the operating system already loaded. If not, skip to step 1 below. If previously loaded all objects and information on the system must be destroyed to meet Common Criteria security requirements. To destroy all objects and information on your system and load the Licensed Internal Code, you will need to perform the following steps.

Attention!
These steps destroy all objects and information from all disk units on your system. If you have already completed the installation of your system and have data loaded, save all information on your system before proceeding with the following step.

Type **PWRDWNSYS *IMMED RESTART(*YES)** and press **Enter**. Reference codes display during this time. When the system attention light flashes and an SRC beginning with the characters A6 displays, the system is waiting for you to perform an action. For example, it could be waiting for you to respond to a message or ready a media device. Some reference codes also display on the console during the installation of licensed internal code.

__ Step 1. Use the control panel on your system unit to place your system in Manual mode.

__ Step 2. Press the **Function Selection** button until 03 (Select IPL) displays in the Function display on the control panel.

__ Step 3. Press **Enter** on the control panel.

__ Step 4. Load the installation media volume that contains Licensed Internal Code (I_1930_01) into the installation device for the alternate initial program load (IPL).

Note: Usually you cannot load the media while the system is powered off. Press the power switch once to power on the server.

a. If you could not load your media, load the licensed internal code media volume into the installation device for the alternate IPL at this time.

b. If the system attention light flashes and a reference code displays, perform the action listed for that reference code. Otherwise, continue with the following step.

It may take some time before the Select a Language Group menu displays. Once the Select a Language Group menu displays, you can change the primary language of your system by specifying a language feature number other than that which is displayed. See Appendix C, “National language version feature codes,” on page 139 for a list of language feature codes.

__ Step 5. Press **Enter** once you have selected a language group on the Select a Language Group menu. The Confirm Language Group dialog displays. The default is 2924 (English).

__ Step 6. Press **Enter** to confirm your language group selection. The Install Licensed Internal Code menu displays.

__ Step 7. Select **option 1** (Install Licensed Internal Code) and press **Enter**. The Install Licensed Internal Code (LIC) dialog displays.

__ Step 8. Select **option 2** (Install Licensed Internal Code and Initialize system) and press **Enter**. The Install Licensed Internal Code (LIC) and Initialize System Confirmation dialog displays.

__ Step 9. Press **F10** to continue. The Initialize the Disk Status screen displays. This function takes several minutes.

Note: Do not press F16 to go to the DST main menu. Wait for the next display. The Disk Configuration Attention Report menu may display.

__ Step 10. Press **F10** to continue. The IPL or Install the System menu displays.

__ Step 11. Select **option 3** (Use Dedicated Service Tools (DST)).

__ Step 12. Sign in using **QSECOFR/QSECOFR** and press **Enter**.

__ Step 13. Change password to **SECOFR**, verify and press **Enter**.

__ Step 14. From the Use Dedicated Service Tools display, select **option 4** (Work with disk units).

__ Step 15. From the Work with disk units display, select **option 1** (Work with disk configuration).

__ Step 16. From the Work with Disk Configuration display, select **option 3** (Work with ASP configuration).

__ Step 17. From the Work with ASP configuration display, select **option 3** (Add units to the ASPs).

__ Step 18. Select each unit by typing a **1** in the space provided on the Specify ASPs to Add Units to display. Press **Enter**. A Problem Report displays, read and then press **F10** to ignore and continue.

__ Step 19. From the Confirm Add Units display, press **F10** to Add and Balance the information on each disk, equalizing the usage of space. The Function Status screen displays. This function takes several minutes. Wait for next display. The menu appears.

__ Step 20. Press **F3** to exit the Work with ASP configuration display.

__ Step 21. Press **F3** on the Work with Disk Units display.

Install the OS/400 operating system

Your server now contains the Licensed Internal Code. You should see the Use the Dedicated Service tools (DST) display.

__ Step 1. Select **option 2** (Install the Operating System) from the Use Dedicated Service Tools (DST) display.

__ Step 2. Select **option 2** (Optical (CD)) from the Install Device Type Selection display.

__ Step 3. Press **Enter** to confirm the install of OS/400.

__ Step 4. After a few seconds, a message displays (CPA2055), indicating that it is time to change CDs. Load the first volume of installation media that contains OS/400.

Note: If you are using IBM-supplied media, the first volume is labeled B_1930_01. Throughout these procedures, load the next volume when prompted by the server. When you are performing installation tasks from optical media, wait until the In Use indicator goes out before your continue. The final volume used to complete the operating system installation is labeled B_1930_02.

__ Step 5. Press **1** and then **Enter** to continue. The Install the Operating System menu displays.

__ Step 6. On the Install the Operating System menu, select Option **1** (take defaults) and then press **Enter** to complete the following tasks.

The following tasks are performed by the server during this phase of installation:

a. Create needed profiles and libraries.
b. Restore programs to library QSYS.
c. Restore language objects to library QSYS.
d. Update program table.
e. Install Database files.
f. Complete OS/400 installation.

When the OS/400 Main Menu appears, you have completed the task of installing the OS/400 operating system.

Set the system values

To meet Common Criteria security requirements, you must activate security on your system immediately after installing the base operating system. To activate security, you set the security level (**QSECURITY**) system value. In addition, you should set some other system values that are required for your system to meet Common Criteria security requirements.

Note: You will set additional system values later when you run the Common Criteria customization programs. See "Run the Common Criteria customization programs" on page 32.

1. Sign in as **QSECOFR** and press **Enter**. This may take some time. The IPL Options screen displays.
2. On the IPL Options display, move the cursor to the row that contains the **System time zone** field and specify the **identifier of a time zone** or press **F4** to open the Select Time Zone Description display.
3. If you are using the Select Time Zone Description dialog to select a time zone, complete the following:
   a. On the Select Time Zone Description display, type **1** next to the time zone that you want to use.
   b. Press **Enter** to return to the IPL Options display. The System time zone field is updated with the time zone you selected.
4. Ensure the System time and System date fields are correct.
5. In the Define or Change the System at IPL field, select Y.
6. Press **Enter** to continue the IPL.

   Note: If you set the **System time zone** field on the IPL Options display, then this new value takes precedence over the previous value set by the system as described in the initial value time zone setting.
7. Press **Enter** once the Set Major System Options screen displays. The Define or Change the System at IPL screen displays.
8. Select **option 3** (System Value commands) and press **Enter**.
9. Select **option 3** (Work with system values) and press **Enter**.
10. Select **QALWUSRDMN** value and type **2** next to the system value, then press **Enter**.
11. Locate ***ALL** on the menu and type **QTEMP** over it for the **QALWUSRDMN** value, and press **Enter**.

    Note: You may specify additional libraries for the **QALWUSRDMN** system value if your applications require them and your auditor or DAA has approved them. However, you will not be running an evaluated Common Criteria security configuration.

    The Change System Value dialog displays again with a confirmation message.
12. Press **Enter** to view the Work with System Values display.
13. Locate the **QSECURITY** system value on the display and type a **2** in front of it. Then press **Enter**.
14. Type **50** for the new value of the **QSECURITY** system value and press **Enter**. This sets the security level of your system to 50.
15. Press **F3** to exit the Work with System Values display and return to the System Value Commands screen.
16. Press **F3** to return to the Define or Change the System at IPL screen.
17. Press **F3** to continue the IPL. You may see a blank display, and several displays that do not require your response. If the Edit Rebuild of Access Paths dialog displays, press **Enter** to continue.
18. Press **Enter** for each message display that appears during this task. Do not respond to blank displays.
19. The signon Information menu displays, indicating that the password has expired for the QSECOFR user profile. Press **Enter** to view the Change Password dialog.
20. After you change the password, the Work with Software Agreements screen displays. Type 5 by each of the items to display them and press **Enter**. The first Software agreement displays.
21. Select F14 to accept each agreement one at a time. Press **Enter** to confirm your selections.
22. Verify that the Accept status for each program is YES and then press **Enter** to continue.
23. Press **Enter** to clear any Display Messages that occur. The OS/400 Main menu displays.
24. To test the new password, type 90 to sign off the system and press **Enter**. The Sign On menu displays. The password prompt appears, indicating that security is active on your system.

25. Press Tab to move between fields. Fill in the User and Password fields, entering the new password that you have assigned to the QSECOFR profile.

    Note: You will not see your password as you type it. This is a security feature.
26. Press **Enter** to submit your credentials. If it is accepted, the Main Menu displays.

Install licensed programs

To meet the requirements of Common Criteria security, you must install individually the optional parts of the operating system and additional licensed programs. Some OS/400 options and licensed programs have been evaluated for Common Criteria security. Other licensed programs run in system state and have not been evaluated as part of the Target of Evaluation (TOE). Licensed programs that have not been evaluated and run in system state should not be installed on a Common Criteria evaluated system.

1. Sign onto the system with the security officer (**QSECOFR**) user profile. The OS/400 Main Menu appears.
2. Load the media volume that contains the licensed programs on your system installation device. The volume is labeled B_1930_01.
3. Type **CHGMSGQ QSYSOPR *BREAK SEV(90)** and press **Enter**.
4. Press **Enter** to clear any messages that display.
5. Type the command, **ENDSBS *ALL *IMMED** and press **Enter**.
6. Type the command, **WRKSBS** and press **Enter**.
7. Press **F11** to display system data.
8. Verify that all subsystems have a restricted status, and Press **F3** to exit and return to the main menu.
9. Type **GO LICPGM** and press **Enter**.
10. The Work with Licensed Programs menu displays:
    a. Select **option 5** (Prepare for installation):
    b. Select the option to work with software agreements and press **Enter**.
    c. Type **5** to display the licensed programs that you want to install and press **Enter**.
    d. Press **F14** to accept the software agreements and then press F3 until you return to the Work with Licensed Programs display.
11. On the Work with Licensed Programs menu, Type **11** to Install licensed programs and press **Enter**.
12. A list of licensed programs that are available for installation displays. To conform to the Common Criteria security evaluation standard, select the items to install from the "Software for the Target of Evaluation" on page 6.
13. Type a **1** next to each option that you want to install and press **Enter**.

    Note: Some options are mandatory, such as **QGPL**, and by default are already selected to install.
14. There are some items that are required for installation, but need to be manually added to the list of licensed programs. Add the following products and all their options: 5722AC3, 5769FNT, 5769FN1. To add options to the list of licensed programs to install, perform the following steps:
    a. At the top of the licensed program table on the Install Licensed Programs screen, there is a blank entry which allows you to add a product to the list. Type **1** in the Option column of this blank product entry line to indicate that you want to install an additional product.
    b. Type the product number of the product that you want to install in the **Licensed Program** column.
    c. Type the **Option number** in the **Product Option** column or ***ALL** if all options of this product should be installed.
    d. Press **Enter** to add this licensed program to the list of items to install. Repeat these steps for additional items that you want to install that are listed in the TOE but are not listed in the licensed program display.
15. Once you have completed the list of items to install, press **Enter**.

16. Press **Enter** to confirm your selection of items to install.
17. Specify the Name of the Installation device **OPT01** on the Install Options display.
18. Select **option 1** (Programs and language objects) for the **Objects to Install** field.
19. Select **option 2** (Display software agreement) for the **Nonaccepted agreement** field.
20. Select **N** to deny an automatic IPL.
21. Press **Enter** to begin the installation of the licensed programs that you have selected. Display messages will appear throughout the installation process, indicating that you need to change discs to continue the installation. After you have received and responded to each message, type **G** to reply to the message, indicating that you want to continue the installation process and press **Enter**.

    The installation process continues until the next disk is needed, or a problem is encountered.

    Note: Each time you install a new disk into the system during the installation process, wait for the Optical drive to finish reading the disk before you press **Enter** on your display message reply. Most optical drives have an LED indicator which flashes during the reading process, and stops flashing when the reading process is complete.
22. If a licensed program requires acceptance of a software agreement, the Software Agreements display appears. Perform one of the following tasks:
    a. Press **F14** to accept the agreement and allow the licensed program to continue installing.
    b. Press **F16** to decline the agreement and end the installation of that licensed program.

    The Work with Licensed Programs display appears when the installation process is completed.
23. Select **option 10** to verify all of the products have installed properly and have the status ***COMPATIBLE** or ***INSTALLED**. If the final completion message indicated success, you have successfully completed the installation of the licensed programs.

Install a secondary language

You may install one or more secondary languages on your system. When you install a secondary language, the system restores additional displays and help information. No changes are made to any of the operating system programs. A secondary language does not affect the security of your system.

Install a PTF package

Feature code 1930 of the OS/400 Licensed Program includes a cumulative PTF (program temporary fix) package that has been evaluated for Common Criteria security. The documentation that you receive with the feature code 1930 identifies which PTF volume has been evaluated for Common Criteria security. Use this volume to install the PTFs.

First-time PTF installation only!

Use these instructions only if this is the first set of PTFs that you are installing on your system. If you already have PTFs installed, you must use the instructions in the OS/400 PTF Shipping Information Letter.

Perform the following steps to install the PTFs:

1. If you are not already signed on the system as the security officer (**QSECOFR**), sign off the system and sign on as **QSECOFR**.

   To sign off, type **signoff** and press **Enter**. On the Sign On display, type the following:

   - **QSECOFR** in the **User** field
   - The password in the **Password** field

   Press **Enter**.
2. Type the following and press **Enter**:

   ```
   CHGSYSVAL SYSVAL(QIPLTYPE) VALUE('0')
   ```

This sets up your system to perform an unattended IPL.

3. Place your system in **B Normal** mode using the system control panel.
4. Perform the following steps to ensure that there are no jobs running and no users signed onto the system:
   a. Type **CHGMSGQ QSYSOPR *BREAK SEV(60)** and press **Enter**.
   b. Press **Enter** to clear any messages that display.
   c. Type **ENDSBS *ALL *IMMED** and press **Enter**.
   d. While subsystems end, one or more messages display that require your action. Press **Enter** to clear each message.
   e. Type **CHGMSGQ QSYSOPR *BREAK SEV(95)** and press **Enter**.
   f. Press **Enter** to clear any messages that display.
5. Load the volume for the cumulative PTF package into the installation unit. On the Media Description report that accompanied your media, the Common Criteria PTF disc is listed under the program feature 1930. The first volume is labeled C4272530_01. There are four volumes.

   Note: Do not use the disc that is marked Cum PTFs. It includes PTFs that have not been evaluated for Common Criteria security.
6. Type **GO PTF** and press **Enter**.
7. Select **option 8** (Install Program Temporary Fix Package) and press **Enter**. The Install Options for Program Temporary Fixes menu displays.
8. Type the name of the device that you are using (example, **OPT01**) in the **Device** field.
9. Type **Y** in the **Automatic IPL** field.
10. Type **1** (Single PTF volume set) in the **Prompt for media** field.
11. Type ***SYS** in the **Restart Type** field.
12. Type **Y** in the **Other Options** field and press **Enter**.
    - If you see the Confirm Install of Lic Int Code Fixes display, you must restart the system. After it has restarted it will be in the correct state to install PTFs to the Licensed Internal Code. Press **F10** to start the IPL. Press **Enter** if the Display messages dialog displays.
    - If you see the Confirm Automatic IPL dialog display, follow the instructions in the dialog and then continue with the next numbered step.
13. Type **N** in the **Omit PTFs** field.
14. Type **1** (All PTFs) in the PTF type field and press **Enter**. You must install all PTFs to have an evaluated Common Criteria evaluation.
15. The PTF load progress displays on the console, and the view refreshes periodically to indicate the current status.

    Notes:
    a. If you have more than one volume of PTFs to install, you will receive prompts to load the next volume. After you have loaded the next volume in the PTF package, type **G** to continue the installation.
    b. During the power down of your service partition for IBM eServer i5, reference code **D6xx430B** or **D6xx430A** may display for an extended period of time. The ″xx″ digits increment periodically. This is a normal part of processing when the server firmware code is being updated.
    c. During the IPL, the reference code **C900 2967** may display on the system unit control panel for an extended period of time. This is a normal occurrence. You may also notice that two power down sequences with a change to the IPL side that is displayed on the system unit.
    d. While applying PTFs, the system may need to reorganize part of the Licensed Internal Code. This can take up to an hour. The following reference codes display during this reorganization: **C600 4400** and **C600 4401**.

    The system performs an IPL when all of the PTFs that you selected are installed.

16. Sign on as **QSECOFR** when the Sign On menu appears.
17. Load the volume for the special PTF package into the installation unit. This volume is labeled C_1930_01.
18. Repeat step 4, as well as steps 6 through 16.
19. Remove the PTF media volume.

You have now completed installing the operating system, licensed programs, and an evaluated PTF package.

Chapter 5. Configure TCP/IP

The steps in this section will guide you through TCP/IP configuration that is designed to meet the requirements for Common Criteria security. Performing updates to your server, such as “Set up the server for iSeries Access for Windows” on page 37 require you to complete these configuration tasks.

Before you start configuring TCP/IP, you need to collect all of the required preliminary information about your network; for example, the IP address and Subnet mask for your system, etc. Work with your network administrator to obtain this information. For additional information, see the TCP/IP information topic in the iSeries Information Center.

You also need to ensure that the appropriate hardware adapters and the appropriate software are installed on all of the systems that will be in your network.

In addition, you should have access to the V5R3 version of the iSeries Information Center.

Note: To determine whether the TCP/IP LP is installed, type

```
GO LICPGM
```

(Go licensed program) on the command line and press **Enter**. The Work with Licensed Programs display appears. Type **10** and press **Enter** to display the installed licensed programs. If the 5722TC1 TCP/IP Connectivity Utilities for OS/400 is not installed on your system, see “Install licensed programs” on page 22 to complete the installation. Rerun the customization programs, and then continue with this section to complete the TCP/IP configuration on your OS/400.

Press **F3** to exit the Work with Licensed Programs display.

You may not need to create a new line description. If a physical line is already configured, this line can be used. To determine if a physical line description already exists, follow these steps:

1. Type

   ```
   WRKHDWRSC *CMN
   ```

   on the command line, and press **Enter**.

   The Work with Communications Resources menu displays.

   In this example, there is already one Ethernet adapter installed with the resource name of CMN04. To determine if a line description exists for this adapter, use **Option 5** (Work with configuration descriptions).

   If a line description does not exist, then `*NONE` is displayed in the Description column. To create a line description, type **1** in the top **Opt** field and type a line description such as `ETHTCP`. Press **Enter**.

   If a line description exists, the name of the line description is displayed as shown in the above example. This is the information you need to continue with the TCP/IP configuration.
2. The Create Line Description command prompt displays. This example illustrates the creation of an Ethernet line description. The creation of a Token Ring line description is similar.

```
                  Create Line Desc (Ethernet)  (CRTLINETH)
Type choices, press Enter.

Line description . . . . . > ETHTCP          Name
Resource name    . . . . . > CMN04           Name, *NWID, *NWSD
Online at IPL    . . . . .   *YES            *YES, *NO
Vary on wait     . . . . .   *NOWAIT         *NOWAIT, 15-180 seconds
Local adapter address  . . .   *ADPT         020000000000 - 7EFFFF...
Exchange identifier  . . . .   *SYSGEN       05600000 - 056FFFFF, *SYSGEN
Ethernet standard  . . . . .   *ALL          *ETHV2, *IEEE8023, *ALL
Enable only for TCP/IP . . . .   *NO          *YES, *NO
Line speed . . . . . .   10M                 10M, 100M, *AUTO
Duplex . . . . . .   *HALF                   *HALF, *FULL, *AUTO
SSAP list:
Source service access point  . .   *SYSGEN   02 - FE, *SYSGEN
SSAP maximum frame . . . . . .               *MAXFRAME, 265 - 1496, 265 ...
SSAP type  . . . . . .                       *CALC, *NONSNA, *SNA, *HPR
                 + for more values
```

In this example, we gave the new line description the name ETHTCP. The resource name field is automatically filled in with the value from the Work with Hardware Resources display.

For Ethernet lines, press **F10** to display additional parameters and type *YES for the value of the Auto-create controller parameter.

Press **Enter** to create the line description.

Press **F3** twice.

3. At the command prompt, type CFGTCP to display the Configure TCP/IP menu and press **Enter**. Use this menu to select configuration tasks. Take a few moments to review the menu before starting to configure your server.
4. To define a TCP/IP interface, Select option 1 (Work with TCP/IP interfaces) and press **Enter**.
5. Specify option 1 (Add) to show the Add TCP/IP Interface display, and press **Enter**.
6. Specify the address value that you want to represent your server, the subnet mask address, and the line description name you previously defined, and then press **Enter**.

   The default for a newly-defined interface is to automatically start when the TCP/IP is activated with the Start TCP/IP (**STRTCP**) command.
7. To start the TCP/IP interface, specify option 9 (Start) and press **Enter**.
8. To add a host table entry to the local host table on your system, select option 10 (Work with TCP/IP Host Table Entries) from the Configure TCP/IP menu, and press **Enter**.
9. Specify option 1 (Add) to go to the Add TCP/IP Host Table Entry display, and press **Enter**.
10. Specify the IP address, the associated local host name and the fully qualified host name, and then press **Enter**.
11. Press F3 to return to the Configure TCP/IP menu.
12. To configure a default route, select option 2 (Work with TCP/IP Routes) on the Configure TCP/IP menu, and press **Enter**.
13. Specify option 1 (Add) to go to the Add TCP/IP Route (ADDTCPRTE) display, and press **Enter**.
14. Specify *DFTROUTE for the route destination, specify *NONE for the subnet mask, specify the IP address for the next hop, and press **Enter**.
15. Press F3 to return to the Configure TCP/IP menu.
16. To define local domain and host names, select option 12 (Change TCP/IP domain) from the Configure TCP/IP menu, and press **Enter**.
17. Specify the names you selected to be your local host name and local domain name, leaving the other parameters at the default values, and press **Enter**.
18. Type

    STRTCP STRSVR(*NO)

on the command line and press **Enter**. The STRTCP command starts TCP/IP processing and starts the TCP interfaces that have been configured to start automatically. No TCP/IP server jobs are started because the STRSVR(*NO) parameter indicates that they should not be started. While specifying this parameter is not absolutely necessary, it does prevent a couple of TCP/IP server jobs from starting which cannot be configured to not automatically start and which are not used by a Common Criteria evaluated system.

Type:

```
STRTCPSVR SERVER(*TELNET *FTP *REXEC)
```

and press **Enter**. The Start TCP/IP Server (STRTCPSVR) command starts the TCP/IP servers specified in the SERVER parameter. You do not have to specify all three servers, but these are the only TCP/IP servers that should be started on a Common Criteria evaluated system.

After a few moments, type

```
WRKACTJOB SBS(QSYSWRK)
```

on the command line and press **Enter**. The job **QTCPIP** should be in the list (along with other TCP/IP application server jobs, such as **QTFTPnnnnn**, **QTVTELNET**, and **QTVDEVICE**).

19. To verify the TCP/IP connection from your system to another system attached to your network, type **PING** (or **VFYTCPCNN**), and then either the host name or the IP address of the system you are trying to contact on the command line, and press **F4**. The command prompt screen displays.
20. Specify the host name of another system in your network and press **Enter**.

    Note: The remote system must have TCP/IP started in order to successfully PING it.

    If the PING operation is successful, the job log should contain messages similar to the following:

```
ping gensys
Verifying connection to host system gensys.domain.name at address 199.5.83.1.
Connection verification 1 took .003 seconds.  1 successful connection verifications.
Connection verification 2 took .002 seconds.  2 successful connection verifications.
Connection verification 3 took .003 seconds.  3 successful connection verifications.
Connection verification 4 took .002 seconds.  4 successful connection verifications.
Connection verification 5 took .002 seconds.  5 successful connection verifications.
Round-trip (in milliseconds) min/avg/max = 2/2/3
Connection verification statistics:  5 of 5 successful (100 %).
```

    If the PING operation is unsuccessful, the job log should contain messages similar to the following:

```
ping gensys
Verifying connection to host system gensys.domain.name at address 199.5.83.1.
No response from host within 1 seconds for connection verification 1.
No response from host within 1 seconds for connection verification 2.
No response from host within 1 seconds for connection verification 3.
No response from host within 1 seconds for connection verification 4.
No response from host within 1 seconds for connection verification 5.
Connection verification statistics:  0 of 5 successful  (0 %).
```

    If this occurs, check your configuration steps. Also check that the configuration at the remote system is correct, the remote system is powered up, and TCP/IP has been started on the remote system.
21. Verify the System Name matches the host name you entered in the previous steps. If not, change the System Name to match the host name. At the command line, type CHGNETA and press F4 to display the Change Network Attributes (CHGNETA) menu.
22. Type the new name in the following three fields:
    - System name
    - Local control point name
    - Default local location name

You have just completed the TCP/IP configuration that meets the requirements for Common Criteria security.

Chapter 6. Customize the OS/400 system for Common Criteria security

Once you have performed the installation tasks required for a Common Criteria evaluated system, you can begin the process of customizing your system according to the Common Criteria security requirements.

Attention: The IBM user profile, QSECOFR, has the required level of authority for the following procedures.

Set up initial security

You need to establish initial security for your newly installed system before you perform any configuration tasks or further customize your OS/400 system for Common Criteria security. Take the following steps to begin protecting your system immediately:

1. Secure physical access to your system.
2. Create one or more security officer profiles to provide individual accountability.
   Example: **CRTUSRPRF USRPRF(XXXXX) PASSWORD(yyyyy) PWDEXP(*YES) USRCLS(*SECOFR)**
3. Change the IBM supplied service tools user ID passwords:
   a. Type the command **STRSST**.
   b. Sign on with QSECOFR. If you have not change the password for the **QSECOFR** service tools user ID, use the default password.
   c. Select **option 8** (Work with service tools user IDs and Devices).
   d. Select **option 1** (Service tools user IDs).
   e. Select **option 2** (Change password) for each of the IBM supplied service tools user IDs.
   f. Type a new password for the service tools user ID.

   Note: The following are the IBM supplied service tools user IDs: QSECOFR, QSRV, 11111111, and 22222222.

Set up initial auditing

After you install the operating system and licensed programs on your system, you should start the security auditing function. The audit log provides a record of security-relevant activity that occurs when you are setting up your system and loading applications.

For example, an audit log may be written if a system state program is restored outside the licensed program installation process.

Note: System state programs can be created only by IBM. System state programs should be restored only during the licensed program installation process or during a recovery.

Another example is an audit record that may be written if a user profile is created or changed.

The customization program creates the security audit journal, the security audit journals initial receiver, and changes system values that will activate security auditing on your system. The customization program does all of this with one invocation of the Change Security Audit command:

```
CHGSECAUD QAUDCTL(*AUDLVL *OBJAUD *NOQTEMP)
QAUDLVL(*AUTFAIL *CREATE *DELETE
*SERVICE *SECURITY *JOBDTA
*PGMADP *PGMFAIL)
```

If necessary the CHGSECAUD command will create the security audit journal and the initial receiver. The security audit journal is QSYS/QAUDJRN *JRN. The default initial receiver is QGPL/AUDRCV0001. However, you can override the initial journal receiver value. The customization program does not activate all the audit options that are available. Use the auditing information in Chapter 9 of the *iSeries Security Reference* to determine whether the values that are set by the customization program meet your auditing and performance requirements.

Notes:

1. Common Criteria security requires a set of auditing capabilities on the system. When and to what extent you activate auditing on your system should be determined by your auditor or Designated Approving Authority (DAA).
2. When the Security Audit journal is created through the CHGSECAUD command, the journal is system managed. Journal receivers will be detached automatically when they fill. If you audit many objects or actions, you can consume a great deal of storage with the detached receivers. To avoid using too much auxiliary storage, be sure to regularly save your detached receivers and delete them from the system.

Run the Common Criteria customization programs

Use the Common Criteria customization programs that are provided as part of the cumulative PTF (program temporary fix) package to perform the additional tasks required for Common Criteria security. The customization programs perform the following tasks:

- Set system values.
- Change the public authority for some commands.
- Change the public authority for some programs.
- Change the public authority for some objects.
- Change the default values for some commands.
- Change the signon error messages.
- Limit the use of TCP on the system.

Appendix A, "Customization programs," on page 123 provides more information about the customization programs. Different customization programs do different tasks. However, there is one driver program that will call them all.

To run the programs, do the following:

1. Sign on with a security administrators profile. You can use **QSECOFR** or a security office profile that you created as described "Set up initial security" on page 31.
2. To submit the job that runs the programs for the **QSYS** (system) library, type the following and press **Enter**:

```
SBMJOB CMD(CALL PGM(QSYS/QSYCCDRV)) JOB(QSYCCDRV) LOG(4 0 *SECLVL) SPLFACN(*KEEP)
```

   The customization program will run for several minutes.To determine if the job has finished, type the command **WRKSBMJOB** and press **Enter**. Find the job **QSYCCDRV** in the list. When the status becomes **OUTQ**, the job has finished. While your on the **WRKSBMJOB** screen, use **F5** to refresh the screen to get the current status. Press **Enter** to return to the command entry screen.
3. If you do not have secondary languages on your system, skip to 7 on page 33.
4. For each secondary language on your system, perform 5 on page 33 and 6 on page 33. Substitute the name of the system library for the secondary language in place of QSYSxx.

5. Run the program that restricts authority to commands by typing:

```
SBMJOB CMD(CALL PGM(QSYS/QSYCCCCA) PARM(QSYSxx)) JOB(QSYCCCCA) LOG(4 0 *SECLVL) SPLFACN(*KEEP)
```

   Press **Enter**.

   The customization program will run for several minutes.

   To determine if the job has finished, type the command **WRKSBMJOB** and press **Enter**. Find the job **QSYCCCCA** in the list. When the status becomes **OUTQ**, the job has finished. While on the **WRKSBMJOB** screen, use **F5** to refresh the screen to get the current status. Press **Enter** to return to the command entry screen.

6. Run the program that changes the default value for parameters for some commands by typing:

```
SBMJOB CMD(CALL PGM(QSYS/QSYCCCCD) PARM(QSYS)) JOB(QSYCCCCD) LOG(4 0 *SECLVL) SPLFACN(*KEEP)
```

   Press **Enter**.

   The customization program will run for several minutes.

   To determine if the job has finished, type the command **WRKSBMJOB** and press **Enter**. Find the job **QSYCCCPA** in the list. When the status becomes OUTQ, the job has finished. While on the **WRKSBMJOB** screen, use **F5** to refresh the screen to get the current status. Press **Enter** to return to the command entry screen.

7. The customization program prevents user profiles with ***ALLOBJ** or ***SERVICE** special authority from signing on except at the console. This is done by setting the system value **QLMTSECOFR** to **1**. This is a recommended value, not one that is required for Common Criteria. If you want to allow users with ***ALLOBJ** or ***SERVICE** special authority to sign on at other workstations, you must do one of the following:
   - Change the system value **QLMTSECOFR** to **0**. This option allows ***ALLOBJ** or ***SERVICE** special authority users to sign on to any work station:

     Type **QSYS/CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('0')** and press **Enter**.
   - Grant the target user explicit authority to the devices they are allowed to sign on:

     Type **GRTOBJAUT OBJ(QSYS/device-name) OBJTYPE(*DEVD) USER(QSECOFR-or-target-user) AUT(*CHANGE)** and press **Enter**.

   Attention: If you enable automatic configuration of devices, use **dsp*** where the command says *device-name* to grant authority to all display devices. Otherwise, type the command for every workstation device to which you want to grant authority.

Analyze the need for an IPL

The **QSYCCSVL** program, which is called by the customization driver, program sets 2 system values that require an IPL to take effect. The system values are **QSECURITY** and **QPWDLVL**. The command DSPSECA (Display Security Attributes) will show the current values and the pending value for both of these system values. An IPL is required if there is a pending value for either system value:

1. Type the command **DSPSECA**.

   An IPL is necessary if the **Pending security level** value is **50** or the **Pending password level** value is **3**.

   - Example output when an IPL **is** required:

```
Display Security Attributes
System: xxxxxxxx
User ID number . . . . . . . . . . . . . . . : 1446
Group ID number . . . . . . . . . . . . . . . : 135
Security level . . . . . . . . . . . . . . . : 40
Pending security level . . . . . . . . . . . : 50
Password level . . . . . . . . . . . . . . . : 0
```

```
Pending password level . . . . . : 3
Allow change of security related system
values . . . . . : *YES
Allow add of digital certificates . . . . : *YES
Allow service tools user ID with default
and expired password to change its own
password . . . . . : *NO
```

- Example output when an IPL is **not** required:

```
Display Security Attributes
System: xxxxxxxx
User ID number . . . . . : 1446
Group ID number . . . . . : 135
Security level . . . . . : 50
Password level . . . . . : 3
Allow change of security related system
values . . . . . : *YES
Allow add of digital certificates . . . . : *YES
Allow service tools user ID with default
and expired password to change its own
password . . . . . : *NO
```

2. If an IPL is not required, continue with the procedure, "Analyze the results of customization." If an IPL is required, continue with the following steps.
3. Type the command, **PWRDWNSYS OPTION(*IMMED) RESTART(*YES)** and press **Enter**.
4. Following the IPL, sign on with a security administrators profile. You can use **QSECOFR** or a security office profile that you created as described in "Set up initial security" on page 31.
5. Type the command **DSPSECA**. Verify that there are no pending values on the display.
6. If the system value QPWDLVL was not set to 2 or 3 when the QSYCCSVL program was run, the program would not have been able to set the QPWDMAXLEN (maximum password length) system value to the recommended value of 128 characters. If you want to ensure the QPWDMAXLEN system value is set to the recommended value, type the command, **QSYS/CHGSYSVAL SYSVAL(QPWDMAXLEN) VALUE(128)** and press **Enter**.

Analyze the results of customization

After you have run the customization programs, you should analyze the results for two purposes:

- Ensure that the programs ran successfully by reviewing the job logs:
  1. If you have signed off, sign on with the same profile that issued the SMBJOB commands.
  2. Type the following and press **Enter**:

     WRKSBMJOB

     You are shown a list of jobs that were submitted by the user.
  3. Next to the job **QSYCCDRV**, type **8** (Work with spooled files) on the console keyboard.

     You are shown the Work with Spooled Files display. The output is usually between 150 and 200 pages long. If you want to view the output Online, skip to 6.
  4. To print the output, use the Release Output Queue (RLSOUTQ) command to send this spooled file (and any others in the output queue) to the printer.
  5. Review the output for errors. Continue with 9 on page 35.
  6. To view the output, type **5** (Display) in the *Option* column and press **Enter**. The Display Spooled File screen displays.
  7. Page down several times to become familiar with the format of the output.

8. When you are familiar with the output format, use the **Find** function to look for the **Escape** and **Diagnostic** character strings. Press **F16** to start a search after typing the characters in the **Find** field.
9. If any commands did not complete successfully, determine why. Some Escape and Diagnostic messages are normal and represent expected situations. For example, messages indicating that objects of a certain type could not be found is not a problem if no such objects exist. A real problem would be if a system value was not set successfully or if the authority change to a command or program that exists on the system is not successful. After you have corrected any problems, run the program again.
10. If you ran any additional customization jobs for secondary language libraries, repeat 3 on page 34 through 9 for the additional jobs.

- Analyze the functions that are performed by the program to ensure that they meet your security requirements. In particular, review the settings for system values. The settings are listed in the table, Table 16 on page 134. Perform the following steps:
  1. Read the descriptions of the system values that were set to be sure that you understand their functions. The table, Table 16 on page 134, shows the settings that are required and recommended for Common Criteria security. Refer to the "System values" information topic that is located in the iSeries Information Center for system value descriptions.
  2. Type **WRKSYSVAL** and press **Enter**.
  3. Do the following for each system value that was set by the program:
     a. Locate the system value on the display. (You can use the **Position to** function or the arrow and page down (roll up) keys.
     b. Display the setting by typing **5** (Display) in the **Option** column and make note of the setting.
     c. Press **Enter**.
     d. If the recommended (not required) setting does not match the information in or if the setting does not meet your requirements, type **2** (Change) in the option column. The Change System Value screen displays.

        Change the setting to the required value.

        Press **F12** (return).
  4. Check all group profiles to ensure they don't have passwords. See Chapter 9, "Auditing Security on the iSeries System" in the *iSeries Security Reference* for details.

After the system values have been set and all necessary IPLs have been completed, it is recommended that you lock down the system value. To lock down the system values, follow these steps:

1. Type the command **STRSST** on the command line.
2. Sign on with Service Tools User ID **QSECOFR**, using the password that you established during the installation procedure.
3. Select **option 7** and press **Enter**.
4. Set the **Allow system value security changes** value to **2** (no) and press **Enter**.

   Note: You must press **Enter** for the value to take effect.
5. Select **option 7** to verify the change (this is an optional step).
6. Press **F3** or **F12** to exit the menu.
7. Press **F3** to exit **System Service Tools**.
8. Press **Enter** to return to the **Command Entry Screen**.

Note: Security related system values cannot be changed unless an administrator goes back into the System Service Tools and sets the **Allow system value security changes** value to **1** (yes).

Chapter 7. Install iSeries Access for Windows

iSeries Access for Windows is the solution for PC-to-server connectivity. Using the iSeries Access for Windows functions, you can use your PC desktop to access and administer your servers. Additionally, users who install iSeries Access for Windows on their PC can use its applications, such as iSeries Navigator, access your server and perform their tasks.

To use iSeries Access for Windows, you must install and configure software on both an iSeries server and a PC.

Note: If you already installed iSeries Access for Windows during the procedure, "Install licensed programs" on page 22, you do not need to repeat this task. However you still need to perform the following tasks:

- "Set up the PC for installation of iSeries Access for Windows" on page 38

Use this information to guide you through the steps necessary to install and configure iSeries Access for Windows on the iSeries server. iSeries Access for Windows needs to be installed on your server before you can install iSeries Access for Windows service packs on your server. After installation on your server, you or your users can install iSeries Access for Windows from the iSeries server to the client PCs.

Set up the server for iSeries Access for Windows

iSeries Access for Windows needs to be installed on your server before you can install iSeries Access for Windows service packs on your server. After installation on your server, you can install iSeries Access for Windows from the iSeries server to the client PCs.

Notes:

1. In order to install on the server, you need a security level of Security Officer (*SECOFR). This is the highest level of security on the server. This security level is required for installation only, not for regular use of iSeries Access for Windows.
2. Your server must have sufficient storage to install iSeries Access for Windows or the installation cannot be completed. This installation requires approximately 170MB of space.

The following steps guide you through installing iSeries Access for Windows (5722-XE1) on the server:

1. Sign off all workstation users and end all connections.
2. Sign on to the iSeries server with ***SECOFR** authority.
3. Configure iSeries NetServer™ on your server:

   Note: The following configuration instructions require you to already have access to a PC that has iSeries Navigator installed. This means you need to complete the procedure, "Set up the PC for installation of iSeries Access for Windows" on page 38, on a PC and ensure that you have installed iSeries Navigator on that PC.

   To configure your server for iSeries NetServer support with iSeries Navigator, do the following:

   a. Use the iSeries NetServer wizard:
      1) Open a connection to iSeries Navigator on your server.
      2) Expand **Network**.
      3) Click **TCP/IP**.
      4) Right-click **iSeries NetServer** and click **Configuration**.
   b. Follow the prompts provided by the wizard.

4. For easier management and resolution of TCP/IP addresses, add an entry for the iSeries NetServer to a Domain Name Server (DNS).
5. Changes made to your iSeries NetServer properties do not take effect until the next time iSeries NetServer is started. To start or stop iSeries NetServer:
   a. Open a connection to iSeries Navigator on your iSeries server.
   b. Expand **Network**.
   c. Expand **Servers**.
   d. Click **TCP/IP**.
   e. Right-click **iSeries NetServer** and click **Start** or **Stop**.

This completes the install of iSeries Access for Windows and the configuration of your server.

Set up the PC for installation of iSeries Access for Windows

Users and administrators alike can use this information to set up a PC for iSeries Access for Windows use, and to install iSeries Access for Windows on workstation computers. There are several tasks to perform in order to complete the PC setup of iSeries Access for Windows:

- "Set up TCP/IP on the PC" on page 39
- "Verify TCP/IP configuration on the PC" on page 41
- "Install iSeries Access for Windows from iSeries NetServer" on page 42

Prerequisites to set up the PC for iSeries Access for Windows

Ensure that the PC you are installing iSeries Access for Windows on meets the following requirements:

Table 5. PC requirements — Processor, memory, and service pack level

Operating system	iSeries Access for Windows	iSeries Access for Windows with iSeries Navigator
Windows NT® 4.0	Pentium® 100 MHz and at least 32 MB, Microsoft® Windows NT Service Pack 6a and Microsoft Internet Explorer 5.01 or later	Pentium 850 MHz minimum and at least 256 MB, 512 MB recommended Microsoft Windows NT Service Pack 6a and Microsoft Internet Explorer 5.01 or later
Windows 2000	Pentium 133 MHz and at least 64 MB	Pentium 850 MHz minimum and at least 256 MB, 512 MB recommended
Windows XP	Pentium 233 MHz and at least 128 MB	Pentium 850 MHz and at least 256 MB, 512 MB recommended
Windows Server 2003, 32-bit PC	Pentium 133 MHz and at least 128 MB	Pentium 850 MHz and at least 256 MB, 512 MB recommended
Windows Server 2003, 64-bit PC	Pentium 733 MHz and at least 192 MB	Pentium 850 MHz and at least 256 MB, 512 MB recommended

Notes:

1. Microsoft Windows Server 2003 comes in several editions. The hardware requirements vary by edition. See Microsoft's Web site for base requirements information for all editions.
2. If you do not plan to use iSeries Navigator for anything other than managing your iSeries connections (adding, removing, and changing connection properties), it is recommended that you do not install the iSeries Navigator base component. Installing that component will result in higher memory usage when managing your iSeries connections.

Table 6. Other PC requirements

PC requirement	Value
Disk Space - Install	• Typical - 148 MB (approximately) • PC5250 User - 39 MB (approximately) • Full - 221 MB (approximately) • Custom - varies, depending on components installed
Adapter Card	A communications adapter card that supports TCP/IP.

Notes:

1. You need 5 MB available on the drive where the Windows operating system is installed to accommodate temporary files that the iSeries Access for Windows setup program creates.
2. Additional files are downloaded from the iSeries server when you use the File Systems function of iSeries Navigator.
3. Service packs require additional space.
4. The size for a full installation could be different depending on whether SSL and plug-ins are in the installation search path.

Set up TCP/IP on the PC

Use this information to configure TCP/IP on Windows 2000, Windows NT, Windows XP, and Windows Server 2003 operating systems. TCP/IP must be correctly installed and configured before you try to connect to an iSeries server.

Install a network adapter or modem

In order to set up TCP/IP on your PC, you must have a network adapter or modem installed in your PC. If you will be connecting to the iSeries server over a LAN, then you will need a network adapter installed. If you will be connecting to the iSeries server using a serial line internet protocol (SLIP) or PPP connection from a remote location, then you will need to install a modem. For information about installing a network adapter or modem, see the manufacturer's documentation provided with the hardware. The manufacturer's documentation should also provide information about installing a driver for the hardware.

Install Dial-Up Networking on the PC

If you will be connecting to the iSeries server over a SLIP or PPP connection (using a modem), you need to install Dial-Up Networking and Remote Access Services on your PC. If you are connecting to your iSeries server over a LAN, or if you already have Dial-Up Networking installed on your PC, you can continue with Verify TCP/IP configuration.

Configure TCP/IP support on the PC

These steps are necessary to configure the Microsoft TCP/IP support that is supplied with the Windows operating system.

Notes:

1. The driver required to support TCP/IP over a twinaxial connection is not shipped with iSeries Access for Windows.
2. If you are not using a domain name server (DNS), see "Add the server name to the HOSTS file" on page 41.
3. For Windows NT 4.0 users, make sure that Windows NT Service Pack 6a and Internet Explorer 5.01 or later are installed.

Install and configure the TCP/IP network protocol on Windows NT

To install and configure the TCP/IP network protocol on Windows NT:

1. Click **Start –> Settings –> Control Panel**.
2. On the control panel, double-click **Network**.
3. Click the **Protocols** tab.
4. Click **Add**.
5. Click **TCP/IP**, and click **OK**.

   TCP/IP is added to the Network protocols page. Close the Network Window by clicking **OK**. You might be asked to restart your PC. Restart the PC and continue with the following steps.
6. Return to the Control Panel to configure the TCP/IP network protocol by clicking **Start –> Settings –> Control Panel**.
7. Double-click **Network**.
8. Click **TCP/IP**, and then click **Properties**.
   a. Click the **IP Address** tab.
   b. Click **Specify an IP address**.
   c. Type the IP address of your PC (for example, `199.5.83.205`).
   d. Type the Subnet Mask (for example, `255.255.255.0`).
   e. If you are using a default route, click **Gateway**, and do the following:
      1) Type the IP address of the gateway or router in **New gateway**.
      2) Click **Add**.
   f. If you are using a domain name server, click DNS, and do the following:
      1) Type the host name of your PC (for example, `cameron`).
      2) Type the domain (for example, `acme.com`).
      3) Type the IP address of the domain name server.
   g. If you are using a Windows Internet name server, click **WINS Address**, and do the following:
      1) Type the primary WINS server (for example, `199.5.83.205`).
      2) Type the secondary WINS server (for example, `199.5.83.206`).
      3) Select **DNS for Windows Resolution**.
      4) Select **LMHOSTS Lookup**.
   h. Click **OK**. You might be asked to restart your computer.
   i. Close any applications that are running, and click **OK**.

Install and configure the TCP/IP network protocol on Windows 2000, Windows XP, and Windows Server 2003

To install and configure the TCP/IP network protocol on Windows 2000, Windows XP, and Windows Server 2003:

1. Click **Start –>Settings –>Control Panel**.
2. On the control panel, double-click **Network Connections**.
3. Right-click **Local Area Connection**.
4. Click **Properties**.

   Note: If Internet Protocol (TCP/IP) does not appear in the list, do the following:
   a. Click **Install**.
   b. Select **Protocol**, and click **Add**.
   c. Select **Internet Protocol (TCP/IP)**.
   d. Click **OK**. This returns you to the **Local Area Connection Properties** window.
5. Select **Internet Protocol (TCP/IP)**, and click **Properties**.

6. Select **Using the Following IP Address**.

   Note: Check with your network administrator to determine the correct settings for this tab. If your PC does not automatically obtain IP and DNS addresses, do the following:
   - Type the IP address of your PC (for example, `199.5.83.205`).
   - Type the subnet mask (for example, `255.255.255.0`).
   - Type the default gateway (for example, `199.5.83.1`).
   - Type the preferred DNS server (for example, `199.5.100.75`).
   - Type the alternate DNS server (for example, `199.5.100.76`).

7. If you are using a Windows Internet Name Server, click the Advanced tab, select WINS Address, and do the following:
   a. Click **Add**.
   b. Type the primary WINS server (for example, `199.5.83.205`).
   c. Type the secondary WINS server (for example, `199.5.83.206`).
   d. The remaining settings should remain as the defaults.
8. Click **OK** on the **Local Area Connection Properties** window. It is not necessary to restart your PC.

Add the server name to the HOSTS file

If you are not using a domain name server, you need to add the iSeries server name with which you want to communicate to the HOSTS file. Also, add the iSeries NetServer server name to the LMHOSTS file if you are relying on iSeries NetServer for file and print serving. Complete the following steps to create or change the HOSTS file:

1. Open a command prompt.
2. Change to the directory that should contain the HOSTS file. For example:
   ```
   c:\>cd\winnt\system32\drivers\etc
   ```

   Note: The examples in this section use the `\winnt\system32\drivers\etc` directory, which is a Windows NT and Windows 2000 directory. On Windows XP and Windows Server 2003, the directory would be c:\windows\system32\drivers\etc. The HOSTS file must remain in this location.
3. If a file named HOSTS already exists in this directory, skip this step. Create a file named HOSTS by copying the sample file (supplied by Windows). The file is in the same directory and is called hosts.sam. For example:
   ```
   c:\winnt\system32\drivers\etc>copy hosts.sam hosts
   ```
4. Edit the HOSTS file. For example:
   ```
   c:\winnt\system32\drivers\etc>edit hosts
   ```

   Follow the instructions in the HOSTS sample file to add the IP address and name of the iSeries server to which you want to connect.
5. Save the HOSTS file.

   Note: For PC5250, if you do not use a name server or hosts table, you cannot start the 5250 emulator delivered with iSeries Access for Windows. The left bottom corner of your emulation display indicates a 657 communication error (Resolving TELNET 5250 server host-domain name).

   You can choose to use a HOSTS file if you have only a few machines using TCP/IP. This requires that you maintain an up-to-date list on each computer. When an iSeries address changes, you must change the HOSTS file entry if one exists.

Verify TCP/IP configuration on the PC

You can verify that TCP/IP is set up correctly on your PC by issuing a PING command to the iSeries server:

1. Open a command prompt.
2. Type **PING system** where system is the name of the iSeries server that you want to connect to.
3. If your TCP/IP configuration is correct, you should see reply messages from the iSeries server. If you do not see these reply messages, here are some possible reasons why the PING command failed:
   a. You might be trying to PING the wrong address. Check the address of the iSeries server.
   b. You might have an incorrect IP address listed for the iSeries server in your HOSTS file or DNS entry. This occurs only when you try to PING an iSeries server by name (as opposed to the IP address). If so, try **PING nnn.nnn.nnn.nnn** where nnn.nnn.nnn.nnn is the IP address of the iSeries server that you want to connect to. You can obtain the IP address of the iSeries server from your system administrator. If that works, update your HOSTS file or DNS entry with the correct address.
   c. Incorrect LAN adapter address is set in the adapter properties on the PC.
   d. There is no physical connection to the iSeries server.
   e. The iSeries server or network name is not correct.
   f. TCP/IP is not configured correctly on the PC.
   g. TCP/IP is not installed or configured correctly, or is not started, on the iSeries server. These problems need to be addressed by the system administrator.
   h. The iSeries server is down.
   i. The iSeries server is located behind a firewall that will not allow you to PING. Try **telnet systemname**.
   j. If none of the above explain your problem, restart and go through the configuration process again.

Install iSeries Access for Windows from iSeries NetServer

You must have iSeries Access for Windows installed on your server before following these instructions. You must also have iSeries NetServer configured on your iSeries server and your PC configured to use iSeries NetServer before following these instructions:

1. From the Windows desktop, right-click the My Network Places icon, and then click Search for Computers.

   Note: Note for Windows NT users: From the Windows desktop, click Start -> Find -> Computer.
2. Type in the iSeries NetServer name that you want to use to install iSeries Access for Windows and click Find Now.

   Note: If you cannot find iSeries NetServer by name, type in the IP address instead of the iSeries NetServer name. To find the IP address, perform a PING to the iSeries server as follows:
   a. Open a DOS window or Command Prompt.
   b. Type **PING system** where system is the name of the server that you wish to connect to.
3. Double-click the computer name when it appears.
4. This starts the Windows Explorer.
5. Double-click **QIBM -> ProdData -> Access -> Windows -> Install -> Image -> Setup.exe** to start the setup program.
6. Once the iSeries Access for Windows setup program begins, continue through the wizard to the Type of Installation panel.
7. Select **Custom** and click **Next**. Continue through the wizard to the Component Selection panel.
8. On the Component Selection panel, deselect and reselect the iSeries Navigator box to select all options.
9. Follow the instructions and online help in the program to complete the wizard.

Notes:

a. If the system administrator creates his own share point (directory capable of being shared by remote users) to the Image directory, you will not be able to install SSL, add-ins, plug-ins, and secondary languages that are installed on the iSeries server during the iSeries Access for Windows installation.

b. If you want to change the install source for automatic service pack and release upgrades, use the Service page of iSeries Access for Windows Properties after the installation completes.

c. If you are installing iSeries Access for Windows for the first time, the Check Version function will automatically receive new service packs and new releases from the drive and directory where the initial install occurred. If your administrator plans to store service packs or new releases in a different location, you can change the source directory on the Service page of iSeries Access for Windows Properties to the location specified by your administrator.

Part 3. Manage an OS/400 system that meets Common Criteria security requirements

After setting up Common Criteria security on your system, you should perform the following normal system management tasks to keep your system running safely and smoothly:

- Back up information regularly.
- Use the automatic cleanup function or perform the same tasks individually.
- Detach and save journal receivers regularly.
- Monitor disk storage and system performance characteristics.

These activities are described in the **Basic operations** topic, located in the iSeries Information Center.

Chapter 9, "Auditing Security on the iSeries System" of the *iSeries Security Reference* describes activities you should perform regularly to ensure that your security requirements are being met.

To ensure that your system continues to meet Common Criteria requirements, you should regularly perform the additional activities described in this chapter.

Chapter 8. Start your system

During the procedure for starting your system, called an **initial program load (IPL)**, your system is not yet running as a Common Criteria evaluated system. Your system must be completely started for all the security controls to be operational. Do the following to ensure that your system is protected when it is performing an IPL and that your system is secure when the IPL is complete:

- Control who has the authority to start the system by limiting the users who have job control (*JOBCTL) special authority.
- Control who can stop and restart the system by using the system key and control panel to keep the system in Secure mode.
- Ensure that the console is in a secure location.

  Note: Any workstation that is attached to the controller at Port 0 Bus 0 should be secured. If the designated console is not operational during an IPL, the system attempts to use another workstation that is attached at Port 0 Bus 0.
- Prevent anyone from starting your system remotely by keeping the remote IPL (QRMTIPL) system value set to 0.
- Ensure that the system has only PTFs that have been approved and tested by always using IPL source A. The *System Operation* book describes how to set the IPL source for your processor model.

You perform an IPL on your system for one of the following reasons:

- You are making changes that do not take effect until you perform an IPL. Examples are changing certain system values or applying PTFs.
- The system has been stopped, either by a scheduled power down command (PWRDWNSYS) or by a power interruption.
- You want to force the system to perform self-diagnostics. If you suspect that you have hardware or software problems, you may want to stop your system and start it again. When you perform an IPL, the system performs many internal diagnostics and reports any error conditions.

You start your system by doing one of the following:

- Use the **PWRDWNSYS** command with the restart option.
- If the system is powered off, a trusted administrator starts it by doing the following:
  1. Use the control panel on the system unit to place the system in **Manual** mode.
  2. Power on the system.
  3. Return the system unit to **Secure** mode and remove the key.

Note: You can also use the Power On/Off Schedule to stop your system at specific times. Use the Power On and Off Tasks menu (**GO POWER**). You cannot use the Power On/Off Schedule to restart the system because Common Criteria security requires the control panel on the system unit to be in **Secure** mode. Only trusted administrators have the authority to change this schedule.

Protect the signon process

To make it more difficult to break into your system, the error messages issued on the Sign On display should not indicate whether the problem is with the user profile name or with the password. The Common Criteria customization program changes the text of the error messages that are displayed for incorrect signon attempts.

When a user signs on the system, the system uses information from a subsystem description, the user profile, and a job description to determine the user's environment. When your system is shipped, the subsystem descriptions are set up so that the basic command processor program QCMD is used whenever a user signs on. The QCMD program is the default routing entry in all the interactive subsystems. You should not change these routing entries to use a program other than QCMD.

Chapter 9. Protect user profiles

When you sign on the system, you get all the authorities associated with the user profile that you specified on the sign on display. If the user has one or more group profiles, you also get any additional authorities associated with the group profiles. Several methods are available to use the authorities associated with another user profile. The security administrator must protect against the unauthorized use of user profiles on the system by doing the following:

- Ensure that the public authority for all user profiles on the system is set to ***EXCLUDE**. User profiles are automatically created this way, because *EXCLUDE is the default for the authority parameter on the Create User Profile (CRTUSRPRF) command.

  When you control the public authority to a user profile you can prevent public users from submitting a job using that profile and changing to that profile by using the set profile (QWTSETP) API.

  Attention: Check Appendix B, "IBM-Supplied User Profiles" in the *iSeries Security Reference* to determine what the public authority for IBM-supplied user profiles should be. Do not change the public authority of these profiles from the shipped value.
- Set the passwords for group profiles to ***NONE**. This prevents system users from signing on with a group profile.
- Do not grant private authority to user profiles because this allows a user to submit jobs under other user's profiles, which makes individual accountability difficult to determine from available auditing information.
- Carefully control the use of programs that adopt authority. Ensure that you understand what functions are being done while authority is adopted and that the program does not provide access to command entry.
- Do not allow programs to adopt the authority of user profiles that have special authorities.

Recommendations for using the Set profile API handle

Allowing a program to switch the user profile of the thread by using the set profile (QWTSETP) API is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user would not normally have. Switching the profile of the thread provides an important tool for meeting diverse authority requirements, but it should be used with care.

You should use the following recommendations to monitor and control the authority of your users:

- Switch to a profile with the minimum authority required to meet the application requirements. Switching the thread to the profile of an application owner is preferable to changing to QSECOFR or a user with *ALLOBJ special authority.
- When switching to a more powerful profile do it for the minimum time necessary.
- Carefully monitor the function provided by programs that switch the user profile. Make sure these programs do not provide a means for the user to access objects outside the control of the program, such as command entry capability.
- Programs that switch the user profile and call other programs must perform a library qualified call. Do not use the library list (*LIBL) on the call.
- Control which users are permitted to call programs that switch the user profile of the job. Use menu interfaces and library security to prevent these programs from being called without sufficient control.

ATTENTION

If a user is running under a switched user profile when a library is added to the library list, the user remains authorized to the library even when the thread has switched back to the original user profile. This represents a potential security exposure. Any entries added to a user's library list by a program running that swaps the user profile should be removed before the program ends.

Adopted authority is described in Chapter 5, "Resource Security" of the *iSeries Security Reference*e. The following table describes differences between using adopted authority and switching the user profile of the thread.

Table 7. Adopted authority and switching the user profile of the thread

Adopted authority	**Switching the user profile of the thread**
Added to any other authority found for the user.	Replaces all authority of the user.
Can adopt program owners authority from multiple programs at one time.	Can switch to only one user profile at a time.
If the owner profile is a member of a group profile, the groups authority is not used.	If the replaced user profile is a member of a group, the groups authority is used.
Public authority is not used for adopted authority. Only owner authority, private authority, and special authorities are used for adopted authority.	Public authority, owner authority, private authority, and special authorities are all used for the switched user.
Adopted authority is active as long as the program using adopted authority remains in the program stack.	Authority from a switched user is active until the user of the thread is switched again, if ever.
If the program running under adopted authority is interrupted, the use of adopted authority is suspended.	If the program that swaps the user profile of the thread is interrupted, the authority of the switched user is available for the user to use. The following function may allow a user to interrupt the current program: • System request • Attention key • Break-message-handling program • Debug functions
If the program running under adopted authority calls a Trigger, or most other types of exit programs, the adopted authority is suspended.	If the program that swaps the user profile of the thread calls a Trigger, or other types of exit programs, the authority of the switched user is available for the user to use.
Adopted authority from previous call levels can be suspended for any called program. See the QUSEADPAUT value for more information	Authority from a switched user is active until the user of the thread is switched again, if ever.
Any objects created, including spooled files that may contain confidential data, are owned by the user of the program or by the user's group profile, not by the owner of the program.	Any objects created are owned by the switched (current) user of the thread or by that user's group profile. Depending on the SPLFOWN printer file option, spooled files can be owned by the following: • The current user of the thread • The original user profile of the job. • The group profile of the current user of the thread. • The group profile of the original user profile of the job.

Table 7. Adopted authority and switching the user profile of the thread (continued)

Adopted authority	Switching the user profile of the thread
Only the owner of a program, or a user with *ALLOBJ and *SECADM special authority can cause a program to adopt its owner's authority. The adopted authority can be used within the program by anyone who is authorized to call the program.	To switch the current user of the thread, the get profile handle (QSYGETPH) and set profile (QWTSETP) APIs must be used. The public authority of both of these APIs is *USE. In addition, to get a profile handle, the current user must either know the password of the target user profile or must have *USE authority to that user profile. All these authorities can be obtained by using adopted authority.

Protect IBM-supplied user profiles

When your system ships, it has several user profiles already created. These user profiles are usually referred to as **IBM-supplied user profiles**. These profiles are used by the system for system functions. They also own IBM-supplied objects.

Follow these guidelines for IBM-supplied user profiles:

- Do not delete any IBM-supplied user profiles. System functions depend on these profiles. In some cases, the system prevents you from deleting critical profiles.

  For example, the restore procedures and the reclaim storage procedure use the default owner (QDFTOWN) profile. If the QDFTOWN profile is not on the system and you attempt to restore an object whose owner is also not on the system, the restore operation fails. The reclaim storage (RCLSTG) procedure checks for the QDFTOWN profile before processing is started.
- Do not change any of the shipped attributes for these profiles, with the exception of the password. System functions depend on the attributes that are provided with the profiles.
- You should not allow system users to sign on the system using an IBM-supplied profile. Most IBM-supplied profiles ship with the password set to *NONE. You can use an option from the SETUP menu to change the passwords for the IBM-supplied profiles that ship with a password. Set all the passwords to *NONE, except the password for the QSECOFR (security officer) profile. Set the password for the QSECOFR profile to something other than the shipped value. Store the new password in a secure place.

  Note: The QSECOFR profile must have a password for certain recovery situations.
- Do not use IBM-supplied profiles to own objects that you create. IBM-supplied profiles own many objects that are supplied with the system or that are created as a result of system functions. These profiles should not be the owner of your application objects.

Appendix B, "IBM-Supplied User Profiles" of the *iSeries Security Reference*e describes all the IBM-supplied profiles and their attributes.

Chapter 10. Remove users from the system

When you delete a user profile from the system, you must also delete any spooled files owned by the user. Use the Work with Spooled Files (WRKSPLF) command to find the user's spooled files and to delete them.

Chapter 11. Immediate revocation of authority

One of the biggest threats to your system security is your users. In a situation in which you discover that a user is compromising your system security, you may choose to revoke that user's authority to the system. When you revoke users' authority to an object, the revocation may not take affect immediately. If the user has already gained access to the object (such as opening a file), the revocation may not take affect until the user gives up access to the object (such as closing the file).

ATTENTION

This procedure causes subsequent IPLs to take longer. This procedure is also disruptive to the normal operations of the system; use this procedure only when the situation requires drastic actions.

If it is necessary to ensure that the revocation takes effect immediately, then perform the following steps:

- Revoke the users' authority to the object.
- Type **ENDJOB** for any jobs the user has started or in extreme cases restart the entire system with the command **PWRDWNSYS OPTION(*IMMED) RESTART(*YES)**

Chapter 12. Control the restoration process

System-state programs can be created only by IBM. If a program appears to be a system-state program and is not supplied by IBM, that program has been tampered with. It should not be restored to your system. When your system is at security level 40 or 50, the system detects this type of tampering and prevents the program from being restored.

To ensure that only trusted system-state programs are on your system and to prevent any possible tampering, do the following when you restore programs (such as applying program temporary fixes (PTFs)):

1. Sign on with a user profile that has *ALLOBJ and *SECADM special authority.
2. Ensure the system is running at security level 50:

   DSPSECA

   Press **Enter**.
3. While you are restoring system-state programs, your system is not running as a Common Criteria evaluated system. To ensure that no other users are on the system until the restore operation is complete, place your system in a restricted state:
4. Set up the system to allow restoring system state programs and programs that adopt authority:

   CHGSYSVAL SYSVAL(QALWOBJRST) VALUE(*ALL)

   Press **Enter**.
5. Perform the operation that restores system-state programs. This operation might be restoring an IBM-supplied library, installing licensed programs, or applying PTFs.
6. Set up the system to prevent restoring system state programs and programs that adopt authority:

   CHGSYSVAL SYSVAL(QALWOBJRST) VALUE(*NONE)

   Press **Enter**.

Verify restored programs

Any program loaded to your system from backup media represents a potential security exposure. When you restore programs other than trusted IBM-supplied programs, you must take measures to ensure that the programs have not been altered. The Force Conversion on Restore system value (QFRCCVNRST) must be set to 7. Setting this value causes all programs not digitally signed by IBM to be retranslated or not restored on the system.

Ensure that messages do not start unauthorized programs

You can define messages separately from the programs that issue the messages. This is a productive programming technique because an application might use the same messages in several different programs. This type of message is defined in a message file (object type *MSGF). You can also specify that when a message is issued, the system should call a program associated with the message. That program might be used for problem analysis.

The ability for a message to call a program represents a potential method to enter the system. You must ensure that unauthorized users cannot associate programs with messages. The simplest way to do this is to set the public authority for message files to *USE. The customization programs do this for the message files that are supplied by IBM. You should do this for any message files that are used by your application programs.

Ensure that the correct version of a program runs

When you call a program on the iSeries system, either you can specify what library to search for the program or you can specify *LIBL. When you specify *LIBL, the system searches the libraries in your library list, in the order in which they appear in the library list, for the program. As security administrator, you need to set policies that provide users with the assurance that the expected version of a program will be run. You do this by doing the following:

- Protecting the system-wide library lists (the QSYSLIBL and QUSRLIBL) system values. These system values are set by the customization programs. The command to change them is restricted.
- Requiring that applications specify both the program name and the library name when calling programs or establish a controlled user library list.

  Chapter 6, "Work Management Security" in the *iSeries Security Reference* describes methods for controlling the security of the library list for a user's job.

Ensure that the correct version of a CL command runs

When you run a command from the command line (CL) on the system, you can either specify what library to search for the command, or you can specify *LIBL. When you specify *LIBL, the system searches the libraries in your library list, in the order in which they appear in the library list, for the command. Security administrators should perform the following steps to set policies that ensure users that the expected version of a CL command runs:

- Protect the system-wide library lists (the QSYSLIBL and QUSRLIBL) system values. These system values are set by the customization programs. The command to change them is restricted.
- Require that applications specify both the program name and the library name when running CL commands or establishing a controlled user library list.

  See Chapter 6, "Work Management Security" in the *iSeries Security Reference* for methods to control the security of library lists for a user jobs.

Verify restored commands

Any command that is restored represents a potential security exposure because it may run system state programs. You should regularly check the audit journal to ensure that commands restored to your system meet your security requirements:

- Look for audit journal records that have entry type OR and object type *CMD (command).
- Check to see if restored commands use programs that run in system state. Use the Display Command (DSPCMD) command to determine the state attribute of programs used by the command.

Chapter 13. Use service tools to display or change disk configuration

Service tools are available on the system to perform functions such as displaying or changing the disk configuration. While you are using service tools, your system is not running as a Common Criteria evaluated system because normal access control and auditing are not enforced.

You must carefully control who has authority to use service tools. Change the DST passwords from the default passwords that are shipped. Ensure that only trusted users have *SERVICE special authority.

You must also ensure that no users are on the system when service tools are running. Two types of services tools are available:

Dedicated service tools (DST)
DST can be run while the operating system is active and during the recovery of the system.

System service tools (SST)
SST can be run while the operating system is active but not during system recovery.

When you have finished using service tools, make the system available to the users by doing the following:

1. Start subsystems again using the Start Subsystem (STRSBS) command.
2. Notify users that the system is available.

Notes:

1. You can use the *SERVICE audit level to detect when someone starts a service tool.
2. After a service tool is run on your system, you can use the Check Object Integrity (CHKOBJITG) command to ensure that no programs have been modified.

Chapter 14. Protect authorization lists

An authorization list is a list of users whose authority is specified in one place for all the objects that are secured by that authorization list. It is a convenient way to manage authority for objects that have similar authority requirements.

You can specify authority to the authorization list itself to control the following:

- Adding or removing users from the list.
- Changing a user's authority to the objects on the list.
- Using the list to secure an object.

Appendix F, "Authority required for objects used by commands," on page 155 provides a complete description of the authorities associated with authorization lists. If you use an authorization list to secure a group of objects, ensure that public authority to the authorization list is *EXCLUDE.

Authority checking is not performed for the Display Authorization List (DSPAUTL) command. This means that any user on the system can display a list of the users that are on an authorization list. If you consider this information confidential, you should not use authorization lists on your system.

Note: The Optical File system uses authorization lists to secure optical volumes.

Chapter 15. Verify the use of authority holders

Authority holders should not be used on a Common Criteria evaluated system because they do not meet the requirement for explicit authority. Take these measures to ensure that authority holders are not used on your system:

- Check to make sure no users have authority to use the command to create new authority holders (CRTAUTHLR). This command is shipped with public authority of *EXCLUDE.
- Use the Display Authority Holder (DSPAUTHLR) command to make sure no authority holders exist on your system.
- Periodically check job logs for the informational message CPI2232, which is issued when an authority holder is associated with a file.

Chapter 16. Control access to journals and journal receivers

When you start journaling for an object, the system writes a copy of every changed record to a journal receiver. Therefore, a journal receiver may contain confidential information. A journal receiver also provides an audit trail of activity that has occurred for an object. Some commands that are associated with journaling are restricted by the customization programs. Journals that are supplied by IBM are also restricted. If you use journaling for your applications, you need to evaluate who should have the ability to do the following:

- Start, stop and change journaling
- Create and delete journals
- Create and delete journal receivers
- Use the Change Journal (CHGJRN) command to associate a new journal receiver with the journal.
- Display the contents of a journal receiver.

The simplest way to control access to a particular journal is to set the public authority for journals and journal receivers to *EXCLUDE.

Chapter 17. Apply program temporary fixes (PTFs)

When you order feature code 1930 for the OS/400 Licensed Program, you receive a cumulative package of program temporary fixes (PTFs) that has been evaluated for Common Criteria security. See “Install a PTF package” on page 23. Additional PTFs may become available later. These PTFs are designed to meet Common Criteria requirements, but in most cases they will not be formally evaluated for Common Criteria compliance.

If you need to apply a PTF that is not part of feature code 1930, your security officer or DAA (Designated Approving Authority) must evaluate whether that PTF might cause a security exposure.

While you are applying PTFs, your system is not running as a Common Criteria evaluated system. Your system must be in a restricted state during the procedure that applies PTFs.

Chapter 18. Reclaim storage

Certain events on your system, such as damaged objects or a disk failure, may require you to use the Reclaim Storage (RCLSTG) command. Before you run the RCLSTG command, ensure that public authority is set to *EXCLUDE for the QRCL library and for the QDFTOWN user profile.

When you run the RCLSTG command, the system attempts to assign ownership for all objects on the system. When the profile that owns an object cannot be found or cannot be determined, the system assigns ownership of that object to the default owner (QDFTOWN) user profile.

After you run the RCLSTG command, you must take care to determine the correct ownership of any objects assigned to the QDFTOWN profile. Use the Work with Objects by Owner (WRKOBJOWN) command to list the objects that are owned by the QDFTOWN profile. When you have determined the correct owner for an object, use the transfer option from the Work with Objects by Owner display to assign the owner of the object to the correct owner. Be sure that you revoke the authority of the QDFTOWN profile when you transfer ownership.

In addition, objects that are damaged may be placed in the Reclaim Storage (QRCL) library if the system cannot determine the correct library. Use the Display Library (DSPLIB) command to list the objects in the QRCL library. Use the Move Object (MOVOBJ) command to move each object to the correct library.

If any integrated file system objects are found with problems, they are placed in the appropriate /QReclaim directory. Objects that are lost from their specified directories are inserted into the '/QReclaim' directory (if the object was originally located in the root file system) or the '/QOpenSys/QReclaim' directory (if the object was originally located in the QOpenSys file system). To manipulate objects in these directories, use the Move Object (MOV) command to move each object to the correct library.

Attention: When you run the RCLSTG procedure, your system is not running as a Common Criteria evaluated system. The RCLSTG procedure always runs in a restricted state, which prevents any other users from signing on.

Chapter 19. Use the integrated security tools

The integrated security tools provide a set of commands to help monitor the security environment on your system. For example, you can use the integrated security tools to help you manage user profiles. You can also use the integrated security tools to identify new objects on your system so that you can evaluate the proper object authority for those new objects.

You can run the integrated security tools commands directly, or you can select them as options from the SECTOOLS menu and the SECBATCH menus.

Because the integrated security tools examine all objects and values on the system, you should be signed on as a security officer to run the commands. Many integrated security tools require at least one special authority. For other integrated security tools, you need *ALLOBJ special authority to ensure that you can access all of the objects that you want to analyze.

All of the integrated security tools ship with the public authority set to *EXCLUDE. Public authority is also set to *EXCLUDE for many objects, such as database files, that are created by the integrated security tools.

You should not use the following integrated security tools commands on a Common Criteria evaluated system:

- The Configure System Security (CFGSYSSEC) command uses system value settings that are less restrictive than Common Criteria requirements. Use the Common Criteria customization program to set your system values.
- The Print System Security Attributes (PRTSYSSECA) command prints the current and recommended settings for security-relevant system values. The recommended settings that this command uses are not the recommended settings for a Common Criteria installation. You should not use this command or its report for evaluating a Common Criteria evaluated system.
- The Revoke Public Authority (RVKPUBAUT) command sets the public authority to *EXCLUDE for some system commands. This command uses a subset of the commands whose public authority is set by the Common Criteria customization program. You must use the Common Criteria customization program to meet Common Criteria requirements.

Chapter 20. Restrict the use of commands

Some commands are shipped with public authority set to *EXCLUDE. The public authority for other commands is set to *EXCLUDE by the Common Criteria customization programs. There are some commands that should not be used on an active Common Criteria evaluated system because these commands have not been evaluated for Common Criteria security. The public authority for these commands is set to *EXCLUDE either when they are shipped or when you run the customization programs. If you use any commands in the following table, your system is not in a trusted state. In some cases, a trusted administrator may need to use these commands when your system is in a restricted state (non-Common Criteria) and no other users are active.

Table 8. Commands That Should Not Be Used on a Common Criteria Evaluated System

ADDACC	ADDEMLCFGE	ADDNODLE
ADDALRACNE	ADDEWCBCDE	ADDNWSSTGL
ADDALRD	ADDEWCM	ADDOPTSVR
ADDALRSLTE	ADDEWCPTCE	ADDPRBACNE
ADDCCTRTE	ADDEWLM	ADDPRBSLTE
ADDCCTSRV	ADDICFDEVE	ADDRDBDIRE
ADDCFGLE	ADDIPIADR	ADDRMTDFN
ADDCMNE	ADDIPIIFC	ADDRMTJRN
ADDCNNLE	ADDIPIRTE	ADDRMTSVR
ADDCOMSNMP	ADDIPSIFC	ADDSNILOC
ADDDIRE	ADDIPSLOC	ADDSOCE
ADDDIRSHD	ADDIPSRTE	ADDTCPRSI
ADDDLOAUT	ADDIPXCCT	ADDTCPRTE
ADDDSTLE	ADDLANADPI	ANSLIN
ADDDSTQ	ADDNCK	APING
ADDDSTRTE	ADDNETJOBE	AREXEC
ADDDSTSYSN		
CFGDEVMLB	CFGSYSSEC	CFGTCPRTD
CFGDSTSRV	CFGTCPBP	CFGTCPSMTP
CFGIPI	CFGTCPLPD	CFGTCPSNMP
CFGIPS	CFGTCPPTP	CFGTCPWSG
CFGIPX		

Table 8. Commands That Should Not Be Used on a Common Criteria Evaluated System (continued)

CHGALRACNE	CHGDLOAUD	CHGLINX25
CHGALRD	CHGDLOAUT	CHGLPDA
CHGALRSLTE	CHGDLOOWN	CHGMODD
CHGALRTBL	CHGDLOPGP	CHGM36
CHGBPA	CHGDOCD	CHGM36CFG
CHGCCTRTE	CHGDSTA	CHGNCK
CHGCCTSRV	CHGDSTD	CHGNETJOBE
CHGCFGL	CHGDSTL	CHGNFSEXP
CHGCFGLE	CHGDSTQ	CHGNODGRPA
CHGCMNE	CHGDSTRTE	CHGNTBD
CHGCNNL	CHGDTA	CHGNWIATM
CHGCNNLE	CHGEMLCFGE	CHGNWIFR
CHGCOMSNMP	CHGEWCBCDE	CHGNWIISDN
CHGCOSD	CHGEWCM	CHGNWIT1
CHGCRQD	CHGEWCPTCE	CHGNWSA
CHGCSI	CHGEWLM	CHGNWSALS
CHGCTLAPPC	CHGFTR	CHGNWSD
CHGCTLASC	CHGICFDEVE	CHGNWSUSRA
CHGCTLBSC	CHGICFF	CHGPOPA
CHGCTLFNC	CHGIPIADR	CHGPRBACNE
CHGCTLHOST	CHGIPIIFC	CHGPRBSLTE
CHGCTLRTL	CHGIPSIFC	CHGRDBDIRE
CHGCTLRWS	CHGIPSLOC	CHGRMTDFN
CHGDDMF	CHGIPSTOS	CHGRMTJRN
CHGDDMTCPA	CHGIPXCCT	CHGRTDA
CHGDEVAPPC	CHGIPXD	CHGRWSPWD
CHGDEVASC	CHGLANADPI	CHGSMTPA
CHGDEVBSC	CHGLINASC	CHGSNILOC
CHGDEVDKT	CHGLINBSC	CHGSNMPA
CHGDEVFNC	CHGLINDDI	CHGSRVA
CHGDEVHOST	CHGLINFAX	CHGSSNMAX
CHGDEVINTR	CHGLINFR	CHGSYSDIRA
CHGDEVRTL	CHGLINIDLC	CHGS36PGMA
CHGDEVSNPT	CHGLINNET	CHGS36PRCA
CHGDEVSNUF	CHGLINPPP	CHGS36SRCA
CHGDHCPA	CHGLINSDLC	CHGTCPRTE
CHGDIRE	CHGLINTDLC	CHGTFTPA
CHGDIRSHD	CHGLINWLS	CHGWSGA
CHKCMNTRC	CLRDKT	CPYFRMDIR
CHKDKT	CMPPTFLVL	CPYFRMDKT
CHKDLO	CPYCFGL	CPYIGCTBL
CHKPRDORD	CPYDOC	CPYTODIR
CPYTODKT	CRTCRQD	CRTCTLHOST
CRTALRTBL	CRTCSI	CRTCTLRTL
CRTAUTHLR	CRTCTLAPPC	CRTCTLRWS
CRTCFGL	CRTCTLASC	CRTDEVDSK
CRTCNNL	CRTCTLBSC	CRTM36
CRTCOSD	CRTCTLFNC	CRTM36CFG
CRTWSCST	CRTDEVDSK	CRTDEVSNPT
CRTDDMF	CRTDEVFNC	CRTDEVSNUF
CRTDEVAPPC	CRTDEVHOST	CRTDOC
CRTDEVASC	CRTDEVINTR	CRTDSTL
CRTDEVBSC	CRTDEVRTL	CRTFLR

Table 8. Commands That Should Not Be Used on a Common Criteria Evaluated System (continued)

CRTFTR	CRTLINPPP	CRTNWIISDN
CRTICFF	CRTLINSDLC	CRTNWIT1
CRTIGCDCT	CRTLINTDLC	CRTNWSALS
CRTIPXD	CRTLINWLS	CRTNWSD
CRTLINASC	CRTLINX25	CRTNWSSTG
CRTLINBSC	CRTMODD	CRTSPADCT
CRTLINDDI	CRTNODGRP	CRTSQLPKG
CRTLINFAX	CRTNODL	CVTDLSNAM
CRTLINFR	CRTNTBD	CVTIPSIFC
CRTLINIDLC	CRTNWIATM	CVTIPSLOC
CRTLINNET	CRTNWIFR	CVTNAMSNMP
DLTALR	DLTDOCL	DLTNODGRP
DLTALRTBL	DLTDST	DLTNTBD
DLTAUTHLR	DLTDSTL	DLTNWID
DLTCFGL	DLTFTR	DLTNWSALS
DLTCNNL	DLTIGCDCT	DLTNWSAPP
DLTCOSD	DLTIGCTBL	DLTNWSD
DLTCRG	DLTIPXD	DLTNWSSTG
DLTCRQD	DLTM36	DLTPTF
DLTCSI	DLTM36CFG	DLTSHF
DLTDFUPGM	DLTMODD	DLTSPADCT
DLTDKTLBL	DLTNETF	DLTWSCST
DLTDLO	DLTNODL	DMPDLO
DMPJOB	DSPCSPOBJ	DSPDTA
DSPACC	DSPDDMF	DSPEWCBCDE
DSPACCAUT	DSPDIRE	DSPEWCM
DSPAPPNINF	DSPDKT	DSPEWCPTCE
DSPAUTHLR	DSPDLOAUD	DSPEWLM
DSPCCTRTE	DSPDLOAUT	DSPFLR
DSPCFGL	DSPDLONAM	DSPHLPDOC
DSPCNNL	DSPDOC	DSPIPXCCT
DSPCNNSTS	DSPDSTL	DSPIPXD
DSPCOSD	DSPDSTLOG	DSPLANSTS
DSPCSI	DSPDSTSRV	DSPMODD
DSPAUTLDLO	DSPNWID	DSPOPTSVR
DSPCCTSRV	DSPNWSA	DSPRDBDIRE
DSPLANADPP	DSPNWSALS	DSPRMTDFN
DSPLANMLB	DSPNWSD	DSPSOCSTS
DSPM36	DSPNWSSSN	DSPSRVA
DSPM36CFG	DSPNWSSTC	DSPSRVSTS
DSPMODSTS	DSPNWSSTG	DSPTRAPRF
DSPNCK	DSPNWSUSR	DSPUPGPRP
DSPNODGRP	DSPNWSUSRA	DSPUSRPMN
DSPNTBD	DSPOPCLNK	DUPDKT
EDTDLOAUT	ENDEPMENV	ENDNWSAPP
EDTDOC	ENDHOSTSVR	ENDPASTHR
EDTS36PGMA	ENDIPIIFC	ENDPRTEML
EDTS36PRCA	ENDIPSIFC	ENDRDBRQS
EDTS36SRCA	ENDIPX	ENDRMTSPT
EJTEMLOUT	ENDIPXCCT	ENDRPCBIND
EMLPRTKEY	ENDM36	ENDSRVJOB
ENDCMNSVR	ENDMOD	ENDTCPPTP
ENDCPYSCN	ENDMSF	ENDTIESSN
ENDDBGSVR	ENDNFSSVR	ENDTRPMGR
ENDDIRSHD	ENDNWIRCY	ESTOBJCVN
		EXPORTFS
FILDOC	HLDDSTQ	INZDKT
GRTACCAUT	INSNTWSVR	INZDSTQ
GRTUSRPMN	INSNWSAPP	IPXPING

Table 8. Commands That Should Not Be Used on a Common Criteria Evaluated System (continued)

LPR	MOVDOC	OVRICFDEVE
OVRICFF	PRTDKTINF	PRTSYSINF
PKGPRDDST	PRTDOC	PRTSYSSECA
PKGPRDOPT	PRTIPSCFG	PRTTNSRPT
PRTCMNSEC	PRTPEXRPT	QRYDOCLIB
QRYDST	QRYPRBSTS	QRYTIEF
RCLDDMCNV	RCVNETF	RLSDSTQ
RCLDLO	RCVTIEF	RLSIFSLCK
RCVDST	RGZDLO	RLSRMTPHS
RMVACC	RMVCFGLE	RMVDIRE
RMVALRD	RMVCMNE	RMVDIRSHD
RMVCCTRTE	RMVCNNLE	RMVDLOAUT
RMVCCTSRV	RMVCOMSNMP	RMVDSTLE
RMVCCSCLT	RMVIPIFC	RMVNWSSTGL
RMVDSTQ	RMVIPIRTE	RMVOPTSVR
RMVDSTRTE	RMVIPSIFC	RMVRDBDIRE
RMVDSTSYSN	RMVIPSLOC	RMVRMTDFN
RMVEMLCFGE	RMVIPSRTE	RMVRMTJRN
RMVEWCBCDE	RMVIPXCCT	RMVSNILOC
RMVEWCPTCE	RMVLANADPI	RMVSOCE
RMVFTRACNE	RMVLANADPT	RMVTCPRSI
RMVFTRSLTE	RMVNCK	RMVTCPRTE
RMVICFDEVE	RMVNETJOBE	RMVTCPTBL
RMVIPIADR	RMVNODLE	RNMCNNLE
RNMDIRE	RQSORDAST	RTVDLONAM
RNMDKT	RSMNWIRCY	RTVDOC
RNMDLO	RSTDLO	RTVPRD
RNMDSTL	RSTS36F	RTVPTF
RNMLANADPI	RSTS36FLR	RTVSYSINF
RNMNCK	RSTS36LIBM	RTVWSCST
RPCBIND	RSTSHF	RUNLPDA
RPLDOC	RTVDLOAUT	RVKACCAUT
RVKPUBAUT	RVKUSRPMN	SAVDLO
SAVS36F	SETCSTDTA	SNDNWSMSG
SAVS36LIBM	SETUPGENV	SNDPRD
SAVSHF	SNDDST	SNDPTFORD
SBMDKTJOB	SNDDSTQ	SNDSRVRQS
SBMFNCJOB	SNDFNCIMG	SNDTCPSPLF
SBMNETJOB	SNDNETF	SNDTIEF
SBMNWSCMD	SNDNETMSG	STRCMNSVR
SBMRMTCMD	SNDNETSPLF	STRCPYSCN
STRDBGSVR	STRIPSIFC	STRPASTHR
STRDFU	STRIPX	STRPRTEML
STRDIRSHD	STRIPXCCT	STRRMTSPT
STRDKTRDR	STRITF	STRRMTWTR
STRDKTWTR	STRM36	STRSPTN
STRDPRCAP	STRM36PRC	STRSRVJOB
STREML3270	STRMOD	STRSST
STREPMENV	STRMSF	STRTCPPTP
STRHOSTSVR	STRNFSSVR	STRTIESSN
STRINFSKR	STRNWSAPP	STRTRPMGR
STRIPIIFC	STROBJCVN	TFRM36
TFRPASTHR	TRCCPIC	TRCICF
UPDDTA	UPDSYSINF	VFYAPPCCNN
VFYCMN	VFYIPXCNN	VFYLNKLPDA

Table 8. Commands That Should Not Be Used on a Common Criteria Evaluated System (continued)

VFYOPCCNN	WRKDPRAPYE	WRKNWSD
WRKALR	WRKDPRCAPE	WRKNWSENR
WRKALRD	WRKDSTL	WRKNWSSSN
WRKALRTBL	WRKDSTQ	WRKNWSSTG
WRKAPPDCT	WRKFLR	WRKNWSSTS
WRKAPPNSTS	WRKFTR	WRKOBJCSP
WRKBPTBL	WRKFTRACNE	WRKOPCACT
WRKCCTRTE	WRKFTRSLTE	WRKORDINF
WRKCCTSRV	WRKHTTPCFG	WRKORDRQS
WRKCFGL	WRKIPXCCT	WRKPGMTBL
WRKCHTFMT	WRKIPXD	WRKPRDINF
WRKCNNL	WRKIPXSTS	WRKRDBDIRE
WRKCNNLE	WRKLANADPT	WRKRMTDFN
WRKCNTINF	WRKM36	WRKRTDCFG
WRKCOSD	WRKM36CFG	WRKS36PGMA
WRKCSI	WRKMODD	WRKS36PRCA
WRKDDMF	WRKNCK	WRKS36SRCA
WRKDIRE	WRKNETF	WRKSOC
WRKDIRLOC	WRKNETJOBE	WRKSPADCT
WRKDIRSHD	WRKNODL	WRKSRVPVD
WRKDOC	WRKNODLE	WRKTCPPTP
WRKDOCLIB	WRKNTBD	WRKTIE
WRKDOCPRTQ	WRKNWID	WRKUSRTBL
WRKDPCQ	WRKNWSALS	

Restrict the use of certain TCP/IP commands

Although the Common Criteria evaluated configuration includes support and some TCP/IP communication functions, it does not include support for all TCP/IP commands available on the system. To keep the system in the evaluated configuration, the administrator must adhere to the following restrictions.

The Common Criteria customization program restricts the usage of all UDP ports. The administrator must not use the ADDTCPPORT CL command to change or remove any UDP port restrictions. UDP support has not been evaluated as part of a Common Criteria evaluated system.

On the STRTCPSRV CL command, the administrator can specify *FTP, *TELNET, and *REXEC for the SERVER parameter. The administrator must not specify any of the other possible values for this parameter including *ALL, *BOOTP, *DCE, *DDM, *DHCP, *DIRSRV, *DLFM, *DNS, *EDRSQL, *HTTP, *INETD, *LPD, *MGTC, *NETSVR, *NSLD, *NSMI, *ONDMD, *POP, *ROUTED, *SMTP, *SNMP, *TFTP, *USF, *VPN, and *WSG. None of these servers have been evaluated as part of a Common Criteria evaluated system.

The administrator must use the ADDTCPPORT CL command to place TCP port restrictions on the ports used by the FTP server, TELNET server, and REXEC server to only be accessible to the QTCP user profile. If the standard, well known, ports are used by the servers, then TCP ports 20 (FTP), 21 (FTP), 423 (TELNET) and 512 (REXEC) must be restricted. If the standard ports are not used, the administrator must display the TCP services table entries and restrict the ports assigned to the FTP, TELNET, and REXEC servers.

On the CHGNETA CL command, the administrator must not specify *YES for the ALWANYNET parameter. The Common Criteria customization program sets this network attribute to *NO. The administrator may specify a value of *NO or *SAME for this parameter.

On the CHGTELNA CL command, the administrator must not specify *NVT for the DFTNVTTYPE parameter. The Common Criteria customization program sets this TELNET attribute to *VT100. The administrator may specify a value of *VT100 or *SAME for this parameter.

On the CFGTCPAPP CL command, the administrator can specify *FTP, *TELNET, and *REXEC for the APP parameter. The administrator must not specify any of the other possible values for this parameter including *BOOTP, *DDM, *DHCP, *DNS, *HTTP, *LPD, *POP, *ROUTED, *SMTP, *SNMP, *TFTP, and *WSG. None of these servers have been evaluated as part of a Common Criteria evaluated system. On the CHGTCPDMN CL command, the administrator must not specify *REMOTE for the HOSTSCHPTY parameter. The administrator may specify a value of *LOCAL or *SAME for this parameter.

The evaluated Common Criteria configuration does not include support for Domain Name Servers (DNS); resolution of host names should be performed locally using the local TCP host table.

Chapter 21. Restrict the use of exit programs

On the system, exit programs are a normal method of communication between system state and user state. Therefore, some exit programs are essential for the operation of your system and have been evaluated as part of the TOE. Other exit programs are not essential. Some of them are not part of the Common Criteria configuration and should not be used on your system. Others should be used only by a trusted administrator when your system is in a restricted state.

The following table lists system-provided exit programs that should not be on a Common Criteria evaluated system. The *Recommendation* column describes how the use of these exit programs is prevented when you set up your system for Common Criteria security:

Table 9. System-Provided Exit Programs That Are Not Allowed

Brief Description	Recommendation
DDM user exit. Specified using the DDMACC program on the CHGNETA command.	Do not specify a value for the DDMACC program. Public authority is *EXCLUDE for the commands that start these exit programs.
User-supplied exit program for file usage information.	This exit is not part of the TOE. It is available only through a special PTF that has not been evaluated for Common Criteria security and is not included in Feature Code 1930.
User-defined DFU program.	DFU is not allowed on a Common Criteria evaluated system. The installation process does not include DFU.
Function key program for 3270 emulation.	3270 emulation is not allowed on a Common Criteria evaluated system. Public authority for the 3270 emulation commands is set to *EXCLUDE by the QSYCCCCA program.
Exit program when Operational Assistant automatic cleanup is run.	Do not replace the system-provided program called QEZUSRCLNP in the QSYS library. The public user cannot change a program in the QSYS library. The public user also cannot place the system library list to place a library ahead of the QSYS library. Using automatic cleanup is optional.
Exit program when Operational Assistant backup is run.	This exit program is registered on the EXITPGM parameter of the CHGBCKUP command. Public authority for this program is set to *EXCLUDE by the QSYCCCCA program. Using Operational Assistant backup is an optional function. Public authority for this program is *EXCLUDE.
Exit program when Operation Assistant backup schedule is changed.	Do not replace the system-provided program with this name. Public authority for this program is *EXCLUDE.
Transaction program for finance device.	The finance system is not part of the TOE.
File system functions, registered using the Register File System API (QHFRGFS).	The QHFRGFS API is restricted to trusted administrators with *ALLOBJ special authority.
Automatic problem analysis. Called when a default program is specified in a message description.	The system uses this function for problem analysis. You should not change any messages to add your own exit programs. QSYCCCCD program sets the public authority to *USE for all message files on the system. This prevents users from defining a default program for a message.

Table 9. System-Provided Exit Programs That Are Not Allowed (continued)

Brief Description	Recommendation
Exit programs for system distribution directory. They are specified on the SCHPGM, VRFPGM, and SUPPGM parameters of the CHGDIRA command.	These commands are related to products that are not allowed on a Common Criteria evaluated system. Using the CHGDIRA command requires *ALLOBJ or *SECADM special authority.
Passthru signon validation. Set by QRMTSIGN system value.	Do not define a pass-through validation program for the QRMTSIGN system value. The public authority for pass-through commands is set to *EXCLUDE by the QSYCCCCA program to prevent the use of the pass-through function.
User-supplied exit program to process data that is collected by the performance monitor. registered on the EXITPGM parameter for the performance monitor commands: ADDPFRCOL, CHGPFRCOL, ENDPFRMON, STRPFRMON.	Public authority for the performance monitor commands is *EXCLUDE.
Exit program during trace job that determines what should be included or excluded from printing. Specified using the EXITPGM parameter on the TRCJOB command.	Public authority for the TRCJOB command is shipped as *EXCLUDE.
Password validation. Set by QPWDVLDPGM system value.	The value for the QPWDVLDPGM system value should be *NONE, which is the default. Changing the QPWDVLDPGM system value requires *ALLOBJ special authority.
Registered in the PRDLOD object. Called by the CHKPRDOPT command.	Public authority for the CHKPRDOPT command is *EXCLUDE.
Program for starting communications.	This program can be called only by communications programs that have public authority of *EXCLUDE after the QSYCCCCA program is run.
User-supplied exit program to process SQL requests directly to a relational database, registered on the ARDPGM parameter for the ADDRDBDIRE command.	Public authority for the ADDRDBDIRE command is *EXCLUDE, and is not to be used on a Common Criteria evaluated system.
FTP Server Logon exit.	Do not register a program for the QIBM_QTMF_SVR_LOGON exit point. The ADDEXITPGM command has public authority of *EXCLUDE.
REXEC (RUNRMTCMD) Server Logon and Command Processor Selection exits.	Do not register a program for either the QIBM_QTMX_SVR_LOGON or QIBM_QTMX_SVR_SELECT exit points. The ADDEXITPGM command has public authority of *EXCLUDE.

The following table lists system-provided exit programs that should be carefully controlled on a Common Criteria evaluated system. The *Recommendation* column describes how you should restrict the use of these exit programs when you set up your system for Common Criteria security:

Table 10. System-Provided Exit Programs That Must Be Restricted

Brief Description	Recommendation
Exit program to receive journal entries in a program. Specified on the EXITPGM parameter of the RCVJRNE command.	Only a trusted system administrator should use this function. Public authority to the RCVJRNE command is set to *EXCLUDE by the QSYCCCCA program.

Table 10. System-Provided Exit Programs That Must Be Restricted (continued)

Brief Description	Recommendation
Exit program when saving, restoring, deleting, and checking licensed programs. Specified on the PREOPRPGM parameter and the PSTOPRPGM parameter of the CRTPRDLOD command.	Authority for the CRTPRDLOD command and the commands that work with licensed programs have public authority of *EXCLUDE. You should make changes to licensed programs only when your system is in a restricted state.
Used when applying PTFs. Registered on the exit program parameter of the Create Program Temporary Fix (CRTPTF) command.	The Apply PTF (APYPTF) command has public authority of *EXCLUDE. It should be used only when the system is in a restricted state.
User-supplied program to create a customized print separator page. Specified on the SEPPGM parameter of the CRTDEVPRT command and the CHGDEVPRT command.	Restricted on a Common Criteria evaluated system because public authority is set to *EXCLUDE for the CRTDEVPRT and CHGDEVPRT commands by the QSYCCCCA program.
User-supplied exit program for commit and rollback processing. Specified as a parameter on the QTNADDCR API.	Public authority to the QTNADDCR API is *EXCLUDE.
User-supplied exit program to be called for insert, delete, update of a record in a physical file. Trigger programs are registered via the ADDPFTRG command.	Public authority for the ADDPFTRG command is *EXCLUDE.
Any exit program registered with the Exit Registration Facility (WRKREGINF).	The ability to use the WRKREGINF command is restricted. Carefully monitor who has access to the command and any changes that are made to registration information.

Chapter 22. Restrict the use of application program interfaces (APIs) and callable programs

Application programming interfaces (APIs) and callable OS/400 programs provide a way for programmers to provide functions that may not be available through commands. In some cases, APIs and callable programs provide better performance than commands that are called by a program. Many APIs perform normal functions that are appropriate for applications used by end-users. Many APIs and callable programs are shipped with public authority of *EXCLUDE. In addition, the public authority for other programs and APIs is set to *EXCLUDE by the Common Criteria customization programs. The following table lists the APIs and callable programs that should not be used on a Common Criteria evaluated system. The QSYCCCPA program sets the public authority to *EXCLUDE for these APIs, except for those APIs that are shipped with the public authority set to *EXCLUDE.

Table 11. APIs That Should Not Be Used on a Common Criteria Evaluated System

CMACCP	CMESUI	CMSERR
CMALLC	CMFLUS	CMSF
CMCFM	CMINIT	CMSLD
CMCFMD	CMPTR	CMSMN
CMCNVI	CMRCV	CMSPLN
CMCNVO	CMRTS	CMSPTR
CMDEAL	CMSCSP	CMSRC
CMECS	CMSCST	CMSRT
CMECT	CMSCSU	CMSSL
CMEMBS	CMSCT	CMSST
CMEMN	CMSDT	CMSTPN
CMEPLN	CMSED	CMTRTS
CMESL	CMSEND	
Q5BBPNFY	Q5BSTACK	QAESTUB3
Q5BROUTE	Q5BWRKJ	QAEDYNAT
QALGENA	QBMGINIT	QBMRSRV
QALRTVA	QBMRCDAT	QBSGET
QALSNDA	QBMRRFSH	QBSPUT
QCCWRKCC	QDBCHGDF	QESCSRVA
QCNCMNT	QDCRLIND	QESDSPSA
QCIMRT	QDCRNWSD	QESRSRVA
QCRADRTN	QDCRTTCP	QESSAVMA
QCRCLEAR	QDXHRTR	QEXCHJCB
QCREXHAN	QDZXDRV	QEXCLRCI
QCRGDDM	QEARBKM	QEXFPGM
QCRHLLST	QEARMVBM	QEZSCNEP
QCRSORT	QEMPESNA	QFPACNUS
QCRSPACE	QESANOTE	QFNREAD
QFNREADI	QFPAACTV	QGLDPUBQ
QFNROUTE	QFPADAPP	QQQSVUSR
QFNWRT	QFPAMON	QHCCCFG
QFNWRTI	QGLDPSPI	QHCQRYLN

Table 11. APIs That Should Not Be Used on a Common Criteria Evaluated System (continued)

QHEENRL	QHFDLTDR	QHFRDDR
QHFCHGAT	QHFDLTSF	QHFRDSF
QHFCHGFP	QHFFRCSF	QHFRNMDR
QHFCLODR	QHFGETSZ	QHFRNMSF
QHFCLOSF	QHFLSTFS	QHFRTVAT
QHFCPYSF	QHFLULSF	QHFSETSZ
QHFCRTDR	QHFMOVSF	QHFWRTSF
QHFCTLFS	QHFOPNDR	QICGET
QHFDRGFS	QHFOPNSF	QICPUT
QHFRGFS		
QINEXIT1	QIZARSTN	QLNRDTAA
QIZACFGM	QIZARSTS	QLNRGDDM
QIZACLN	QIZARTVN	QMARQSOA
QIZADOBJ	QIZARTVS	QMOTCNTL
QIZAINTI	QIZASBS	QNMCHGMN
QIZAPDP	QIZAUIM	QNMCTLEC
QNMDRGAP	QNMRCVOC	QNMSARTR
QNMDRGFN	QNMREGAP	QNMSNDER
QNMDRGTI	QNMRGFN	QNMSNDRP
QNMECSJB	QNMRGTI	QNMSNDRQ
QNMENDAP	QNMRRGF	QNMSTRAP
QNMRCVDT	QNMRTVMN	QOCXEMN
QOCCTLOF	QOEUSRMV	QOKSCHD
QOCLOADM	QOGCHGOE	QOLDLINK
QODDLSMA	QOGRTVOE	QOLELINK
QODTRCTL	QOHFIXIX	QOLQLIND
QODXITPG	QOHFIXQ	QOLRECV
QOECMPRT	QOKADDDP	QOLSEND
QOEUAADD	QOKCHGDP	QOLSETF
QOEUARMV	QOKDSPX4	QOLTIMER
QOEUSADD	QOKRMVDP	QOSPRINT
QPARTVDA	QPDUGO01	QPWFSERVSO
QPASTRPT	QPDXPARL	QP0ZSBUS
QPDJYNM5	QPMBPCS	QQDAPROC
QRFPTHRU	QSOCIP03	QS2SNPLD
QRNXGDDM	QSOCIP04	QS2SNPMF
QSCBMKTE	QSOCPTFC	QS2SNPND
QSCBPSP	QSOCRTVIP	QTMMATCV
QSCBSRVE	QSOCWIFC	QTMMATTM
QSDORDPTF	QSOCWRTC	QTMMCCAD
QSDPTS	QSPSETWX	QTMMCUTL
QSIGET	QSQXRLF	QTMMENV
QSIPUT	QSYGETCM	QTMMFUTL
QTMMJRNL	QTMMSND	QTMTEXIT
QTMMLCLD	QTMMSNDM	QTMTRMVP
QTMMNDEL	QTMMSUTL	QTMTSRV
QTMMPARS	QTMMTUNL	QTMTWSG
QTMMRCST	QTMTADDP	QTOACRTQ
QTMMRMX1	QTMTBLDQ	QTOADELQ

Table 11. APIs That Should Not Be Used on a Common Criteria Evaluated System (continued)

QTOADSPC	QTOSSAPI	QYYCFEOD
QTOCPPSM	QTQRECOV	QYYCGETD
QTOCRTTC	QTSGET	QYYCGETK
QTODBOOT	QTSPUT	QYYCGETM
QTODDXAD	QTSUDR	QYYCGETS
QTODDXRM	QTVCLOVT	QYYCPUT
QTOMAPI	QTVOPNVT	QYYCPUTD
QTOMEAPI	QTVRDVT	QYYCPUTM
QTOMMAIN	QTVSNDRQ	QYYCUDR
QTOMRCVR	QTVWRTVT	QY2FTML
QTOSMAIN	QUSRGFIN	QZCACLT
QTOSRCVR	QYYCCLOS	QZCATHR
QZDAGFS	QZDSNPOC	QZMFDUMP
QZDASNID	QZDS2MSG	QZMFLSTC
QZDCRFSO	QZDWTFSO	QZMFSNPA
QZDLSTID	QZMFACHG	QZMFXDIR
QZDRDFSO	QZMFACRT	QZMFXPG1
QZDRTVID	QZMFADDC	QZMFXPG2
QZDRVKID	QZMFALOG	QZMFXPG3
QZDSNPAC	QZMFAPG1	QZMFXPG4
QZDSNPAD	QZMFAQRY	QZPAIJOB
QZDSNPAM	QZMFARSV	QZSPMJOB
QZDSNPND	QZMFARTV	QZSPWIPA
QZDSNPEC	QZMFASCR	QZSPWIPR
QZDSNPLD	QZMDASQC	QZSPWLOC
QZDSNPLE	QZMFCATR	
QZDSNPMF	QZMFDLTC	

Chapter 23. Restrict system from clusters

The OS/400 system that is Common Criteria compliant must not be configured as part of a cluster of OS/400 systems. The OS/400 clustering support has not been evaluated as part of the Common Criteria environment. The administrator must check that the **Allow Add to Cluster** (ALWADDCLU) network attribute is set to a value of *NONE. This network attribute value prevents other systems from adding this system as part of a cluster. The current setting for the ALWADDCLU network attribute can be displayed by the **Display Network Attributes** (DSPNETA) CL command. If the ALWADDCLU network attribute needs to be changed, an administrator with *IOSYSCFG special authority can use the Change Network Attribute (CHGNETA) CL command to change the value of the ALWADDCLU attribute to *NONE.

Note: OS/400 clustering support is dependent on other functions which have not been evaluated for Common Criteria. These include: OS/400 option 23, Opticonnect (not allowed to be installed), INETD TCP/IP server (not allowed to be started), and TCP/IP UDP protocols (all UDP ports are restricted).

Chapter 24. Restrict system from logical partitions

The OS/400 operating system that is Common Criteria-compliant must not be configured with more than one logical partition. A system configured with multiple partitions has not been evaluated as part of the Common Criteria environment. The administrator must not use the System Service Tools (SST) or Dedicated Service Tools (DST) Work with System Partitions function to configure multiple partitions on the OS/400 operating system.

Chapter 25. Manage database column level authorities

Through the SQL interface, REFERENCE and UPDATE authorities can be granted and revoked on individual columns of a table (*FILE). Refer to the iSeries Information Center on the Internet and click **Database—>Reference—>SQL Reference—>Statements** for information on how to perform the following tasks:

- Grant (table or view privileges)
- Revoke (table or view privileges)

CL commands can not be used to manage column level authorities. This requires extra care by an administrator to ensure that column level authorities are managed correctly in certain situations.

An administrator can use the DSPOBJAUT CL command to display the authorities users have on a database file (*FILE). The presence of a '/' (instead of a 'X') indicates that the user is authorized to some but not all columns. The command does not indicate which columns the user has authority to.

An administrator can also use the EDTOBJAUT CL command to display and change the authorities users have on a database file (*FILE). The presence of a '/' (instead of a 'X') indicates that the user is authorized to some but not all columns. The administrator can revoke a user's authority to all columns in the table (replacing the '/' or 'X' with a blank) or grant access to all columns in the table (replacing a blank with an 'X'). However, EDTOBJAUT can not be used to grant authority to specific columns of a file.

An administrator must be careful when using the GRTUSRAUT CL command when the referenced user has column level authorities. The GRTUSRAUT CL command does not handle column level authorities. If the referenced user has column level authorities, the administrator must use SQL statements to grant the appropriate column level authorities to the specified user. If this is not done, the specified user could have more authority to the database file (authority to all columns) than the referenced user had.

Part 4. Audit security events on an OS/400 operating system that meets Common Criteria security requirements

This chapter discusses special considerations when you use security auditing to meet the requirements of Common Criteria security. For more information about security auditing, see Appendix G, ″Object Operation and Auditing″ in the *iSeries Security Reference*.

Common Criteria security requires several specific auditing capabilities. Whether and how you use them depends on the security requirements of your installation.

Chapter 26. Protect the audit function

Common Criteria security requires that only security administrators be allowed to administer security audit journal functions. The iSeries system provides several methods for enforcing this protection:

- Restricting who can start, stop, change and display security auditing. Only a user with *AUDIT special authority is allowed to change auditing values on the system. This includes all system values that control auditing, the auditing values in user profiles, and the auditing values for objects. Assigning *AUDIT special authority to a user should be carefully controlled.
- Stopping all system activity if an audit failure occurs. To meet Common Criteria security requirements, a system must have the ability to stop immediately if audit records cannot be written. The system provides this capability using the auditing end action (QAUDENDACN) system value. If your auditing needs are critical enough to require this protection, set the QAUDENDACN system value to *PWRDWNSYS. Otherwise, set it to *NOTIFY.
- Ensuring that audit records are not lost if a system failure occurs. Normally, the system updates information in main storage and writes a copy of it to auxiliary storage periodically. The system balances the need to protect from data loss against performance requirements. If a system failure, such as a power loss, occurs, any new information in main storage that has not been copied to auxiliary storage is lost.

  Common Criteria security requires the capability to prevent the loss of audit records. The system meets this requirement with the audit force level (QAUDFRCLVL) system value. If the protection of all auditing records is critical to your installation, set the QAUDFRCLVL system value to 1. This ensures that no more than 1 audit record is lost if a system failure or a power failure occurs.

  If you leave the QAUDFRCLVL system value set to *SYS, the system manages writing audit entries from memory to auxiliary storage. How often the entries are written to auxiliary storage depends on how many types of events you are auditing, how busy your system is, and how much paging of memory is occurring.

  If a system failure or a power failure occurs, you will have no way of knowing how many audit journal entries were lost.

Chapter 27. Set up auditor profiles

You need to set up user profiles for people who will be performing security audits on your system. At a minimum, the profiles that you create for security auditors should have *AUDIT special authority. *AUDIT special authority allows the user to display and change the auditing characteristics of the system:

- System values that control auditing
- Auditing for user profiles
- Auditing for objects

The auditor may also need additional authority to perform other auditing functions. As system administrator, you want to give the auditor sufficient authority to perform the audit function without allowing the auditor to change information. Following are several examples:

- The auditor will probably want to examine entries in the security audit journal. Give the auditor *USE authority to the QAUDJRN (audit) journal and to the journal receivers.
- The auditor may want to examine user profiles. This would require *SECADM special authority and *ALLOBJ special authority because user profiles have public authority of *EXCLUDE.

  Note: Instead of giving the auditor these special authorities, you may want to create a CL program that adopts the authority of a profile that has *SECADM and *ALLOBJ special authority. The program can run the Display User Profile (DSPUSRPRF) command with prompting to allow the auditor to choose parameters. Make public authority to the program *EXCLUDE and grant the auditor *USE authority.
- The auditor may want to look at journal entries for journaled objects. This requires *USE authority to the journal and the receivers of the journaled object.

You may want to begin by giving the auditor a profile that has *AUDIT special authority and authority to the security audit journal and receivers. You can grant additional authority as it is needed for specific activities.

Be sure to revoke any authorities when they are no longer needed. You may also want to set up security auditing for the auditor profile while additional authorities (other than *AUDIT special authority and authority to the audit journal) are active.

Chapter 28. Plan auditing requirements

The topic, ″Planning Security Auditing″ in Chapter 9, ″Auditing Security on the iSeries System″ of the *iSeries Security Reference* describes the ability to audit actions, users, and objects on the system. It shows how to set up auditing to meet different needs, such as the following:

- Logging all the actions of a particular user.
- Logging all the accesses of a particular object.

Careful planning is required before setting up the auditing characteristics of users and objects on your system. You need to anticipate the questions an auditor may ask so that the correct information is captured in the audit journal. You also need to balance the auditing requirements with the performance requirements of your system. If possible, focus your auditing efforts on critical objects and powerful users on your system.

Set up your system to simplify object auditing

When you want to audit an object on your system, the auditing value for the object must do one of the following:

- Specify the type of auditing that is required.
- Point to the user profile that is accessing the object to determine the auditing that is required.

One method to simplify the job of the security audit is to make all objects ready for audit by having them point to the user profile for audit requirements. Then the security auditor only needs to specify auditing for the profile that is being examined.

If you want to use this method, do the following:

Note: Steps 3 and 4 below access all objects in libraries and directories on the system. They will require significant system resources and will run for a long time. Consider using the Submit Job (SBMJOB) command to run these steps when your system is not busy.

1. Sign on with a user profile that has *AUDIT special authority.
2. Set up the system so that all newly created objects will point to the user profile for auditing requirements by typing:

   ```
   CHGSYSVAL SYSVAL(QCRTOBJAUD) VALUE(*USRPRF)
   ```

   Press **Enter**.
3. Set the auditing value for all objects in libraries on the system by typing:

   ```
   CHGOBJAUD OBJ(*ALL/*ALL) OBJTYPE(*ALL) OBJAUD(*USRPRF)
   ```

   Press **Enter**.
4. Set the auditing value for all objects in a directory by typing the following commands and pressing **Enter**:
   a. `CHGAUD OBJ(/) OBJAUD(*USRPRF)`
   b. `CHGAUD OBJ('/*') OBJAUD(*USRPRF)`
   c. `CHGAUD OBJ('/directory-name/*') OBJAUD(*USRPRF)`

   This step must be repeated for each directory in the system, including subdirectories.
5. Set up the audit journal object so that it is not audited. Auditing of this object is usually not necessary and may affect performance significantly:

   ```
   CHGOBJAUD OBJ(QSYS/QAUDJRN) OBJTYPE(*JRN) OBJAUD(*NONE)
   ```

   Press **Enter**.

To audit a specific object for all users, you can use the Change Object Auditing (CHGOBJAUD) command or the Change Auditing Value (CHGAUD) command to set the audit value for that object. For example:

```
CHGOBJAUD OBJ(library-name/object-name)
   OBJTYPE(*FILE) OBJAUD(*CHANGE)
```

To audit the change activity for a specific user, you can use the Change User Auditing (CHGUSRAUD) command. For example:

```
CHGUSRAUD USRPRF(USERA) OBJAUD(*CHANGE)
```

Press **Enter**.

To audit all activity for a specific user, you can use the Change User Auditing (CHGUSRAUD) command. For example:

```
CHGUSRAUD USRPRF(USERA) OBJAUD(*ALL)
```

Press **Enter**.

Attention!

If the object auditing for an object is set to *NONE, this overrides the auditing value in a user profile. No auditing is done for that user for that object no matter how the object auditing value in the user profile is set.

Chapter 9, "Auditing Security on the iSeries System" of the *iSeries Security Reference* provides more information about how to set up auditing on your system.

Chapter 29. Audit the use of restricted commands and programs

You restrict commands and programs that should not be used on a Common Criteria evaluated system by setting the public authority for them to *EXCLUDE. However, a user who has *ALLOBJ special authority can use objects that have public authority of *EXCLUDE. To audit the use of commands by a user with *ALLOBJ special authority, you can use the audit function to write a record of all the commands issued by that user. Type the following (substituting the user profile name for QSECOFR):

```
CHGUSRAUD USRPRF(QSECOFR) AUDLVL(*CMD)
```

When this type of auditing is active, an auditor can review the CD (command string) entries in the audit journal to see what commands were used.

A system administrator with *ALLOBJ and *SECADM special authorities can prevent the accidental use of restricted commands. This is done by registering the QSYBLKCMD program at an QIBM_QCA_RTV_COMMAND exit point for the command to be restricted. For example, to prevent anyone from accidentally using the CHGNETA command, type this:

```
ADDEXITPGM EXITPNT(QIBM_QCA_RTV_COMMAND)
FORMAT(RTVC0100) PGMNBR(*LOW)
PGM(QSYS/QSYBLKCMD)
PGMDTA(*JOB *CALC 'CHGNETA   QSYS      ' )
```

Chapter 30. Audit attempted actions

You may want to audit certain security-relevant actions that are attempted by a user but that do not complete successfully. Some unsuccessful completions cause an audit record. Others do not. Following are two examples:

Unsuccessful actions: audit record written

1. USERA attempts to change USERB's profile.
2. The attempt fails because USERA does not have sufficient authority to USERB's user profile.
3. An AF audit record is written if your auditing definition includes *AUTFAIL.

Unsuccessful actions: no audit record written

1. The security administrator, USERX, attempts to change the job description field in USERB's user profile.
2. USERX spells the name of the job description incorrectly and receives an error message that the job description is not found.
3. No security audit record is written because the CHGUSRPRF command did not complete successfully.

To create a record for this type of event, do the following:

1. Set up command-string auditing for USERX. Use the Change User Auditing (CHGUSRAUD) command and specify *CMD for the AUDLVL parameter.
2. Check the security audit journal for CD audit records that show security-relevant commands, such as the CHGUSRPRF command.
3. If the CD record for the security-relevant command is not followed by the appropriate *SECURITY record (such as CP for CHGUSRPRF), then you know that the attempt was not successful.

Chapter 31. Considerations for auditing user activity

When you use the audit journal to monitor user activity on the system, you may find that the audit journal contains some audit records that you do not expect. An evaluation of the action performed by the user and the underlying work that the system does can explain the additional audit records.

Following are two examples:

Audit records for Query/400

When someone uses the Query/400 program, you expect to see audit records for the database files that the user accesses. You may also see a ZC (change) record for the file that contains the query programs. If the user creates a new query program, the system adds a member to the file that contains query programs resulting in a ZC record.

If the user directs the output of the query to a database file, you will also see a CO (create object) record.

Audit records for object creation

When you create an object, the system sets public authority for the object based on the CRTAUT value of the target library. This results in a CA (change authority) record in the audit journal before the CO (create object) record.

If a user profile is set up to give the group profile authority to newly created objects, this results in an additional CA record before the CO record.

Chapter 32. Monitor authority failures by using the audit journal

If the audit level (AUDLVL) system value includes *AUTFAIL, the system writes an AF entry to the audit journal when an authority failure occurs. An **authority failure** is an unsuccessful attempt to access an object because of insufficient object authority.

Sometimes, either because of internal system requirements or for performance reasons, the system may write a different number of AF audit records than you might expect for a particular action. When you use the audit journal to monitor authority failures, you should be aware of the following situations:

- **Extra Audit Records for a Failed Attempt** Some system operations require more than one authority. For example, you may need *USE authority (*OBJOPR, *READ, and *EXECUTE) and *OBJMGT authority to perform a function. The system optimizes for the successful attempt. Therefore, it may check *USE authority and *OBJMGT authority concurrently before it runs the program that handles authority failures. Therefore, if the user has neither *USE authority nor *OBJMGT authority, two AF records would be written to the audit journal for the same failed attempt.
- **Audit Record for an Internal Control-Block Object** Some high-level languages (such as C/400®) provide the ability to access an object by its address. Using this capability, a user program might attempt to access an internal system object that is protected by any of the following:
  - Object authority
  - System domain
  - Hardware storage protection

  The AF record that results from the attempt will contain an internal system object type, such as *QTSP (temporary space). The violation type depends on the type of protection for the internal object:
  - A (object authority)
  - D (object domain)
  - R (hardware storage protection)
- **Audit Record for a Successful Attempt** To improve performance and simplify maintenance, the operating system often uses the same system module for multiple functions. Sometimes, the system module may require more authority to objects than some of the programs that call the module. For example, USERA has *READ authority to an object and wants to perform an operation that requires *READ authority. The program that performs the function calls a system module that requires *USE authority. The module attempts to access the object without evaluating the source of the call (fast path method) and receives an authority failure. An AF record is written to the audit journal. The module then determines the source of the call and the actual authority required. It temporarily acquires sufficient authority to perform the called function, so that the user's attempt is successful.

The following information explains audit strategies for special authorities.

Chapter 33. Audit special authority violations

Some OS/400 commands require special authority. When a user attempts a command and fails because the user does not have the required special authority, in some cases no authority failure (AF) audit record is written. The following topics describe several ways that you can capture audit information about actions that require special authorities.

Audit interfaces that require special authority

You can set up object auditing for the commands and programs that require special authority. Whenever someone uses the interface, an object auditing record is written to the audit journal. For example, you may want to audit the Change Object Owner (CHGOBJOWN) command. To change the ownership of a program that adopts authority, you must have *ALLOBJ and *SECADM special authority. Type the following: **CHGOBJAUD OBJ(QSYS/CHGOBJOWN) OBJTYPE(*CMD) OBJAUD(*ALL)**

For many actions that require special authority, an audit record is written when the action completes successfully if the appropriate action auditing is set. For example, if a user successfully changes object ownership, an OW record is written if the audit level for the system or the user includes *SECURITY.

The audit level (QAUDLVL) system value and the audit level for specific users provide a wide variety of auditing capabilities, including the following:

- Security-related events, many of which require *ALLOBJ or *SECADM special authority.
- Job-related events, many of which require *JOBCTL or *SPLCTL special authority.
- Service-related events, many of which require *SERVICE special authority.
- Restore events, many of which require *SAVSYS special authority.

An auditor can review the sequence of events in the audit journal. For example, was the CHGOBJOWN command followed closely by an OW record? If not, perhaps the user did not have the special authority required for the attempt. Was the ENDJOB (End Job) command followed closely by a record? If not, perhaps the user did not have authority to end the job.

Audit objects that relate to special authority

Some actions that require special authority operate on specific objects on the system. You can audit those objects to determine the success or failure of an operation. For example, all of the job scheduling commands use the job scheduler object, QDFTJOBSCD. When auditing is active for this object you will be able to determine if the job scheduler commands (such as the CHGJOBSCDE command), succeed or fail based on the existence of an audit record in the journal.

Restrict the interfaces that require special authority

place of or in addition to setting up auditing to monitor the use of special authorities, you may also want to restrict public authority to commands and programs that require special authority. You can then grant authority to specific users who should be authorized to the command or program. For example, if you want to control who can use the Change Job Schedule Entry (CHGJOBSCDE) command, type the following commands (substituting users who should be authorized for USERA):

```
GRTOBJAUT OBJ(QSYS/CHGJOBSCDE) OBJTYPE(*CMD)
USER(*PUBLIC) AUT(*EXCLUDE)
GRTOBJAUT OBJ(QSYS/CHGJOBSCDE) OBJTYPE(*CMD)
USER(USERA) AUT(*USE)
```

In this example, only USERA (who has *JOBCTL special authority) will now be able to use the interface that requires the special authority. With this approach, do the following:

- Provide more specific controls than the system provides with special authorities.
- Ensure that an audit record will be written when someone without the proper authority attempts to use the command.

Special considerations for *ALLOBJ special authority

All object (*ALLOBJ) special authority gives the user the ability to access any resource on the system, whether or not the user has private authorities. However, a user with *ALLOBJ special authority cannot directly perform operations that require other special authorities; therefore, to meet the Common Criteria requirements for auditing the use of special privilege all users that have *ALLOBJ special authority should also be granted all other special authorities. By granting all special authorities this user will be able to use all OS/400 interfaces that require special privilege.

Chapter 34. Immediate enforcement of audit settings

When an authority setting is changed, the change may not take affect immediately.

WARNING

This procedure will cause the subsequent IPL to take longer. This procedure is also disruptive to the normal operations of the system; therefore, use this procedure only when the situation calls for drastic measures.

If it is necessary to ensure that the audit setting change takes effect immediately, then perform the following steps:

- Make the desired audit setting changes.
- Turn power off to the system by pressing the power switch two times.

Chapter 35. Audit TCP/IP connections for REXEC, FTP and TELNET

Audit REXEC and RUNRMTCMD connections

If you want to audit the actions of a user that uses REXEC or RUNRMTCMD CL command, you should:

- Ensure that the QAUDLVL system value includes the *NETCMN, *JOBDTA, *SECURITY, and *AUTFAIL option values on both the client and server systems.
- Ensure that the QAUDCTL system value includes the *AUDLVL option value on both the client and server systems.

After these system values are set, the appropriate auditing will occur on both the client and server systems.

You can view the audit records on both the client and server systems and determine which REXEC job was used by a specific user and what user profile was used to run the command on the server. The following paragraphs describe how to view the audit records on both the client and server systems.

On the client system, display the audit entries in the QAUDJRN journal for the specific user. This can be done with the DSPJRN CL command. For example,

```
DSPJRN JRN(QAUDJRN) ENTTYP(SK) USRPRF(JOHNNY)
```

will display all of the socket connection (SK) requests for user profile JOHNNY. On the DSPJRN display, type a **5** next to an SK record to be looked at in detail and press **Enter**. This will display the entry specific data for the audit record. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  10165
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  SK - Secure sockets connections
Incomplete Data  . . :  No
                               Entry specific data
Column                         *...+....1....+....2....+....3....+....4....+....5
00001                         'C9.5.29.77      5168 9.5.7.91       512      '
```

This record indicates that a connection function (C) was performed on the client system whose IP address is 9.5.29.77 using port number 5168. The connection request was to a server system whose IP address is 9.5.7.91 and to the service that was listening on port 512. You can display the TCP/IP Host Table to associate names with the IP addresses. For example, using the Work with TCP/IP Host Table Entries function of the Configure TCP (CFGTCP) command. Type:

```
CFGTCP
```

and press **Enter**. The Configure TCP/IP display is shown. Type 10 and press **Enter**. The Work with TCP/IP Host Table Entries display is shown, which will display the contents of the host table similar to the following:

```
                      Work with TCP/IP Host Table Entries
                                                                 System:    XXXXXXXXX
Type options, press Enter.
  1=Add  2=Change   4=Remove   5=Display   7=Rename
     Internet        Host
Opt  Address         Name
     127.0.0.1       LOOPBACK
     9.5.29.77       CLIENTSYS
     9.5.7.91        SERVERSYS
```

Port 512 is the well-known port for REXEC, but, to verify that REXEC is actually configured to use port 512, use the WRKSRVTBLE CL command on the server system to display the configured TCP/IP services. It should look similar to:

```
                  Work with Service Table Entries
                                                                      System:
Type options, press Enter.
  1=Add   4=Remove   5=Display

Opt  Service                              Port   Protocol

     exec                                  512   tcp
     ftp-control                            21   tcp
     ftp-control                            21   udp
     ftp-data                               20   tcp
     ftp-data                               20   udp
```

To locate the corresponding audit records on the server system, perform the following steps.

1. On the DSPJRN screen, on the client system, when you are looking at the SK audit record, press F10 to display the entry details. The resulting display will contain the date and time that the SK audit record was created. Write the date and time down on a piece of paper.
2. On the server system, type a DSPJRN command restricting the display to audit records for the same date and time as you recorded in step 1. For example:

   DSPJRN JRN(QAUDJRN) FROMTIME('04/09/1999' '10:00')

   Note: The time value may have to be adjusted depending on any time zone differences and how well the system times of the client and server systems are coordinated.
3. On the server system, examine the DSPJRN display looking for SK audit records for jobs whose names begin with the characters QTRXC. The names of REXEC server jobs all begin with this sequence of characters.
4. For each SK audit record found, display the SK audit entry until you locate the audit record that corresponds to the connection request initiated by the client. You can identify the matching entry by the presence of the same IP addresses and port numbers, but they will appear in the reverse order. For example, the matching entry for the client request shown above would look like:

```
                               Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  2853
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  SK - Secure sockets connections
Incomplete Data  . . :  No
                               Entry specific data
Column                         *...+....1....+....2....+....3....+....4....+....5
00001                         'A9.5.7.91      512   9.5.29.77      5168      '
```

The audit record indicates that the server system with IP address 9.5.7.91 accepted (A) a connection request on port 512 from a client system whose IP address is 9.5.29.77 and was using port 5168 on the client system. Notice that both of the IP addresses and port numbers match exactly those shown in the SK audit record on the client system.

Write down the Job name associate with the audit record. This is the specific REXEC server job used by the client user.

Then exit the DSPJRN display by pressing **F12**.

5. On the server system, display all of the audit records associated with the REXEC server job you recorded in step 4. For example,

   ```
   DSPJRN JRN(QAUDJRN) FROMTIME('04/09/1999' '10:00') JOB(QTRXC00981)
   ```

   This will display all of the audit records for the QTRXC00981 server job. This will include the SK audit record you examined in step 4.

6. You can now examine the audit records associated with the client's command request that was executed by the server system. One record that may be of particular interest is the PS audit record. The PS audit record of type H records that the server job has been changed to execute under a different user profile. In this case, it is the user profile that the client specified on the RUNRMTCMD CL command. For example:

   ```
                                 Display Journal Entry

   Object . . . . . :
   Library. . . . . :
   Member . . . . . :
   Sequence . . . . . :  2857
   Code . . . . . :  T  - Audit trail entry
   Type . . . . . :  PS - Process user profile swap
   Incomplete Data  . . :  No
                                  Entry specific data
   Column                         *...+....1....+....2....+....3....+....4....+....5
   00001                         'HJOHNNY2
   00051                         '           0'
   ```

   In this case, the server job was changed to use the JOHNNY2 user profile. Notice that this is not the same user profile as was used on the client system (JOHNNY).

Audit FTP connections

If you want to audit the actions of a user that uses the FTP CL command, you should

- Ensure that the QAUDLVL system value includes the *NETCMN, *JOBDTA, *SECURITY, and *AUTFAIL option values on both the client and server systems.
- Ensure that the QAUDCTL system value includes the *AUDLVL option value on both the client and server systems.

After these system values are set, the appropriate auditing will occur on both the client and server systems.

You can view the audit records on both the client and server systems and determine which FTP job was used by a specific user and what user profile was used to perform the FTP sub-commands on the server. The following paragraphs describe how to view the audit records on both the client and server systems.

On the client system, display the audit entries in the QAUDJRN journal for the specific user. This can be done with the DSPJRN CL command. For example,

```
DSPJRN JRN(QAUDJRN) ENTTYP(SK) USRPRF(LESLIE)
```

will display all of the socket connection (SK) requests for user profile LESLIE. On the DSPJRN display, type a **5** next to an SK record to be looked at in detail and press **Enter**. This will display the entry specific data for the audit record. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  3190
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  SK - Secure sockets connections
Incomplete Data  . . :  No
                             Entry specific data
Column                       *...+....1....+....2....+....3....+....4....+....5
00001                       'C9.5.7.91      5321  9.5.29.77      21       '
```

Examine SK audit entries until you find one that contains a 21 in positions 37–38 of the entry specific data. This record indicates that a connect request (C) was performed on the client system whose IP address is 9.5.7.91 using port number 5321. The connection request was to a server system whose IP address is 9.5.29.77 and to the service that was listening on port 21. You can display the TCP/IP Host Table to associate names with the IP addresses. For example, using the Work with TCP/IP Host Table Entries function of the Configure TCP (CFGTCP) command. Type:

CFGTCP

and press **Enter**. The Configure TCP/IP display is shown. Type **10** and press **Enter**. The Work with TCP/IP Host Table Entries display is shown, which will display the contents of the host table similar to the following:

```
                        Work with TCP/IP Host Table Entries
                                                                    System:  XXXXXXXXX
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

     Internet       Host
Opt  Address        Name
     127.0.0.1      LOOPBACK
     9.5.29.77      SERVERSYS
     9.5.7.91       CLIENTSYS
```

Port 21 is the well-known port for FTP control data, but, to verify that FTP is actually configured to use port 21, use the WRKSRVTBLE CL command on the server system to display the configured TCP/IP services. It should look similar to:

```
                  Work with Service Table Entries
                                                                    System:
Type options, press Enter.
  1=Add   4=Remove   5=Display

Opt  Service                            Port   Protocol

     exec                                512   tcp
     ftp-control                          21   tcp
     ftp-control                          21   udp
     ftp-data                             20   tcp
     ftp-data                             20   udp
```

To locate the corresponding audit records on the server system, perform the following steps:

1. On the DSPJRN screen, on the client system, when you are looking at the SK audit record, press F10 to display the entry details. The resulting display will contain the date and time that the SK audit record was created. Write the date and time on piece of paper.

2. On the server system, type a DSPJRN command restricting the display to audit records for the same date and time as you recorded in step 1. For example,

   ```
   DSPJRN JRN(QAUDJRN) FROM TIME('04/12/1999' '08:00')
   ```

   Note: The time value may have to be adjusted depending on any time zone differences and how well the system times of the client and server systems are coordinated.
3. On the server system, examine the DSPJRN display looking for SK audit records for jobs whose names begin with the characters QTFTP. The names of FTP server jobs all begin with this sequence of characters.
4. For each SK audit record found, display the SK audit entry until you locate the audit record that corresponds to the connection request initiated by the client. You can identify the matching entry by the presence of the same IP addresses and port numbers, but they will appear in the reverse order. For example, the matching entry for the client request shown above would look like:

   ```
                                Display Journal Entry

   Object . . . . . :
   Library. . . . . :
   Member . . . . . :
   Sequence . . . . . :  15852
   Code . . . . . :  T  - Audit trail entry
   Type . . . . . :  SK - Secure sockets connections
   Incomplete Data  . . :  No
                                 Entry specific data
   Column                        *...+....1....+....2....+....3....+....4....+....5
   00001                        'A9.5.29.77      21  9.5.7.91      5321       '
   ```

   The audit record indicates that the server system with IP address 9.5.29.77 accepted (A) a connection request on port 21 from a client system whose IP address is 9.5.7.91 and was using port 5321 on the client system. Notice that both of the IP addresses and port numbers match exactly those shown in the SK audit record on the client system.

   Write down the Job name associated with the audit record. This is the specific FTP server job used by the client user.

   Then exit the DSPJRN display by pressing **F12**.
5. On the server system, display all of the audit records associated with the FTP server job you recorded in step 4. For example,

   ```
   DSPJRN JRN(QAUDJRN) FROMTIME('04/12/1999' '08:00') JOB(QTFTP00674)
   ```

   This will display all of the audit records for the QTFTP00674 server job. This will include the SK audit record you examined in step 4.
6. You can now examine the audit records associated with the client's FTP requests that were executed by the server system. Audit records that may be of particular interest include:
   - PS audit record. The PS audit record of type H records that the server job has been changed to execute under a different user profile. In this case, it is the user profile that the client specified on the USER FTP subcommand. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  2857
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  PS - Process user profile swap
Incomplete Data  . . :  No
                              Entry specific data
Column                        *...+....1....+....2....+....3....+....4....+....5
00001                         'HLESLIE2
00051                         '              0'
```

In this case, the server job was changed to use the LESLIE2 user profile. Notice that this is not the same user profile as was used on the client system (LESLIE).

- SK audit records. Additional SK audit records will be present if the FTP client performed a PUT or GET FTP subcommand. These additional connections are used to transfer the data associated with an FTP subcommand. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  15856
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  SK - Secure sockets connections
Incomplete Data  . . :  No
                              Entry specific data
Column                        *...+....1....+....2....+....3....+....4....+....5
00001                        'A9.5.29.77      5174 9.5.7.91      5322       '
```

In this case, the server job accepted a connection using port 5174 for a connection request from the client that used port 5322. There would be a corresponding SK audit record on the client system.

Audit TELNET connections

If you want to audit the actions of a user that uses TELNET or STRTCPTELN CL commands, you should

- Ensure that the QAUDLVL system value includes the *JOBDTA, *SECURITY, and *AUTFAIL option values on both the client and server systems.
- Ensure that the QAUDCTL system value includes the *AUDLVL option value on both the client and server systems. In addition, the *OBJAUD option value must be present on the client system.
- Set the TELNET and STRTCPTELN command objects to be audited by issuing the following commands:

  CHGOBJAUD OBJ(QSYS/TELNET) OBJTYPE(*CMD) OBJAUD(*ALL)
  CHGOBJAUD OBJ(QSYS/STRTCPTELN) OBJTYPE(*CMD) OBJAUD(*ALL)

After these system values and object auditing values are set, the appropriate auditing will occur on both the client and server systems.

The following paragraphs describe how to view the audit records on both the client and server systems.

On the client system, display the audit entries in the QAUDJRN journal for the specific user. This can be done with the DSPJRN CL command. For example:

DSPJRN JRN(QAUDJRN) ENTTYP(CD) USRPRF(MARY)

will display all of the command string (CD) requests for user profile MARY. On the DSPJRN display, type a **5** next to a CD record to be looked at in detail and press **Enter**. This will display the entry specific data for the audit record. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  3223
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  CD - Command string
Incomplete Data  . . :  No
                               Entry specific data
Column                         *...+....1....+....2....+....3....+....4....+....5
00001                         'CTELNET    QSYS      *CMD    NTELNET RMTSYS (RMTASR'
00051                         'C2'
```

This record indicates that a CL command (C) whose object name is TELNET located in library QSYS and which is a *CMD type object was run interactively (N). Starting in column 31 of the entry specific data is the actual command that was run. In this case, it shows that a TELNET connection was requested with the server system RMTASRC2.

On the DSPJRN screen, press F10 to display the entry details. The resulting display will contain the date and time that the CD audit record was created. Write the date and time down on a piece of paper.

To locate the corresponding audit records on the server system RMTASRC2, signon to the server system and perform the following steps.

1. On the server system, type a DSPJRN command restricting the display to audit records for the same date and time as you recorded above and only display job change (JS) audit records. For example:

   ```
   DSPJRN JRN(QAUDJRN) FROMTIME('04/12/1999' '10:15') ENTTYP(JS)
   ```

   Note: The time value may have to be adjusted depending on any time zone differences and how well the system times of the client and server systems are coordinated.
2. On the server system, examine the DSPJRN display looking for JS audit records for jobs whose names begin with the characters QPDEV. The names of TELNET initiated jobs all begin with this sequence of characters.
3. For each PS audit record found that matches the correct time frame and is associated with a job whose name starts with QPADEV, display the PS audit entries until you locate one whose entry specific data begins with the characters SI. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  18654
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  JS - Job data
Incomplete Data  . . :  No
                               Entry specific data
Column                         *...+....1....+....2....+....3....+....4....+....5
00001                         'SI QPADEV000KMARY      032662QPADEV000KMARY      Q'
00051                         'DFTJOBD  QGPL                            *DEV       '
00101                         '         PRT01     QSYS      QSYS2     QHLPSYS   Q'
00151                         'USRSYS   SYC2TOOLS QGPL      QTEMP                 '
00201                         '                                                   '
00251                         '                                                   '
00301                         '                                                   '
00351                         '                                                   '
```

The audit record indicates that it is for a job start (S) of an interactive job (I) with a job name of QPADEV000K.MARY.032662 on device QPADEV000K and user profile MARY.

Note: If the client uses a different user name to sign on to the remote system, the user profile names will not match between the client and server systems.

4. You can now examine the audit records associated with the client's TELNET session. One record that may be of particular interest is the JS audit record. The JS audit record whose entry specific data begins with EI indicates that the client has signed off the TELNET session. For example:

```
                              Display Journal Entry

Object . . . . . :
Library. . . . . :
Member . . . . . :
Sequence . . . . . :  18655
Code . . . . . :  T  - Audit trail entry
Type . . . . . :  JS - Job data
Incomplete Data  . . :  No
                               Entry specific data
Column                         *...+....1....+....2....+....3....+....4....+....5
00001                         'EI QPADEV000KMARY      032662QPADEV000KMARY      Q'
00051                         'DFTJOBD  QGPL                            *DEV       '
00101                         '         PRT01     QSYS      QSYS2     QHLPSYS   Q'
00151                         'USRSYS   SYC2TOOLS QGPL      QTEMP                '
00201                         '                                                    '
00251                         '                                                    '
00301                         '                                                    '
00351                         '                                                    '
```

In this case, the interactive (I) job QPADEV000K.MARY.032662 has ended (E).

Part 5. Appendixes

Appendix A. Customization programs

To meet Common Criteria security requirements, you must perform customization tasks on your system. Most of the tasks involve changing the public authority for objects and commands to create a more secure, restrictive environment. Feature code 1930 of the OS/400 Licensed Program includes programs to perform most of the customization tasks for you.

The following customization programs are included with feature code 1930:

QSYCCDRV
: This program calls the other programs using QSYS as the parameter.

  Note: After QSYCCDRV has been run, you must determine if an IPL is necessary:

  1. To determine whether or not you must IPL your system, type the command `DSPSECA` on the command line. If either of the system values QSECURITY or QPWDLVL have a **pending** value, then you must IPL your system.
  2. To initiate the IPL, type `PWRDWNSYS OPTION(*IMMED) RESTART(*YES)` on the command line.
  3. After the IPL has completed, type `CHGSYSVAL SYSVAL(QPWDMAXLEN) VALUE(128)`[1] on the command line.

  [1] If the current Password Level (QPWDLVL) system value was 0 or 1 at the time you ran QSYCCSVL, QSYCCSVL was unable to change the Password Maximum Length (QPWDMAXLEN) system value to the recommended value of 128. At password level 0 and 1, QPWDMAXLEN cannot exceed the value of 10. Use the CHGSYSVAL command to set the QPWDMAXLEN system value to the recommended value after the IPL.

QSYCCCCA
: This programs restricts public authority to commands.

QSYCCCCD
: This program changes the default value of parameters on some commands.

QSYCCCOA
: This program restricts public authority to objects that may exist on your system.

QSYCCCPA
: This program restricts authority to operating system programs.

QSYCCSVL
: This program sets security-relevant system values and changes the error messages that are sent for incorrect signon attempts.

The basic philosophy on a tightly secured system is that the average user should have only enough authority to perform necessary functions. Therefore, the programs restrict many commands and objects that are normally not needed by the average end-user.

Attention!

After you have run the customization programs, you must thoroughly test your applications. Applications may fail initially because of insufficient authority.

This appendix describes the tasks performed by the customization programs and the reason for these tasks. It also lists the commands, programs, and objects that are changed by the programs.

Tasks performed by the customization programs

The topics that follow describe each of the major tasks performed by the customization programs. Each topic describes why the task is being performed. If your applications do not function successfully after running the programs, you may use the information to make changes to these tasks. You should consult with your DAA (Designated Approving Authority) or security auditor before making changes.

See the following tables for the specific changes to commands and other objects that are made by the customization programs:

- Table 12 on page 127
- Table 13 on page 130
- Table 14 on page 130
- Table 15 on page 131
- Table 16 on page 134

Set up explicit authority

Common Criteria security requires that users be explicitly authorized to access an object. On the system, this means that the public authority to objects or to libraries must be set to *EXCLUDE. See “Plan explicit authority” on page 10 for information about how you can use library authority to meet this requirement.

The QSYCCCCD program changes the default value of the public authority (AUT) parameter for the Create Library (CRTLIB) command. This ensures that any new libraries that are created on your system have a public authority of *EXCLUDE.

The QSYCCSVL program changes the QCRTAUT system value to *EXCLUDE. This ensures that new objects that are created in libraries have a public authority of *EXCLUDE (if your libraries use the default value of *SYSVAL for the CRTAUT parameter). The QSYCCCOA program sets public authority for directories.

After QSYCCDRV has been run, you must determine if an IPL is necessary. To make the determination, type the command DSPSECA. If either of the system values QSECURITY or QPWDLVL have a pending value, then you must IPL your machine. Example of a machine that must be IPLed:

Restrict save and restore capability

Restricting the capability to save objects from your system and to restore objects is important for your system security. To meet Common Criteria security requirements, you must make sure that only trusted system users have save and restore capabilities on your system. You can do this several ways:

- Carefully controlling which user profiles have *SAVSYS (save system) special authority.
- Making sure that user profiles with *SAVSYS special authority are used only when necessary. Users who need to save and restore objects should have another user profile for their normal activities.
- Restricting physical access to the devices and the media used for save and restore operations.
- Setting up object auditing for tape device descriptions and diskette device descriptions.
- Excluding public users on the system from using commands that save and restore objects on the system. The QSYCCCCA program sets the public authority to *EXCLUDE for all save and restore commands.
- Using the QALWOBJRST system value to prevent anyone from restoring either system state programs or programs that adopt authority.

Restrict communications capabilities

Your system is shipped with the capability to provide a communications link between your system and your support organization. This capability must be carefully restricted to make sure that data communications capabilities are not used to send confidential information or to load untrusted programs.

To prevent unauthorized individuals from performing data communications on your system, the customization programs do the following:

- The QSYCCCCA program restricts access to commands that configure communications.
- The QSYCCCCA program restricts commands that are used to access communications devices.
- The QSYCCCOA program restricts access to any communications configuration objects that may already exist on your system.

Protect subsystem descriptions

Subsystem descriptions can significantly affect the performance on your system. They can also be used to allow jobs to enter your system. The QSYCCCCA program ensures that only authorized users can configure subsystems by restricting authority to subsystem commands.

Control printing

You can use parameters on both printer device descriptions and output queues to control who can print and who can work with spooled files waiting to print. The QSYCCCCA program restricts authority to the commands that work with printing on your system.

Protect message files

Messages can be used to send information between jobs. The QSYCCCOA program restricts message files to prevent users from changing the content or format of messages. The QSYCCCCD program changes the default authority parameter for the Create Message File (CRTMSGF) command.

Restrict the System/38 environment

The System/38™ Environment and CL programs of type CLP38 represent a potential security exposure. In the System/38 environment, the system searches the library list in a different sequence than it does for the integrated OS/400 environment. If a user issues a command from the System/38 environment or runs a CLP38 program, the system searches in the following sequence:

1. Library QUSER38 (if it exists)
2. Library QSYS38

A programmer or other knowledgeable user could place another CL command in either of these libraries. The system would use that command instead of one from a library in the library list.

Although the System/38 environment is not part of the TOE (Target of Evaluation), the QSYCCCCD program restricts the System/38 libraries to make sure that no one attempts to use the System/38 environment capabilities on your system.

Protect the printing environment

Advanced function printing provides the capability to merge printed output with stored overlays. The system searches the following libraries for the overlays:

- QFNTCPL
- QFNT00 through QFNT19

- QFNT61 through QFNT69

A knowledgeable user could cause mischief on your system by creating an overlay and placing it in one of these libraries. Your printed output might be merged with inappropriate images or messages. To control the advanced function printing environment on your system, the QSYSCCCCD program does the following:

- Creates each QFNTxx library if it does not already exist. This prevents someone else from creating the libraries later.
- For each QFNTxx library, the program removes any the public authority greater than *USE. This prevents an unauthorized user from adding new forms overlays to the library.

Remove functions that are not a part of the Target of Evaluation

Some functions that are included as part of the base operating system have not been evaluated for Common Criteria security. These functions include the following:

- Application development tools (except source entry utility)
- Double-byte character support
- Authority holders
- Support for OfficeVision® and object distribution
- Some service functions
- System/36 environment

The QSYCCCCA program and the QSYCCCOA program restrict authority to the commands and objects that are used by these functions.

Note: If you have followed the installation and customization instructions in this book, many of these functions will not be on your system. The customization programs exclude any commands and objects they find as an added precaution.

Prevent unauthorized signon attempts

You can take steps on your system to make it more difficult for an unauthorized person to guess a valid user profile and password combination. For example, your policies and system values should require non-trivial passwords. The QSYCCSVL program sets several password system values.

The QSYCCSVL program also changes the content of the error messages that are sent when an incorrect user ID or password is entered on the signon display. Both messages are changed to the same text. Therefore, a would-be intruder does not know whether the user ID or the password is incorrect.

Details of the customization programs

The following table shows all the commands whose public authority is changed to *EXCLUDE by the QSYCCCCA program.

Table 12. Commands Excluded by the QSYCCCCA Program

ADDALRACNE	ADDEWCM	ADDPFXDLFM
ADDALRD	ADDEWCPTCE	ADDPRBACNE
ADDALRSLTE	ADDEWLM	ADDPRBSLTE
ADDCFGLE	ADDHDBDLFM	ADDRDBDIRE
ADDCMNE	ADDICFDEVE	ADDSMTPLE
ADDCOMSNMP	ADDIPSIFC	ADDSOCE
ADDDIRE	ADDIPSLOC	ADDTCPPTP
ADDDIRSHD	ADDIPSRTE	ADDTCPSVR
ADDDLOAUT	ADDLANADPI	ANSLIN
ADDDSTLE	ADDNCK	ANZJVAPGM
ADDDTADFN	ADDNODLE	ANZUSRPC3
ADDEMLCFGE	ADDNWSSTGL	APINGAREXEC
ADDEWCBCDE	ADDPFVLM	ASKQST
CFGDEVMLB	CHGCOMSNMP	CHGDEVHOST
CFGIPS	CHGCOSD	CHGDEVINTR
CFGPM400	CHGCRQD	CHGDEVPRT
CFGTCPBP	CHGCSI	CHGDEVRTL
CFGTCPLPD	CHGCTLAPPC	CHGDEVSNPT
CFGTCPPTP	CHGCTLASC	CHGDEVSNUF
CFGTCPRTD	CHGCTLBSC	CHGDHCPA
CFGTCPRXC	CHGCTLFNC	CHGDIRE
CFGTCPSMTP	CHGCTLHOST	CHGDIRSHD
CFGTCPSNMP	CHGCTLLWS	CHGDKTF
CHGALRACNE	CHGCTLRTL	CHGDLOAUD
CHGALRD	CHGCTLRWS	CHGDLOAUT
CHGALRSLTE	CHGDDMF	CHGDLOOWN
CHGALRTBL	CHGDDMTCPA	CHGDLOPGP
CHGBCKUP	CHGDEVAPPC	CHGDOCD
CHGBPA	CHGDEVASC	CHGDSTA
CHGCFGL	CHGDEVASP	CHGDSTD
CHGCFGLE	CHGDEVBSC	CHGDSTL
CHGCLURCY	CHGDEVDKT	CHGDTA
CHGCMNE	CHGDEVFNC	CHGEMLCFGE
CHGEWCBCDE	CHGLINWLS	CHGSECA
CHGEWCM	CHGLINX25	CHGSMTPA
CHGEWCPTCE	CHGLPDA	CHGSNMPA
CHGEWLM	CHGMODD	CHGSRVCFG
CHGFTR	CHGNCK	CHGSSNMAX
CHGICFDEVE	CHGNODGRPA	CHGSYSDIRA
CHGICFF	CHGNTBD	CHGS36PGMA
CHGIPSIFC	CHGNTPA	CHGS36PRCA
CHGIPSLOC	CHGNWIFR	CHGS36SRCA
CHGIPSTOS	CHGNWSD	CHGTCPSVR
CHGJVAPGM	CHGNWSUSRA	CHGTFTPA
CHGLANADPI	CHGPCOPRF	CHGUSRTRC
CHGLINASC	CHGPOPA	CHKDKT
CHGLINBSC	CHGPRBACNE	CHKDLO
CHGLINDDI	CHGPRBSLTE	CHKIGCTBL
CHGLINFAX	CHGRDBDIRE	CLRDKT
CHGLINFR	CHGRTDA	CPYCFGL
CHGLINSDLC	CHGRWSPWD	CPYDOC
CHGLINTDLC	CHGRXCA	CPYFRMDIR

Table 12. Commands Excluded by the QSYCCCCA Program (continued)

CPYFRMDKT	CRTDEVBSC	CRTLINFR
CPYFRMPCD	CRTDEVDKT	CRTLINSDLC
CPYIGCTBL	CRTDEVFNC	CRTLINTDLC
CPYTODIR	CRTDEVHOST	CRTLINWLS
CPYTODKT	CRTDEVINTR	CRTLINX25
CPYTOPCD	CRTDEVPRT	CRTMODD
CRTALRTBL	CRTDEVRTL	CRTNODGRP
CRTCOSD	CRTDEVSNPT	CRTNODL
CRTCRQD	CRTDEVSNUF	CRTNTBD
CRTCSI	CRTDKTF	CRTNWIFR
CRTCTLAPPC	CRTDOC	CRTNWSD
CRTCTLASC	CRTDSTL	CRTNWSSTG
CRTCTLBSC	CRTDTADCT	CRTSPADCT
CRTCTLFNC	CRTFLR	CRTSRVCFG
CRTCTLHOST	CRTFTR	CRTWSCST
CRTCTLLWS	CRTIGCDCT	CVTDLSNAM
CRTCTLRTL	CRTJVAPGM	CVTIPSIFC
CRTCTLRWS	CRTLINASC	CVTIPSLOC
CRTDEVAPPC	CRTLINBSC	CVTNAMSMTP
CRTDEVASC	CRTLINDDI	CVTTOFLR
CRTDEVASP	CRTLINFAX	CVTUSRCERT
DLTALR	DLTIGCDCT	DLTUSRTRC
DLTALRTBL	DLTIGCSRT	DLTWSCST
DLTAUTHLR	DLTIGCTBL	DMPCLUTRC
DLTCLD	DLTIPXD	DMPUSRTRC
DLTCNNL	DLTJVAPGM	DSPACC
DLTCOSD	DLTMEDDFN	DSPACCAUT
DLTCRG	DLTMGTCOL	DSPAPPNINF
DLTCRQD	DLTMODD	DSPAUTHLR
DLTCSI	DLTNETF	DSPAUTLDLO
DLTDEVMLB	DLTNODGRP	DSPBCKSTS
DLTDFUPGM	DLTNODL	DSPBCKUP
DLTDKTLBL	DLTNTBD	DSPBCKUPL
DLTDLO	DLTNWID	DSPCLUINF
DLTDOCL	DLTNWSD	DSPCNNL
DLTDST	DLTNWSSTG	DSPCOSD
DLTDSTL	DLTSPADCT	DSPCRGINF
DLTDTADCT	DLTSQLPKG	DSPCSI
DLTFTR	DLTSRVCFG	DSPDDMF
DSPDIRE	DSPJVAPGM	DSPRDBDIRE
DSPDKT	DSPLANADPP	DSPRMTDFN
DSPDLOAUD	DSPLANMLB	DSPSOCSTS
DSPDLOAUT	DSPLANSTS	DSPSRVA
DSPDLONAM	DSPMODD	DSPUSRPMN
DSPDOC	DSPMODSTS	DSPVTMAP
DSPDSTL	DSPNCK	DUPDKT
DSPDSTSRV	DSPNODGRP	EDTBCKUPL
DSPDTA	DSPNTBD	EDTDLOAUT
DSPDTADCT	DSPNWID	EDTDOC
DSPEWCBCDE	DSPNWSA	EDTIGCDCT
DSPEWCM	DSPNWSD	EDTS36PGMA
DSPEWCPTCE	DSPNWSSTG	EDTS36PRCA
DSPEWLM	DSPNWSUSR	EDTS36SRCA
DSPFLR	DSPNWSUSRA	EDTWSOAUT
DSPHLPDOC	DSPOPTLCK	EJTEMLOUT
DSPIGCDCT	DSPOPTSVR	EMLPRTKEY
DSPIPXD	DSPPRB	ENDAGTSRV

Table 12. Commands Excluded by the QSYCCCCA Program (continued)

ENDDIRSHD	PING	RMVCMNE
ENDEPMENV	PMLINMON	RMVCOMSNMP
ENDNWIRCY	PRTCMNSEC	RMVDIRE
ENDPASTHR	PRTDOC	RMVDIRSHD
ENDPRTEML	PRTIPSCFG	RMVDLOAUT
ENDRDBRQS	PRTSWL	RMVDSTLE
ENDTIESSN	PRTTCPPTP	RMVEMLCFGE
EXTPGMINF	QRYDOCLIB	RMVEWCBCDE
FILDOC	QRYDST	RMVEWCPTCE
FMTDTA	QRYTIEF	RMVFTRACNE
GRTUSRPMN	RCLDDMCNV	RMVFTRSLTE
GRTWSOAUT	RCLDLO	RMVICFDEVE
INZDKT	RCVDST	RMVIPSIFC
INZDLFM	RCVNETF	RMVIPSLOC
INZPCS	RCVTIEF	RMVIPSRTE
LNKDTADFN	RGZDLO	RMVLANADPI
LPR	RMVALRD	RMVNCK
MOVDOC	RMVBNDDIRE	RMVNODLE
OVRDKTF	RMVCFGLE	RMVNWSSTGL
RMVRDBDIRE	RTVSWLSRC	SNDNETMSG
RMVSMTPLE	RTVWSCST	SNDNETSPLF
RMVSOCE	RUNBCKUP	SNDTCPSPLF
RMVTCPPTP	RVKACCAUT	SNDTIEF
RMVTCPSVR	RVKUSRPMN	STRAGTSRV
RNMDIRE	RVKWSOAUT	STRDFU
RNMDKT	SAVDLO	STRDIRSHD
RNMDLO	SAVS36F	STRDKTRDR
RNMDSTL	SAVS36LIBM	STRDKTWTR
RNMLANADPI	SBMDKTJOB	STREML3270
RNMNCK	SBMNETJOB	STRFMA
RPLDOC	SBMRMTCMD	STRIDD
RSMLINRCY	SETASPGRP	STRITF
RSMNWIRCY	SETCSTDTA	STRPASTHR
RTVBCKUP	SETVTMAP	STRPCCMD
RTVDLONAM	SETVTTBL	STRPCO
RTVDOC	SNDDST	STRPGMMNU
RTVQMQRY	SNDNETF	STRPRTEML
STRQST	WRKCNNL	WRKIPXD
STRRMTWTR	WRKCOSD	WRKLANADPT
STRSPTN	WRKCSI	WRKMODD
STRTIESSN	WRKDBFIDD	WRKNAMSMTP
TFRJOB	WRKDDMF	WRKNCK
TFRPASTHR	WRKDIRE	WRKNETF
TRACEROUTE	WRKDIRLOC	WRKNETJOBE
TRCREX	WRKDIRSHD	WRKNODL
TRCTCPRTE	WRKDOC	WRKNODLE
UPDDTA	WRKDOCLIB	WRKNTBD
VFYAPPCCNN	WRKDOCPRTQ	WRKNWSD
VFYSRVCFG	WRKDSTL	WRKNWSENR
VFYTCPCNN	WRKDTADCT	WRKNWSSTG
WRKALR	WRKDTADFN	WRKNWSSTS
WRKALRD	WRKFLR	WRKPMRMTS
WRKALRTBL	WRKFTR	WRKPMRPTO
WRKAPPNSTS	WRKFTRACNE	WRKPMSCH
WRKBPTBL	WRKFTRSLTE	WRKPRDINF
WRKCHTFMT	WRKGSS	WRKPSFCFG

Table 12. Commands Excluded by the QSYCCCCA Program (continued)

WRKQST	WRKSPADCT	WRKS36SRCA
WRKRDBDIRE	WRKSRVTBLE	WRKTCPPTP
WRKRTDCFG	WRKS36PGMA	WRKTIE
WRKSOC	WRKS36PRCA	

The following table shows the commands that have the default value changed for one of the command parameters by the QSYCCCCD program.

Table 13. Commands with Default Values That Are Changed by the QSYCCCCD Program

Command Name	Parameter Whose Default Value Is Changed	Default Value Set by Program	Command Description
CRTLIB	Public authority (AUT)	*EXCLUDE	Create library
CRTJRN	Public authority (AUT)	*EXCLUDE	Create journal
CRTJRNRCV	Public authority (AUT)	*EXCLUDE	Create journal receiver
CRTMSGF	Public authority (AUT)	*USE	Create message file

In addition, the QSYCCCCD program does the following:

- It removes any public authority greater than *USE for the QSYS38 library and the QUSER38 library. If these libraries do not exist, the program creates them to prevent another user from creating them with a different public authority.
- It ensures that the exit programs for automatic cleanup (QEZUSRCLNP) and for automatic power off (QEZPWROFFP) do not adopt authority.
- It creates the following libraries if they do not already exist:
  - QFNTCPL
  - QFNT00 through QFNT19
  - QFNT61 through QFNT69
- It sets the public authority to *USE for each of the QFNTxx libraries, unless the public authority for the library is already less than *USE.

The following table lists the object types whose authority is changed by the QSYCCCOA program. The table shows whether the public authority is set to *EXCLUDE or to *USE by the program.

Table 14. Objects Whose Authorities are Restricted by the QSYCCCOA Program

Object Type	Public Authority Set by Program	Description of Object Type
*ALRTBL	*USE[1]	Alert table
*CNNL	*USE[1,2]	Connection list
*COSD	*USE[1,2]	Class-of-service description
*DOC	*USE[1,3]	Document
*FLR	*USE[1,3]	Folder
*JRN	*EXCLUDE	Journal
*JRNRCV	*EXCLUDE	Journal receiver
*MODD	*USE[1]	Mode description
*MSGF	*USE[1]	Message file
*NTBD	*EXCLUDE	NetBIOS

Table 14. Objects Whose Authorities are Restricted by the QSYCCCOA Program (continued)

Object Type	Public Authority Set by Program	Description of Object Type

[1] The program removes any authority greater than *USE. Therefore, if an object on your system has *EXCLUDE authority or *READ authority, the program does not change that authority.

[2] Some objects of this type are created when the system is installed. They are used for operating system functions. You should not create any additional objects of this type. The QSYCCCCA program changes the public authority for the CRTxxx commands to *EXCLUDE.

[3] Some Online help information is contained in documents and folders. Therefore, system users need *USE authority to these objects.

The public authority of directories is changed to be no more than *RX for public data authority, and *NONE for public object authority. The only exception is for the /tmp directory.

Some programs that are part of the operating system can be called by a user. Other programs are blocked. The following table lists callable OS/400 programs whose public authority is set to *EXCLUDE by the QSYCCCPA program.

Table 15. Callable Programs and service programs whose authorities are changed by the QSYCCCPA program

CMACCP	CMSCSP	QAHASBMTEE
CMALLC	CMSCST	QALGENA
CMCFM	CMSCSU	QALRTVA
CMCFMD	CMSCT	QALSNDA
CMCNVI	CMSDT	QCCWRKCC
CMCNVO	CMSED	QCIGETUL
CMDEAL	CMSEND	QCRADRTN
CMECS	CMSERR	QCRCLEAR
CMECT	CMSF	QCREXHAN
CMEMBS	CMSLD	QCRGDDM
CMEMN	CMSMN	QCRHLLST
CMEPLN	CMSPLN	QCRSORT
CMESL	CMSPTR	QCRSPACE
CMESUI	CMSRC	QCSTCHTEXT
CMFLUS	CMSRT	QCSTCRGEXT
CMINIT	CMSSL	QCSTCRGVRY
CMPTR	CMSST	QCSTCTCFRM
CMRCV	CMSTPN	QCSTCTMBAS
CMRTS	CMTRTS	QCSTCTMCCR

Table 15. Callable Programs and service programs whose authorities are changed by the QSYCCCPA program (continued)

QCSTCTMCLD	QEMPEBSC	QFNREAD
QCSTCTMCLR	QEMPESNA	QFNREADI
QCSTCTMCMR	QESISRV	QFNWRT
QCSTCTMCRF	QESISTR	QFNWRTI
QCSTCTMCRM	QESRSRVA	QFPAACTV
QCSTCTMCRS	QEZBCKUP	QFPADOLD
QCSTCTMCRU	QEZBKMSG	QFPADOLS
QCSTCTMCSP	QEZBKSCD	QFPADOLU
QCSTCTMCSR	QEZBKWM	QFPADPNU
QCSTCTRMCD	QEZCHBKL	QFPADRNI
QCSTDCMEX	QEZCHBKS	QFPADRUA
QCSTEXTPWR	QEZOLBKL	QFPAMONB
QCSTINETD	QEZRTBKD	QFPAMONN
QCSTRPTTR	QEZRTBKH	QFPAPRFJ
QDBRCLXR	QEZRTBKO	QFPARAPI
QDCRNWID	QEZRTBKS	QFPARAPP
QDCRNWSD	QEZSVIBM	QFPASAPI
QDZXDRV	QFIEXIT1	QFPAUAPP
QFSMAIN	QGYRDEV	QHFCLODR
QFVLSTA	QGYRLIB	QHFCLOSF
QFVLSTNL	QGYRLOG	QHFCPYSF
QFVRMVA	QGYRSPL	QHFCRTDR
QFVRTVCD	QGYRTVJ	QHFCTLFS
QGLDPUEXIT	QGYRTVJS	QHFDLTDR
QGLDUSTB	QGYRTVM	QHFDLTSF
QGYCLSC	QGYRTVPR	QHFFRCSF
QGYCST	QGYRTVS	QHFGETSZ
QGYDLTC	QGYRUSR	QHFLSTFS
QGYENDM	QGYSCST	QHFLULSF
QGYEOJSM	QGYSETM	QHFMOVSF
QGYMMSG	QGYUSRA	QHFOPNDR
QGYOLSQL	QGYVMSG	QHFOPNSF
QGYOPNC	QHCCCFG	QHFRDDR
QGYRCST	QHCQRYLN	QHFRDSF
QGYRCVI	QHEENRL	QHFRNMDR
QGYRCVM	QHFCHGAT	QHFRNMSF
QHFRTVAT	QLPEXIT1	QNMSNDRP
QHFSETSZ	QLPLPRDS	QNMSNDRQ
QHFWRTSF	QLPWRKIP	QNMSTRAP
QHNAPRST	QMARQSOA	QOCCTLOF
QHSMMOVF	QMFBMHDL	QOCXEMN
QHSMMOVL	QMFRCVR	QODDLSMA
QHUCVTTF	QMFSNDR	QOECMPRT
QHUCVTVC	QMNHCMD	QOGCHGOE
QHUOVRTB	QMNSBS	QOGRTVOE
QHUUPKBD	QMNUIM	QOHFIXIX
QHWPMSVR	QNEOSOEM	QOKADDDP
QILCRTMD	QNMCHGMN	QOKCHGDP
QILFILIL	QNMDRGAP	QOKDSPDP
QILOMAIN	QNMDRGTI	QOKRMVDP
QIMGSERV	QNMENDAP	QOKSCHD
QJOCHCAA	QNMRCVDT	QOLDLINK
QJVAANZJVM	QNMRCVOC	QOLELINK
QJVADBST	QNMREGAP	QOLQLIND
QJVAMAT	QNMRGTI	QOLRECV
QJVAQUIT	QNMRTVMN	QOLSEND
QLPCRTDT	QNMSNDER	QOLSETF

Table 15. Callable Programs and service programs whose authorities are changed by the QSYCCCPA program (continued)

QOLTIMER	QQAEXIT2	QSXRMTR2
QORPR	QQDAPROC	QSYEIMSSL
QORTS	QRQSRVX	QSYEIMUSTB
QORXT	QRQSRV0	QSZSPTPR
QOSPRINT	QRQSRV1	QTADMPDV
QPCCOLUM	QRWCHRDB	QTALCTG
QPCMSG0	QRWSSL	QTAPIPE
QPCSPCOL	QSCBMKTE	QTATHPRC
QPCSTATS	QSCBPSP	QTESDBGHUB
QPMBPCS	QSCBSRVE	QTESDBGSVR
QPMMRCLS	QSCWCLNP	QTESPASSVR
QPWFSERVSO	QSOCIP03	QTMMJOBS
QPWFSERVS2	QSOCIP04	QTMMREGT
QPYRTJWA	QSOCPTFC	QTMMSADD
QP0ZOLIP	QSOCWIFC	QTMMSRVR
QP0ZOLSM	QSOCWRTE	QTMPJOBS
QP0ZPCPJ	QSOMAINT	QTMPLPDC
QP0ZPCPT	QSOSSOCK	QTMPLPDQ
QP0ZSPWP	QSQEXIT1	QTMRTVDT
QP0ZSPWT	QSQXRLF	QTMRTVRP
QTMSCRTF	QTOACLS	QTOAURCV
QTMSFWD	QTOACRTQ	QTOAUSND
QTMSHADV	QTOADELQ	QTOAUSTT
QTMSJOBS	QTOADSPC	QTOCCFGIP6
QTMSMALI	QTOAEND	QTOCCHGP
QTMSMCP5	QTOAGHBN	QTOCCNNFTP
QTMSMCVB	QTOAGTID	QTOCGETHST
QTMSMCVF	QTOAISLA	QTOCLPPJ
QTMSMDIR	QTOAISUP	QTOCNETLST
QTMSMTNM	QTOAOPN	QTOCPPJU
QTMSMTPT	QTOAPING	QTOCRTEU
QTMSNDMG	QTOAQRYD	QTOCWRKP
QTMSTATE	QTOARCV	QTODADDP
QTMULSTO	QTOASND	QTODDB2D
QTNCLRLU	QTOASTRM	QTODEXIT
QTNRTNLU	QTOASTT	QTODJOBS
QTOAABRT	QTOATIME	QTODJOBT
QTOAAPID	QTOAUCLS	QTODRMVP
QTOAAPIU	QTOAUOPN	QTODTBL
QTOFRPRS	QXDASSL	QZDFMCOD
QTOKDNLS	QYASPOL	QZDFMCPD
QTOVWRKC	QYASPONA	QZDFMCSA
QTOVWRKP	QYDOTRACE	QZDFMDBR
QTVCLOVT	QYPSCLNUP	QZDFMDB2
QTVDMGR	QYPSJPRC	QZDFMDFG
QTVDMIEX	QYPSJSVR	QZDFMDGD
QTVENDTN	QYPSPRC	QZDFMGCD
QTVOPNVT	QYPSSSL	QZDFMPFR
QTVRDVT	QYPSSVRCHK	QZDFMRTD
QTVSNDRQ	QYPSUSRPEX	QZDFMSTR
QTVSTRTN	QYTXSJVM	QZDFMSVR
QTVWRTVT	QYYCSCHK	QZDFMUPD
QTWAIDSP	QY2FTML	QZDFSTRC
QTWCHKSP	QZBSEVTM	QZLCTRC
QVTRMSTG	QZBSSSL	QZLSADFS
QWCINTPO	QZDAXRLF	QZLSADPS
QXDAGETKEY	QZDFMADD	QZLSCHFS
QXDALISTEN	QZDFMCHD	QZLSCHPS

Table 15. Callable Programs and service programs whose authorities are changed by the QSYCCCPA program (continued)

QZLSCHSG	QZLSOLST	QZSSNTHD
QZLSCHSI	QZLSRMS	Q1PMENU
QZLSCHSN	QZLSSTRS	Q1PRM1
QZLSENDS	QZMFCTXT	Q5BBPNFY
QZLSENSS	QZNFRTVE	Q5BROUTE
QZLSLSTI	QZPAIPTF	SUBRA1
QZLSMAINT		
Service programs		
QCSTCHT	QSYEIM2	QYCPCSMD
QCSTCRG3	QSYITKN	QYCPPROVDR
QCSTCTL1	QTASTIFC	QYDOADD1
QCSTSWT	QTMMDUTL	QYDOBUFFER
QDBCRTHA	QTMMSNDM	QYDOCHK1
QDBRUNHA	QTOCPPPAPI	QYDORTV1
QGLDPAPI	QTOCSRVC	QYDOSGN1
QGYRHR	QTOFTRXI	QYJSPSCK
QIMGCIMG	QTOMAPI	QYKMSYNC
QJVAJDBS	QTOMEAPI	QYPESVPG
QJVANIO14	QTOQMONAPI	QYPSJNI
QJVARJPI	QTOQRAPIL	QZNFNLSR
QJVIO13	QTOSSAPI	QZNFRTLI
QJVIO14	QTOVWRKC	QZSSNTSV
QPMLPMGT	QTOVWRKP	Q5BSTACK
QP0MSRTVSO	QXDADBBK	Q5BSUGAR
QSOCRTVIPA	QXDAEVT	Q5BWRKJ
QSXSRVPL	QXDAIASP	
QSYEIMAPI	QXOBBASS	

The following table shows how system values are set by the QSYCCSVL program.

Table 16. System Values Set by the QSYCCSVL Program

System Value	Setting
These values are **required** for Common Criteria security:	
QALWOBJRST	*NONE
QALWUSRDMN	QTEMP
QATNPGM	*NONE
QAUTOVRT	0
QCFGMSGQ	QSYSOPR
QCRTAUT	*EXCLUDE
QFRCCVNRST	′7′
QMLTTHDACN	′3′
QPASTHRSVR	′0′
QPWDLVL	′3′
QPWDVLDPGM	*NONE
QRETSVRSEC	′0′
QRMTIPL	′0′
QRMTSIGN	*FRCSIGNON
QRMTSRVATR	′0′
QSECURITY	′50′
QSFWERRLOG	*NOLOG
QSHRMEMCTL	′0′
QSPCENV	*NONE

Table 16. System Values Set by the QSYCCSVL Program (continued)

System Value	Setting
QSRVDMP	*NONE
QSYSLIBL	'QSYS QSYS2 QHLPSYS QUSRSYS'
QUSRLIBL	'QGPL QTEMP'
QVFYOBJRST	'3'
The following values are **recommended** for Common Criteria security:	
QAUTOSPRPT	'0'
QDSCJOBITV	'5'
QDSPSGNINF	'1'
QHSTLOGSIZ	32
QINACTITV	'5'
QINACTMSGQ	*ENDJOB
QIPLTYPE	'0'
QJOBMSGQFL	*NOWRAP
QLMTDEVSSN	'1'
QLMTSECOFR	'1'
QMAXSIGN	'3'
QMAXSGNACN	'3'
QPWDEXPITV	'30'
QPWDLMTAJC	'1'
QPWDLMTREP	'1'
QPWDMAXLEN	128
QPWDMINLEN	6
QPWDPOSDIF	'1'
QPWDRQDDGT	'1'
QPWDRQDDIF	'5'
QPWRRSTIPL	'0'
QRCLSPLSTG	'12'
QUSEADPAUT	*NONE
QAUDENDACN	*PWRDWNSYS
QAUDCTL	*AUDLVL *OBJAUD *NOQTEMP
QAUDLVL	*AUTFAIL *CREATE *DELETE *SERVICE *SECURITY *JOBDTA *PGMADP *PGMFAIL
The following values are available if your environment requires them, but the QSYCCSVL program does not change their settings. There are no recommended settings for these system values. The settings shown are the default values set when the system is installed.	
QAUDFRCLVL	*SYS
QCRTOBJAUD	*NONE

The QSYCCSVL program changes the text that is displayed for signon error messages:

Message ID	New Text to Be Displayed
CPF1107	signon information is not correct
CPF1120	signon information is not correct

The QSYCCSVL program sets up the journaling environment by creating the following objects:

QUSRSYS/AUDRCV0001 journal receiver

QSYS/QAUDJRN journal

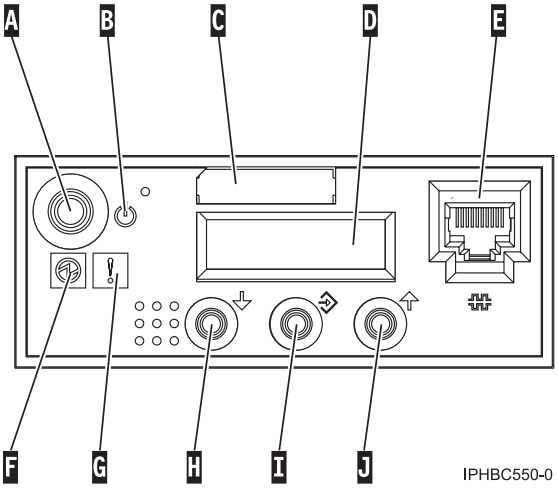
It sets object auditing for the QAUDJRN journal to *NONE.

The QSYCCSVL program sets the CRTAUT parameter for the QSPL library to *CHANGE. It also removes any public authority that is greater than *USE for the following IBM-supplied libraries:

QGDDM
QHLPSYS
QPDA
QSQL
QQRYLIB
QQALIB
QUSRTOOL

Appendix B. System unit control panel

The control panel is used by system operators and service representatives. You can use the control panel to do an initial program load (IPL) and problem analysis. The details of the control panels are described following the illustration.



Control panel details

The following descriptions correspond to the alphabetical call-outs in the control panel display:

- A — Power Button
- B — Reset Button
- C — MTMS Location (Machine Type Model Serial Number)
- D — Display
- E — Service Port
- F — Activity Light
- G — Attention light
- H — Display Scroll Buttons
- I — Display Enter Button
- J — Display Scroll Buttons

Mode descriptions

There are four modes that you can select from the control panel on your system. These modes are:

- **Manual** — When the mode is set to Manual, the system allows you to do all manual IPLs, such as an operator-attended IPL from CD ROM or tape, and manual control functions, such as select an IPL or display the kind of IPL that the system is set to run. However, you cannot perform a remote IPL, an IPL by date and time, or an IPL after a power failure.

  Note: You should only set the mode to Manual when necessary. This ensures that no one can accidentally press the Power button and cause the system to stop.

- **Normal** — The Normal mode allows you to manually turn the power on and to do each of the automatic operations. That is, you can start the system by doing a manual or remote IPL, an IPL by

date and time, or an IPL after a power failure. If you want to stop the system when the mode is set to Normal, use the Power Down System (PWRDWNSYS) command at any display station. You must have QSYSOPR authority to use the PWRDWNSYS command.

- **Auto** — The Auto (automatic) mode allows a remote IPL, an IPL by date and time, and an IPL after a power failure. When the mode is set to Auto, you cannot perform the following tasks:
  - Start the system by performing a manual IPL
  - Stop the system by pressing the Power button
  - Select a different IPL type by using the Increment and Decrement buttons.
- **Secure** — The Secure mode locks the control panel on the system unit. You can only stop the system from a display station by using the PWRDWNSYS command.

Appendix C. National language version feature codes

Each language has an assigned national language feature code, which enables you to order primary and secondary languages for your system. The following table details each national language feature code:

Table 17. Feature Codes

Primary Language Feature Code	Secondary Language Feature Code	National Language
Note: The system prompts for the primary language and secondary language in the form 29xx. The secondary language feature code (57xx) is only used when ordering secondary languages. When you install OS/400, the system prompts for the primary language in the form 29xx. When you install the secondary language you select a feature code, in the form 29xx, from a list of national language feature code identifiers. For example, if you ordered French as a secondary language (5728), you would select 2928 from the list of feature codes when you install the secondary language.		
2911	5711	Slovene
2912	5712	Croatian
2922	5722	Portuguese
2923	5723	Dutch Netherlands
2924	5724	English
2925	5725	Finnish
2926	5726	Danish
2928	5728	French
2929	5729	German
2931	5731	Spanish
2932	5732	Italian
2933	5733	Norwegian
2937	5737	Swedish
2938	5738	English Uppercase Support for Double-Byte Character Set (DBCS)
2939	5739	German Multinational Character Set
2940	5740	French Multinational Character Set
2942	5742	Italian Multinational Character Set
2950	5750	English Uppercase
2954	5754	Arabic
2956	5756	Turkish
2957	5757	Greek
2958	5758	Icelandic
2961	5761	Hebrew
2962	5762	Japanese Double-Byte Character Set (DBCS)
2963	5763	Belgian Dutch
2966	5766	Belgian French
2972	5772	Thai
2975	5775	Czech
2976	5776	Hungarian
2978	5778	Polish
2979	5779	Russian
2980	5780	Brazilian Portuguese
2981	5781	Canadian French
2984	5784	English Uppercase and Lowercase Support for Double-Byte Character Set (DBCS)
2986	5786	Korean Double-Byte Character Set (DBCS)
2987	5787	Traditional Chinese Double-Byte Character Set (DBCS)

Table 17. Feature Codes (continued)

Primary Language Feature Code	Secondary Language Feature Code	National Language
2989	5789	Simplified Chinese Double-Byte Character Set (DBCS) (PRC)
2994	5794	Slovak
2996	5796	Portuguese Multinational Character Set
2998	5798	Farsi

Appendix D. User responsibilities for security

The information on your OS/400 operating system is vital to your organization. Some of the information is also confidential.

As a user of the system, you share the responsibility to protect the information on the system. You do this by:

Keeping your password confidential

Signing off the system when you leave your workstation

Reporting any suspected violations of our security policy

You may also own objects on the system. If you do, you are responsible for controlling access to those objects.

To the Security Administrator:

This appendix is designed to be copied and distributed to the users of your system. It explains what they should do to protect the security of your system.

A few spaces have been left to allow you to fill in specific information that applies to your system:

- In the section **Changing your password**, fill in how often passwords must be changed (the QPWDEXPITV system value).
- In the section **Password rules**, describe the rules you have chosen for password composition (the QPWD... system values).
- In the section **If you forget your password**, fill in whom to contact if a user forgets a password and needs a temporary one.
- In the section **Signing onto the system**, fill in the following information:
  - The number of incorrect signon attempts allowed (the QMAXSIGN system value).
  - Whom to contact if a device or user profile becomes unavailable because of too many incorrect signon attempts.
  - Whom to contact for problems with authorization to a device.
- In the section **Leaving your workstation**, enter the length of time a workstation can be inactive before the user's job is ended or disconnected (**QINACTITV** system value).
- In the section **Accessing information**, fill in whom to contact if a user needs access to an object.
- In the section **Protecting objects you own**, fill in whom to contact for assistance with managing authorization to owned objects.

Note to the system administrator: Copy the rest of this appendix. The last section is intended for users who own objects and are responsible for controlling access to those objects. You may want to distribute that section only to users who have ownership responsibility.

User profiles

Everyone who is authorized to use the system has a unique user profile. Your user profile identifies you to the system and describes your characteristics, such as:

What menu you see when you sign on

What printer you use

How your batch jobs are run

What options you see on system menus

To perform some system functions, such as setting up new users or backing up the system, you need special authorities in your user profile. You may have a separate user profile to use when you perform these system functions. Using a separate user profile prevents you from performing unintended operations while you are doing your normal work.

Some user profiles are provided with the system to manage system jobs and to own system objects. The names of these IBM-supplied user profiles all start with "Q", such as QSECOFR and QPGMR.

Protect user passwords

Everyone who uses the system has a unique user ID and password. Your user ID identifies you to the system and controls what you are permitted to do on the system. When you attempt to sign on, the system uses your password to verify that you are who you say you are.

To protect your password, follow these rules:

1. Keep your password private. Every system user has a password: no one else should need to know yours.
2. Keep your password in your head, *not* on a slip of paper near your workstation.
3. Use a password that is not trivial or easy to guess. For example, avoid using your initials or a password that is the same as your user ID.
4. Check behind you. Do not sign on the system when someone is looking over your shoulder.
5. Situate your keyboard so that it is difficult for someone to watch you type your password.

Change user passwords

System users are required to change their passwords regularly. This limits the amount of time anyone could use a stolen password. Beginning seven days before your password is due to expire, you will see the signon Information display whenever you sign on the system. This display informs you when your password is about to expire.

You can change your password from the signon Information display by pressing F9. In addition, you can use the Change Password (CHGPWD) command. If you try to sign on and your password is expired, you see this message at the top of the signon Information display, which explains that your password has expired and needs to be changed before you can signon.

If you get this message, you have two choices:

- Press **Enter** to change your password. The Change Password display appears.
- Press **F12** to cancel your signon attempt.

When your password is expired, you will not be allowed to sign on until you change it.

When you type your old and new passwords on the display, they do not appear on the screen. When you press **Enter**, the system checks your new password to see if it follows our rules for passwords. You receive a message telling you whether your new password has been accepted. If it is not acceptable, try a different one.

Password rules

The security administrator for the system can define a set of rules that users must follow when assigning passwords. These rules are designed to prevent the use of passwords that are easy to guess. For example, vowels might not be permitted in a password to prevent the use of words.

You may find it difficult to choose a password that meets all these requirements. Here is one suggestion. Think of a sentence that you can easily remember and use the letters and numbers from that sentence to

create your password. For example, if your sentence is “July 4th fishing was great”, your password could be J4FWGR8. Or your sentence might be “Last night we ate pizza for dinner”: LNW8P4D.

If you forget your password

If you do not use the system regularly or if you have just changed to a new password, you might not remember what it is. The security administrator will assign a temporary password for you. When you sign on using the temporary password, the system requires you to assign a new password immediately.

No one, including the security administrator, can tell you what your current password is. Passwords are stored on the system using a technique called one-way encryption. This means that a password is scrambled and coded before it is stored and cannot be decoded. Whenever you sign on, the system encrypts the password you type and compares it to the one that is stored.

Sign on to the system from a workstation

When you attempt to sign on, the system checks several things before allowing you to complete the signon process:

Your user ID and password
: If the user ID you enter is not on the system or the password is incorrect, you see an error message at the bottom of the Sign On display. If you make several incorrect signon attempts in a row, the system prevents you from trying again. The security administrator can make your profile and the device available for signon, as well as assign a temporary password if necessary.

Authority to the workstation
: Some workstations are restricted to certain users. If you are not allowed to sign on at a workstation, you receive a message at the bottom of the Sign On display.

Multiple sessions
: You may not be allowed to sign on at more than one workstation at a time. If you receive a message on the Sign On display indicating you are already signed on, return to the previous workstation and sign yourself off.

Leave a workstation without compromising system security

When you leave your workstation, remember to sign off or to end your session temporarily. If you leave your workstation unattended without signing off, anyone can use your workstation to do whatever you are allowed to do.

To end your session temporarily, use the temporary signoff option on the Assist menu or type DSCJOB (Disconnect Job) on a command line. When you return to your workstation and sign on, your job resumes where you left it.

If you leave your workstation signed on and inactive, the system automatically ends your session after a defined period of inactivity. Inactive means that you have not pressed any key, such as the Enter key or a function key, to cause the system to read information from your workstation.

Security auditing

Your actions on the system may be audited periodically. We can set up the system to keep a log of actions you perform that might affect system security, such as:

Changing a user profile

Attempting to sign on

Using a particular file

Access information

Your ability to access information on the system is determined by your authority to objects. An example of an object is a database file, such as a customer file.

Different types of authority are available to prevent unauthorized access to database information. The security administrator can specify whether someone can read the file, add new information to the file, or delete the entire file. Usually, the security administrator uses these options to manage access to objects, such as files, on the system:

***USE** You may look at information in a file, but you are not allowed to change it.

***CHANGE**
You may change data in a file.

***ALL** You may delete the entire file. You may give other people authority to use the file.

***EXCLUDE**
You are not allowed to use the file in any way.

You may get authority through:

Your own user profile

Your group profile

An authorization list

Public authority

Adopted authority

You can use the Display Object Authority (DSPOBJAUT) command to find out what authority you have to a particular object. Your authority to objects on the system has been set based on your job responsibilities. If you discover that you do not have sufficient authority to perform necessary tasks, contact your system administrator.

Access information with UNIX-style applications

For your OS/400 work, you might need to access objects by using The "root" (/) file system, QOpenSys file system, or user-defined file systems. These file systems are part of the OS/400 integrated file system. They blend the access and authority capabilities of OS/400, PC operating systems, and UNIX-like operating systems to support a rich set of applications. OS/400 supports all the authority values (such as read, update, delete, and hidden) that are available for each of these operating environments. However, every possible authority value is not “visible” through every interface. For example, UNIX-like operating systems do not have the concept of a special authority value for setting referential integrity (*OBJREF). Therefore, when you use a UNIX-like API, the *OBJREF authority for an object is not “visible”.

When you attempt to access an object in any file system, OS/400 enforces all of the authority values for the object, whether or not those authority values are “visible” through the interface that you are using. For example, when you use the create() API, you can set the public authority for the new object to include *R, *W, and *X. The system automatically sets *OBJOPR because you will need that authority later when you try to use (open) the object.

To see the integrated file system view of your authority to an object, you can use the Display Authority (DSPAUT) command. You can also use the DSPOBJAUT command to see the OS/400 view of your authority to an object.

Run batch jobs

When you run a batch job on the system, you can run it using your own profile or another user profile. To run a job using another user profile, you must have *USE authority to that profile.

When your user profile is created, no one else is allowed to use it to run jobs. The public authority to your profile is set to *EXCLUDE. If you give someone else *USE authority to your user profile, you are giving them the authority to run batch jobs in your name. This is the same as giving someone else your password.

Print information

When you print something on the system, your report is usually stored on disk before it is printed. This process is called **print spooling**. Print spooling helps us to manage printing on the system and to share printers.

The copy of your report that is stored on the system is called a **spooled file**. It is stored in an **output queue**, which is a list of spooled files waiting to print. The system has different output queues with different security characteristics. When you print confidential information, make sure you send it to a secure output queue.

When you make a printing request, you are the owner of the spooled file that is created. You are responsible for the security of that spooled file, just as you are responsible for any other data you own. You can find out what spooled files you own by using the Work with Spooled Files (WRKSPLF) command.

Create new objects

All objects on the system reside in libraries or directories. A library is like a directory used by the system to locate objects. When you create a new object such as a query program, personal file or directory-based stream file, it is put in a library or directory. Usually, library-based objects you create go into your current library, which is specified in your user profile. Usually, directory-based objects go into your home directory.

When you create a new object, it is owned either by you or by your group. Your user profile determines whether you or your group owns new objects. The owner of an object has *ALL authority to the object. The owner can give authority to use the object to other system users.

When you create an object, the initial public authority is determined by the library's CRTAUT (create authority) value or by its directory information. The CRTAUT value can also assign new objects in the library to an authorization list. An **authorization list** is used to group objects that have similar authority requirements.

Your user profile may specify that your group is automatically given authority to any new objects you create. If your profile is set up this way, make sure you do not create any information that other members of your group should not see.

Protect objects that you own

If you own objects on the system, you are responsible for determining who should have access to those objects and for granting the proper authority. You can find out what objects you own using the Work with Objects by Owner (WRKOBJOWN) command. Type: `WRKOBJOWN` *`your-profile-name`*. You can use options from this display to transfer ownership to someone else or to edit authority. The Edit Object Authority display allows you to specify who can use an object and how they can use it. On a system that is configured to meet Common Criteria security requirements, it is recommended that any objects that you create should by default have its public authority set to *EXCLUDE.

During the Common Criteria configuration, the public authorities of all directories had the *W data authority and any object authorities removed. This means that a typical user cannot create objects in directories, including ″root.″ If users are going to create directory based objects, it will be necessary to setup a home directory for the user. The name of the users home directory is stored in the user profile.

The default value is /home/profile-name. Home directories are not automatically created by the system. An administrator will have to create the home directory and grant the target user authority to it.

When you create objects in this directory, you will be able to access them but other users will not (because the default is to inherit authority for new objects from the authority set up for your directory). If necessary, you can use the following commands to give other users authority to your objects and to change the object's security characteristics:

- Change Auditing (CHGAUD)
- Change Authority (CHGAUT)
- Change Owner (CHGOWN)
- Change Primary Group (CHGPGP)
- Display Authority (DSPAUT)
- Work with Authority (WRKAUT)

Appendix E. Commands set to Public Authority *Exclude

The following table identifies which commands have restricted authorization (public authority is *EXCLUDE) when your system is shipped. It shows what IBM-supplied user profiles are authorized to use these restricted commands. For more information about IBM-supplied user profiles, see "Protect IBM-supplied user profiles" on page 51.

In this table, commands that are restricted to the security officer, and any user profile with *ALLOBJ authority, have an **R** in the QSECOFR profile. Commands that are specifically authorized to one or more IBM-supplied user profiles, in addition to the security officer, have an **S** under the profile names for which they are authorized).

Any commands not listed here are public, which means they can be used by all users. However, some commands require special authority, such as *SERVICE or *JOBCTL. See Appendix F, "Authority required for objects used by commands," on page 155 for the special authorities that are required for a specific command.

If you choose to grant other users or the public *USE authority to these commands, update this table to indicate that commands are no longer restricted on your system. Using some commands may require the authority to certain objects on the system as well as to the commands themselves. See Appendix F, "Authority required for objects used by commands," on page 155 for the object authorities required for commands.

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDACC	R				
ADDCMDCRQA		S	S	S	S
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	R				
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOMSMTA		S	S	S	S
ADDOMSRTE		S	S	S	S
ADDOSI*xxx* (1)		S	S	S	S
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ANSQST	R				
ANZDFTPWD	R				
ANZPRB		S	S	S	S
ANZPRFACT	R				
ANZS34OCL	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ANZS36OCL	R				
APYJRNCHG		S		S	
APYPTF				S	
APYRMTPTF		S	S	S	S
CFGDSTSRV		S	S		
CFGRPDS		S	S		
CFGSYSSEC	R				
CHGACTSCDE	R				
CHGCMDCRQA		S	S	S	S
CHGDSTPWD (2)	R				
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	R				
CHGJRN		S	S	S	
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGNETA	R				
CHGNETJOBE	R				
CHGOBJCRQA		S	S	S	S
CHGOMSMTA		S	S	S	S
CHGOMSRTE		S	S	S	S
CHGOSI*xxx* (1)		S	S	S	S
CHGPRB		S	S	S	S
CHGPRDCRQA		S	S	S	S
CHGPTFCRQA		S	S	S	S
CHGPTR				S	
CHGQSTDB	R				
CHGRCYAP		S	S		
CHGRPYLE		S			
CHGRSCCRQA		S	S	S	S
CHGSYSLIBL	R				
CHGSYSVAL		S	S	S	
CHGS34LIBM	R				
CHGS36SRCA	R				
CHKCMNTRC				S	
CHKPRDOPT		S	S	S	S
CPYPTF		S	S	S	S
CRTAUTHLR	R				
CRTCLS	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CRTJOBD	R				
CRTLASREP		S			
CRTQSTDB	R				
CRTQSTLOD	R				
CRTSBSD		S	S		
CVTBASSTR	R				
CVTBASUNF	R				
CVTBGUDTA	R				
CVTS36CFG	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS36QRY	R				
CVTS38JOB	R				
CVTTCPCL		S	S	S	S
DLTAPARDTA		S	S	S	S
DLTCMNTRC				S	
DLTLICPGM	R				
DLTPRB		S	S	S	S
DLTPTF		S	S	S	S
DLTQST	R				
DLTQSTDB	R				
DLTRMTPTF		S	S	S	S
DLTSMGOBJ		S	S	S	S
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S
DMPJOBINT		S	S	S	S
DMPOBJ		S	S	S	S
DMPSYSOBJ		S	S	S	S
DSPDSTLOG	R				
DSPMGDSYSA		S	S	S	S
DSPOSISAP				S	S
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENDCMNTRC				S	
ENDDBGSVR		S	S	S	S
ENDIDXMON	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDOMS		S		S	S
ENDOSI	R				
ENDOSIASN			S		
ENDOSINL			S		
ENDSRVJOB		S	S	S	S
ENDSYSMGR		S	S	S	S
ENDTCP		S	S	S	S
ENDTCPCNN		S	S	S	S
ENDTCPIFC		S	S	S	S
ENDTCPSVR		S	S	S	S
GENS36RPT	R				
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF (4)				S	
INSRMTPRD		S	S	S	S
INZDSTQ		S	S		
INZSYS	R				
LODPTF				S	
LODQSTDB	R				
MGRS36	R				
MGRS36APF	R				
MGRS36CBL	R				
MGRS36DFU	R				
MGRS36DSPF	R				
MGRS36ITM	R				
MGRS36LIB	R				
MGRS36MNU	R				
MGRS36MSGF	R				
MGRS36QRY	R				
MGRS36RPG	R				
MGRS36SEC	R				
MGRS38OBJ	R				
MIGRATE	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
PKGPRDDST		S	S	S	S
PRTCMNTRC				S	
PRTDSKINF	R				
PRTERRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PWRDWNSYS	R				
QMUS36		S	S	S	S
RCLSPLSTG	R				
RCLSTG		S	S	S	S
RCLTMPSTG		S	S	S	S
RESMGRNAM	R	S	S	S	S
RLSCMNDEV		S	S	S	S
RLSDSTQ		S	S		
RLSRMTPHS		S	S		
RMVACC	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVEXITPGM	R				
RMVJRNCHG		S		S	
RMVLANADP	R				
RMVNETJOBE	R				
RMVOMSCTE		S	S	S	S
RMVOMSMTA		S	S	S	S
RMVOMSRTE		S	S	S	S
RMVOSIABSN		S	S	S	S
RMVOSIADJN		S	S	S	S
RMVOSIAGT			S	S	S
RMVOSIAGTR		S	S	S	S
RMVOSIAPPE		S	S	S	S
RMVOSIAPPM		S	S	S	S
RMVOSIAPPX		S	S	S	S
RMVOSIAUNN		S	S	S	S
RMVOSICLPS		S	S	S	S
RMVOSICMPS		S	S	S	S
RMVOSIDUAR		S	S	S	S
RMVOSILINE		S	S	S	S
RMVOSILINS		S	S	S	S
RMVOSIMGR			S	S	S
RMVOSIMGRR		S	S	S	S

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVOSINSAP		S	S	S	S
RMVOSIOX25		S	S	S	S
RMVOSIQOSM		S	S	S	S
RMVOSIRTE		S	S	S	S
RMVOSISSEL		S	S	S	S
RMVOSISUBN		S	S	S	S
RMVOSITPTM		S	S	S	S
RMVPTF				S	
RMVRMTPTF		S	S	S	S
RMVRPYLE		S			
RSTAUT	R				
RST	R				
RSTCFG	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ	R				
RSTS38AUT	R				
RSTUSRPRF	R				
RTVDSKINF	R				
RTVPRD		S	S	S	S
RTVPTF		S	S	S	S
RTVSMGOBJ		S	S	S	S
RUNLPDA		S	S	S	S
RUNSMGCMD		S	S	S	S
RUNSMGOBJ		S	S	S	S
RVKPUBAUT	R				
SAVAPARDTA		S	S	S	S
SAVLICPGM	R				
SBMFNCJOB	R				
SETOSIATR			S	S	S
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
STRCMNTRC				S	
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRIDXMON	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
STRIPSIFC		S	S	S	S
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF(3)			S	S	S
STROMS		S	S	S	S
STROSINL			S		
STRRGZIDX	R				
STRSAM		S		S	S
STRSRVJOB		S	S	S	S
STRSST				S	
STRSYSMGR		S	S	S	S
STRS36MGR	R				
STRS38MGR	R				
STRTCP		S	S	S	S
STRTCPIFC		S	S	S	S
STRTCPSVR		S	S	S	S
STRUPDIDX	R				
TRCCPIC	R				
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCOSIASN				S	S
TRCOSIPCL				S	S
VFYCMN		S	S	S	S
VFYLNKLPDA		S	S	S	S
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKCNTINF				S	S
WRKDEVTBL	R				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFSTAF	R				
WRKFSTPCT	R				
WRKJRN		S	S	S	
WRKLICINF	R				
WRKOMSMTA		S	S	S	S
WRKOMSMTAQ		S	S	S	S
WRKOMSRTE		S	S	S	S
WRKORDINF			S	S	
WRKPGMTBL	R				

Table 18. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
WRKPRB		S	S	S	S
WRKSRVPVD				S	S
WRKTXTIDX	R				
WRKUSRTBL	R				

[1] The same IBM-supplied user profiles are authorized to all ADDOSI and CHGOSI commands.

[2] The CHGDSTPWD command is shipped with public authority *USE, but you must be signed on as QSECOFR to use this command. You cannot authorize other users to the command.

[3] The QMSF user profile is also authorized to this command.

[4] QSRV can only run this command if an IPL is not being done.

Appendix F. Authority required for objects used by commands

The tables in this appendix show what authority is needed for objects referenced by commands. For example, in the entry for the Change User Profile (CHGUSRPRF) command the table lists all the objects you need authority to, such as the user's message queue, job description, and initial program.

The tables are organized in alphabetical order according to object type. In addition, tables are included for items that are not OS/400 objects (jobs, spooled files, network attributes, and system values) and for some functions (device emulation and finance). Additional considerations (if any) for the commands are included as footnotes to the table.

Following are descriptions of the columns in the tables:

Referenced object

The objects listed in the *Referenced Object* column are objects to which the user needs authority when using the command. See "Command usage assumptions" on page 157 for information about objects which are not listed for each command.

Authority required for object

The authorities specified in the tables show the object authorities and the data authorities required for the object when using the command. The following table describes the authorities that are specified in the *Authority Needed* column. The description includes examples of how the authority is used. In most cases, accessing an object requires a combination of object and data authorities.

Authority required for library

This column shows what authority is needed for the library containing the object. For most operations, *EXECUTE authority is needed to locate the object in the library. Adding an object to a library usually requires *READ and *ADD authority. This table describes the authorities that are specified in the *Authority Needed* column.

Table 19. Description of Authority Types

Authority	Name	Functions Allowed
Object Authorities:		
*OBJOPR	Object Operational	Look at the description of an object. Use the object as determined by the user's data authorities.
*OBJMGT	Object Management	Specify the security for the object. Move or rename the object. All functions defined for *OBJALTER and *OBJREF.
*OBJEXIST	Object Existence	Delete the object. Free storage of the object. Perform save and restore operations for the object [1]. Transfer ownership of the object.
*OBJALTER	Object Alter	Add, clear, initialize and reorganize members of the database files. Alter and add attributes of database files: add and remove triggers. Change the attributes of SQL packages. Move a library or folder to a different ASP.

Table 19. Description of Authority Types (continued)

Authority	Name	Functions Allowed
*OBJREF	Object Reference	Specify a database file as the parent in a referential constraint. For example, you want to define a rule that a customer record must exist in the CUSMAS file before an order for the customer can be added to the CUSORD file. You need *OBJREF authority to the CUSMAS file to define this rule.
*AUTLMGT	Authorization List Management	Add and remove users and their authorities from the authorization list [2].
Data Authorities:		
*READ	Read	Display the contents of the object, such as viewing records in a file.
*ADD	Add	Add entries to an object, such as adding messages to a message queue or adding records to a file.
*UPD	Update	Change the entries in an object, such as changing records in a file.
*DLT	Delete	Remove entries from an object, such as removing messages from a message queue or deleting records from a file.
*EXECUTE	Execute	Run a program, service program, or SQL package. Locate an object in a library or a directory.

[1] If a user has save system (*SAVSYS) special authority, object existence authority is not required to perform save and restore operations on the object.

[2] Refer to the *iSeries Security Reference* for more information.

In addition to these values, the *Authority Needed* columns of the table may show system-defined subsets of these authorities. The following table shows the subsets of object authorities and data authorities.

Table 20. System-Defined Authority

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

The following table shows additional authority subsets that are supported by the CHGAUT and WRKAUT commands.

Table 21. System-Defined Authority

Authority	*RWX	*RW	*RX	*R	*WX	*W	*X
Object Authorities							
*OBJOPR	X	X	X	X	X	X	X

Table 21. System-Defined Authority (continued)

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

Refer to the *iSeries Security Reference* for more information on these authorities and their descriptions.

Command usage assumptions

1. To use any command, *USE authority is required to the command. This authority is not specifically listed in the tables.
2. To enter any display command, you need operational authority to the IBM-supplied display file, printer output file, or panel group used by the command. These files and panel groups are shipped with public authority *USE.

General rules for object authorities on commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
Change (CHG) with F4 (Prompt)[7]	Current values	The current values are displayed if the user has authority to those values.	*EXECUTE
Command accessing object in directory	Directories in path prefix for QLANSrv file system	*R	
	Directories in path prefix for all other file systems	*X	
	Directory when pattern is specified (* or ?) for QLANSrv file system	None	
	Directory when pattern is specified (* or ?) for all other file system	*R	
Creating object in directory	Directories in path prefix	*X	
	Directory to contain new object	*WX	

Command	Referenced Object	Authority Needed	
		For Object	For Library
Copy (CPY) where to-file is a database file	Object to be copied	*OBJOPR, *READ	*EXECUTE
	CRTPF command, if CRTFILE (*YES) is specified	*OBJOPR	*EXECUTE
	To-file, if CRTFILE (*YES) is specified[1]		*ADD, *EXECUTE
	To-file, if it exists and new member is added	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	To-file, if file and member exist and *ADD option is specified	*OBJOPR, *ADD	*EXECUTE
	To-file, if file and member exist and *REPLACE option is specified	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	To-file, if it exists, a new member is added, and *UPDADD option is specified.[8]	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
	To-file, if file and member exist and *UPDADD option is specified.[8]	*OBJOPR, *ADD, *UPD	*EXECUTE
Create (CRT)	Object to be created[2]		*READ, *ADD
	User profile that will own created object (either the user profile running the job or the user's group profile)	*ADD	
Create (CRT) if REPLACE(*YES) is specified [6, 9]	Object to be created (and replaced)[2]	*OBJMGT, *OBJEXIST, *READ[5]	*READ, *ADD
	User profile that will own created object (either the user profile running the job or the user's group profile)	*ADD	
Display (DSP) or other operation using output file (OUTPUT(*OUTFILE))	Output file, if file does not exist[3]		*ADD, *EXECUTE
	Output file, if file exists and new member is added and *REPLACE option specified and member did not previously exist	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Output file, if file exists and new member is added and *ADD option specified and member did not previously exist.	OBJOPR, *OBJMGT or *OBJALTER, *ADD	*ADD, *EXECUTE
	Output file, if file and member exist and *ADD option is specified	*OBJOPR, *ADD	*EXECUTE
	Output file, if file and member exist and *REPLACE option is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*EXECUTE
	Format file (QAxxxxx), if output file does not exist	*OBJOPR	
Display (DSP) using *PRINT or Work (WRK) using *PRINT	Object to be displayed	*USE	*EXECUTE
	Output queue[4]	*READ	*EXECUTE
	Printer file (QPxxxxx in QSYS)	*USE	*EXECUTE
Save (SAV) or other operation using device description	Device description	*USE	*EXECUTE
	Device file associated with device description, such as QSYSTAP for the TAP01 device description	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] The user profile running the copy command becomes the owner of the to-file, unless the user is a member of a group profile and has OWNER(*GRPPRF). If the user's profile specifies OWNER(*GRPPRF), the group profile becomes the owner of the to-file. In that case, the user running the command must have *ADD authority to the group profile and the authority to add a member and write data to the new file. The to-file is given the same public authority, primary group authority, private authorities, and authorization list as the from-file.			
[2] The user profile running the create command becomes the owner of the newly created object, unless the user is a member of a group profile and has OWNER(*GRPPRF). If the user's profile specifies OWNER(*GRPPRF), the group profile becomes the owner of the newly created object. Public authority to the object is controlled by the AUT parameter.			
[3] The user profile running the display command becomes the owner of the newly created output file, unless the user is a member of a group profile and has OWNER(*GRPPRF). If the user's profile specifies OWNER(*GRPPRF), the group profile becomes the owner of the output file. Public authority to the output file is controlled by the CRTAUT parameter of the output file library.			
[4] If the output queue is defined as OPRCTL (*YES), a user with *JOBCTL special authority does not need any authority to the output queue. A user with *SPLCTL special authority does not need any authority to the output queue.			
[5] For device files, *OBJOPR authority is also required.			
[6] The REPLACE parameter is not available in the S/38 environment. REPLACE(*YES) is equivalent to using a function key from the programmer menu to delete the current object.			
[7] Authority to the corresponding (DSP) command is also required.			
[8] The *UPDADD option in only available on the MBROPT parameter of the CPYF command.			
[9] This does not apply to the REPLACE parameter on the CRTJVAPGM command.			

Common commands for all objects

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Table 22. Common commands for all objects

Command	Referenced Object	Authority Needed	
		For Object	For Library
ALCOBJ [1,2,11]	Object	*OBJOPR	*EXECUTE
ANZUSROBJ [20]			
CHGOBJAUD [18]	ASP Device (if specified)	*USE	
CHGOBJD [3]	Object, if it is a file	*OBJOPR, *OBJMGT	*EXECUTE
	Object, if it is not a file	*OBJMGT	*EXECUTE
CHGOBJOWN [3,4]	Object	*OBJEXIST	*EXECUTE
	Object (if file, library, subsystem description)	*OBJOPR, *OBJEXIST	*EXECUTE
	Object (if *AUTL)	Ownership or *ALLOBJ	*EXECUTE
	Old user profile	*DLT	*EXECUTE
	New user profile	*ADD	*EXECUTE
	ASP Device (if specified)	*USE	

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	**For Library**
CHGOBJPGP [3]	Object	*OBJEXIST	*EXECUTE
	Object (if file, library, subsystem description)	*OBJOPR, *OBJEXIST	*EXECUTE
	Object (if *AUTL)	Ownership and *OBJEXIST, or *ALLOBJ	*EXECUTE
	Old user profile	*DLT	
	New user profile	*ADD	
	ASP Device (if specified)	*USE	
CHKOBJ [3]	Object	Authority specified by AUT parameter [14]	*EXECUTE
CPROBJ	Object	*OBJMGT	*EXECUTE
CHKOBJITG [11](Q)			
CRTDUPOBJ [3,9,11,21]	New object		*USE, *ADD
	Object being copied, if it is an *AUTL	*AUTLMGT	*USE, *ADD
	Object being copied, all other types	*OBJMGT, *USE	*USE
	CRTSAVF command (if the object is a save file)	*OBJOPR	
	ASP Device (if specified)	*USE	
DCPOBJ	Object	*USE	*EXECUTE
DLCOBJ [1,11]	Object	*OBJOPR	*EXECUTE
DMPOBJ (Q) [3]	Object	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Object	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT [3]	Object (to see all authority information)	*OBJMGT or *ALLOBJ special authority or ownership	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
	ASP Device (if specified)	*USE	
DSPOBJD [2, 28]	Output file	Refer to "General rules for object authorities on commands" on page 157.	
	Object	Some authority other than *EXCLUDE	*EXECUTE
	ASP Device (if specified)	*EXECUTE	
EDTOBJAUT [3,5,6,15]	Object	*OBJMGT	*EXECUTE
	Object (if file)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, if used to secure object	Not *EXCLUDE	
	ASP Device (if specified)	*USE	

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	**For Library**
GRTOBJAUT [3,5,6,15]	Object	*OBJMGT	*EXECUTE
	Object (if file)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, if used to secure object	Not *EXCLUDE	
	ASP Device (if specified)	*USE	
	Reference ASP Device (if specified)	*EXECUTE	
	Reference object	*OBJMGT or Ownership	*EXECUTE
MOVOBJ [3,7,12]	Object	*OBJMGT	
	Object (if *FILE)	*ADD, *DLT, *EXECUTE	
	Object (not *FILE),	*DLT, *EXECUTE	
	From-library		*CHANGE
	To-library		*READ, *ADD
	ASP Device (if specified)	*USE	
PRTADPOBJ [26](Q)			
PRTPUBAUT [26]			
PRTUSROBJ [26]			
PRTPVTAUT [26]			
RCLSTG (Q)			
RCLTMPSTG (Q)	Object	*OBJMGT	*EXECUTE
RNMOBJ [3,11]	Object	*OBJMGT	*UPD, *EXECUTE
	Object, if *AUTL	*AUTLMGT	*EXECUTE
	Object (if *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	ASP Device (if specified)	*USE	

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	**For Library**
RSTOBJ [3,13] (Q)	Object, if it already exists in the library	*OBJEXIST [8]	*EXECUTE, *ADD
	Object, if it is *CFGL, *CNNL, *CTLD, *DEVD, *LIND, or *NWID	*CHANGE and *OBJMGT	*EXECUTE
	Media definition	*USE	*EXECUTE
	Message queues being restored to library where they already exist	*OBJOPR, *OBJEXIST [8]	*EXECUTE, *ADD
	User profile owning objects being created	*ADD [8]	
	Program that adopts authority	Owner or *SECADM and *ALLOBJ special authority	*EXECUTE
	To-library	*EXECUTE, *ADD [8]	
	Library for saved object if VOL(*SAVVOL) is specified	*USE [8]	
	Save file	*USE	*EXECUTE
	Tape unit, diskette unit or optical unit	*USE	*EXECUTE
	Tape (QSYSTAP) file or diskette (QSYSDKT) file	*USE [8]	*EXECUTE
	Optical File (OPTFILE)[22]	*R	N/A
	Parent Directory of optical file (OPTFILE)[22]	*X	N/A
	Path prefix of OPTFILE[22]	*X	N/A
	Optical volume[24]	*USE	N/A
	QSYS/QPSRLDSP print file, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASRRSTO field reference file for output file, if an output file is specified and does not exist	*USE	*EXECUTE
	ASP device description[25]	*USE	
RVKPUBAUT [20]	Tape (QSYSTAP) file or diskette (QSYSDKT) file	*USE [8]	*EXECUTE
RTVOBJD [2, 29]	Object	Some authority other than *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Path prefix of OPTFILE[22]	*X	N/A
	Optical volume[24]	*USE	N/A
	QSYS/QPSRLDSP print file, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	ASP Device (if specified)	*USE	

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	**For Library**
SAVCHGOBJ [3]	Object (8)	*OBJEXIST	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Save active message queue	*OBJOPR, *ADD	*EXECUTE
	Optical File (OPTFILE)[22]	*RW	N/A
	Parent Directory of optical file (OPTFILE)[22]	*WX	N/A
	Path prefix of optical file (OPTFILE)[22]	*X	N/A
	Root Directory (/) of optical volume[22, 23]	*RWX	N/A
	Optical volume[24]	*CHANGE	
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE [8]	*EXECUTE
	QSYS/QPSAVOBJ print file	*USE [8]	*EXECUTE
	ASP device description[25]	*USE	
SAVOBJ [3]	Object	*OBJEXIST [8]	*EXECUTE
	Media definition	*USE	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Save active message queue	*OBJOPR, *ADD	*EXECUTE
	Optical File (OPTFILE) [22]	*RW	N/A
	Parent Directory of optical file (OPTFILE)[22]	*WX	N/A
	Path prefix of OPTFILE[22]	*X	N/A
	Root directory (/) of optical volume [22, 23]	*RWX	N/A
	Optical volume[24]	*CHANGE	
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE [8]	*EXECUTE
	QSYS/QPSAVOBJ print file	*USE [8]	*EXECUTE
	ASP device description[25]	*USE	
SAVSTG [10]			
SAVSYS [10]	Tape unit, optical unit	*USE	*EXECUTE
	Root directory (/) of optical volume[22]	*RWX	N/A
	Optical volume[24]	*CHANGE	N/A

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	For Library
SAVRSTCHG	On the source system, same authority as required by SAVCHGOBJ command.		
	On the target system, same authority as required by RSTOBJ command.		
	ASP device description[25]	*USE	
SAVRSTLIB	On the source system, same authority as required by SAVLIB command.		
	On the target system, same authority as required by RSTLIB command.		
SAVRSTOBJ	On the source system, same authority as required by SAVOBJ command.		
	On the target system, same authority as required by RSTOBJ command.		
	ASP device description[25]	*USE	
SETOBJACC	Object	*OBJOPR	*EXECUTE
WRKOBJ [19]	Object	Any authority	*USE
WRKOBJLCK	Object		*EXECUTE
	ASP Device	*EXECUTE	
WRKOBJOWN [17]	User profile	*READ	*EXECUTE
WRKOBJPGP [17]	User profile	*READ	*EXECUTE
WRKOBJPVT[17]	User profile	*READ	*EXECUTE

1 See the OBJTYPE keyword of the ALCOBJ command for the list of object types that can be allocated and deallocated.

2 Some authority to the object (other than *EXCLUDE) is required.

3 This command cannot be used for documents or folders. Use the equivalent Document Library Object (DLO) command.

4 You must have *ALLOBJ and *SECADM special authority to change the object owner of a program, service program, or SQL package that adopts authority.

5 You must be the owner or have *OBJMGT authority and the authorities being granted or revoked.

6 You must be the owner or have *ALLOBJ special authority to grant *OBJMGT or *AUTLMGT authority.

7 This command cannot be used for user profiles, controller descriptions, device descriptions, line descriptions, documents, document libraries, and folders.

8 If you have *SAVSYS special authority, you do not need the authority specified.

9 If the user running the CRTDUPOBJ command has OWNER(*GRPPRF) in his user profile, the owner of the new object is the group profile. To successfully copy authorities to a new object owned by the group profile, the following applies:

- The user running the command must have authority to the from-object. Authorities can be obtained from adopted authority or through the group profile.
- If an error occurs while copying authorities to the new object, the newly created object is deleted.

10 You must have *SAVSYS special authority.

Table 22. Common commands for all objects (continued)

Command	Referenced Object	Authority Needed	
		For Object	For Library
[11] This command cannot be used for journals and journal receivers. [12] This command cannot be used for journals and journal receivers, unless the from-library is QRCL and the to-library is the original library for the journal or journal receiver. [13] You must have *ALLOBJ special authority to specify ALWOBJDIF(*ALL). [14] To check a user's authority to an object, you must have the authority you are checking. For example, to check whether a user has *OBJEXIST authority for FILEB, you must have *OBJEXIST authority to FILEB. [15] To secure an object with an authorization list or remove the authorization list from the object, you must (one of the following): • Own the object. • Have *ALL authority to the object. • Have *ALLOBJ special authority.			
[16] If either the original file or the renamed file has an associated authority holder, *ALL authority to the authority holder is required. [17] This command does not support the QOPT file system. [18] You must have *AUDIT special authority. [19] To use an individual operation, you must have the authority required by the individual operation. [20] You must have *ALLOBJ special authority.			
[21] All authorities on the from-object are duplicated to the new object. The primary group of the new object is determined by the group authority type (GRPAUTTYP) field in the user profile that is running the command. If the from-object has a primary group, the new object may not have the same primary group, but the authority that the primary group has on the from-object will be duplicated to the new object. [22] This authority check is only made when the Optical media format is Universal Disk Format. [23] This authority check is only made if you are clearing the optical volume [24] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function. [25] Authority required only if save or restore operation requires a library name space switch. [26] You must have *ALLOBJ or *AUDIT special authority to use this command. [27] *** **Security Risk** *** Revoking all authorities specifically given to a user for an object can result in the user having more authority than before the revoke operation. If a user has *USE authority for and object and *CHANGE authority on the authorization list that secures the object, revoking *USE authority results in the user having *CHANGE authority to the object. [28] You must have either *ALLOBJ or *AUDIT special authority to have the current object auditing value displayed. Otherwise, the value *NOTAVL will be displayed to indicate that the value is not available for display. [29] You must have either *ALLOBJ or *AUDIT special authority to retrieve the current object auditing value. Otherwise, the value *NOTAVL will be returned to indicate that the values are not available for retrieval.			

Access path recovery commands: authorities required

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix E, "Commands set to Public Authority *Exclude," on page 147 shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require object authorities.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGRCYAP [1] (Q)	ASP Device (if specified)	*USE	
DSPRCYAP [1]	ASP Device (if specified)	*USE	
EDTRBDAP [2] (Q)			
EDTRCYAP [1] (Q)	ASP Device (if specified)	*USE	

[1] You must have *JOBCTL special authority to use this command.

[2] You must have *ALLOBJ special authority to use this command.

Advanced function printing* commands: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDFNTTBLE	Font table	*CHANGE	*EXECUTE
CHGCDEFNT	Font resource	*CHANGE	*EXECUTE
CHGFNTTBLE	Font table	*CHANGE	*EXECUTE
CRTFNTRSC	Source file	*USE	*EXECUTE
	Font resource: REPLACE(*NO)		*READ, *ADD
	Font resource: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTFNTTBL	Font table		*READ, *ADD
CRTFORMDF	Source file	*USE	*EXECUTE
	Form definition: REPLACE(*NO)		*READ, *ADD
	Form definition: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTOVL	Source file	*USE	*EXECUTE
	Overlay: REPLACE(*NO)		*READ, *ADD
	Overlay: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTPAGDFN	Source file	*USE	*EXECUTE
	Page definition: REPLACE(*NO)		*READ, *ADD
	Page definition: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTPAGSEG	Source file	*USE	*EXECUTE
	Page segment: REPLACE(*NO)		*READ, *ADD
	Page segment: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
DLTFNTRSC	Font resource	*OBJEXIST	*EXECUTE
DLTFNTTBL	Font table	*CHANGE	*EXECUTE
DLTFORMDF	Form definition	*OBJEXIST	*EXECUTE
DLTOVL	Overlay	*OBJEXIST	*EXECUTE
DLTPAGDFN	Page definition	*OBJEXIST	*EXECUTE
DLTPAGSEG	Page segment	*OBJEXIST	*EXECUTE
DSPCDEFNT	Font resource	*USE	*EXECUTE
DSPFNTRSCA	Font resource	*USE	*EXECUTE
DSPFNTTBL	Font table	*USE	*EXECUTE
RMVFNTTBLE	Font table	*CHANGE	*EXECUTE
WRKFNTRSC [1]	Font resource	*USE	*USE
WRKFORMDF [1]	Form definition	*USE	*USE
WRKOVL [1]	Overlay	*USE	*USE
WRKPAGDFN [1]	Page definition	Any authority	*USE
WRKPAGSEG [1]	Page segment	*USE	Any authority
[1] To use individual operations, you must have the authority required by the individual operation.			

AF_INET sockets over SNA Commands: authorities required

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix E, "Commands set to Public Authority *Exclude," on page 147 shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others. These commands do not require any authority to objects:

These commands do not require any authority to objects:			
ADDIPSIFC[1]	CHGIPSIFC[1]	CVTIPSLOC	RMVIPSLOC[1]
ADDIPSRTE[1]	CHGIPSLOC[1]	ENDIPSIFC (Q)	RMVIPSRTE[1]
ADDIPSLOC[1]	CHGIPSTOS[1]	PRTIPSCFG	STRIPSIFC (Q)
CFGIPS	CVTIPSIFC	RMVIPSIFC[1]	

[1]	You must have *IOSYSCFG special authority to use this command.

Alerts: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDALRD	Alert table	*USE, *ADD	*EXECUTE
CHGALRD	Alert table	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Alert table	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Alert table		*READ, *ADD
DLTALR	Physical file QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Alert table	*OBJEXIST	*EXECUTE
RMVALRD	Alert table	*USE, *DLT	*EXECUTE
WRKALR [1]	Physical file QAALERT	*USE	*EXECUTE
WRKALRD [1]	Alert table	*USE	*EXECUTE
WRKALRTBL [1]	Alert table	*READ	*USE
[1] To use individual operations, you must have the authority required by the individual operation.			

Application development commands: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For Library
FNDSTRPDM	Source part	*READ	*EXECUTE
MRGFORMD	Form description	*READ	*EXECUTE
STRAPF [1]	Source file	*OBJMGT, *CHANGE	*READ, *ADD
	Commands CRTPF, CRTLF, ADDPFM, ADDLFM, and RMVM	*USE	*EXECUTE
STRBGU [1]	Chart	*OBJMGT, *CHANGE	*EXECUTE
STRDFU [1]	Program (if create program option)		*READ, *ADD
	Program (if change or delete program option)	*OBJEXIST	*EXECUTE
	Program (if change or display data option)	*USE	*EXECUTE
	Database file (if change data option)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Database file (if display data option)	*USE	*EXECUTE
	Display file (if display or change data option)	*USE	*EXECUTE
	Display file (if change program option)	*USE	*EXECUTE
	Display file (if delete program option)	*OBJEXIST	*EXECUTE
STRPDM [1]			

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRRLU	Source file	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Edit, add, or change a member	*OBJOPR, *OBJMGT	*READ, *ADD
	Browse a member	*OBJOPR	*EXECUTE
	Print a prototype report	*OBJOPR	*EXECUTE
	Remove a member	*OBJOPR, *OBJEXIST	*EXECUTE
	Change type or text of member	*OBJOPR	*EXECUTE
STRSDA	Source file	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Update and add new member	*CHANGE, *OBJMGT	*READ, *ADD
	Delete member	*ALL	*EXECUTE
STRSEU [1]	Source file	*USE	*EXECUTE
	Edit or change a member	*CHANGE, *OBJMGT	*EXECUTE
	Add a member	*USE, *OBJMGT	*READ, *ADD
	Browse a member	*USE	*EXECUTE
	Print a member	*USE	*EXECUTE
	Remove a member	*USE, *OBJEXIST	*EXECUTE
	Change type or text of a member	*USE, *OBJMGT	*EXECUTE
WRKLIBPDM [1]			
WRKMBRPDM [1]	Source file	*USE	*EXECUTE
WRKOBJPDM [1]	File	*READ or Ownership	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

[2] A group corresponds to a library.

[3] A project consists of one or more groups (libraries).

Authority holder commands: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTAUTHLR (Q)	Associated object if it exists	*ALL	*EXECUTE
DLTAUTHLR	Authority holder	*ALL	*EXECUTE
DSPAUTHLR	Output file	Refer to "General rules for object authorities on commands" on page 157.	

Authorization list commands: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For QSYS Library
ADDAUTLE [1]	*AUTL	*AUTLMGT or ownership	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For QSYS Library
CHGAUTLE [1]	*AUTL	*AUTLMGT or ownership	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Owner or *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
EDTAUTL [1]	*AUTL	*AUTLMGT or ownership	*EXECUTE
RMVAUTLE [1]	*AUTL	*AUTLMGT or ownership	*EXECUTE
RTVAUTLE [2]	*AUTL	*AUTLMGT or ownership	*EXECUTE
WRKAUTL [3,4,5]	*AUTL		

[1] You must be the owner or have authorization list management authority and have the authorities being given or taken away.

[2] If do not have *OBJMGT or *AUTLMGT, you can retrieve *PUBLIC authority and your own authority. You must have *READ authority to your own profile to retrieve your own authority.

[3] To use an individual operation, you must have the authority required by the operation.

[4] You must not be excluded (*EXCLUDE) from the authorization list.

[5] Some authority to the authorization list is required.

Binding directory commands: authorities required

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDBNDDIRE	Binding directory	*OBJOPR, *ADD	*USE
CRTBNDDIR	Binding directory		*READ, *ADD
DLTBNDDIR	Binding directory	*OBJEXIST	*EXECUTE
DSPBNDDIR	Binding directory	*READ, *OBJOPR	*USE
RMVBNDDIRE	Binding directory	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBNDDIR [1]	Binding directory	Any authority	*USE
WRKBNDDIRE [1]	Binding directory	*READ, *OBJOPR	*USE

[1] To use individual operations, you must have the authority required by the operation.

Change Request Description Commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDCMDCRQA (Q)	Change request description	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Change request description	*CHANGE	*EXECUTE
ADDPRDCRQA (Q)	Change request description	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Change request description	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CHGCRQD	Change request description	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CRTCRQD	Change request description		*READ, *ADD
DLTCRQD	Change request description	*OBJEXIST	*EXECUTE
RMVCRQDA	Change request description	*CHANGE	*EXECUTE
WRKCRQD [1]	Change request description		*EXECUTE

[1] To use an individual operation, you must have the authority required by the operation.

Chart commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTCHTFMT	Chart format	*OBJEXIST	*EXECUTE
DSPCHT	Chart format	*USE	*USE
	Database file	*USE	*USE
DSPGDF	Database file	*USE	*USE
STRBGU (Option 3) [2]	Chart format	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT [1]	Chart format	Any authority	*USE

[1] To use an individual operation, you must have the authority required by the operation.

[2] Option 3 on the BGU menu (shown when STRGBU is run) is the Change chart format option.

Class commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCLS	Class	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Class		*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTCLS	Class	*OBJEXIST	*EXECUTE
DSPCLS	Class	*USE	*EXECUTE
WRKCLS [1]	Class	*OBJOPR	*USE

[1] To use an individual operation, you must have the authority required by the operation.

Class-of-Service commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCOSD [3]	Class-of-service description	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD [3]	Class-of-service description		
DLTCOSD	Class-of-service description	*OBJEXIST	*EXECUTE
DSPCOSD	Class-of-service description	*USE	*EXECUTE
WRKCOSD [1,2]	Class-of-service description	*OBJOPR	*EXECUTE

[1] To use individual operations, you must have the authority required by the individual operation.

[2] Some authority to the object is required.

[3] To use this command, you must have *IOSYSCFG special authority.

Cluster commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-Supplied user profiles are authorized to the command. The security officer can grant *USE to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDCLUNODE (Q)[1]	QCSTCTL service program	*USE	
ADDCRGDEVE (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
ADDCRGNODE (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
	Distribute information user queue	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q)[1]	QCSTDD service program	*USE	
CHGCLUCFG (Q)[1]	QCSTCTL2 service program	*USE	

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCLUNODE (Q)[1]	QCSTCTL service program	*USE	
CHGCLURCY (Q)	Cluster resource group	*USE	
		*JOBCTL	
		*SERVICE or Service Trace function	
CHGCLUVER (Q)[1]	QCSTCTL2 service program	*USE	
CHGCRG (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
CHGCRGDEVE (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
CHGCRGPRI (Q)[1]	QCSTCRG2 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Vary configuration VFYCFG) command	*USE	
CRTCLU (Q)[1]	QCSTCTL service program	*USE	
CRTCRG (Q) [1]	QCSTCRG1 service program	*USE	
	Cluster resource group library		*OBJOPR, *ADD, *READ (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Distribute information user queue	*OBJOPR, *ADD	*EXECUTE
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
DLTCLU (Q)[1]	QCSTCTL service program	*USE	
DLTCRG (Q) [1]	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTCRGCLU (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
DMPCLUTRC	Cluster resource group	*USE	
		*SERVICE or Service Trace function	
DSPCLUINF			
DSPCRGINF			
	Cluster resource group	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q)[1]	QCSTCTL service program	*USE	
ENDCHTSVR (Q)	Authorization list	*CHANGE	
ENDCRG (Q)[1]	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
RMVCLUNODE (Q)[1]	QCSTCTL service program	*USE	
RMVCRGDEVE (Q)[1]	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
RMVCRGNODE (Q) [1]	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE, *OBJEXIST	*EXECUTE
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
RMVDEVDMNE (Q)[1]	QCSTDD service program	*USE	
STRCHTSVR	Authorization list	*CHANGE	
STRCLUNOD (Q)[1]	QCSTCTL service program	*USE	
STRCRG (Q)[1]	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE
	Exit program	*EXECUTE[2]	*EXECUTE[2]
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	

[1] You must have *IOSYSCFG special authority to use this command.

[2] Applies to calling user profile and user profile to run exit program.

Command (*CMD) commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCMD	Command	*OBJMGT	*EXECUTE
CHGCMDDFT	Command	*OBJMGT, *USE	*EXECUTE
CRTCMD	Source file	*USE	*EXECUTE
	Command: REPLACE(*NO)		*READ, *ADD
	Command: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	
DLTCMD	Command	*OBJEXIST	*EXECUTE
DSPCMD	Command	*USE	*EXECUTE
GENCMDOC	Command	*USE	*EXECUTE
	Panel group (associated)	*USE	*EXECUTE
	Output file: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Command	*OBJOPR	*EXECUTE
	DDM file	*USE	*EXECUTE
SLTCMD [1]	Command	Any authority	*USE
WRKCMD [2]	Command	Any authority	*USE

[1] Ownership or some authority to the object is required.

[2] To use individual operations, you must have the authority required by the individual operation.

Commitment control commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
COMMIT			
ENDCMTCTL	Message queue, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR, *ADD	*EXECUTE
	Data area, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*CHANGE	*EXECUTE
	File, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Message queue, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR, *ADD	*EXECUTE
	Data area, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*CHANGE	*EXECUTE
	File, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR *ADD	*EXECUTE
WRKCMTDFN [1]			

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] Any user can run this command for commitment definitions that belong to a job that is running under the user profile of the user. A user who has job control (*JOBCTL) special authority can run this command for any commitment definition.			

Communications side information commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCSI	Communications side information object	*USE, *OBJMGT	*EXECUTE
	Device description [1]	*CHANGE	
CRTCSI	Communications side information object		*READ, *ADD
	Device description [1]	*CHANGE	
DLTCSI	Communications side information object	*OBJEXIST	*EXECUTE
DSPCSI	Communications side information object	*READ	*EXECUTE
WRKCSI	Communications side information objects	*USE	*EXECUTE
[1] Authority is verified when the communications side information object is used.			

Configuration commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
PRTDEVADR	Controller description (CTL)	*USE	*EXECUTE
	Device description	*USE	*EXECUTE
RSTCFG (Q) [5]	Every object being restored over by a saved version	*OBJEXIST [1]	*EXECUTE
	To-library		*ADD, *EXECUTE [1]
	User profile owning objects being created	*ADD [1]	
	Tape unit	*USE	*EXECUTE
	Tape file (QSYSTAP)	*USE [1]	*EXECUTE
	Save file, if specified	*USE	*EXECUTE
	Print file (QPSRLDSP), if output(*print) is specified	*USE	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASRRSTO field reference file, if output file is specified and it does not exist	*USE	*EXECUTE
RTVCFGSTS	Object	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
RTVCFGSRC	Object	*USE	*EXECUTE
	Source file	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*EXECUTE, *ADD
SAVCFG [2]	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	On the source system, same authority as required by SAVCFG command.		
	On the target system, same authority as required by RSTCFG command.		
VRYCFG [3,6]	Object	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Object	*OBJOPR	*EXECUTE

[1] If you have *SAVSYS special authority, you do not need the authority specified.

[2] You must have *SAVSYS special authority.

[3] If a user has *JOBCTL special authority, authority to the object is not needed.

[4] To use the individual operations, you must have the authority required by the individual operation.

[5] You must have *ALLOBJ special authority to specify ALWOBJDIF(*ALL).

[6] You must have *IOSYSCFG special authority for media library when status is *ALLOCATE or *DEALLOCATE.

Configuration list commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDCFGLE [2]	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL [2]	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE [2]	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL [2]	Configuration list	*USE, *OBJMGT	*ADD
CRTCFGL [2]	Configuration list		
DLTCFGL	Configuration list	*OBJEXIST	*EXECUTE
DSPCFGL [2]	Configuration list	*USE, *OBJMGT	*EXECUTE
RMVCFGLE [2]	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL [1, 2]	Configuration list	*OBJOPR	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

Connection list commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTCNNL	Connection list	*OBJEXIST	*EXECUTE
DSPCNNL	Connection list	*USE	*EXECUTE
WRKCNNL [1]	Connection list	*OBJOPR	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

Controller description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGCTLAPPC [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CHGCTLNET [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP [2]	Controller description	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS [2]	Controller	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLASC [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTCTLBSC [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLFNC [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLHOST [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLLWS [2]	Device description (DEV)	*USE	*EXECUTE
	Controller description		
	Program (INZPGM)	*USE	*EXECUTE
CRTCTLNET [2]	Line description (LINE)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLRTL [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLRWS [2]	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLTAP [2]	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLVWS [2]	Device description (DEV)	*USE	*EXECUTE
	Controller description		
DLTCTLD	Controller description	*OBJEXIST	*EXECUTE
DSPCTLD	Controller description	*USE	*EXECUTE
ENDCTLRCY	Controller description	*USE	*EXECUTE
PRTCMNSEC [3]			
RSMCTLRCY	Controller description	*USE	*EXECUTE
WRKCTLD [1]	Controller description	*OBJOPR	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

[3] To use this command, you must have *ALLOBJ and *IOSYSCFG, or *AUDIT special authority.

Data area commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGDTAARA [1]	Data area	*CHANGE	*EXECUTE
CRTDTAARA [1]	Data area		*READ, *ADD
	APPC device description[4]	*CHANGE	
DLTDTAARA	Data area	*OBJEXIST	*EXECUTE
DSPDTAARA	Data area	*USE	*EXECUTE
RTVDTAARA [2]	Data area	*USE	*EXECUTE
WRKDTAARA [3]	Data area	Any authority	*USE

[1] If the create and change data area commands are run using high-level language functions, these authorities are still required although authority to the command is not.

[2] Authority is verified at run time, but not at compilation time.

[3] To use an individual operation, you must have the authority required by the operation.

[4] Authority is verified when the data area is used.

Data queue commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTDTAQ	Data queue		*READ, *ADD
	Target data queue for the QSNDDTAQ program	*OBJOPR, *ADD	*EXECUTE
	Source data queue for the QRCVDTAQ program	*OBJOPR, *READ	*EXECUTE
	APPC device description[2]	*CHANGE	
DLTDTAQ	Data queue	*OBJEXIST	*EXECUTE
WRKDTAQ [1]	Data queue	*READ	*USE

[1] To use individual operations, you must have the authority required by the individual operation.

[2] Authority is verified when the data area is used.

Device description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CFGDEVMLB [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVAPPC [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Mode description (MODE)	*USE	*EXECUTE
CHGDEVASC [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP[4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGDEVCRP[4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Printer (PRINTER)	*USE	*EXECUTE
CHGDEVFNC [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPRT [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Validation list (if specified)	*READ	*EXECUTE
CHGDEVRTL [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNUF [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP [4]	Device description	*CHANGE, *OBJMGT	*EXECUTE
CRTDEVAPPC [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
	Mode description (MODE)	*USE	*EXECUTE
CRTDEVASC [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVASP [4]	Device description		*EXECUTE
CRTDEVBSC [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVCRP[4]	Device description		*EXECUTE
CRTDEVDKT [4]	Device description		*EXECUTE
CRTDEVDSP [4]	Printer description (PRINTER)	*USE	*EXECUTE
	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVFNC [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVHOST [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVINTR [4]	Device description		
CRTDEVMLB [4]	Device description		*EXECUTE
CRTDEVNET [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVOPT [4]	Device description		*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTDEVPRT [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
	Validation list (if specified)	*READ	*EXECUTE
CRTDEVRTL [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVSNPT [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVSNUF [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVTAP [4]	Controller description (CTL)	*USE	*EXECUTE
	Device description		
DLTDEVD [1]	Device description	*OBJEXIST	*EXECUTE
DSPCNNSTS	Device description	*OBJOPR	*EXECUTE
DSPDEVD	Device description	*USE	*EXECUTE
ENDDEVRCY	Device description	*USE	*EXECUTE
HLDCMNDEV [2]	Device description	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Device description	*OBJOPR	*EXECUTE
RSMDEVRCY	Device description	*USE	*EXECUTE
WRKDEVD [3]	Device description	*OBJOPR	*EXECUTE

[1] To remove an associated output queue, object existence (*OBJEXIST) authority to the output queue and read authority to the QUSRSYS library are required.

[2] You must have job control (*JOBCTL) special authority and object operational authority to the device description.

[3] To use individual operations, you must have the authority required by the individual operation.

[4] You must have *IOSYSCFG special authority to run this command.

[5] You must have *ALLOBJ special authority to run this command.

Device emulation commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDEMLCFGE	Emulation configuration file	*CHANGE	*EXECUTE
CHGEMLCFGE	Emulation configuration file	*CHANGE	*EXECUTE
EJTEMLOUT	Emulation device description when specified	*OBJOPR	*EXECUTE
	Emulation device description when location specified	*OBJOPR	*EXECUTE
ENDPRTEML	Emulation device description when specified	*OBJOPR	*EXECUTE
	Emulation device description when location specified	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
EMLPRTKEY	Emulation device description when specified	*OBJOPR	*EXECUTE
	Emulation device description when location specified	*OBJOPR	*EXECUTE
EML3270	Emulation device description	*OBJOPR	*EXECUTE
	Emulation controller description	*OBJOPR	*EXECUTE
RMVEMLCFGE	Emulation configuration file	*CHANGE	*EXECUTE
STREML3270	Emulation configuration file	*OBJOPR	*EXECUTE
	Emulation device, emulation controller description, display station device, and display station controller description	*OBJOPR	*EXECUTE
	Printer device description, user exit program, and translation tables when specified	*OBJOPR	*EXECUTE
STRPRTEML	Emulation configuration file	*OBJOPR	*EXECUTE
	Emulation device description and emulation controller description	*OBJOPR	*EXECUTE
	Printer device description, print file, message queue, job description, job queue, and translation tables when specified	*OBJOPR	*EXECUTE
SNDEMLIGC	From-file	*OBJOPR	*EXECUTE
TRMPRTEML	Emulation device description	*OBJOPR	*EXECUTE

Directory and directory shadowing commands

These commands do not require any object authorities:

ADDDIRE [2]	CHGDIRSHD [1]	ENDDIRSHD [4]	STRDIRSHD [4]
ADDDIRSHD [1]	CPYFRMDIR [1]	RMVDIRE [1]	WRKDIRE [3,5]
CHGSYSDIRA [2]	CPYTODIR [1]	RMVDIRSHD [1]	WRKDIRLOC [1,5]
CHGDIRE [3]	DSPDIRE	RNMDIRE [2]	WRKDIRSHD [1,5]

1 You must have *SECADM special authority.

2 You must have *SECADM or *ALLOBJ special authority.

3 A user with *SECADM special authority can work with all directory entries. Users without *SECADM special authority can work only with their own entries.

4 You must have *JOBCTL special authority.

5 To use an individual operation, you must have the authority required by the operation.

Disk commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands to not require authority to any objects:

ENDDSKRGZ (Q) [1]	STRDSKRGZ (Q) [1]	WRKDSKSTS

[1] To use this command, you must have *ALLOBJ special authority.

Display station pass-through commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ENDPASTHR			
STRPASTHR	APPC device on source system	*CHANGE	*EXECUTE
	APPC device on target system	*CHANGE	*EXECUTE
	Virtual controller on target system [1]	*USE	*EXECUTE
	Virtual device on target system [1,2]	*CHANGE	*EXECUTE
	Program specified in the QRMTSIGN system value on target system, if any[1]	*USE	*USE
TFRPASTHR			

[1] The user profile that requires this authority is the profile that runs the pass-through batch job. For pass-through that bypasses the signon display, the user profile is the one specified in the remote user (RMTUSER) parameter. For pass-through that uses the normal signon procedure (RMTUSER(* NONE)), the user is the default user profile specified in the communications entry of the subsystem that handles the pass-through request. Generally, this is QUSER.

[2] If the pass-through is one that uses the normal signon procedure, the user profile specified on the signon display on the target system must have authority to this object.

Distribution commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD [1]	Document [2]	*CHANGE	*EXECUTE
CHGDSTQ (Q)			
CHGDSTRTE (Q)			
DLTDST [1]			
DSPDSTLOG (Q)	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST [1]	Requested file	*CHANGE	*EXECUTE
RCVDST [1]	Requested file	*CHANGE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
RLSDSTQ (Q)			
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST [1]	Requested file or document	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			

[1] If the user is asking for distribution for another user, the user must have the authority to work on behalf of the other user.

[2] When the Distribution is filed.

Distribution list commands

These commands do not require any object authorities:

ADDDSTLE [1]	CRTDSTL	DSPDSTL	RNMDSTL [1]
CHGDSTL[1]	DLTDSTL [1]	RMVDSTLE [1]	WRKDSTL [2]

[1] You must have *SECADM special authority or own the distribution list.

[2] To use an individual operation, you must have the authority required by the operation.

Document library object commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDDLOAUT	Document library object	*ALL or owner	*EXECUTE
CHGDLOAUD [1]			
CHGDLOAUT	Document library object	*ALL or owner	*EXECUTE
CHGDLOOWN	Document library object	Owner or *ALLOBJ special authority	*EXECUTE
	Old user profile	*DLT	*EXECUTE
	New user profile	*ADD	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGDLOPGP	Document library object	Owner or *ALLOBJ special authority	*EXECUTE
	Old primary group profile	*DLT	*EXECUTE
	New primary group profile	*ADD	*EXECUTE
CHGDOCD [2]	Document description	*CHANGE	*EXECUTE
CHKDLO [2]	Document library object	As required by the AUT keyword	*EXECUTE
CPYDOC	From-document	*USE	*EXECUTE
	To-document, if replacing existing document	*CHANGE	*EXECUTE
	To-folder if to-document is new	*CHANGE	*EXECUTE
CRTDOC	In-folder	*CHANGE	*EXECUTE
CRTFLR	In-folder	*CHANGE	*EXECUTE
DLTDLO [3]	Document library object	*ALL	*EXECUTE
DLTDOCL[20]	Document list	*ALL [4]	*EXECUTE
DMPDLO [15]			
DSPAUTLDLO	Authorization list	*USE	*EXECUTE
	Document library object	*USE	*EXECUTE
DSPDLOAUD[21]	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
DSPDLOAUT	Document library object	*USE or owner	*EXECUTE
DSPDLONAM[22]	Document library object	*USE	*EXECUTE
DSPDOC	Document	*USE	*EXECUTE
DSPFLR	Folder	*USE	*EXECUTE
EDTDLOAUT	Document library object	*ALL or owner	*EXECUTE
EDTDOC	Document	*CHANGE	*EXECUTE
FILDOC [2]	Requested file	*USE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
MOVDOC	From-folder, if source document is in a folder	*CHANGE	*EXECUTE
	From-document	*ALL	*EXECUTE
	To-folder	*CHANGE	*EXECUTE
PRTDOC	Folder	*USE	*EXECUTE
	Document	*USE	*EXECUTE
	DLTPF, DLTF, and DLTOVR commands, if an *INDEX* instruction is specified	*USE	*EXECUTE
	CRTPF, OVRPRTF, DLTSPLF, and DLTOVR commands, if a *RUN* instruction is specified	*USE	*EXECUTE
	Save document, if SAVOUTPUT (*YES) is specified	*USE	*EXECUTE
	Save folder, if SAVOUTPUT (*YES) is specified	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
QRYDOCLIB [2,6]	Requested file	*USE	*EXECUTE
	Document list, if it exists	*CHANGE	*EXECUTE
RCLDLO	Document library object		
	Internal documents or all documents and folders[16]		
RGZDLO	Document library object	*CHANGE or owner	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY), or DLO(*ALL) FLR(*ANY) MAIL(*YES)[16]		
RMVDLOAUT	Document library object	*ALL or owner	*EXECUTE
RNMDLO	Document library object	*ALL	*EXECUTE
	In-folder	*CHANGE	*EXECUTE
RPLDOC [2]	Requested file	*READ	*EXECUTE
	Document	*CHANGE	*EXECUTE
RSTDLO	Document library object, if replacing	*ALL[10]	*EXECUTE
	Parent folder, if new DLO	*CHANGE[10]	*EXECUTE
	Owning user profile, if new DLO	*ADD[10]	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	Save file	*USE	*EXECUTE
	Optical file (OPTFILE)[17]	*R	N/A
	Path prefix of optical file (OPTFILE)[17]	*X	N/A
	Optical volume[19]	*USE	N/A
	Tape, diskette, and optical unit	*USE	*EXECUTE
RSTS36FLR [11,12,14]	S/36 folder	*USE	*EXECUTE
	To-folder	*CHANGE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
RTVDLONAM[22]	Document library object	*USE	*EXECUTE
RTVDOC [2]	Document if checking out	*CHANGE	*EXECUTE
	Document if not checking out	*USE	*EXECUTE
	Requested file	*CHANGE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
SAVDLO [7,13]	Document library object	*ALL[10]	*EXECUTE
	Tape unit, diskette unit, and optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*USE, *ADD, *OBJMGT	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	Optical File (OPTFILE)[17]	*RW	N/A
	Parent directory of optical file (OPTFILE)[17]	*WX	N/A
	Path Prefix of optical file (OPTFILE)[17]	*X	N/A
	Root Directory (/) of volume[17, 18]	*RWX	N/A
	Optical Volume[19]	*CHANGE	N/A
SAVRSTDLO	On the source system, same authority as required by SAVDLO command.		
	On the target system, same authority as required by RSTDLO command.		
WRKDOC	Folder	*USE	
WRKFLR	Folder	*USE	

1 You must have *AUDIT special authority.

2 If the user is working on behalf of another user, the other user's authority to the object is checked.

3 The user must have *ALL authority to all the objects in the folder in order to delete the folder and all the objects in the folder.

4 If you have *ALLOBJ or *SECADM special authority, you do not need all *ALL authority to the document library list.

5 The user must have authority to the object being used as the merge source. For example, if MRGTYPE(*QRY) is specified, the user must have use authority to the query specified for the QRYDFN parameter.

6 Only objects that meet the criteria of the query and to which the user has at least *USE authority are returned in the document list or output file.

7 *SAVSYS, *ALLOBJ, or enrollment in the system distribution directory is required.

8 *SAVSYS or *ALLOBJ special authority is required to use the following parameter combination: RSTDLO DLO(*MAIL).

9 *ALLOBJ is required to specify ALWOBJDIF(*ALL).

10 If you have *SAVSYS or *ALLOBJ special authority, you do not need the authority specified.

Command	Referenced Object	Authority Needed	
		For Object	For Library
[11] You need *ALL authority to the document if replacing it. You need operational and all the data authorities to the folder if restoring new information into the folders, or you need *ALLOBJ special authority.			
[12] If used for a data dictionary, only the authority to the command is required.			
[13] *SAVSYS or *ALLOBJ special authority is required to use the following parameter combinations: SAVDLO DLO(*ALL) FLR(*ANY) SAVDLO DLO(*MAIL) SAVDLO DLO(*CHG) SAVDLO DLO(*SEARCH) OWNER(not *CURRENT)			
[14] You must be enrolled in the system distribution directory if the source folder is a document folder.			
[15] You must have *ALLOBJ special authority to dump internal document library objects.			
[16] You must have *ALLOBJ or *SECADM special authority.			
[17] This authority check is only made when the Optical Media Format is Universal Disk Format (UDF).			
[18] This authority check is only made when you are clearing the optical volume.			
[19] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function.			
[20] The user must have *ALLOBJ special authority when OWNER (*ALL) or OWNER (name) and Name is a different user profile than the caller.			
[21] The user must have all object (*ALLOBJ) or audit (*AUDIT) special authority to use this command.			
[22] The user must have all object (*ALLOBJ) special authority to use this command when specifying *DST for the object class to locate.			

Double-byte character set commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CPYIGCTBL	DBCS sort table (*IN)	*ALL	*EXECUTE
	DBCS sort table (*OUT)	*USE	*EXECUTE
CRTIGCDCT	DBCS conversion dictionary		*READ, *ADD
DLTIGCDCT	DBCS conversion dictionary	*OBJEXIST	*EXECUTE
DLTIGCSRT	DBCS sort table	*OBJEXIST	*EXECUTE
DLTIGCTBL	DBCS font table	*OBJEXIST	*EXECUTE
DSPIGCDCT	DBCS conversion dictionary	*USE	*EXECUTE
EDTIGCDCT	DBCS conversion dictionary	*USE, *UPD	*EXECUTE
	User dictionary	*ADD, *DLT	*EXECUTE
STRCGU	DBCS sort table	*CHANGE	*EXECUTE
	DBCS font table	*CHANGE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRFMA	DBCS font table, if copy-to option specified	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	DBCS font table, if copy-from option specified	*OBJOPR, *READ	*EXECUTE
	Font management aid work file (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

Edit description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTEDTD	Edit description		*EXECUTE, *ADD
DLTEDTD	Edit description	*OBJEXIST	*EXECUTE
DSPEDTD	Edit description	*OBJOPR	*EXECUTE
WRKEDTD [1]	Edit description	Any authority	*USE

1 To use an individual operation, you must have the authority required by the operation.

Environment variable commands

These commands do not require any object authorities.			
ADDENVVAR[1]	CHGENVVAR [1]	RMVENVVAR[1]	WRKENVVAR[1]

1 To update system-level environment variables, you need *JOBCTL special authority.

Extended wireless LAN configuration commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDEWCBCDE	Source file	*USE	*EXECUTE
ADDEWCM	Source file	*USE	*EXECUTE
ADDEWCPTCE	Source file	*USE	*EXECUTE
ADDEWLM	Source file	*USE	*EXECUTE
CHGEWCBCDE	Source file	*USE	*EXECUTE
CHGEWCM	Source file	*USE	*EXECUTE
CHGEWCPTCE	Source file	*USE	*EXECUTE
CHGEWLM	Source file	*USE	*EXECUTE
DSPEWCBCDE	Source file	*USE	*EXECUTE
DSPEWCM	Source file	*USE	*EXECUTE
DSPEWCPTCE	Source file	*USE	*EXECUTE
DSPEWLM	Source file	*USE	*EXECUTE
RMVEWCBCDE	Source file	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
RMVEWCPTCE	Source file	*USE	*EXECUTE

File commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	Logical file	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE, *ADD
	File referenced in DTAMBRS parameter, when logical file is keyed	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE
	File referenced in DTAMBRS parameter, when logical file is not keyed	*OBJOPR	*EXECUTE
ADDPFCST	Dependent file, if TYPE(*REFCST) is specified	*OBJMGT or *OBJALTER	*EXECUTE
	Parent file, if TYPE(*REFCST) is specified	*OBJMGT or *OBJREF	*EXECUTE
	File, if TYPE(*UNQCST) or TYPE(*PRIKEY) is specified	*OBJMGT	*EXECUTE
ADDPFM	Physical file	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Physical file, to insert trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Physical file, to delete trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Physical file, to update trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Trigger program	*EXECUTE	*EXECUTE
CHGDDMF	DDM file	*OBJOPR, *OBJMGT	*EXECUTE
	Device description [7]	*CHANGE	
CHGDKTF	Diskette file	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified in the command	*OBJOPR	*EXECUTE
CHGDSPF	Display file	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified	*OBJOPR	*EXECUTE
CHGDTA	Data file	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Program	*USE	*EXECUTE
	Display file	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Logical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGLFM	Logical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPF	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFCST	Dependent file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFM	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFTRG	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPRTF	Print file	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified	*OBJOPR	*EXECUTE
CHGSAVF	Save file	*OBJOPR, *OBJMGT	*EXECUTE
CHGSRCPF	Source physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGTAPF	Tape file	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified	*OBJOPR	*EXECUTE
CLRPFM	Physical file	*OBJOPR, *OBJMGT or *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Save file	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
	Based-on file if from-file is logical file	*READ	*EXECUTE
CPYFRMDKT	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
CPYFRMIMPF	From-file	*OBJOPR, *READ	*USE
	To-file (device file)	*OBJOPR, *READ	*USE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
	Based-on file if from-file is logical file	*READ	*USE
CPYFRMQRYF [1]	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	

Command	Referenced Object	Authority Needed	
		For Object	For Library
CPYFRMSTMF	Stream file	*R	
	Directories in stream file path name prefix	*X	
	Target database file, if MBROPT(*ADD) specified	*X, *ADD	*X
	Target database file, if MBROPT(*REPLACE) specified	*X, *ADD, *DLT, *OBJMGT	*X
	Target database file, if new member created	*X, *OBJMGT, *ADD	*X, *ADD
	Conversion table *TBL used to translate data	*OBJOPR	*X
	Target save file exists	*RX, *ADD, *OBJMGT	*X
	Target save file is created		*RX, *ADD
CPYFRMTAP	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
CPYSRCF	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
CPYTODKT	To-file and from-file	*OBJOPR, *READ	*EXECUTE
	Device if device name specified on the command	*OBJOPR, *READ	*EXECUTE
	Based-on physical file if from-file is logical file	*READ	*EXECUTE
CPYTOIMPF	From-file	*OBJOPR, *READ	*USE
	To-file (device file)	*OBJOPR, *READ	*USE
	To-file (physical file)	Refer to "General rules for object authorities on commands" on page 157.	
	Based-on file if from-file is logical file	*READ	*USE
CPYTOSTMF	Database file or save file	*RX	*X
	Stream file, if it already exists	*W	
	Stream file parent directory, if the stream file does not exist	*WX	
	Stream file path name prefix	*X	
	Conversion table *TBL used to translate data	*OBJOPR	*X
CPYTOTAP	To-file and from file	*OBJOPR, *READ	*EXECUTE
	Device if device name is specified	*OBJOPR, *READ	*EXECUTE
	Based-on physical file if from-file is logical file	*READ	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTDDMF	DDM file: REPLACE(*NO)		*READ, *ADD
	DDM file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Device description [7]	*CHANGE	
CRTDKTF	Device if device name is specified	*OBJOPR	*EXECUTE
	Diskette file: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Diskette file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *EXECUTE
CRTDSPF	Source file	*USE	*EXECUTE
	Device if device name is specified	*OBJOPR	*EXECUTE
	File specified in REF and REFFLD keywords	*OBJOPR	*EXECUTE
	Display file: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Display file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *EXECUTE
CRTICFF	Source file	*USE	*EXECUTE
	File specified in REF and REFFLD keywords	*OBJOPR	*EXECUTE
	ICF file: REPLACE(*NO)		*READ, *ADD
	ICF file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTLF	Source file	*USE	*EXECUTE
	File specified on PFILE or JFILE keyword, when logical file is keyed	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE
	File specified on PFILE or JFILE keyword, when logical file is not keyed	*OBJOPR	*EXECUTE
	Files specified on FORMAT and REFACCPTH keywords	*OBJOPR	*EXECUTE
	Tables specified in the ALTSEQ keyword	*OBJOPR	*EXECUTE
	Logical file		*EXECUTE, *ADD
	File referenced in DTAMBRS parameter, when logical file is keyed	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE
	File referenced in DTAMBRS parameter, when logical file is not keyed	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTPF	Source file	*USE	*EXECUTE
	Files specified in FORMAT and REFFLD keywords and tables specified in the ALTSEQ keyword	*OBJOPR	*EXECUTE
	Physical file		*EXECUTE, *ADD
CRTPRTF	Source file	*USE	*EXECUTE
	Device if device name is specified	*OBJOPR	*EXECUTE
	Files specified in the REF and REFFLD keywords	*OBJOPR	*EXECUTE
	Print file: Replace(*NO)		*READ, *ADD, *EXECUTE
	Print file: Replace(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *EXECUTE
CRTSAVF	Save file		*READ, *ADD, *EXECUTE
CRTSRCPF	Source physical file		*READ, *ADD, *EXECUTE
CRTS36DSPF	To-file source file when TOMBR is not *NONE	*ALL	*CHANGE
	Source file QS36SRC	*USE	*EXECUTE
	Display file: REPLACE(*NO)		*READ, *ADD
	Display file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Create Display File (CRTDSPF) command	*OBJOPR	*EXECUTE
CRTTAPF	Tape file: REPLACE(*NO)		*READ, *ADD
	Tape file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Device if device name is specified	*OBJOPR	*EXECUTE
DLTF	File	*OBJOPR, *OBJEXIST	*EXECUTE
DSPCPCST	Database file that has constraint pending	*OBJOPR, *READ	*EXECUTE
DSPDBR	Database file	*OBJOPR	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
DSPDDMF	DDM file	*OBJOPR	
DSPDTA	Data file	*USE	*EXECUTE
	Program	*USE	*EXECUTE
	Display file	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPFD [2]	File	*OBJOPR	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
	File is a physical file and TYPE(*ALL, *MBR, OR *MBRLST) is specified	A data authority other than *EXECUTE	*EXECUTE
DSPFFD	File	*OBJOPR	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPPFM	Physical file	*USE	*EXECUTE
DSPSAVF	Save file	*USE	*EXECUTE
EDTCPCST	Data area, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*CHANGE	*EXECUTE
	Files, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
INZPFM	Physical file, when RECORD(*DFT) is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD	*EXECUTE
	Physical file, when RECORD(*DLT) is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Target file	*CHANGE, *OBJMGT	*CHANGE
	Maintenance file	*USE	*EXECUTE
	Root file	*USE	*EXECUTE
OPNDBF	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
OPNQRYF	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
PRTTRGPGM [11]			
RGZPFM	File containing member	*OBJOPR, *OBJMGT or *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	File containing member	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPFCST	File	*OBJMGT or *OBJALTER	*EXECUTE
RMVPFTRG	Physical file	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	File containing member	*OBJOPR, *OBJMGT	*EXECUTE, *UPD

Command	Referenced Object	Authority Needed	
		For Object	For Library
RSTS36F [4] (Q)	To-file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	From-file	*USE	*EXECUTE
	Based on physical file, if file being restored is a logical (alternative) file	*CHANGE	*EXECUTE
	Device description for diskette or tape	*USE	*EXECUTE
RTVMBRD	File	*USE	*EXECUTE
SAVSAVFDTA	Tape, diskette, or optical device description	*USE	*EXECUTE
	Save file	*USE	*EXECUTE
	Optical Save/Restore File[8] (if previously exists)	*RW	N/A
	Parent Directory of OPTFILE[8]	*WX	N/A
	Path Prefix of OPTFILE[8]	*X	N/A
	Root Directory (/) of Optical Volume [8,9]	*RWX	N/A
	Optical Volume[10]	*CHANGE	N/A
SAVS36F	From-file	*USE	*EXECUTE
	To-file, when it is a physical file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	Device file or device description	*USE	*EXECUTE
SAVS36LIBM	To-file, when it is a physical file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	From-file	*USE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
STRAPF [3]	Source file	*OBJMGT, *CHANGE	*READ, *ADD
	Commands CRTPF, CRTLF, ADDPFM, ADDLFM, and RMVM	*USE	*EXECUTE
STRDFU [3]	Program (if create program option)		*READ, *ADD
	Program (if change or delete program option)	*OBJEXIST	*READ, *ADD
	File (if change or display data option)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	File (if display data option)	*READ	*EXECUTE
UPDDTA	File	*CHANGE	*EXECUTE
WRKCMTDFN [1]			
WRKDDMF [3]	DDM file	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
WRKF [3,5]	Files	*OBJOPR	*USE
WRKPFCST[3]			*EXECUTE

[1] The CPYFRMQRYF command uses a FROMOPNID parameter rather than a FROMFILE parameter. A user must have sufficient authority to perform the OPNQRYF command prior to running the CPYFRMQRYF command. If CRTFILE(*YES) is specified on the CPYFRMQRYF command, the first file specified on the corresponding OPNQRYF FILE parameter is considered to be the from-file when determining the authorities for the new to-file.

[2] Ownership or operational authority to the file is required.

[3] To use individual operations, you must have the authority required by the individual operation.

[4] If a new file is created and an authority holder exists for the file, then the user must have all (*ALL) authority to the authority holder or be the owner of the authority holder. If there is no authority holder, the owner of the file is the user who entered the RSTS36F command and the public authority is *ALL.

[5] Some authority to the object is required.

[6] You must have *ALLOBJ special authority.

[7] Authority is verified when the DDM file is used.

[8] This authority check is only made when the Optical media format is Universal Disk Format (UDF).

[9] This authority check is only made if you are clearing the optical volume.

[10] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function.

[11] You must have *ALLOBJ or *AUDIT special authority to use this command.

Filter commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDALRACNE	Filter	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filter	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filter	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filter	*USE, *ADD	*EXECUTE
CHGALRACNE	Filter	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filter	*USE, *UPD	*EXECUTE
CHGFTR	Filter	*OBJMGT	*EXECUTE
CHGPRBACNE	Filter	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filter	*USE, *UPD	*EXECUTE
CRTFTR	Filter		*READ, *ADD
DLTFTR	Filter	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filter	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filter	*USE, *DLT	*EXECUTE
WRKFTR [1]	Filter	Any authority	*EXECUTE
WRKFTRACNE [1]	Filter	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
WRKFTRSLTE [1]	Filter	*USE	*EXECUTE

[1] To use an individual operation, you must have the authority required by the operation.

Finance commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
SBMFNCJOB (Q)	Job description and message queue [1]	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Job description and message queue [1]	*OBJOPR	*EXECUTE
WRKDEVTBL (Q)	Device description [1]	At least one data authority	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			

[1] The QFNC user profile must have this authority.

OS/400 Graphical operations

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGFCNUSG[5]			
DSPFCNUSG			
EDTWSOAUT	Workstation object [1]	*OBJMGT [2,3,4]	*EXECUTE
GRTWSOAUT	Workstation object [1]	*OBJMGT [2,3,4]	*EXECUTE
RVKWSOAUT	Workstation object [1]	*OBJMGT [2,3,4]	*EXECUTE
SETCSTDTA	Copy-from user profile	*CHANGE	*EXECUTE
	Copy-to user profile	*CHANGE	*EXECUTE
WRKFCNUSG			

[1] The workstation object is an internal object that is created when you install the OS/400 Graphical Operations feature. It is shipped with public authority of *USE.

[2] You must be the owner or have *OBJMGT authority and the authorities being granted or revoked.

[3] You must be the owner or have *ALLOBJ authority to grant *OBJMGT or *AUTLMGT authority.

[4] To secure the workstation object with an authorization list or remove the authorization list, you must have one of the following:

- Own the workstation object.
- Have *ALL authority to the workstation object.
- Have *ALLOBJ special authority.

[5] You must have security administrator (*SECADM) special authority to change the usage of a function.

Graphics symbol set commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTGSS	Source file	*USE	*EXECUTE
	Graphics symbol set		*READ, *ADD
DLTGSS	Graphics symbol set	*OBJEXIST	*EXECUTE
WRKGSS [1]	Graphics symbol set	*OBJOPR	*USE

[1] Ownership or some authority to the object is required.

Host server commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require object authorities.	
ENDHOSTSVR (Q)	STRHOSTSVR (Q)

Image commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDIMGCLGE (Q)[1]				
CHGIMGCLG (Q)[1]				
CHGIMGCLGE (Q)[1]				
CRTIMGCLG (Q)[1]				
DLTIMGCLG (Q)[1]				
LODIMGCLG (Q)[1]				
RMVIMGCLGE (Q)[1]				
VFYIMGCLG (Q)[1]				
WRKIMGCLGE (Q)[1]				

[1] You must have *ALLOBJ and *SECADM special authority to use this command.

Integrated file system commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
ADDLNK	Object	*STMF	QOpenSys, 'root,'UDFS	*OBJEXIST
	Parent of new link	*DIR	QOpenSys, 'root,' UDFS	*WX
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
CHGATR	Object when setting an attribute other than *USECOUNT, *ALWCKPWRT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL	Any	All except QSYS.LIB	*W
	Object when setting *USECOUNT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV	Any	All except QSYS.LIB	*OBJMGT
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	*X, *OBJMGT (authority inherited from parent *FILE)
		other	QSYS.LIB	*OBJMGT
	Object when setting *ALWCKPWRT	Any	All	*OBJMGT
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory	All	*RX
	Object when setting the following attributes: *CRTOBJSCAN or *SCAN	*DIR and *STMF	QOpenSys, 'root,' UDFS	See note[26]
	Object when setting the following attributes: *SETUID, *SETGID, *RSTDRNMUNL	Any	All except QSYS.LIB and QDLS	Ownership [15]
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
CHGAUD [4]				
CHGAUT	Object	All	QOpenSys, 'root,' UDFS	Ownership[15]
			QSYS.LIB, QOPT[11]	Ownership or *ALLOBJ
			QDLS	Ownership, *ALL, or *ALLOBJ
				*OBJMGT
	Optical volume	*DDIR	QOPT[8]	*CHANGE
CHGCURDIR	Object	Any directory		*R
	Optical volume	*DDIR	QOPT[8]	*X
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
CHGOWN[24]	Object	All	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		All	QOpenSys, 'root,' UDFS	Ownership and *OBJEXIST[15]
		All	QDLS	Ownership or *ALLOBJ
			QOPT[11]	Ownership or *ALLOBJ
	User profile of old owner—all except QOPT, QDLS	*USRPRF	All	*DLT
	User profile of new owner—all except QOPT	*USRPRF	All	*ADD
	Optical volume	*DDIR	QOPT[8]	*CHANGE
CHGPGP	Object	All	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		All	QOpenSys, 'root,' UDFS	Ownership[5, 15]
		All	QDLS	Ownership or *ALLOBJ
			QOPT[11]	Ownership or *ALLOBJ
	User profile of old primary group—all except QOPT	*USRPRF	All	*DLT
	User profile of new primary group—all except QOPT	*USRPRF	All	*ADD
	Optical volume	*DDIR	QOPT[8]	*CHANGE
CHKIN	Object, if the user who checked it out.	*STMF	QOpenSys, 'root,' UDFS	*W
		*DOC	QDLS	*W
	Object, if not the user who checked it out.	*STMF	QOpenSys, 'root,' UDFS	*ALL or *ALLOBJ or Ownership
		*DOC	QDLS	*ALL or *ALLOBJ or Ownership
	Path, if not the user who checked out	*DIR	QOpenSys, 'root,' UDFS	*X
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
CHKOUT	Object	*STMF	QOpenSys, 'root,' UDFS	*W
		*DOC	QDLS	*W
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
CPY[25]	Object being copied, origin object	Any	QOpenSys, 'root,' UDFS	*R, and *OBJMGT or ownership
		*DOC	QDLS	*RWX and *ALL or ownership
		*MBR	QSYS.LIB	None
		others	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT[11]	*R
	Destination object when REPLACE(*YES) specified (if destination object already exists)	Any	All[10]	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT[11]	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF or LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Directory being copied that contains objects when SUBTREE(*ALL) is specified, so that its contents are copied	*DIR	QOpenSys, 'root,' UDFS	*RX, *OBJMGT
	Path (target), parent directory of destination object	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*RWX
		*DDIR	QOPT[11]	*WX
	Source Optical volume	*DDIR	QOPT[8]	*USE
	Target Optical volume	*DDIR	QOPT[8]	*CHANGE
	Parent directory of origin object	*DIR	QOpenSys, 'root,' UDFS	*X
		*FLR	QDLS	*X
		Others	QSYS.LIB	*RX
		*DDIR	QOPT[11]	*X
	Path prefix (target destination)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, 'root,' UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Path prefix (origin object)	*DDIR	QOPT[11]	*X

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
CRTDIR[21, 22]	Parent directory	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Any		*ADD
		*DDIR	QOPT[11]	*WX
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Optical volume	*DDIR	QOPT[8]	*CHANGE
CVTDIR (Q)[16]				
DSPAUT	Object	All	QDLS	*ALL
		All	All others	*OBJMGT or ownership
		ALL	QOPT[11]	None
	Optical volume	*DDIR	QOPT[8]	*USE
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
DSPCURDIR	Path prefix	*DIR	QOpenSys, 'root,' UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT[11]	*RX
	Current directory	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT[11]	*X
	Optical volume	*DDIR*	QOPT[8]	*USE

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
DSPLNK	Any	Any	'root,' QOpenSys, UDFS QSYS.LIB, QDLS, QOPT[11]	None
	File, Option 12 (Display Links)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	'root,' QOpenSys, UDFS	*R
	Symbolic link object	*SYMLNK	'root,' QOpenSys, UDFS	None
	Optical volume	*DDIR	QOPT[8]	*USE
	Parent directory of referenced object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Parent directory of referenced object - Pattern specified[13]	*DIR	'root,' QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Parent directory of referenced object- Option 8 (Display Attributes)	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Parent directory of referenced object - Option 12 (Display Links)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
DSPLNK (continued)	Prefix of parent referenced object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Pattern specified[13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Option 12 (Display Links)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
DSPLNK (continued)	Relative Path Name [14] : Current working directory containing object - No Pattern[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*X	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] : Current working directory containing object - Pattern Specified[13]	*DIR	'root,' QOpenSys, UDFS	'root,' QOpenSys, UDFS
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] : Prefix of current working directory containing object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] : Prefix of current working directory containing object - Pattern specified[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Object	Any	Any	None
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
ENDJRN	Object	*DIR if Subtree (*ALL)	QOpenSys, 'root,' UDFS	*R, *X, *OBJMGT
		*DIR if Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Parent Directory	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*X
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Journal			*OBJMGT, *OBJOPR
MOV[19]	Object moved within same file system	*DIR	QOpenSys, 'root'	*OBJMGT, *W
		not *DIR	QOpenSys, 'root'	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	None
		other	QSYS.LIB	None
		*STMF	QOPT[11]	*W
	Path (source), parent directory	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, 'root'	*RX, *OBJEXIST
		others	QOpenSys, 'root'	*RWX
MOV[19] (continued)	Path (target), parent directory	*DIR	QSYS.LIB	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *ADD, *DLT, *OBJMGT
		*LIB	QSYS.LIB	*RWX
		*DDIR	QOPT[11]	*WX
	Path prefix (target)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	others	*X
		*DDIR	QOPT[11]	*X

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
MOV[19] (continued)	Object moved across file systems into QOpenSys, root or QDLS (stream file *STMF and *DOC, *MBR only) .	*STMF	QOpenSys, 'root,' UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	N/A
		*DSTMF	QOPT[11]	*RW
	Moved into QSYS *MBR	*STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW
	Path (source) moved across file systems, parent directory	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS. LIB	ownership, *RX, *OBJEXIST
		*DDIR	QOPT[11]	*WX
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Optical volume (Source and Target)	*DDIR	QOPT[8]	*CHANGE
RLSIFSLCK [18]	some_stmf	*STMF	"root", QOpenSys, UDFS	*R
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
RMVDIR[19,20]	Directory	*DIR	QOpenSys, 'root,' UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT[11]	*W
	Parent directory	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT[11]	*WX
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Optical volume	*DDIR	QOPT[8]	*CHANGE

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
RMVLNK[19]	Object	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		other	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT[11]	*W
		any	QOpenSys, 'root,' UDFS	*OBJEXIST
	Parent Directory	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, 'root,' UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Optical volume	*DDIR	QOPT[8]	*CHANGE
RNM[19]	Object	*DIR	QOpenSys, 'root,' UDFS	*OBJMGT, *W
		Not *DIR	QOpenSys, 'root,' UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	N/A
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		others	QSYS.LIB	*OBJMGT
		*DSTMF	QOPT[11]	*W
	Optical Volume (Source and Target)	*DDIR	QOPT[8]	*CHANGE
	Parent directory	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT[11]	*WX
	Path prefix	*LIB	QSYS.LIB	*X, *UPD
		Any	QOpenSys, 'root,' UDFS, QDLS	*X

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
RST (Q) [23]	Object, if it exists[2]	Any	QOpenSys, 'root,' UDFS	*W, *OBJEXIST
			QSYS.LIB	Varies [10]
			QDLS	*ALL
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Parent directory of object being restored[2]	*DIR	QOpenSys, 'root,' UDFS	*WX
	Parent directory of object being restored, if the object does not exist[2]	*FLR	QDLS	*CHANGE
		*DIR		*OBJMGT, *OBJALTER, *READ, *ADD, *UPD
	User profile owning new object being restored[2]	*USRPRF	QSYS.LIB	*ADD
	Tape unit, diskette unit, optical unit, or save file	*DEVD, *FILE	QSYS.LIB	*RX
	Library for device description or save file	*LIB	QSYS.LIB	*EXECUTE
	Output file, if specified	*STMF	QOpenSys, 'root,' UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Path prefix of output file	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*RX
	Optical volume if restoring from optical device	*DDIR	QOPT[8]	*USE
	Optical path prefix and parent if restoring from optical device	*DDIR	QOPT[11]	*X
	Optical file if restoring from optical device	*DSTMF	QOPT[11]	*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
RTVCURDIR	Path prefix	*DIR	QOpenSys, 'root,' UDFS, QDLS, QOPT[11]	*RX
		*DDIR	QOPT[11]	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Any		*R
	Current directory	*DIR	QOpenSys, 'root,' UDFS, QOPT [11]	*X
		*DDIR	QOPT[11]	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Any		*R
SAV	Object[2]	Any	QOpenSys, 'root,' UDFS	*R, *OBJEXIST
			QSYS.LIB	Varies [10]
			QDLS	*ALL
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Tape unit, diskette unit, or optical unit	*DEVD	QSYS.LIB	*RX
	Save file, if empty	*FILE	QSYS.LIB	*USE, *ADD
	Save file, if not empty	*FILE	QSYS.LIB	*OBJMGT, *USE, *ADD
	Save-while-active message queue	*MSGQ	QSYS.LIB	*OBJOPR, *ADD
	Libraries for device description, save file, save-while-active message queue	*LIB	QSYS.LIB	*EXECUTE
	Output file, if specified	*STMF	QOpenSys, 'root,' UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Path prefix of output file	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*RX
	Optical volume, if saving to optical device	*DDIR	QOPT[8]	*CHANGE
	Optical path prefix if saving to optical device	*DDIR	QOPT[11]	*X
	Optical parent directory if saving to optical device	*DDIR	QOPT[11]	*WX
	Optical file (If it previously exists)	*DSTMF	QOPT[11]	*RW

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
SAVRST	On the source system, same authority as required by SAV command.			
	On the target system, same authority as required by RST command.			
STATFS	Object	Any	Any	None
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		
STRJRN	Object	*DIR if Subtree (*ALL)	QOpenSys, 'root,' UDFS	*R, *X, *OBJMGT
		*DIR if subtree (*NONE), *SYMLNK, *STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Parent Directory	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*X
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Journal	*JRN		*OBJMGT, *OBJOPR
WRKAUT[6, 7]	Object	*DOC or *FLR	QDLS	*ALL
		All	not QDLS	*OBJMGT or ownership
		*DDIR and *DSTMF	QOPT[11]	*NONE
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
	Optical volume	*DDIR	QOPT[8]	*USE

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
WRKLNK	Any	Any	'root,' QOpenSys, UDFS, QSYS.LIB, QDLS, QOPT[11]	None
	File, Option 12 (Display Links)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	'root,' QOpenSys, UDFS	*R
	Symbolic link object	*SYMLNK	'root,' QOpenSys, UDFS	None
	Optical volume	*DDIR	QOPT[8]	*USE
	Parent directory of referenced object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Parent directory of referenced object - Pattern Specified	*DIR	'root,' QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Parent directory of referenced object- Option 8 (Display Attributes)	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Parent directory of referenced object - Option 12 (Display Links)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
WRKLNK (continued)	Prefix of parent referenced object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Pattern specified[13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
	Prefix of parent referenced object - Option 12 (Display Links)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]
WRKLNK (continued)	Relative Path Name [14,] : Current working directory containing object - No Pattern[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] : Current working directory containing object - Pattern Specified[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] : Prefix of current working directory containing object - No Pattern [13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Relative Path Name [14] Prefix of current working directory containing object - Pattern specified[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

[1] Adopted authority is not used for Integrated file system commands.

[2] If you have *SAVSYS special authority, you do not need the authority specified for the QSYS.LIB, QDLS, QOpenSys, and "root" file systems.

[3] The authority required varies by object type. See the description of the QLIRNMO API in the Information Center. If the object is a database member, see the authorities for the Rename Member (RNMM) command.

[4] You must have *AUDIT special authority to change an auditing value.

[5] If the user issuing the command does not have *ALLOBJ authority, the user must be a member of the new primary group.

[6] This command is not supported for the QLANSrv file system.

[7] These commands require the authority shown plus the authorities required for the DSPCURDIR command.

[8] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function.

Command	Referenced Object	Object Type	File System	Authority Needed for Object[1]

[9] See Chapter 7 of iSeries Optical Support book for information on restrictions regarding this command.

[10] Authority required varies by the native command used. See the respective SAVOBJ or RSTOBJ command for the required authority.

[11] Authority required by QOPT against media formatted in ″Universal Disk Format″ (UDF).

[12] *ADD is needed only when object being moved to is a *MBR.

[13] Pattern: In some commands, an asterisk (*) or a question mark (?) can be used in the last component of the path name to search for names matching a pattern.

[14] Relative path name: If a path name does not begin with a slash, the predecessor of the first component of the path name is taken to be the current working directory of the process. For example, if a path name of 'a/b' is specified, and the current working directory is '/home/john', then the object being accessed is '/home/john/a/b'.

[15] If you have *ALLOBJ special authority, you do not need the listed authority.

[16] You must have *ALLOBJ special authority to use this command.

[17] In the above table, QSYS.LIB refers to independent ASP QSYS.LIB file systems as well as QSYS.LIB file system.

[18] To use this command, you must have *IOSYSCFG special authority.

[19] If the restricted renames and unlinks attribute (also known as S_ISVTX bit) is on for a directory, it will restrict unlinking objects from that directory unless one of these authorities is met: *ALLOBJ; the user is the owner of the object being unlinked; or the user is the owner of the directory.

[20] If RMVLNK (*YES) is specified, the user must also have *OBJEXIST authority to all objects in the specified directory.

[21] For QSYS.LIB, 'root', QOpenSys, and user-defined file systems, the audit (*AUDIT) special authority is required if a value other than *SYSVAL is specified for the CRTOBJAUD parameter.

[22] The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authorities to specify a value for the Scanning option for objects (CRTOBJSCAN) parameter other than *PARENT.

[23] You must have *ALLOBJ special authority to specify a value other than *NONE for the ALWOBJDIF parameter.

[24] The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority when changing the owner of a stream file (*STMF) with an attached Java program whose authority checking while the program is running includes the user and the owner.

[25] The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority when copying a stream file (*STMF) with an attached Java program whose authority checking includes the user and the owner.

[26] The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority to specify the *CRTOBJSCAN and *SCAN attributes.

Interactive data definition commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDDTADFN	Data dictionary	*CHANGE	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
CRTDTADCT	Data dictionary		*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTDTADCT [3]	Data dictionary	OBJEXIST, *USE	
DSPDTADCT	Data dictionary	*USE	*EXECUTE
LNKDTADFN [1]	Data dictionary	*USE	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT [2]	Data dictionary	*OBJOPR	*EXECUTE
WRKDBFIDD [2]	Data dictionary	*USE [4]	*EXECUTE
	Database file	*OBJOPR	*EXECUTE
WRKDTADFN [1]	Data dictionary	*USE, *CHANGE	*EXECUTE

[1] Authority to the data dictionary is not required to unlink a file.

[2] To use individual operations, you must have the authority required by the individual operation.

[3] Before the dictionary is deleted, all linked files are unlinked. Refer to the LNKDTADFN command for authority required to unlink a file.

[4] You need use authority to the data dictionary to create a new file. No authority to the data dictionary is needed to enter data in an existing file.

Internetwork packet exchange (IPX) commands

Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTIPXD	IPX description	*OBJEXIST	*EXECUTE
DSPIPXD	IPX description	*USE	*EXECUTE
WRKIPXD	IPX description	*OBJOPR	*EXECUTE

Information search index commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDSCHIDXE	Search index	*CHANGE	*USE
	Panel group	*USE	*EXECUTE
CHGSCHIDX	Search index	*CHANGE	*USE
CRTSCHIDX	Search Index		*READ, *ADD
DLTSCHIDX	Search index	*OBJEXIST	*EXECUTE
RMVSCHIDXE	Search index	*CHANGE	*USE
STRSCHIDX	Search index	*USE	*EXECUTE
WRKSCHIDX [1]	Search index	*ANY	*USE
WRKSCHIDXE	Search index	*USE	*USE

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] This command is not supported for the QLANSrv file system.			

IPL Attribute commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require authorities to objects:
CHGIPLA (Q) [1] DSPIPLA
[1] To use this command, you must have *SECADM and *ALLOBJ special authorities.

Java commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANZJVM	QSYS/STRSRVJOB command	*USE	
	QSYS/STRDBG command	*USE	

Job commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
BCHJOB	Job description [9,11]	*USE	*EXECUTE
	Libraries in the library list (system, current, and user)[7]	*USE	
	User profile in job description [10]	*USE	
	Sort sequence table [7]	*USE	*EXECUTE
	Message queue [10]	*USE, *ADD	*EXECUTE
	Job queue [10,11]	*USE	*EXECUTE
	Output queue [7]	*READ	*EXECUTE
CHGACGCDE [1]			
CHGGRPA [4]	Message queue if associating a message queue with a group	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGJOB [1,2,3]	New job queue, if changing the job queue[10,11]	*USE	*EXECUTE
	New output queue, if changing the output queue[7]	*READ	*EXECUTE
	Current output queue, if changing the output queue[7]	*READ	*EXECUTE
	Sort sequence table[7]	*USE	*EXECUTE
CHGPJ	User profile for the program start request to specify *PGMSTRRQS	*USE	*EXECUTE
	User profile and job description	*USE	*EXECUTE
CHGSYSJOB(Q) [13]			
CHGUSRTRC[14]	User trace buffer when CLEAR (*YES) is used.[15]	*OBJOPR	*EXECUTE
	User trace buffer when MAXSTG is used[15]	*CHANGE, *OBJMGT	*USE
	User trace buffer when TRCFULL is used. [15]	*OBJOPR	*EXECUTE
DLTUSRTRC	User trace buffer [15]	*OBJOPR, *OBJEXIST	*EXECUTE
DLYJOB [4]			
DMPUSRTRC	User trace buffer [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ			
DSPJOB [1]			
DSPJOBTBL			
DSPJOBLOG [1,5]	Outfile and member exist	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Member does not exist	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Outfile does not exist	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB [1]			
ENDJOBABN [1]			
ENDPJ [6]			
HLDJOB [1]			
RLSJOB [1]			
RRTJOB			
RTVJOBA			
SBMDBJOB	Database file	*USE	*EXECUTE
	Job queue	*READ	*EXECUTE
SBMDKTJOB	Message queue	*USE, *ADD	*EXECUTE
	Job queue and device description	*READ	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
SBMJOB [2, 12]	Job description [9,11]	*USE	*EXECUTE
	Libraries in the library list (system, current, and user)[7]	*USE	
	Message queue[10]	*USE, *ADD	*EXECUTE
	User profile [10,11]	*USE	
	User profile in job description [10]	*USE (at level 40)	
	Job queue [10,11]	*USE	*EXECUTE
	Output queue [7]	*READ	*EXECUTE
	Sort sequence table [7]	*USE	*EXECUTE
	ASP devices in the initial ASP group	*USE	
SBMNETJOB	Database file	*USE	*EXECUTE
STRPJ [6]	Subsystem description	*USE	
	Program		*EXECUTE
TFRBCHJOB	Job queue	*READ	*EXECUTE
TFRGRPJOB	Initial group program	*USE	*EXECUTE
TFRJOB [8]	Job queue	*USE	*EXECUTE
	Subsystem description to which the job queue is allocated	*USE	
TFRSECJOB			
WRKACTJOB			
WRKJOB [1]			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

1 Any user can run these commands for jobs running under his own user profile. A user with job control (*JOBCTL) special authority can run these commands for any job. If you have *SPLCTL special authority, you do not need any authority to the job queue. However, you need authority to the library that contains the job queue.

2 You must have the authority (specified in your user profile) for the scheduling priority and output priority specified.

3 To change certain job attributes, even in the user's own job, requires job control (*JOBCTL) special authority. These attributes are RUNPTY, TIMESLICE, PURGE, DFTWAIT, and TSEPOOL.

4 This command only affects the job in which it was specified.

5 To display a job log for a job that has all object (*ALLOBJ) special authority, you must have *ALLOBJ special authority or be authorized to the All Object Job Log function of the OS/400 through iSeries Navigator's Application Administration support. The Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_ACCESS_ALLOBJ_JOBLOG, can also be used to change the list of users that are allowed to display a job log of a job with *ALLOBJ special authority.

Command	Referenced Object	Authority Needed	
		For Object	For Library
[6] To use this command, job control *JOBCTL special authority is required.			
[7] The user profile under which the submitted job runs is checked for authority to the referenced object. The adopted authority of the user submitting or changing the job is not used.			
[8] If the job being transferred is an interactive job, the following restrictions apply: • The job queue where the job is placed must be associated with an active subsystem. • The work station associated with the job must have a corresponding work station entry in the subsystem description associated with the new subsystem. • The work station associated with the job must not have another job associated with it that has been suspended by means of the Sys Req (System Request) key. The suspended job must be canceled before the Transfer Job command can run. • The job must not be a group job.			
[9] Both the user submitting the job and the user profile under which the job will run are checked for authority to the referenced object.			
[10] The user submitting the job is checked for authority to the referenced object.			
[11] The adopted authority of the user issuing the CHGJOB or SBMJOB command is used.			
[12] You must be authorized to the user profile and the job description; the user profile must also be authorized to the job description.			
[13] To change certain job attributes, even in the user's own job, requires job control (*JOBCTL) and all object (*ALLOBJ) special authorities.			
[14] Any user can run these commands for jobs running under his own user profile. A user with job control (*JOBCTL) special authority can run these commands for any job.			
[15] A user trace buffer is a user space (*USRSPC) object in library QUSRSYS by the name QPOZnnnnnn, where 'nnnnnn' is the job number of the job using the user trace facility.			

Job description commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGJOBD	Job description	*OBJOPR, *OBJMGT, *READ	
	User profile (USER)	*USE	*EXECUTE
CPYAUDJRNE[8]	Output file already exists	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Output file does not exist		*EXECUTE *ADD
CRTJOBD (Q)	Job description		*READ, *ADD
	User profile (USER)	*USE	
DLTJOBD	Job description	*OBJEXIST	*EXECUTE
DSPJOBD	Job description	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			
WRKJOBD	Job description	Any	*USE

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] You must have *ALLOBJ or *AUDIT special authority to use this command.			

Job queue commands

Command	Referenced Object	Job Queue Parameters [4]		Special Authority	Authority Needed	
		AUTCHK	OPRCTL		For Object	For Library
CLRJOBQ [1]	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ [1]	Job queue					*READ, *ADD
DLTJOBQ	Job queue				*OBJEXIST	*EXECUTE
HLDJOBQ [1]	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [5]						
RLSJOBQ [1]	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ [1,3]	Job queue	*DTAAUT			*READ	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

[1] If you have *SPLCTL special authority, you do not need any authority to the job queue but you need authority to the library containing the job queue.

[2] You must be the owner of the job queue.

[3] If you request to work with all job queues, your list display includes all the job queues in libraries to which you have *EXECUTE authority.

[4] To display the job queue parameters, use the QSPRJOBQ API.

[5] You must have *ALLOBJ or *AUDIT special authority to use this command.

Job schedule commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDJOBSCDE	Job schedule	*CHANGE	*EXECUTE
	Job description [1]	*USE	*EXECUTE
	Job queue [1,2]	*READ	*EXECUTE
	User profile	*USE	*EXECUTE
	Message queue [1]	*USE, *ADD	*EXECUTE
CHGJOBSCDE [3]	Job schedule	*CHANGE	*EXECUTE
	Job description [1]	*USE	*EXECUTE
	Job queue [1,2]	*READ	*EXECUTE
	User profile	*USE	*EXECUTE
	Message queue [1]	*USE, *ADD	*EXECUTE
HLDJOBSCDE [3]	Job schedule	*CHANGE	*EXECUTE
RLSJOBSCDE [3]	Job schedule	*CHANGE	*EXECUTE
RMVJOBSCDE [3]	Job schedule	*CHANGE	*EXECUTE
WRKJOBSCDE [4]	Job schedule	*USE	*EXECUTE

[1] Both the user profile adding the entry and the user profile under which the job will run are checked for authority to the referenced object.

[2] Authority to the job queue cannot come from adopted authority.

[3] You must have *JOBCTL special authority or have added the entry.

[4] To display the details of an entry (option 5 or print format *FULL), you must have *JOBCTL special authority or have added the entry.

Journal commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library or Directory
ADDRMTJRN	Source journal	*CHANGE, *OBJMGT	*EXECUTE
	Target journal		*EXECUTE, *ADD
APYJRNCHG (Q)	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Non-integrated file system objects whose journaled changes are being applied	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	integrated file system objects whose journal changes are being applied	*RW, *OBJMGT	*RX (if subtree *ALL)

Command	Referenced Object	Authority Needed	
		For Object	For Library or Directory
APYJRNCHGX	Journal	*USE	
	Journal receiver	*USE	
	File	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
CHGJRN (Q)	Journal receiver, if specified	*OBJMGT, *USE	*EXECUTE
	Attached journal receiver	*OBJMGT, *USE	*EXECUTE
	Journal	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Journal if RCVSIZOPT(*MINFIXLEN) is specified.	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNOBJ [9]	Non-integrated file system objects	*READ, *OBJMGT	*EXECUTE
	Integrated file system objects	*R, *OBJMGT	
	Object path SUBTREE(*ALL)	*RX, *OBJMGT	
	Object path SUBTREE(*NONE)	*R, *OBJMGT	
	Parent directory	*X	
	Path Prefix	Refer to "General rules for object authorities on commands" on page 157.	
CHGRMTJRN	Source journal	*CHANGE, *OBJMGT	*EXECUTE
	Source journal	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File	*USE	*EXECUTE
CRTJRN	Journal		*READ, *ADD
	Journal receiver	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Journal	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			
DSPJRN [6]	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, the specified file has been deleted from the system or *IGNFILSLT is specified for any selected journal codes or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File if specified	*USE	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPJRNMNU[1]			
ENDJRN	See "Integrated file system commands" on page 200.		
ENDJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library or Directory
ENDJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP [2]			
JRNPF [3]			
RCVJRNE	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, the specified file has been deleted from the system or *IGNFILSLT is specified for any selected journal codes or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File	*USE	*EXECUTE
	Exit program	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Non-integrated file system objects whose journaled changes are being removed	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, the specified file has been deleted from the system or *IGNFILSLT is specified for any selected journal codes or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File	*USE	*EXECUTE
RMVRMTJRN	Source journal	*CHG, *OBJMGT	
SNDJRNE	Journal	*OBJOPR, *ADD	*EXECUTE
	Non-integrated file system object if specified	*OBJOPR	*EXECUTE
	integrated file system object if specified	*R	*X
STRJRN	See “Integrated file system commands” on page 200.		
STRJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNPF	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library or Directory
WRKJRN [4] (Q)	Journal	*USE	*READ[7]
	Journal receiver if receiver information is requested	*USE	*EXECUTE
	File if forward or backout recovery is requested	*OBJMGT, *CHANGE	*EXECUTE
	Objects that are deleted during recovery	*OBJEXIST	*EXECUTE
WRKJRNA [6]	Journal	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
	Journal receiver [5]	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE

1 See the WRKJRN command (this command has the same function)

2 See the STRJRNAP command.

3 See the STRJRNPF command.

4 Additional authority is required for specific functions called during the operation selected. For example, to restore an object you must have the authority required for the RSTOBJ command.

5 *OBJOPR and *OBJEXIST authority is required for journal receivers if the option is chosen to delete receivers.

6 To specify JRN(*INTSYSJRN), you must have *ALLOBJ special authority.

7 *READ authority to the journal's library is required to display the WRKJRN menu. *EXECUTE authority to the library is required to use an option on the menu.

8 You must have *AUDIT special authority to use this command.

9 To specify PTLTNS(*ALWUSE), you must have *ALLOBJ special authority.

Journal receiver commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTJRNRCV	Journal receiver		*READ, *ADD
DLTJRNRCV	Journal receiver	*OBJOPR, *OBJEXIST, and a data authority other than *EXECUTE	*EXECUTE
	Journal	*OBJOPR	*EXECUTE
DSPJRNRCVA	Journal receiver	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
	Journal, if attached	*OBJOPR	*EXECUTE
WRKJRNRCV [1], [2], [3]	Journal receiver	Any authority	*USE

Command	Referenced Object	Authority Needed	
		For Object	For Library

[1] To use an individual operation, you must have the authority required by the operation.

[2] *OBJOPR and *OBJEXIST authority is required for journal receivers if the option is chosen to delete receivers.

[3] *OBJOPR and a data authority other than *EXECUTE is required for journal receivers if the option is chosen to display the description.

Language commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTBNDC	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTBNDCBL	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Binding directory	*USE	*EXECUTE
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTBNDCL	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTBNDCPP	Source File	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Headers generated by TEMPLATE parameter	*USE	*EXECUTE
CRTBNDRPG	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Binding directory	*USE	*EXECUTE
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCBLMOD	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCLD	Source file	*USE	*EXECUTE
	Locale object - REPLACE(*NO)		*READ, *ADD
	Locale object - REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTCLMOD	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCLPGM	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCBLPGM (COBOL/400* licensed program or S/38 environment)	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCMOD	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTCPPMOD	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Headers generated by TEMPLATE parameter	*USE	*EXECUTE
CRTRPGMOD	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTRPGPGM (RPG/400* licensed program and S/38 environment)	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTRPTPGM (RPG/400® licensed program and S/38 environment)	Source file	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Source file for generated RPG program	Refer to "General rules for object authorities on commands" on page 157.	
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTS36CBL (S/36 environment)	Source file	*USE	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTS36RPG	Source file	*USE	*READ, *ADD
	Program: REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTS36RPGR	Source file	*USE	*READ, *ADD
	Display file: REPLACE(*NO)		*READ, *ADD
	Display file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
CRTS36RPT	Source file	*USE	*EXECUTE
	Source file for generated RPG program	Refer to "General rules for object authorities on commands" on page 157.	
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTSQLC OS/400' (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLCI (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Object: REPLACE(*NO)		*READ, *ADD
	Object: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLCBL (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTSQLCBLI (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Object: REPLACE(*NO)		*READ, *ADD
	Object: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLCPPI (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLFTN (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTSQLPLI (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLRPG (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLRPGI (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Object: REPLACE(*NO)		*READ, *ADD
	Object: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CVTRPGSRC	Source file	*USE	*EXECUTE
	Output file	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Log file	*OBJOPR, *OBJMGT, *ADD	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CVTSQLCPP [1]	Source file	*OBJOPR, *READ	*EXECUTE
	To Source file	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Data description specifications	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
ENDCBLDBG (COBOL/400® licensed program or S/38 environment)	Program	*CHANGE	*EXECUTE
ENTCBLDBG (S/38 environment)	Program	*CHANGE	*EXECUTE
DLTCLD	Locale object	*OBJEXIST, *OBJMGT	*EXECUTE
RTVCLDSRC	Locale object	*USE	*EXECUTE
	To-file	Refer to "General rules for object authorities on commands" on page 157.	
RUNSQLSTM (SQL/400® licensed program) [1]	Source file	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRREXPRC	Source file	*USE	*EXECUTE
	Exit program	*USE	*EXECUTE
STRSQL (DB2 Query Manager and SQL Development for OS/400 licensed program) [1]	Sort sequence table	*USE	*EXECUTE
	Printer device description	*USE	*EXECUTE
	Printer output queue	*USE	*EXECUTE
	Printer file	*USE	*EXECUTE

[1] See the **Authorization, privileges and object ownership** information in the **DB2 for iSeries SQL Reference** (located in the iSeries Information Center) for more information about security requirements for structured query language (SQL) statements.

Library commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library Being Acted On
ADDLIBLE	Library		*USE
CHGCURLIB	New current library		*USE
CHGLIB [8]	Library		*OBJMGT
CHGLIBL	Every library being placed in the library list		*USE
CHGSYSLIBL (Q)	Libraries in new list		*USE
CLRLIB [3]	Every object being deleted from library	*OBJEXIST	*USE
	Object types *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ[14], *SBSD[14]	See the authority required by the DLTxxx command for the object type	
	ASP device (if specified)	*USE	
CPYLIB [4]	From-Library		*USE
	To-library, if it exists		*USE, *ADD
	CHKOBJ, CRTDUPOBJ commands	*USE	
	CRTLIB command, if the target library is being created	*USE	
	Object being copied	The authority that is required when you use the CRTDUPOBJ command to copy the object type.	
CRTLIB [9]	ASP device (if specified) *USE		
DLTLIB [3]	Every object being deleted from library	*OBJEXIST	*USE, *OBJEXIST
	Object types *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ, *SBSD[14]	See the authority required by the DLTxxx command for the object type	
	ASP device (if specified)	*USE	
DSPLIB	Library		*READ
	Objects in the library [5]	Some authority other than *EXCLUDE	
	ASP device (if specified)	*EXECUTE	
DSPLIBD	Library		Some authority other than *EXCLUDE
EDTLIBL	Library to add to list		*USE
RCLLIB	Library		*USE, *OBJEXIST

Command	Referenced Object	Authority Needed	
		For Object	For Library Being Acted On
RSTLIB [7] (Q)	Media definition	*USE	*EXECUTE
	Library, if it does exist		*READ, *ADD
	Message queues being restored to library where they already exist	*OBJOPR, *OBJEXIST [7]	*EXECUTE. *READ, *ADD
	Programs that adopt authority	Owner or *ALLOBJ and *SECADM	*EXECUTE
	Library saved if VOL(*SAVVOL) is specified		*USE [6]
	Every object being restored over in the library	*OBJEXIST [3]	*EXECUTE, *READ, *ADD
	User profile owning objects being created	*ADD [6]	
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE	*EXECUTE
RSTLIB [7] (Q)	Tape (QSYSTAP) or diskette (QSYSDKT) file	*USE [6]	*EXECUTE
	QSYS/QPSRLDSP print file, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Save file	*USE	*EXECUTE
	Optical File (OPTFILE)[12]	*R	N/A
	Path prefix of optical file (OPTFILE)[12]	*X	N/A
	Optical volume[11]	*USE	
	ASP device description[15]	*USE	
RSTS36LIBM	From-file	*USE	*EXECUTE
	To-file	*CHANGE	*EXECUTE
	To-library	*CHANGE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
RTVLIBD	Library		Some authority other than *EXCLUDE

Command	Referenced Object	Authority Needed	
		For Object	For Library Being Acted On
SAVLIB	Every object in the library	*OBJEXIST [6]	*READ, *EXECUTE
	Media definition	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*USE, *ADD, *OBJMGT	*EXECUTE
	Save active message queue	*OBJOPR, *ADD	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	QSYS/QASAVOBJ field reference file, if output file is specified and does not exist	*USE [6]	*EXECUTE
	QSYS/QPSAVOBJ print file	*USE [6]	*EXECUTE
SAVLIB	Optical File[12]	*RW	N/A
	Parent Directory of optical file (OPTFILE)[12]	*WX	N/A
	Path Prefix of optical file (OPTFILE)[12]	*X	N/A
	Root Directory (/) of Optical Volume[12, 13]	*RWX	N/A
	Optical volume[11]	*CHANGE	
	ASP device description[15]	*USE	
SAVRSTLIB	ASP device description[15]	*USE	
SAVS36LIBM	Save to a physical file	*OBJOPR, *OBJMGT	*EXECUTE
	Either QSYSDKT for diskette or QSYSTAP for tape, and all commands need authority to the device	*OBJOPR	*EXECUTE
	Save to a physical file if MBROPT(*ADD) is specified	*ADD	*READ, *ADD
	Save to a physical file if MBROPT(*REPLACE) is specified	*ADD, *DLT	*EXECUTE
	From-library		*USE
WRKLIB [10.]	Library		*USE

Command	Referenced Object	Authority Needed	
		For Object	For Library Being Acted On
[1] The authority needed for the library being acted upon is indicated in this column. For example, to add the library CUSTLIB to a library list using the ADDLIBLE command requires Use authority to the CUSTLIB library.			
[2] The authority needed for the QSYS library is indicated in this column, because all libraries are in QSYS library.			
[3] If object existence is not found for some objects in the library, those objects are not deleted, and the library is not completely cleared and deleted. Only authorized objects are deleted.			
[4] All restrictions that apply to the CRTDUPOBJ command, also apply to this command.			
[5] If you do not have authority to an object in the library, the text for the object says *NOT AUTHORIZED.			
[6] If you have *SAVSYS special authority, you do not need the authority specified.			
[7] You must have *ALLOBJ special authority to specify ALWOBJDIF(*ALL).			
[8] You must have *AUDIT special authority to change the CRTOBJAUD value for a library. *OBJMGT is **not** required if you change only the CRTOBJAUD value. *OBJMGT **is** required if you change the CRTOBJAUD value and other values.			
[9] You must have *AUDIT special authority to specify a CRTOBJAUD value other than *SYSVAL.			
[10] You must have the authority required by the operation to use an individual operation.			
[11] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function.			
[12] This authority check is only made when the Optical media format is Universal Disk Format.			
[13] This authority check is only made when you are clearing the optical volume.			
[14] This object is allowed on independent ASP.			
[15] Authority required only if save or restore operation requires a library name space switch.			

License key commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDLICKEY (Q)	Output file	*USE	*EXECUTE
DSPLICKEY (Q)	Output file	Refer to "General rules for object authorities on commands" on page 157.	
RMVLICKEY (Q)	Output file	*CHANGE	*EXECUTE

Licensed program commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGLICINF (Q)	WRKLICINF command	*USE	*EXECUTE
DLTLICPGM [1,2] (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM [1,2] (Q)			
SAVLICPGM [1,2] (Q)			
WRKLICINF (Q)			

[1] Some licensed programs can be deleted, saved, or restored only if you are enrolled in the system distribution directory.

[2] If deleting, restoring, or saving a licensed program that contains folders, all restrictions that apply to the DLTDLO command also apply to this command.

[3] To use individual operations, you must have the authority required by the individual operation.

Line description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGLINASC [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP[2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
	Connection list (CNNLSTIN or CNNLSTOUT)	*USE	*EXECUTE
	Network interface description (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS [2]	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CRTLINASC [2]	Controller description (CTL and SWTCTLLST)	*USE	*EXECUTE
	Line description		*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTLINBSC [2]	Controller description (SWTCTLLST and CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINDDI [2]	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Controller description (NETCTL)	*USE	*EXECUTE
CRTLINETH [2]	Controller description (NETCTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Network server description (NWS)	*USE	*EXECUTE
CRTLINFAX [2]	Line description		*READ, *ADD
	Controller description	*USE	*EXECUTE
CRTLINFR [2]	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Controller description (NETCTL)	*USE	*EXECUTE
CRTLINPPP[2]	Controller description (NETCTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINSDLC [2]	Controller description (CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINTDLC [2]	Controller description (WSC and CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINTRN [2]	Controller description (NETCTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Network server description (NWS)	*USE	*EXECUTE
CRTLINX25 [2]	Controller description (SWTCTLLST)	*USE	*EXECUTE
	Permanent virtual circuit (PVC) controller description (LGLCHLE)	*USE	*EXECUTE
	Line description		*READ, *ADD
	Connection list (CNNLSTIN or CNNLSTOUT)	*USE	*EXECUTE
	Network interface description (NWI or SWTNWILST)	*USE	*EXECUTE
CRTLINWLS [2]	Line description		*READ, *ADD
	Controller description (NETCTL)	*USE	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
DLTLIND	Line description	*OBJEXIST	*EXECUTE
DSPLIND	Line description	*USE	*EXECUTE
ENDLINRCY	Line description	*OBJOPR	*EXECUTE
PRTCMNSEC [2, 3]			
RSMLINRCY	Line description	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
WRKLIND [1]	Line description	*OBJOPR	*EXECUTE

[1] To use individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

[3] To use this command, you must have *ALLOBJ special authority.

Local area network (LAN) commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require any object authorities:			
ADDLANADPI	DSPLANADPP	RMVLANADPT (Q)	WRKLANADPT
CHGLANADPI	DSPLANSTS	RMVLANADPI	

Locale commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTLOCALE	Source file	*USE	*USE, *ADD
DLTLOCALE	Locale	*OBJEXIST	*USE

Mail server framework commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

This command does not require any object authorities:	
ENDMSF (Q)	STRMSF (Q)

Media commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDTAPCTG	Tape Library description	*USE	*EXECUTE
CFGDEVMLB[1]	Tape Library description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Tape Library description	*USE	*EXECUTE
CHGJOBMLBA[4]	Tape Library description	*CHANGE	*EXECUTE
CHGTAPCTG	Tape Library description	*USE	*EXECUTE
CHKDKT	Diskette device description	*USE	*EXECUTE
CHKTAP	Tape device description	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CLRDKT	Diskette device description	*USE	*EXECUTE
CRTTAPCGY	Tape Library description		
DLTDKTLBL	Diskette device description	*USE	*EXECUTE
DLTMEDDFN	Media definition	*OBJEXIST	*EXECUTE
DLTTAPCGY	Tape Library description		
DMPTAP (Q)	Tape device description	*USE	*EXECUTE
DSPDKT	Diskette device description	*USE	*EXECUTE
DSPTAP	Tape device description	*USE	*EXECUTE
DSPTAPCGY	Tape Library description		
DSPTAPCTG	Tape Library description	*USE	*EXECUTE
DSPTAPSTS	Tape Library description	*USE	*EXECUTE
DUPDKT	Diskette device description	*USE	*EXECUTE
DUPTAP	Tape device description	*USE	*EXECUTE
INZDKT	Diskette device description	*USE	*EXECUTE
INZTAP	Tape device description	*USE	*EXECUTE
RMVTAPCTG	Tape Library description	*USE	*EXECUTE
RNMDKT	Diskette device description	*USE	*EXECUTE
SETTAPCGY	Tape Library description	*USE	*EXECUTE
WRKMLBRSCQ [3]	Tape Library description	*USE	*EXECUTE
WRKMLBSTS [2] (Q)	Tape Library description	*USE	*EXECUTE
WRKTAPCTG	Tape Library description	*USE	*EXECUTE

[1] To use this command, you must have *IOSYSCFG special authority.

[2] To use individual operation, you must have the authority required by the operation.

[3] To change the session media library attributes, you must have *CHANGE authority to the Tape Library description. To change the priority or work with another users job you must have *JOBCTL special authority.

[4] To change the priority or work with another user's job you must have *JOBCTL special authority.

Menu and panel group commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGMNU	Menu	*CHANGE	*USE
CRTMNU	Source file	*USE	*EXECUTE
	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTPNLGRP	Panel group: Replace(*NO)		*READ, *ADD
	Panel group: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Source file	*USE	*EXECUTE
	Include file	*USE	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Source file	*USE	*EXECUTE
	Message files named in source	*OBJOPR, *OBJEXIST	*EXECUTE
	To-file source file when TOMBR is not *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	Menu display file when REPLACE(*YES) is specified	*OBJOPR, *OBJEXIST	*EXECUTE
	Command text message file	*OBJOPR, *OBJEXIST	*EXECUTE
	Create Message File (CRTMSGF) command	*OBJOPR	*EXECUTE
	Add Message Description (ADDMSGD) command	*OBJOPR	*EXECUTE
	Create Display File (CRTDSPF) command	*OBJOPR	*EXECUTE
DLTMNU	Menu	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Panel group	*OBJEXIST	*EXECUTE
DSPMNUA	Menu	*USE	*USE
GO	Menu	*USE	*USE
	Display file and message files with *DSPF specified	*USE	*EXECUTE
	Current and product libraries	*USE	
	Program with *PGM specified	*USE	*EXECUTE
WRKMNU [1]	Menu	Any	*USE
WRKPNLGRP [1]	Panel group	Any	*EXECUTE

[1] To use an individual operation, you must have the authority required by the operation.

Message commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPMSG	Message queue	*USE	*USE
	Message queue that receives the reply to an inquiry message	*USE, *ADD	*USE
	Remove messages from message queue	*USE, *DLT	*USE
RCVMSG	Message queue	*USE	*EXECUTE
	Remove messages from queue	*USE, *DLT	*EXECUTE
RMVMSG	Message queue	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Message file	*USE	*EXECUTE
SNDBRKMSG	Message queue that receives the reply to inquiry messages	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Message queue	*OBOPR, *ADD	*EXECUTE
	Message queue that receives the reply to inquiry message	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Message queue	*OBJOPR, *ADD	*EXECUTE
	Message file, when sending predefined message	*USE	*EXECUTE
	Message queue that receives the reply to inquiry message	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Message queue	*USE, *ADD	*EXECUTE
	Remove messages from queue	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Message queue	*OBJOPR, *ADD	*EXECUTE
	Message file, when sending predefined message	*USE	*EXECUTE
WRKMSG	Message queue	*USE	*USE
	Message queue that receives the reply to inquiry message	*USE, *ADD	*USE
	Remove messages from message queue	*USE, *DLT	*USE

Message description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDMSGD	Message file	*USE, *ADD	*EXECUTE
CHGMSGD	Message file	*USE, *UPD	*EXECUTE
DSPMSGD	Message file	*USE	*EXECUTE
RMVMSGD	Message file	*OBJOPR, *DLT	*EXECUTE
WRKMSGD [1]	Message file	*USE	*EXECUTE

[1] To use individual operations, you must have the authority required by the individual operation.

Message file commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGMSGF	Message file	*USE, *DLT	*EXECUTE
CRTMSGF	Message file		*READ, *ADD
DLTMSGF	Message file	*OBJEXIST	*EXECUTE
DSPMSGF	Message file	*USE	*EXECUTE
MRGMSGF	From-message file	*USE	*EXECUTE
	To-message file	*USE, *ADD, *DLT	*EXECUTE
	Replace-message file	*USE, *ADD	*EXECUTE
WRKMSGF [1.]	Message file	Any authority	*USE

[1] To use individual operations, you must have the authority required by the individual operation.

Message queue commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGMSGQ	Message queue	*USE, *DLT	*EXECUTE
CLRMSGQ	Message queue	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Message queue		*READ, *ADD
DLTMSGQ	Message queue	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ [1]	Message queue	Any authority	*USE

[1] To use individual operations, you must have the authority required by the individual operation.

Migration commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
RCVMGRDTA	File	*ALL	*READ, *ADD
	Device	*CHANGE	*EXECUTE
SNDMGRDTA	File	*ALL	*READ, *ADD
	Device	*CHANGE	*EXECUTE
The following commands do not require any object authorities. They are shipped with public authority *EXCLUDE. You must have *ALLOBJ special authority to use these commands.			

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANZS34OCL	CVTS36JOB	MGRS36DSPF	MIGRATE
ANZS36OCL	CVTS36QRY	MGRS36ITM	QMUS36
CHGS34LIBM	CVTS38JOB	MGRS36LIB	RESMGRNAM
CHKS36SRCA	GENS36RPT	MGRS36MNU	RSTS38AUT
CVTBASSTR	GENS38RPT	MGRS36MSGF	STRS36MGR
CVTBASUNF	MGRS36	MGRS36QRY [1]	STRS38MGR
CVTBGUDTA	MGRS36APF [1]	MGRS36RPG	
CVTS36CFG	MGRS36CBL	MGRS36SEC	
CVTS36FCT	MGRS36DFU [1]	MGRS38OBJ	

[1] You must have *ALLOBJ special authority and have OS/400 option 4 installed.

Mode description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGMODD [2]	Mode description	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD [2]	Mode description		*READ, *ADD
CHGSSNMAX	Device description	*OBJOPR	*EXECUTE
DLTMODD	Mode description	*OBJEXIST	*EXECUTE
DSPMODD	Mode description	*USE	*EXECUTE
DSPMODSTS	Device	*OBJOPR	*EXECUTE
	Mode description	*OBJOPR	*EXECUTE
ENDMOD	Device description	*OBJOPR	*EXECUTE
STRMOD	Device description	*OBJOPR	*EXECUTE
WRKMODD [1]	Mode description	*OBJOPR	*EXECUTE

[1] To use individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

Module commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGMOD	Module	*OBJMGT, *USE	*USE
	Module, if OPTIMIZE specified	*OBJMGT, *USE	*USE, *ADD, *DLT
	Module, if FRCCRT(*YES) specified	*OBJMGT, *USE	*USE, *ADD, *DLT
	Module, if ENBPRFCOL specified	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Module	*OBJEXIST	*EXECUTE
DSPMOD	Module	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
RTVBNDSRC [1]	Module	*USE	*EXECUTE
	*SRVPGMs and modules specified with *SRVPGMs	*USE	*EXECUTE
	Database source file if file and member exists and MBROPT(*REPLACE) is specified.	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Database source file if file and member exists and MBROPT(*ADD) is specified	*OBJOPR, *ADD	*EXECUTE
	Database source file if file exists and member needs to be created.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Database source file if file and member needs to be created.		*EXECUTE, *READ, *ADD
	CRTSCRPF command if file does not exist		*EXECUTE
	ADDPFM command if member does not exist		*EXECUTE
	RGZPFM command to reorganize source file member	*OBJMGT	*EXECUTE
WRKMOD [2]	Module	Any authority	*USE

[1] You need *USE authority to the:

- CRTSRCPF command if the file does not exist.
- ADDPFM command if the member does not exist.
- RGZPFM command so the source file member is reorganized. Either *CHANGE and *OBJALTER authorities or *OBJMGT authority is required to reorganize the source file member. The RTVBNDSRC command function then completes with the source file member reorganized with sequence numbers of zero.

[2] To use individual operations, you must have the authority required by the individual operation.

NetBIOS description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGNTBD [2]	NetBIOS description	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD [2]	NetBIOS description		*EXECUTE
DLTNTBD	NetBIOS description	*OBJEXIST	*EXECUTE
DSPNTBD	NetBIOS description	*USE	*EXECUTE
WKRNTBD[1]	NetBIOS description	*OBJOPR	*EXECUTE

[1] To use individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

Network commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDNETJOBE (Q)	User profile in the network job entry	*USE	
APING	Device description	*CHANGE	
AREXEC	Device description	*CHANGE	
CHGNETA (Q) [4]			
CHGNETJOBE (Q)	User profile in the network job entry	*USE	
DLTNETF [2]	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPNETA			
RCVNETF [2]	To-file member does not exist, MBROPT(*ADD) specified	*OBJMGT, *USE	*EXECUTE, *ADD
	To-file member does not exist, MBROPT(*REPLACE) specified	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	To-file member exists, MBROPT(*ADD) specified	*USE	*EXECUTE
	To-file member exists, MBROPT(*REPLACE) specified	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	User profile in the network job entry	*USE	
RTVNETA			
RUNRMTCMD	Device description	*CHANGE	
SNDNETF	Physical file or save file	*USE	*EXECUTE
SNDNETMSG to a local user	Message queue	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Device description	*CHANGE	
WRKNETF [2,3]			
WRKNETJOBE [3]	QUSRSYS/QANFNJE	*USE	*EXECUTE

[1] You must have *ALLOBJ special authority.

[2] A user can run these commands on the user's own network files or on network files owned by the user's group profile. *ALLOBJ special authority is required to process network files for another user.

[3] To use an individual operation, you must have the authority required by that operation.

[4] To change some network attributes, you must have *IOSYSCFG, or *ALLOBJ and *IOSYSCFG special authorities.

Network file system commands

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDMFS [1,3]	dir_to_be_ mounted_over	*DIR	"root"	*W
CHGNFSEXP [1,2]	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
DSPMFSINF	some_dirs	*DIR	"root"	*RX
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ENDNFSSVR [1,4]	none			
EXPORTFS [1,2]	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
MOUNT [1,3]	dir_to_be_ mounted_over	*DIR	″root″	*W
RLSIFSLCK [1]	object	*STMF	″root″, QOpenSys, UDFS	*R
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
RMVMFS [1]				
STATFS	some_dirs	*DIR	″root″	*RX
	Path prefix	Refer to "General rules for object authorities on commands" on page 157.		
STRNFSSVR [1]	none			
UNMOUNT [1]				

[1] To use this command, you must have *IOSYSCFG special authority.

[2] When the -F flag is specified and the /etc/exports file does not exist, you must have write, execute (*WX) authority to the /etc directory. When the -F flag is specified and the /etc/exports file does exist, you must have read, write (*RW) authority to the /etc/exports file and *X authority to the /etc directory.

[3] The directory that is mounted over (dir_to_be_mounted_over) is any integrated file system directory that can be mounted over.

[4] To end any daemon jobs started by someone else, you must have *JOBCTL special authority.

Network interface description commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGNWIFR [2]	Network interface description	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR [2]	Network interface description		*READ, *ADD
	Line description (DLCI)	*USE	*EXECUTE
DLTNWID	Network interface description	*OBJEXIST	*EXECUTE
DSPNWID	Network interface description	*USE	*EXECUTE
WRKNWID [1]	Network interface description	*OBJOPR	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

[2] To use this command, you must have *IOSYSCFG special authority.

Network server commands

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDNWSSTGL [2]	Path (/QFPNWSSTG)	*DIR	″root″	*X
	Parent directory (name of the storage space)	*DIR	″root″	*WX
	Files that make up the storage space	*FILE	″root″	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSUSRA [4]	User Profile	*USRPRF		*OBJMGT, *USE
CRTNWSSTG [2]	Path (root and /QFPNWSSTG)	*DIR	″root″	*WX
DLTNWSSTG [2]	Path (/QFPNWSSTG)	*DIR	″root″	*WX
	Parent directory (name of the storage space)	*DIR	″root″	*RWX, *OBJEXIST
	Files that make up the storage space	*FILE	″root″	*OBJEXIST
DSPNWSSTG	Path to the storage space	*DIR	″root″	*X
	Files that make up the storage space	*FILE	″root″	*R
RMVNWSSTGL [2]	Path (/QFPNWSSTG)	*DIR	″root″	*X
	Parent directory (name of the storage space)	*DIR	″root″	*WX
	Files that make up the storage space	*FILE	″root″	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Path to the storage space	*DIR	″root″	*X
	Files that make up the storage space	*FILE	″root″	*R

These commands do not require any object authorities:

ADDRMTSVR	DSPNWSALS	SNDNWSMSG
CHGNWSA [4](Q)	DSPNWSSSN	WRKNWSALS
CHGNWSALS	DSPNWSSTC	WRKNWSENR
CRTNWSALS	DSPNWSUSR	WRKNWSSSN
DLTNWSALS	DSPNWSUSRA	WRKNWSSTS
DSPNWSA	SBMNWSCMD (Q) [3]	

[1] Adopted authority is not used for Network Server commands.

[2] To use this command, you must have *IOSYSCFG special authority.

[3] To use this command, you must have *JOBCTL special authority.

[4] You must have *SECADM special authority to specify a value other than *NONE for the NDSTREELST and the NTW3SVRLST parameters.

Network server description commands

Command	Referenced Object	Authority Needed	
		For Object	For QSYS Library
CHGNWSD [2]	Network server description	*CHANGE, *OBJMGT	*EXECUTE
	NetBIOS description (NTB)	*USE	*EXECUTE
CRTNWSD [2]	NetBIOS description (NTB)	*USE	*EXECUTE
	Line description (PORTS)	*USE	*EXECUTE
DLTNWSD	Network server description	*OBJEXIST	*EXECUTE
DSPNWSD	Network server description	*USE	*EXECUTE
WRKNWSD[1]	Network server description	*OBJOPR	*EXECUTE

[1] To use an individual operation, you must have the authority required by the operation.

[2] To use this command, you must have *IOSYSCFG special authority.

Node list commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDNODLE	Node list	*OBJOPR, *ADD	*EXECUTE
CRTNODL	Node list		*READ, *ADD
DLTNODL	Node list	*OBJEXIST	*EXECUTE
RMVNODLE	Node list	*OBJOPR, *READ, *DLT	*EXECUTE
WRKNODL [1]	Node list	*USE	*USE
WRKNODLE	Node list	*USE	*EXECUTE

[1] To use the individual operations, you must have the authority required by the individual operation.

Office services commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require object authorities.		
ADDACC (Q)	GRTACCAUT [2,3,6] (Q)	RVKUSRPMN [1,2]
DSPACC	GRTUSRPMN [1,2]	WRKDOCLIB [4]
DSPACCAUT	RMVACC [1] (Q)	WRKDOCPRTQ [5]
DSPUSRPMN	RVKACCAUT [1]	

[1] You must have *ALLOBJ special authority to grant or revoke access code authority or document authority for other users.

[2] Access is restricted to documents, folders, and mail that are not personal.

[3] The access code must be defined to the system (using the Add Access Code (ADDACC) command) before you can grant access code authority. The user being granted access code authority must be enrolled in the system distribution directory.

[4] You must have *SECADM special authority.

[5] Additional authorities are required for specific functions called by the operations selected. The user also needs additional authorities for any commands called during a specific function.

[6] You must have all object (*ALLOBJ) or security administrator (*SECADM) special authority to grant access code authority for other users.

Online education commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CVTEDU			
STREDU			

Operational Assistant commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			
CHGPWRSCD [3]		*USE	*EXECUTE
CHGPWRSCDE [3]		*USE	*EXECUTE
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUPL	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
DSPPWRSCD			
EDTBCKUPL [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE
ENDCLNUP [4]	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, member QCURRENT	*USE	*EXECUTE
	ASP device (if specified)	*USE	

Command	Referenced Object	Authority Needed	
		For Object	For Library
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) [5]	ASP device (if specified)	*USE	
RTVPWRSCDE	DSPPWRSCD command	*USE	
RUNBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Commands: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP[4]	QPGMR User profile	*USE	
	Job queue	*USE	*EXECUTE

[1] You must have *ALLOBJ or *SAVSYS special authority.

[2] You must have *ALLOBJ, *SECADM, and *JOBCTL special authorities.

[3] You must have *ALLOBJ and *SECADM special authorities.

[4] You must have *JOBCTL special authority.

[5] You must have *ALLOBJ special authority.

Optical commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Table 23.

Command	Referenced Object	Authority Needed		
		Object	Library	Optical Volume [1]
ADDOPTCTG (Q)	Optical Device	*USE	*EXECUTE	
ADDOPTSVR (Q)	Server CSI	*USE	*EXECUTE	
CHGDEVOPT[4]	Optical Device	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				
CHGOPTVOL	Root directory (/) of volume when changing the Text Description[5]	*W	N/A	N/A
	Optical Device	*USE	*EXECUTE	*CHANGE[3]
	Server CSI	*USE	*EXECUTE	N/A

Table 23. (continued)

Command	Referenced Object	Authority Needed		
		Object	**Library**	**Optical Volume [1]**
CPYOPT	Optical Device	*USE	*EXECUTE	*USE - Source Volume
				*ALL - Target Volume
	Each preceding dir in path of source file	*X	N/A	N/A
	Each preceding dir in path of target file	*X	N/A	N/A
	Source file (*DSTMF)[5]	*R	N/A	N/A
	Parent dir of target file	*WX	N/A	N/A
	Parent of parent dir if creating dir	*WX	N/A	N/A
CPYOPT	Target file if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target file if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
	Each dir in path that precedes source dir	*X	N/A	N/A
	Each dir in path that precedes target dir	*X	N/A	N/A
CPYOPT	Dir being copied[5]	*R	N/A	N/A
	Dir being copied if it contains entries	*RX	N/A	N/A
	Parent of target dir	*WX	N/A	N/A
	Target dir if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target dir if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
	Target dir if entries are to be created	*WX	N/A	N/A
CPYOPT	Source files	*R	N/A	N/A
	Target file if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target file if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
CRTDEVOPT[4]	Optical Device		*EXECUTE	
CVTOPTBKU	Optical Device	*USE	*EXECUTE	*ALL
DSPOPT	Path Prefix when DATA (*SAVRST)[5]	*X	N/A	N/A
	File Prefix when (*SAVRST)[2]	*R	N/A	N/A
	Optical Device	*EXECUTE	*USE	
	Server CSI	*USE	*EXECUTE	

Table 23. (continued)

Command	Referenced Object	Authority Needed		
		Object	Library	Optical Volume [1]
DSPOPTLCK				
DSPOPTSVR	Server CSI	*USE	*EXECUTE	
DUPOPT	Optical Device	*USE	*EXECUTE	*USE - Source Volume
				*ALL - Target Volume
INZOPT	Root directory (/) of volume	*RWX	N/A	N/A
	Optical Device	*USE	*EXECUTE	*ALL
RCLOPT (Q)	Optical Device	*USE	*EXECUTE	
RMVOPTCTG (Q)	Optical Device	*USE	*EXECUTE	
RMVOPTSVR (Q)	Server CSI	*USE	*EXECUTE	
WRKHLDOPTF[2]	Optical Device	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTDIR[2]	Optical Device	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTF[2]	Optical Device	*USE	*EXECUTE	*USE
	Server CSI	*USE	*EXECUTE	
WRKOPTVOL[2]	Optical Device	*USE	*EXECUTE	

[1] Optical volumes are not actual system objects. The link between the optical volume and the authorization list used to secure the volume is maintained by the optical support function.

[2] There are seven options that can be invoked from the optical utilities that are not commands themselves. These options and their required authorities to the optical volume are shown below.

Delete File: *CHANGE

Rename File: *CHANGE

Delete Directory: *CHANGE

Create Directory: *CHANGE

Rename Volume: *ALL

Release Held Optical File: *CHANGE

Save Held Optical File: *USE - Source Volume, *Change - Target Volume

[3] Authorization list management authority to the authorization list currently securing the optical volume is needed to change the authorization list used to secure the volume.

[4] To use this command, you must have *IOSYSCFG special authority.

[5] This authority check is only made when the Optical media format is Universal Disk Format (UDF).

Output queue commands

Command	Referenced Object	Output Queue Parameters		Special Authority	Authority Needed	
		AUTCHK	OPRCTL		For Object	For Library
CHGOUTQ [1]	Data queue				*READ	*EXECUTE
	Output queue	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLROUTQ [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTOUTQ	Data queue				*READ	*EXECUTE
	Output queue					*READ, *ADD
DLTOUTQ	Output queue				*OBJEXIST	*EXECUTE
HLDOUTQ [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [4]						
RLSOUTQ [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQ [1,3]	Output queue				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQD [1,3]	Output queue				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

1 If you have *SPLCTL special authority, you do not need authority to the output queue. You do need *EXECUTE authority, however, to the library for the output queue.

2 You must be the owner of the output queue.

3 If you request to work with all output queues, your list display includes all the output queues in libraries to which you have *EXECUTE authority.

4 You must have *ALLOBJ special authority to use this command.

Package commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTSQLPKG	Program	*OBJOPR, *READ	*EXECUTE
	SQL package: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	SQL package: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Package	*OBJEXIST	*EXECUTE
PRTSQLINF	Package	*OBJOPR, *READ	*EXECUTE
	Program	*OBJOPR, *READ	*EXECUTE
	Service program	*OBJOPR, *READ	*EXECUTE
STRSQL			

Performance commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-Supplied user profiles are authorized to the command. The security officer can grant *USE to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDPEXDFN (Q) [5]	PGM Library		*EXECUTE
ADDPEXFTR (Q)[5]	PGMTRG Library		*EXECUTE
	PGMFTR Library		*EXECUTE
	JVAFTR Path	*X for directory	
	PATHFTR Path	*X for directory	
ANZACCGRP (Q) [4]	QPFR/QPTPAGA0 *PGM	*USE	*EXECUTE
	Model library		*EXECUTE, *ADD
	Job description	*USE	*EXECUTE
	QPFR/QCYRBCPP *PGM	*USE	*EXECUTE
	QPFR/QCYMBREX *PGM	*USE	*EXECUTE
ANZBESTMDL (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Application libraries that contain the database files to be analyzed		*EXECUTE
	Job description	*USE	*EXECUTE
ANZDBF (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Job description	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Application libraries that contain the programs to be analyzed		*EXECUTE
	Job description	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANZPFRDTA (Q)[4]	QPFR/QACVPP *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ
ANZPFRDT2 (Q)[4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE	*CHANGE	*EXECUTE
	DLTFCNARA command (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
CFGPFRCOL (Q)	Collection library		*EXECUTE
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE	*CHANGE	*EXECUTE
	QAPGGPHF *FILE	*USE	*EXECUTE
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE	*CHANGE	*EXECUTE
CHGJOBTYP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGPEXDFN (Q)[5]	PGM Library		*EXECUTE
CHKPFRCOL (Q)			
CPYFCNARA (Q)[4]	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE in ″From″ library	*USE	*EXECUTE
	″To″ library (if QAPGGPHF *FILE does not exist)		*EXECUTE, *ADD
	QAPGGPHF *FILE in ″To″ library (if adding a new graph format or replacing an existing one)	*CHANGE	*EXECUTE
CPYGPHFMT (Q)[4]	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE in ″From″ library	*USE	*EXECUTE
	″To″ library (if QAPGPKGF *FILE does not exist)		*EXECUTE, *ADD
	QAPGPKGF *FILE in ″To″ library (if adding a new graph package or replacing an existing one)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE in ″To″ library (if adding a new graph package or replacing an existing one)	*USE	*EXECUTE
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	From library		*EXECUTE
	To library		*EXECUTE, *ADD
	Job description	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	Performance data (all QAPM* files)	*USE	*EXECUTE
	Model library		*EXECUTE, *ADD
	Job description	*USE	*EXECUTE
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE
	Library where the Functional Area is created		*EXECUTE, *ADD
	QAPTAPGP *FILE in target library (if adding a new functional area)	*CHANGE	*EXECUTE
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Library where the Graph Format is created		*EXECUTE, *ADD
	QAPGGPHF *FILE in target library (if adding a new graph format)	*CHANGE	*EXECUTE
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Library where the Graph Package is created		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE in target library (if adding a new graph package)	*USE	*EXECUTE
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Library where the historical data is created		*ADD, *READ
	Job description	*USE	*EXECUTE
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE
	To Library		*ADD, *READ
CRTPEXDTA (Q)[5]	*MGTCOL Library		*EXECUTE
	Data library[1]		*READ, *ADD[2]
CRTPFRDTA (Q)	From Library		*EXECUTE
	To Library		*ADD, *READ
	From Library		*USE
CVTPFRDTA (Q)	Job description	*USE	*EXECUTE
CVTPFRTHD (Q)	Performance data[2]		*ADD, *READ
	Model library		*EXECUTE, *ADD
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE
DLTBESTMDL (Q)[4]	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE in the functional area library	*CHANGE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTFCNARA (Q)[4]	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE in the graph format library	*CHANGE	*EXECUTE
DLTGPHFMT (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE in the graph package library	*CHANGE	*EXECUTE
DLTGPHPKG (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGHSTD *FILE in the historical data library	*CHANGE	*EXECUTE
	QAPGHSTI *FILE in the historical data library	*CHANGE	*EXECUTE
	QAPGSUMD *FILE in the historical data library	*CHANGE	*EXECUTE
DLTHSTDTA (Q)[4]	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE
DLTPEXDTA (Q)[5]	Data Library [1]		*EXECUTE, *DELETE [2]
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPTRC (Q)[5]	Library where the trace data will be stored		*EXECUTE, *ADD
	Output file (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPACCGRP (Q)[4]	QPFR/QPTPAGD0 *PGM	*USE	*EXECUTE
	Format or package library		*EXECUTE
	Historical data library		*EXECUTE
	Output file library		*EXECUTE, *ADD
	Output queue	*USE	*EXECUTE
	Job description	*USE	*EXECUTE
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Historical data library		*EXECUTE
DSPPFRDTA (Q) [4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Format or package library		*EXECUTE
	Performance data[2]		*EXECUTE
	Output file library		*EXECUTE, *ADD
	Output queue	*USE	*EXECUTE
	Job description	*USE	*EXECUTE
DSPPFRGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Output file library		*EXECUTE
	Job description	*USE	*EXECUTE
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDPEX (Q)[5]	Data Library [1]		*READ, *ADD [2]
ENDPFRCOL (Q)			

Command	Referenced Object	Authority Needed	
		For Object	For Library
PRTACTRPT (Q)[4]	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Performance data[2]	*USE	*ADD, *READ
	Job description	*USE	*EXECUTE
PRTCPTRPT (Q)[4]	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ
	Job description	*USE	*EXECUTE
PRTJOBRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ
	Job description	*USE	*EXECUTE
PRTJOBTRC (Q)[4]	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Job trace file (QAPTTRCJ) library		*EXECUTE
	Job description	*USE	*EXECUTE
PRTLCKRPT (Q)[4]	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE
PRTPEXRPT[5]	Data Library[1]		*EXECUTE[2]
	Outfile	*USE	*EXECUTE, *ADD
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE
PRTPOLRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ
	Job description	*USE	*EXECUTE
PRTRSCRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Performance data[2]		*ADD, *READ
	Job description	*USE	*EXECUTE
PRTSYSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Job description	*USE	*EXECUTE
PRTTNSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	Trace file (QTRJOBT) library		*EXECUTE
	Job description	*USE	*EXECUTE
PRTTRCRPT (Q)[4]	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	Output file	*OBJOPR, *ADD	*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRPEX (Q)[5]			
STRPFRCOL (Q)			
STRPFRG (Q)[4]	QPFR/QPGSTART *PGM	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRPFRT (Q)[4]	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE in the functional areas library	*CHANGE	*EXECUTE
	CHGFCNARA command (Q)	*USE	*EXECUTE
	CPYFCNARA command (Q)	*USE	*EXECUTE
	CRTFCNARA command (Q)	*USE	*EXECUTE
	DLTFCNARA command (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
WRKFCNARA (Q)[4]	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	Output file (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q)[5]			
WRKPEXFTR (Q)[5]			
WRKSYSACT (Q)[3, 4]	QPFR/QITMONCP *PGM	*USE	*EXECUTE
These commands do not require any object authorities: • ENDDBMON[3] • ENDPFRTRC (Q) • STRPFRTRC (Q)			

[1] If the default library (QPEXDATA) is specified, authority to that library is not checked.

[2] Authority is needed to the library that contains the set of database files. Authority to the individual set of database files is not checked.

[3] To use this command, you must have *JOBCTL special authority.

[4] To use this command, you must have *SERVICE special authority.

[5] To use this command, you must have *SERVICE special authority or you must be authorized to the Service Trace function of Operating System/400 through iSeries Navigator's Application Administration support. The Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_TRACE, can also be used to change the list of users that are allowed to perform trace operations.

Print descriptor group commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGPDGPRF	User profile	*OBJMGT	
CRTPDG	Print descriptor group		*READ, *ADD
DLTPDG	Print descriptor group	*OBJEXIST	*EXECUTE
DSPPDGPRF	User profile	*OBJMGT	
RTVPDGPRF	User profile	*READ	

Print Services Facility™ configuration commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGPSFCFG [1, 2]			
CRTGPSFCFG [1, 2]			*READ, *ADD
DLTPSFCFG [1, 2]	PSF Configuration	*OBJEXIST	*EXECUTE
DSPPSFCFG [1]	PSF Configuration	*USE	*EXECUTE
WRKPSFCFG [1]	PSF Configuration	*READ	*EXECUTE

[1] The PSF/400 feature is required to use this command.

[2] *IOSYSCFG special authority is required to use this command.

Problem commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDPRBACNE (Q)	Filter	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Filter	*USE, *ADD	*EXECUTE
ANZPRB (Q)	SNDSRVRQS command	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filter	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filter	*USE, *UPD	*EXECUTE
DLTPRB (Q) [3]	Command: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	Output file	Refer to "General rules for object authorities on commands" on page 157.	
PTRINTDTA (Q)			
QRYPRBSTS (Q)			
VFYCMN (Q)	Line description [1]	*USE	*EXECUTE
	Controller description [1]	*USE	*EXECUTE
	Network ID [1]	*USE	*EXECUTE
VFYOPT (Q)	Device description	*USE	*EXECUTE
VFYTAP[4] (Q)	Device description	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Device description	*USE	*EXECUTE
WRKPRB (Q) [2]	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library

[1] You need *USE authority to the communications object you are verifying.

[2] You must have *USE authority to the SNDSRVRQS command to be able to report a problem.

[3] You must have authority to DLTAPARDTA if you want the APAR data associated with the problem to be deleted also. See DLTAPARDTA in the Service Commands-Authorities Needed table to determine additional authorities that are needed.

[4] You must have *IOSYSCFG special authority when the device description is allocated by a media library device.

Program commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
The object authorities required for the CRTxxxPGM commands are listed in the Languages table in "Language commands" on page 229.			
ADDBKP [1]	Breakpoint handling program	*USE	*EXECUTE
ADDPGM [1,2]	Program	*CHANGE	*EXECUTE
ADDTRC [1]	Trace handling program	*USE	*EXECUTE
CALL	Program	*OBJOPR, *EXECUTE	*EXECUTE
	Service program [4]	*EXECUTE	*EXECUTE
CHGDBG	Debug operation	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR [1]			
CHGPGM	Program	*OBJMGT, *USE	*USE
	Program, if recreate option specified, optimization level changed, or performance data collection changed	*OBJMGT, *USE	*USE, *ADD, *DLT
	Program, if USRPRF or USEADPAUT parameter is being changed	Owner [7]	*USE, *ADD, *DLT
CHGPGMVAR [1]			
CHGPTR [1]			
CHGSRVPGM	Service program	*OBJMGT, *USE	*USE
	Service program, if recreate option specified, optimization level changed, or performance data collection changed	*OBJMGT, *USE	*USE, *ADD, *DLT
	Service program, if USRPRF or USEADPAUT parameter is being changed.	Owner [7], *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA [1]			

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTPGM	Program, Replace(*NO)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Program, Replace(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Service program specified in the BNDSRVPGM parameter.	*USE	*EXECUTE
	Module	*USE	*EXECUTE
	Binding directory	*USE	*EXECUTE
CRTSRVPGM	Service program, Replace(*NO)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Service program, Replace(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Module	*USE	*EXECUTE
	Service program specified in BNDSRVPGM parameter	*USE	*EXECUTE
	Export source file	*OBJOPR *READ	*EXECUTE
	Binding directory	*USE	*EXECUTE
CVTCLSRC	From-file	*USE	*EXECUTE
	To-file	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Program	*OBJEXIST	*EXECUTE
	Display file	*OBJEXIST	*EXECUTE
DLTPGM	Program	*OBJEXIST	*EXECUTE
DLTSRVPGM	Service program	*OBJEXIST	*EXECUTE
DMPCLPGM	CL Program	*USE	None [3]
DSPBKP [1]			
DSPDBG [1]			
DSPDBGWCH			
DSPMODSRC[2, 4]	Source file	*USE	*USE
	Any include files	*USE	*USE
	Program	*CHANGE	*EXECUTE
DSPPGM	Program	*READ	*EXECUTE
	Program, if DETAIL(*MODULE) specified	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPPGMREF	Program	*OBJOPR	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPPGMVAR [1]			
DSPSRVPGM	Service program	*READ	*EXECUTE
	Service program, if DETAIL(*MODULE) specified	*USE	*EXECUTE
DSPTRC [1]			
DSPTRCDTA [1]			
ENDCBLDBG (COBOL/400 licensed program or S/38 environment)	Program	*CHANGE	*EXECUTE
ENDDBG [1]	Source debug program	*USE	*USE
ENDRQS [1]			*EXECUTE
ENTCBLDBG (S/38 environment)	Program	*CHANGE	*EXECUTE
EXTPGMINF	Source file and database files	*OBJOPR	*EXECUTE
	Program information		*READ, *ADD
PRTCMDUSG	Program	*USE	*EXECUTE
RMVBKP [1]			
RMVPGM [1]			
RMVTRC [1]			
RSMBKP [1]			
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Database source file	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	Attention-key-handling program	*EXECUTE	*EXECUTE
SETPGMINF	Database files	*OBJOPR	*EXECUTE
	Source file	*USE	*EXECUTE
	Root program	*CHANGE	*READ, *ADD
	Subprogram	*USE	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRDBG	Program [2]	*CHANGE	*EXECUTE
	Source file [4]	*USE	*EXECUTE
	Any include files [4]	*USE	*EXECUTE
	Source debug program	*USE	*EXECUTE
	Unmonitored message program	*USE	*EXECUTE
TFRCTL [4]	Program	*USE or a data authority other than *EXECUTE	*EXECUTE
	Some language functions when using high-level languages	*READ	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
UPDPGM	Program	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Service program specified in the BNDSRVPGM parameter.	*USE	*EXECUTE
	Module	*USE	*EXECUTE
	Binding directory	*USE	*EXECUTE
UPDSRVPGM	Service Program	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Service program specified in BNDSRVPGM parameter	*USE	*EXECUTE
	Module	*USE	*EXECUTE
	Binding directory	*USE	*EXECUTE
	Export source file	*OBJOPR *READ	*EXECUTE
WRKPGM [6]	Program	Any authority	*USE
WRKSRVPGM [6]	Service program	Any authority	*USE

[1] When a program is in a debug operation, no further authority is needed for debug commands.

[2] If you have *SERVICE special authority, you need only *USE authority to the program.

[3] The DMPCLPGM command is requested from within a CL program that is already running. Because authority to the library containing the program is checked at the time the program is called, authority to the library is not checked again when the DMPCLPGM command is run.

[4] Applies only to ILE programs.

[5] See the Authorization, privileges and object ownership topic in the SQL Reference (located in the iSeries Information Center) for more information about security requirements for SQL statements.

[6] To use individual operations, you need the authority required by the individual operation.

[7] You must own the program or have *ALLOBJ and *SECADM special authorities.

Query commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANZQRY	Query definition	*USE	*EXECUTE
CHGQRYA[4]			
CRTQMFORM	Query management form: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Query management form: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTQMQRY	Query management query: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Query management query: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE
	OVRDBF command	*USE	*EXECUTE
DLTQMFORM	Query management form	OBJEXIST	*EXECUTE
DLTQMQRY	Query management query	*OBJEXIST	*EXECUTE
DLTQRY	Query definition	*OBJEXIST	*EXECUTE
RTVQMFORM	Query manager form	*OBJEXIST	*EXECUTE
	Target source file	*ALL	*READ, *ADD, *EXECUTE
	ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RTVQMQRY	Query manager query	*USE	*EXECUTE
	Target source file	*ALL	*READ, *ADD
	ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RUNQRY	Query definition	*USE	*USE
	Input files	*USE	*EXECUTE
	Output files	Refer to "General rules for object authorities on commands" on page 157.	
STRQMQRY [1]	Query management query	*USE	*EXECUTE
	Query management form, if specified	*USE	*EXECUTE
	Query definition, if specified	*USE	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
	ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM commands (if OUTPUT(*OUTFILE) is specified)	*USE	*EXECUTE
STRQMPRC [1]	Source file containing query manager procedure	*USE	*EXECUTE
	Source file containing command source file, if specified	*USE	*EXECUTE
	OVRPRTF command, if statements result in printed report or query object.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM [3]	Query management form	Any authority	*USE
WRKQMQRY [3]	Query management query	Any authority	*USE
WRKQRY [3]			

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] To run STRQM, you must have the authority required by the statements in the query. For example, to insert a row in a table requires *OBJOPR, *ADD, and *EXECUTE authority to the table. [2] Ownership or some authority to the object is required. [3] To use individual operations, you must have the authority required by the individual operation. [4] To use individual command, you must have *JOBCTL special authority.			

QSH Shell Interpreter commands

Command	Referenced object	Authority needed for object
STRQSH [1] QSH[1]	Script stream file	*RX
	Directories in path to script stream file	*X
[1] QSH is an alias for the STRQSH CL command.		

Question and Answer commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANSQST (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
ASKQST	Database file QAQAxxBBPY [1] or QAQAxxBQPY [1]	*READ	*READ
CHGQSTDB (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
CRTQSTDB [2] (Q)	Database files		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
DLTQST (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
DLTQSTDB (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
EDTQST (Q)	Database file QAQAxxBQPY [1]	*READ	*READ
LODQSTDB [2] (Q)	Database file QAQAxxBQPY [1,3]	*READ	*READ, *ADD, *EXECUTE
STRQST [4]	Database file QAQAxxBBPY [1] or QAQAxxBQPY [1]	*READ	*READ
WRKQST	Database file QAQAxxBBPY [1] QAQAxxBQPY [1]	*READ	*USE
WRKCNTINF			*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library

[1] The "xx" portion of the file name is the index of the Question and Answer database being operated on by the command. The index is a two-digit number in the range 00 to 99. To obtain the index for a particular Question and Answer database, use the WRKCNTINF command.

[2] The user profile running the command becomes the owner of newly created files, unless the OWNER parameter of the user's profile is *GRPPRF. Public authority for new files, except QAQAxxBBPY, is set to *EXCLUDE. Public authority for QAQAxxBBPY is set to *READ.

[3] Authority to the file is required only if loading a previously existing Question and Answer database.

[4] The command displays the Question and Answer menu. To use individual options, you must have the authority required by those options.

Reader commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRDBRDR	Message queue	*OBJOPR, *ADD	*EXECUTE
	Database file	*OBJOPR, *USE	*EXECUTE
	Job queue	*READ	*EXECUTE
STRDKTRDR	Message queue	*OBJOPR, *ADD	*EXECUTE
	Job queue	*READ	*EXECUTE
	Device description	*OBJOPR, *READ	*EXECUTE
These commands to not require any authority to objects:			
ENDRDR [1]	HLDRDR [1]	RLSRDR [1]	

[1] You must be the user who started the reader, or you must have all object (*ALLOBJ) or job control (*JOBCTL) special authority.

Registration facility commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Relational database commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE
	Remote location device description[7]	*CHANGE	
DSPRDBDIRE	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
These commands do not require any authority to objects:			
RMVRDBDIRE WRKRDBDIRE			
[1] Authority verified when the RDB directory entry is used.			

Resource commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPHDWRSC			
DSPSFWRSC	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
EDTDEVRSC			
WRKHDWRSC [1]			
[1] If you use the option to create a configuration object, you must have authority to use the appropriate CRT command.			

Remote job entry (RJE) commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDFCTE	Forms control table	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Device file [1,2]	*USE	*READ, *EXECUTE
	Physical file [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file [1,2] (member specified)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Message queue [1,2]	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
ADDRJECMNE	Session description	*USE, *ADD, *DLT	*READ, *EXECUTE
	BSC/CMN file [1,2]	*USE	*READ, *EXECUTE
	Device description [2]	*USE	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
ADDRJERDRE	Session description	*READ, *ADD, *DLT	*READ, *EXECUTE
	Job queue [2]	*READ	*READ, *EXECUTE
	Message queue [2]	*READ, *ADD	*READ, *EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDRJEWTRE	Session description	*READ, *ADD, *DLT	*READ, *EXECUTE
	Device file [1,2]	*USE	*READ, *EXECUTE
	Physical file [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file [1,2] (member specified)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Message queue [1,2]	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
CHGFCT	Forms control table	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Forms control table	*USE	*READ, *EXECUTE
	Device file [1,2]	*USE	*READ, *EXECUTE
	Physical file [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file [1,2] (member specified)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Message queue [1,2]	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
CHGRJECMNE	Session description	*USE	*READ, *EXECUTE
	BSC/CMN file [1,2]	*USE	*READ, *EXECUTE
	Device description [2]	*USE	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
CHGRJERDRE	Session description	*USE, *ADD, *DLT	*READ, *EXECUTE
	Job queue [2]	*USE	*READ, *EXECUTE
	Message queue [2]	*USE, *ADD	*READ, *EXECUTE
CHGRJEWTRE	Session description	*USE	*READ, *EXECUTE
	Device File [1,2]	*USE	*READ, *EXECUTE
	Physical file [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file [1,2] (member specified)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Message queue [1,2]	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
CHGSSND	Session description	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Job queue [1,2]	*USE	*EXECUTE
	Message queue [1,2]	*USE, *ADD	*EXECUTE
	Forms control table [1,2]	*USE	*EXECUTE
	QUSER user profile	*USE	*EXECUTE
CNLRJERDR	Session description	*USE	*EXECUTE
	Message queue	*USE, *ADD	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CNLRJEWTR	Session description	*USE	*EXECUTE
	Message queue	*USE, *ADD	*EXECUTE
CRTFCT	Forms control table		*READ, *ADD
CRTRJEBSCF	BSC file		*READ, *EXECUTE, *ADD
	Source physical file (DDS)	*READ	*EXECUTE
	Device description	*READ	*EXECUTE
CRTRJECFG	Session description		*READ, *ADD, *UPD, *OBJOPR
	Job queue		*READ, *ADD
	Job description		*READ, *OBJOPR, *ADD
	Subsystem description		*READ, *OBJOPR, *ADD
	Message queue		*READ, *ADD
	CMN file		*READ, *EXECUTE, *ADD
	BSC file		*READ, *EXECUTE, *ADD
	Printer file		*USE, *ADD
CRTRJECFG	Physical file		*EXECUTE, *ADD
	User profile QUSER [3]	*USE	*EXECUTE
	Output queue	*READ	*EXECUTE
	Forms control table	*READ	*READ
	Device description		*EXECUTE
	Controller description		*EXECUTE
	Line description		*EXECUTE
CRTRJECMNF	Communication file		*READ, *EXECUTE, *ADD
	Source physical file (DDS)	*READ	*EXECUTE
	Device description	*READ	*EXECUTE
CRTSSND	Session description		*READ, *ADD, *UPD, *OBJOPR
	Job queue [1,2]	*USE	*EXECUTE
	Message queue [1,2]	*USE, *ADD	*EXECUTE
	Forms control table [1,2]	*USE	*EXECUTE
	QUSER user profile	*USE	*EXECUTE
CVTRJEDTA	Forms control table	*USE	*EXECUTE
	Input file	*USE, *UPD	*EXECUTE
	Output file (RJE generates member)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Output file (member specified)	*USE, *ADD	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTFCT	Forms control table	*OBJEXIST	*EXECUTE
DLTRJECFG	Session description	*OBJEXIST	*EXECUTE
	Job queue	*OBJEXIST	*EXECUTE
	BSC/CMN file	*OBJEXIST, *OBJOPR	*EXECUTE
	Physical file	*OBJEXIST, *OBJOPR	*EXECUTE
	Printer file	*OBJEXIST, OBJOPR	*EXECUTE
	Message queue	*OBJEXIST, *USE, *DLT	*EXECUTE
	Job description	*OBJEXIST	*EXECUTE
	Subsystem description	*OBJEXIST, *USE	*EXECUTE
	Device description [4]	*OBJEXIST	*EXECUTE
	Controller description [4]	*OBJEXIST	*EXECUTE
	Line description [4]	*OBJEXIST	*EXECUTE
DLTSSND	Session description	*OBJEXIST	*EXECUTE
DSPRJECFG	Session description	*READ	*EXECUTE
ENDRJESSN [5]	Session description	*USE	*EXECUTE
RMVFCTE	Forms control table	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJECMNE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Session description	*USE	*EXECUTE
SBMRJEJOB	Session description	*USE	*EXECUTE
	Input file [6]	*USE	*EXECUTE
	Message queue	*USE, *ADD	*EXECUTE
	Job-related objects [7]		
SNDRJECMD	Session description	*USE	*EXECUTE
STRRJECSL	Session description	*USE	*EXECUTE
	Message queue	*USE	*EXECUTE
STRRJERDR	Session description	*USE	*USE
STRRJESSN [5]	Session description	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	User profile QUSER	*USE	*EXECUTE
	Job-related objects [7]		*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRRJEWTR	Session description	*USE	*USE
	Program [1]	*USE	*READ, *EXECUTE
	Device file [1]	*USE, *ADD	*READ, *EXECUTE
	Physical file [1] (RJE generates members)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Physical file [1] (member specified)	*READ, *ADD	*READ, *EXECUTE
	Message queue [1]	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
WRKFCT [8]	Forms control table	*USE	*EXECUTE
WRKRJESSN [8]	Session description	*USE	*EXECUTE
WRKSSND [8]	Session description	*CHANGE	*EXECUTE

1 User profile QUSER requires authority to this object.

2 If the object is not found or the required authority is not held, an information message is sent and the function of the command is still performed.

3 This authority is required to create job description QRJESSN.

4 This authority is only required when DLTCMN(*YES) is specified.

5 You must have *JOBCTL special authority.

6 Input files include those imbedded using the .. READFILE control statement.

7 Review the authorities that are required for the SBMJOB command.

8 To use an individual operation, you must have the authority required by the operation.

Security attributes commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGSECA [1]			
CHGSECAUD [2,3]			
CFGSYSSEC [1,2,3]			
DSPSECA			
DSPSECAUD [3]			
PRTSYSSECA [4]			

1 You must have *SECADM special authority to use this command.

2 You must have *ALLOBJ special authority to use this command.

3 You must have *AUDIT special authority to use this command.

4 You must have *ALLOBJ or *AUDIT special authority to use this command.

Server authentication entry commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDSVRAUTE[1]			
CHGSVRAUTE[1]			
DSPSVRAUTE	User profile	*READ	*EXECUTE
RMVSVRAUTE[1]			

[1] If the user profile for this operation is not *CURRENT or the current user for the job, you must have *SECADM special authority and *OBJMGT and *USE authority to the profile.

Service commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDTRCFTR[11]			
APYPTF (Q)	Product library	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE
CHKPRDOPT (Q)	All objects in product option [4]		
CPYPTF[2](Q)	From file	*USE	*EXECUTE
	To-file[8]	Same requirements as the SAVOBJ command	Same requirements as the SAVOBJ command
	Device description	*USE	*EXECUTE
	Licensed program		*USE
	Commands: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF, and OVRTAPF	*USE	*EXECUTE
	QSRV library	*USE	*EXECUTE
CPYPTFGRP[2] (Q)	Device description	*USE	*EXECUTE
	To-file	*Same requirements as the SAVOBJ command	*Same requirements as the SAVOBJ command
	From-file	*USE	*EXECUTE
	Commands: CHKTAP, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDTA (Q)			
DLTCMNTRC [3] (Q)	NWID (network ID) or line description	*USE	*EXECUTE
DLTPTF (Q)	Cover letter file [4]		*EXECUTE
	PTF save file [4]		*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTTRC (Q)	RMVM command	*USE	
	QSYS Library	*EXECUTE	
	Database Files	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPSRVA (Q)			
DSPSRVSTS (Q)			
ENDCMNTRC [3] (Q)	NWID or line description	*USE	*EXECUTE
ENDCPYSCN (Q)	Device description	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	QSYS Library	*ADD, *EXECUTE	
	Database files	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Commands: PTRTRC, DLTTRC	*USE	
INSPTF[9] (Q)			
LODPTF (Q)	Device Description	*USE	*EXECUTE
LODRUN [2]	RSTOBJ command	*USE	*EXECUTE
PRTCMNTRC [3] (Q)	NWID (network ID) or line description	*USE	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
PRTERRLOG (Q)	Output file	Refer to "General rules for object authorities on commands" on page 157.	
PRTINTDTA[12,13] (Q)			
PRTTRC[11] (Q)	QSYS Library	*EXECUTE	
	Database Files	*USE	
	DLTTRC command	*USE	
RMVPTF (Q)	Product library	*OBJMGT	
RMVTRCFTR[11]			
RUNLPDA (Q)	Line description	*READ	*EXECUTE
SAVAPARDTA [6] (Q)	Commands: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERRLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB, and WRKSYSVAL	*USE	*EXECUTE
	Existing problem [7]	*CHANGE	*EXECUTE
SNDPTFORD [10] (Q)			
SNDSRVRQS (Q)			

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRCMNTRC [3] (Q)	NWID (network ID) or line description	*USE	*EXECUTE
STRCPYSCN	Job queue	*USE	*EXECUTE
	Device description	*USE	*EXECUTE
	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
STRSRVJOB (Q)	User profile of job	*USE	*EXECUTE
STRSST [3] (Q)			
STRTRC[11, 15] (Q)			
TRCCNN[11]			
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT[11] (Q)			
TRCJOB (Q)	Output file, if specified	Refer to "General rules for object authorities on commands" on page 157.	
	Exit program, if specified	*USE	*EXECUTE
TRCTCPAPP[11] (Q)	User exit program	*USE	*EXECUTE
	Line description	*USE	
	Network interface	*USE	
	Network server	*USE	
VFYCMN (Q)	Line description [5]	*USE	*EXECUTE
	Controller description [5]	*USE	*EXECUTE
	Network ID [5]	*USE	*EXECUTE
VFYLNKLPDA (Q)	Line description	*READ	*EXECUTE
VFYPRT (Q)	Device description	*USE	*EXECUTE
VFYOPT (Q)	Device description	*USE	*EXECUTE
VFYTAP[14] (Q)	Device description	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QPVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB [1, 10] (Q)	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKSRVPVD (Q)			

1 You need authority to the PRTERRLOG command for some analysis procedures or if the error log records are being saved.

2 All restrictions for the RSTOBJ command also apply.

3 Service (*SERVICE) special authority is required to run this command.

4 The objects listed are used by the command, but authority to the objects is not checked. Authority to use the command is sufficient to use the objects.

5 You need *USE authority to the communications object that you are verifying.

Command	Referenced Object	Authority Needed	
		For Object	For Library
[6] You must have *SPLCTL special authority to save a spooled file.			
[7] When SAVAPARDTA is run for a new problem, a unique APAR library is created for that problem. If you run SAVAPARDTA again for the same problem to collect more information, you must have Use authority to the APAR library for the problem.			
[8] The option to add a new member to an existing output file is not valid for this command.			
[9] This command has the same authorities and restrictions as the APYPTF command and the LODPTF command.			
[10] To access options 1 and 3 on the ″Select Reporting Option″ display, you must have *USE authority to the SNDSRVRQS command.			
[11] To use this command, you must have *SERVICE special authority, or be authorized to the Service Trace function of OS/400 through iSeries Navigator's Application Administration support. The Change Function Usage Information (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_TRACE, can also be used to change the list of users that are allowed to perform trace operations.			
[12] To use this command, you must have *SERVICE special authority, or be authorized to the Service Dump Function of OS/400 through iSeries Navigator's Application Administration support. The Change Function Usage Information (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_DUMP, can also be used to change the list of users that are allowed to perform dump operations.			
[13] This command must be issued from within the job with internal data being printed, or the issuer of the command must be running under a user profile which is the same as the job user identity of the job with internal data being printed, or the issuer of the command must be running under a user profile which has job control (*JOBCTL) special authority.			
[14] You must have *IOSYSCFG special authority when the device description is allocated by a media library device.			
[15] If you specify a generic user name for the Job name (JOB) parameter, you must have all object (*ALLOBJ) special authority, or be authorized to the Trace Any User function of OS/400 through iSeries Navigator's Application Administration support. The Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_ALLOBJ_TRACE_ANY_USER can also be used to change the list of users that are allowed to perform trace operations. When the WCHJOB parameter is specified, the issuer of the command must be running under a user profile which is the same as the job user identity of the job being watched, or the issuer of the command must be running under a user profile which has job control (*JOBCTL) special authority.			

Spelling aid dictionary commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTSPADCT	Spelling aid dictionary	*OBJEXIST	*EXECUTE
	Dictionary - REPLACE(*NO)		*READ, *ADD
	Dictionary - REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
DLTSPADCT	Spelling aid dictionary	*OBJEXIST	*EXECUTE
WRKSPADCT [1]	Spelling aid dictionary	Any authority	*USE
[1] To use an individual operation, you must have the authority required by the operation.			

Sphere of control commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDSOCE	Sphere of control [1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sphere of control [1]	*USE, *DLT	*EXECUTE
WRKSOC	Sphere of control [1]	*USE	*EXECUTE

1 The sphere of control is physical file QUSRSYS/QAALSOC.

Spooled file commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Output Queue Parameters			Special Authority	Authority Needed	
		DSPDTA	AUTCHK	OPRCTL		For Object	For Library
CHGSPLFA [1,2]	Output queue [3]		*DTAAUT			*READ, *DLT, *ADD	
			*OWNER			Owner [4]	
				*YES	*JOBCTL		
CHGSPLFA [1], if moving spooled file	Original output queue [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner [4]	
				*YES	*JOBCTL		
	Spooled file	*OWNER				Owner [6]	
	Target output queue[7]					*READ	*EXECUTE
				*YES	*JOBCTL		*EXECUTE
	Target device					*USE	
CPYSPLF [1]	Database file					Refer to "General rules for object authorities on commands" on page 157.	
	Spooled file	*OWNER				Owner [6]	
	Output queue [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner [4]	
		*YES or *NO		*YES	*JOBCTL		

Command	Referenced Object	Output Queue Parameters			Special Authority	Authority Needed	
		DSPDTA	AUTCHK	OPRCTL		For Object	For Library
DLTSPLF [1]	Output queue [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner [4]	
				*YES	*JOBCTL		
DSPSPLF [1]	Output queue [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner [4]	
		*YES or *NO		*YES	*JOBCTL		
	Spooled file	*OWNER				Owner [6]	
HLDSPLF [1]	Output queue [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner [4]	
				*YES	*JOBCTL		
RCLSPLSTG (Q)							
RLSSPLF [1, 8]	Output queue [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner [4]	
				*YES	*JOBCTL		
SNDNETSPLF [1,5]	Output queue [3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner [4]	
		*YES or *NO		*YES	*JOBCTL		
	Spooled file	*OWNER				Owner [6]	
WRKSPLF							

1 Users are always authorized to control their own spooled files.

2 To move a spooled file to the front of an output queue (PRTSEQ(*NEXT)) or change its priority to a value greater than the limit specified in your user profile, you must have one of the authorities shown for the output queue or have *SPLCTL special authority.

3 If you have *SPLCTL special authority, you do not need any authority to the output queue.

4 You must be the owner of the output queue.

5 You must have *USE authority to the recipient's output queue and output queue library when sending a file to a user on the same system.

Command	Referenced Object	Output Queue Parameters			Special Authority	Authority Needed	
		DSPDTA	AUTCHK	OPRCTL		For Object	For Library

[6] You must be the owner of the spooled file.

[7] If you have *SPLCTL special authority, you do not need authority to the target output queue but you must have *EXECUTE authority to its library.

[8] When the spooled file has been held with HLDJOB SPLFILE(*YES) and the spooled file was also decoupled from the job, the user will need to have *USE authority to the RLSJOB command and either have *JOBCTL special authority or be the owner of the spooled file.

Subsystem description commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
	User profile	*USE	
ADDJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	User profile	*USE	
	Job description	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
CHGAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
	User profile	*USE	
CHGJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	User profile	*USE	
	Job description	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5]	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	signon display file[4]	*USE	*EXECUTE
CHGWSE	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
CRTSBSD [5] (Q)	Subsystem description		*READ, *ADD
	signon display file [4]	*USE	*EXECUTE
DLTSBSD	Subsystem description	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Subsystem description	*OBJOPR, *READ	*EXECUTE
ENDSBS [1]			
PRTSBSDAUT [6]			
RMVAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVRTGE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
STRSBS [1]	Subsystem description	*USE	*EXECUTE
WRKSBS [2, 3]	Subsystem description	Any authority	*USE
WRKSBSD [3]	Subsystem description	Any authority	*USE

1 You must have job control (*JOBCTL) special authority to use this command.

2 Requires some authority (anything but *EXCLUDE)

3 To use an individual operation, you must have the authority required by the operation.

4 The authority is needed to complete format checks of the display file. This helps predict that the display will work correctly when the subsystem is started. When you are not authorized to the display file or its library, those format checks will not be performed.

5 You must have *SECADM or *ALLOBJ special authority to specify a specific library for the subsystem library.

6 You must have *ALLOBJ or *AUDIT special authority to use this command.

System commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
PWRDWNSYS[1]	Image catalog (if specified)	*USE	
These commands do not require any object authorities:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] RCLACTGRP[1]	RCLRSC RETURN RTVGRPA	SIGNOFF WRKSHRPOOL	WRKSYSSTS

[1] You must have job control (*JOBCTL) special authority to use this command.

System reply list commands

These commands do not require object authorities:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

System value commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

These commands do not require any authority to objects:			
CHGSYSVAL (Q) [1,2]	DSPSYSVAL[3]	RTVSYSVAL[3]	WRKSYSVAL [1,2, 3]

[1] To change some system values, you must have *ALLOBJ, *ALLOBJ and *SECADM, *AUDIT, *IOSYSCFG, or *JOBCTL special authorities.

[2] To use this command as shipped by IBM, you must be signed on as QPGMR, QSYSOPR, or QSRV, or have *ALLOBJ special authority.

[3] To display or retrieve auditing-related system values, you must have either *AUDIT or *ALLOBJ special authority.

System/36 Environment commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGS36	S/36 configuration object QS36ENV	*UPD	*EXECUTE
CHGS36A	S/36 configuration object QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Program	*OBJMGT, *USE	*EXECUTE
CHGS36PRCA	File QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Source	*OBJMGT, *USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTMSGFMNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD
	Display file if it exists	*ALL	*EXECUTE
	Message file	*USE	*CHANGE
	Source file QS36SRC	*ALL	*EXECUTE
CRTS36DSPF	Display file: REPLACE(*NO)		*READ, *ADD
	Display file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *CHANGE
	To-file source file when TOMBR is not *NONE	*ALL	*CHANGE
	Source file QS36SRC	*USE	*EXECUTE
	Create Display File (CRTDSPF) command	*OBJOPR	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Menu: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *CHANGE
	To-file source file when TOMBR is not *NONE	*ALL	*CHANGE
	Source file QS36SRC	*USE	*EXECUTE
	Display file when REPLACE(*YES) is specified	*ALL	*EXECUTE
	Message files named in source	*ALL	*EXECUTE
	Display file		*CHANGE
	CRTMSGF command	*OBJOPR, *OBJEXIST	*EXECUTE
	ADDMSGD command	*OBJOPR	*EXECUTE
	CRTDSPF command	*OBJOPR	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTS36MSGF	Message file: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Message file: REPLACE(*YES)	Refer to "General rules for object authorities on commands" on page 157.	*READ, *ADD, *CHANGE
	To-file source file when TOMBR is not *NONE	*ALL	*CHANGE
	Source file QS36SRC	*USE	*EXECUTE
	Display file when REPLACE(*YES) is specified	*ALL	*EXECUTE
	Message file named in source	*ALL	*EXECUTE
	Message file named in source when OPTION is *ADD or *CHANGE	*CHANGE	*EXECUTE
	Message files named in source when OPTION(*CREATE) is specified	*ALL	*EXECUTE
	CRTMSGF command	*OBJOPR, *OBJEXIST	*EXECUTE
	ADDMSGD command	*OBJOPR	*EXECUTE
	CHGMSGD command when OPTION(*CHANGE) is specified	*OBJOPR	*EXECUTE
DSPS36	S/36 configuration object QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Program, to modify attributes	*OBJMGT, *USE	*EXECUTE
	Program, to view attributes	*USE	*EXECUTE
EDTS36PRCA	File QS36PRC, to modify attributes	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, to view attributes	*USE	*EXECUTE
EDTS36SRCA	Source file QS36SRC, to modify attributes	*OBJMGT, *USE	*EXECUTE
	Source file QS36SRC, to view attributes	*USE	*EXECUTE
RSTS36F (Q)	From-file	*USE	*EXECUTE
	To-file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	Based-on physical file, if file being restored is a logical (alternative) file	*CHANGE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
RSTS36FLR [1,2,3] (Q)	S/36 folder	*USE	*EXECUTE
	To-folder	*CHANGE	*EXECUTE
	Device file or device description	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
RSTS36LIBM (Q)	From-file	*USE	*EXECUTE
	To-file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	Device file or device description	*USE	*EXECUTE
RTVS36A	S/36 configuration object QS36ENV	*UPD	*EXECUTE
SAVS36F	From-file	*USE	*EXECUTE
	To-file, when it is a physical file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	Device file or device description	*USE	*EXECUTE
SAVS36LIBM	From-file	*USE	*EXECUTE
	To-file, when it is a physical file	*ALL	Refer to "General rules for object authorities on commands" on page 157.
	Device file or device description	*USE	*EXECUTE
WRKS36	S/36 configuration object QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Program, to modify attributes	*OBJMGT, *USE	*EXECUTE
	Program, to view attributes	*USE	*EXECUTE
WRKS36PRCA	File QS36PRC, to modify attributes	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, to view attributes	*USE	*EXECUTE
WRKS36SRCA	Source file QS36SRC, to modify attributes	*OBJMGT, *USE	*EXECUTE
	Source file QS36SRC, to view attributes	*USE	*EXECUTE

[1] You need *ALL authority to the document if replacing it. You need operational and all the data authorities to the folder if restoring new information into the folders, or you need *ALLOBJ special authority.

[2] If used for a data dictionary, only the authority to the command is required.

[3] You must be enrolled in the system distribution directory if the source folder is a document folder.

Table commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTTBL	Table		*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE
DLTTBL	Table	*OBJEXIST	*EXECUTE
WRKTBL [1]	Table	Any authority	*USE

Command	Referenced Object	Authority Needed	
		For Object	For Library
[1] To use an individual operation, you must have the authority required by the operation.			

TCP/IP commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ADDTCPSVR[1]	Program to call	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Program to call	*EXECUTE	*EXECUTE
CVTTCPCL (Q)	File objects	*USE	*EXECUTE
ENDTCP (Q)	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE
	File Objects	*USE	*EXECUTE
ENDTCPIFC (Q)	File objects	*USE	*EXECUTE
	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE
ENDTCPPTP	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE
	File Objects	*USE	*EXECUTE
ENDTCPSRV (Q)	File objects	*USE	*EXECUTE
FTP	File objects	*USE	*EXECUTE
	Table objects	*USE	*EXECUTE
LPR [2]	Workstation customizing object	*USE	*EXECUTE
SETVTTBL	Table objects	*USE	*EXECUTE
SNDTCPSPLF [2]	Workstation customizing object	*USE	*EXECUTE
STRTCP (Q)	File objects	*USE	*EXECUTE
	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE
STRTCPFTP	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE
STRTCPIFC (Q)	File objects	*USE	*EXECUTE
	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE

Command	Referenced Object	Authority Needed	
		For Object	For Library
STRTCPPTP	Line description[4]	*USE	*EXECUTE
	Controller description[4]	*USE	*EXECUTE
	Device description[4]	*USE	*EXECUTE
	File Objects	*USE	*EXECUTE
STRTCPSVR (Q)	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE
STRTCPTELN	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE
	Virtual workstation device[5]	*USE	*EXECUTE
TELNET	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE
	Virtual workstation device[5]	*USE	*EXECUTE
These commands do not require any object authorities:			
ADDCOMSNMP [1]	CFGTCPSMTP	CHGVTMAP	RMVTCPRSI [1]
ADDNETTBLE [1]	CFGTCPSNMP	DSPVTMAP	RMVTCPRTE [1]
ADDPCLTBLE [1]	CFGTCPTELN	ENDTCPCNN	RMVTCPSVR [1]
ADDSRVTBLE [1]	CHGCOMSNMP [1]	MGRTCPHT [1]	RNMTCPHTE [1]
ADDTCPHTE [1]	CHGFTPA [1]	NETSTAT	SETVTMAP
ADDTCPIFC [1]	CHGLPDA [1]	PING	VFYTCPCNN
ADDTCPPORT [1]	CHGSMTPA [1]	RMVCOMSNMP [1]	WRKNAMSMTP [3]
ADDTCPRSI [1]	CHGSNMPA [1]	RMVNETTBLE [1]	WRKNETTBLE[1]
ADDTCPRTE [1]	CHGTCPA [1]	RMVPCLTBLE [1]	WRKPCLTBLE[1]
CFGTCP	CHGTCPHTE[1]	RMVSRVTBLE [1]	WRKSRVTBLE[1]
CFGTCPAPP	CHGTCPIFC[1]	RMVTCPHTE[1]	WRKTCPSTS
CFGTCPFTP [1]	CHGTCPRTE [1]	RMVTCPIFC[1]	
CFGTCPLPD [1]	CHGTELNA [1]	RMVTCPPORT [1]	

[1] You must have *IOSYSCFG special authority to use this command.

[2] The SNDTCPSPLF command and the LPR command use the same combinations of referenced object authorities as the SNDNETSPLF command.

[3] You must have *SECADM special authority to change the system alias table or another user profile's alias table.

[4] If you have *JOBCTL special authority, you do not need the specified authority to the object.

[5] If you have *JOBCTL special authority, you do not need the specified authority to the object on the remote system.

Time zone description commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGTIMZON	Time zone description	*CHANGE	*EXECUTE
CRTTIMZON	Time zone description		*READ, *ADD

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTTIMZON[1]	Time zone description	*OBJEXIST	*EXECUTE
WRKTIMZON[2]	Time zone description	*USE	*USE

1 The time zone description specified in the QTIMZON system value cannot be deleted.

2 If a message is used to specify the abbreviated and full names of the time zone description, you must have *USE authority to the message file and *EXECUTE authority to the message file's library in order to see the abbreviated and full names.

Upgrade order information data commands

These commands are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
WRKORDINF	QGPL/QMAHFILE file	*CHANGE, *OBJALTER	*EXECUTE

User index, user queue, and user space commands

Table 24.

Command	Referenced Object	Authority Needed	
		For Object	For Library
DLTUSRIDX	User index	*OBJEXIST	*EXECUTE
DLTUSRQ	User queue	*OBJEXIST	*EXECUTE
DLTUSRSPC	User space	*OBJEXIST	*EXECUTE

User profile commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Command	Referenced Object	Authority Needed	
		For Object	For Library
ANZDFTPWD [3, 14, 15](Q)			
ANZPRFACT [3, 14, 15](Q)			
CHGACTPRFL [14](Q)			
CHGACTSCDE [3, 14, 15](Q)			
CHGDSTPWD [1]			
CHGEXPSCDE [3, 14, 15](Q)			

Command	Referenced Object	Authority Needed	
		For Object	For Library
CHGPRF	User profile	*OBJMGT, *USE	
	Initial program [2]	*USE	*EXECUTE
	Initial menu [2]	*USE	*EXECUTE
	Job description [2]	*USE	*EXECUTE
	Message queue [2]	*USE	*EXECUTE
	Output queue [2]	*USE	*EXECUTE
	Attention-key- handling program [2]	*USE	*EXECUTE
	Current library [2]	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD [11](Q)			
CHGUSRPRF [3]	User profile	*OBJMGT, *USE	*EXECUTE
	Initial program [2]	*USE	*EXECUTE
	Initial menu [2]	*USE	*EXECUTE
	Job description [2]	*USE	*EXECUTE
	Message queue [2]	*USE	*EXECUTE
	Output queue [2]	*USE	*EXECUTE
	Attention-key-handling program [2]	*USE	*EXECUTE
	Current library [2]	*USE	*EXECUTE
	Group profile (GRPPRF or SUPGRPPRF)[2,4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPRTI	User profile	*CHANGE	
CHKPWD			
CRTUSRPRF [3, 12, 17]	Initial program	*USE	*EXECUTE
	Initial menu	*USE	*EXECUTE
	Job description	*USE	*EXECUTE
	Message queue	*USE	*EXECUTE
	Output queue	*USE	*EXECUTE
	Attention-key- handling program	*USE	*EXECUTE
	Current library	*USE	*EXECUTE
	Group profile (GRPPRF or SUPGRPPRF)[4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT[3, 14]			
DLTUSRPRF [3,9]	User profile	*OBJEXIST, *USE	*EXECUTE
	Message queue [5]	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPACTPRFL [14](Q)			
DSPACTSCD [14](Q)			
DSPAUTUSR [6]	User profile	*READ	
DSPEXPSCD [14](Q)			

Command	Referenced Object	Authority Needed	
		For Object	For Library
DSPPGMADP	User profile	*OBJMGT	
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPUSRPRF[19]	User profile	*READ	*EXECUTE
	Output file	Refer to "General rules for object authorities on commands" on page 157.	
DSPUSRPRTI	User profile	*USE	
GRTUSRAUT [7]	Referenced user profile	*READ	
	Objects you are granting authority to	*OBJMGT	*EXECUTE
PRTPRFINT [14](Q)			
PRTUSRPRF [18]			
RSTAUT (Q) [8]			
RSTUSRPRF (Q) [8,10, 16]			
RTVUSRPRF[20]	User profile	*READ	
RTVUSRPRTI	User profile	*USE	
SAVSECDTA [8]	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF [13]	User profile	Any authority	

1 This command can be run only if you are signed on as QSECOFR.

2 You need authority only to the objects for fields you are changing in the user profile.

3 *SECADM special authority is required.

4 *OBJMGT authority to the group profile cannot come from adopted authority.

5 The message queue associated with the user profile is deleted if it is owned by that user profile. To delete the message queue, the user running the DLTUSRPRF command must have the authorities specified.

6 The display includes only user profiles to which the user running the command has the specified authority.

7 See the authorities required for the GRTOBJAUT command.

8 *SAVSYS special authority is required.

9 If you select the option to delete objects owned by the user profile, you must have the necessary authority for the delete operations. If you select the option to transfer ownership to another user profile, you must have the necessary authority to the objects and to the target user profile. See information for the CHGOBJOWN command.

10 You must have *ALLOBJ special authority to specify ALWOBJDIF(*ALL).

Command	Referenced Object	Authority Needed	
		For Object	For Library

[11] You must have *AUDIT special authority.

[12] The user whose profile is created is given these authorities to it: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.

[13] To use an individual operation, you must have the authority required by the operation.

[14] You must have *ALLOBJ special authority to use this command.

[15] You must have *JOBCTL special authority to use this command.

[16] You must have *ALLOBJ and *SECADM special authorities to specify SECDTA(*PWDGRP), USRPRF(*ALL) or OMITUSRPRF.

[17] When you perform a CRTUSRPRF, you can not create a user profile (*USRPRF) into an independent disk pool. However, when a user is privately authorized to an object in the independent disk pool, is the owner of an object on an independent disk pool, or is the primary group of an object on an independent disk pool, the name of the profile is stored on the independent disk pool. If the independent disk pool is moved to another system, the private authority, object ownership, and primary group entries will be attached to the profile with the same name on the target system. If a profile does not exist on the target system, a profile will be created. The user will not have any special authorities and the password will be set to *NONE.

[18] You must have *ALLOBJ or *AUDIT special authority to use this command.

[19] You must have either *ALLOBJ or *AUDIT special authority to have the current object auditing value and action auditing value displayed. Otherwise, the value *NOTAVL will be displayed to indicate that the values are not available for display.

[20] You must have either *ALLOBJ or *AUDIT special authority to retrieve the current OBJAUD and AUDLVL values. Otherwise, the value *NOTAVL will be returned to indicate that the values are not available for retrieval.

User-defined file system commands

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDMFS [1,2,3]	dir_to_be_mounted_over	*DIR	″root″	*W
	Path Prefix	Refer to “General rules for object authorities on commands” on page 157.		
CRTUDFS [1,2,6,7] (Q)	/dev/QASPxx	*DIR	″root″	*RWX
DLTUDFS [1,2,4,5] (Q)	/dev/QASPxx	*DIR	″root″	*RWX
	any_epfs_object		″root″	*RWX, *OBJEXIST
DSPUDFS	some_dirsxx	*DIR	″root″	*RX
MOUNT [1,2,3]	dir_to_be_ mounted_over	*DIR	″root″	*W
	Path Prefix	Refer to “General rules for object authorities on commands” on page 157.		
RMVMFS [1]				
UNMOUNT [1]				

Command	Referenced Object	Object Type	File System	Authority Needed for Object

[1] To use this command, you must have *IOSYSCFG special authority.

[2] QASPxx is either 01 (system asp) or 02-16 based on which user asp is needed. This is the directory that contains the *BLKSF that is being mounted.

[3] The directory that is mounted over (dir_to_be_mounted_over) is any integrated file system directory that can be mounted over.

[4] A UDFS can contain an entire subtree of objects, so when you delete a UDFS, you delete objects of all types that can be stored in the user-defined file system.

[5] When using the DLTUDFS commands, you must have *OBJEXIST authority on every object in the UDFS or no objects are deleted.

[6] The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authorities to specify a value for the Scanning option for objects (CRTOBJSCAN) parameter other than *PARENT.

[7] The audit (*AUDIT) special authority is required when specifying a value other than *SYSVAL on the Auditing value for objects (CRTOBJAUD) parameter.

Validation list commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTVLDL	Validation list		*ADD, *READ
DLTVLDL	Validation list	*OBJEXIST	*EXECUTE

Workstation customization commands

Command	Referenced Object	Authority Needed	
		For Object	For Library
CRTWSCST	Source file	*USE	*EXECUTE
	Workstation customizing object, if REPLACE(*NO)		*READ, *ADD
	Workstation customizing object, if REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Workstation customizing object	*OBJEXIST	*EXECUTE
RTVWSCST	To-file, if it exists and a new member is added	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	To-file, if file and member exist	*OBJOPR, *ADD, *DLT	*EXECUTE
	To-file, if the file does not exist		*READ, *ADD

Writer commands

Command	Referenced Object	Output Queue Parameters		Special Authority	Authority Needed	
		AUTCHK	OPRCTL		For Object	For Library
CHGWTR [2, 4]	Current output queue[1]	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		
ENDWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		
HLDWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		
RLSWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		
STRDKTWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Message queue				*OBJOPR, *ADD	*EXECUTE
	Device description				*OBJOPR, *READ	
STRPRTWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Message queue				*OBJOPR, *ADD	*EXECUTE
	User-defined driver program				*READ	*EXECUTE
	Data transform program				*READ	*EXECUTE
	Separator program				*READ	*EXECUTE
	Device description				*OBJOPR, *READ	

Command	Referenced Object	Output Queue Parameters		Special Authority	Authority Needed	
		AUTCHK	OPRCTL		For Object	For Library
STRRMTWTR [1]	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
	Message queue	*OWNER			Owner [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
					*OBJOPR, *ADD	*EXECUTE
	User driver program				*READ	*EXECUTE
	User data transform				*READ	*EXECUTE
WRKWTR						

[1] If you have *SPLCTL special authority, you do not need any authority to the output queue.

[2] To change the output queue for the writer, you need one of the specified authorities for the new output queue.

[3] You must be the owner of the output queue.

[4] You must have *EXECUTE authority to the new output queue's library even if the user has *SPLCTL special authority.

Appendix G. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. 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 IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information 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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This *Configure Your System For Common Criteria Security* publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

400
Advanced Function Printing
AFP
AS/400
C/400
COBOL/400
DB2
DB2 Universal Database
e(logo)server
eServer
i5/OS
IBM
IBM (logo)
iSeries
GDDM
NetServer
OfficeVision
Operating System/400
OS/400
Print Services Facility
RPG/400
SQL/400
System/36
System/38

Intel®, Intel Inside® (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Code license disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Index

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Printed in USA

SC41-5336-00