



IBM i
Security
Security reference

7.1

SC41-5302-11





IBM i

Security
Security reference

7.1

SC41-5302-11

Note

Before using this information and the product it supports, read the information in Appendix I, "Notices," on page 725.

This edition applies to IBM i 7.1 (product number 5770-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.

This edition replaces SC41-5302-10.

© **Copyright IBM Corporation 1996, 2010.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

	iii	Limit Security Officer (QLMTSECOFR)	29
		Maximum Sign-On Attempts (QMAXSIGN)	30
		Action When Sign-On Attempts Reached (QMAXSGNACN)	30
		Retain Server Security (QRETSVRSEC)	31
		Remote power-on and restart (QRMTIPL)	32
		Remote Sign-On Control (QRMTSIGN)	32
		Scan File Systems (QSCANFS)	33
		Scan File Systems Control (QSCANFSCTL)	33
		Share Memory Control (QSHRMEMCTL)	34
		Use Adopted Authority (QUSEADPAUT)	35
		Security-related system values	36
		Automatic Device Configuration (QAUTOCFG)	37
		Automatic Configuration of Virtual Devices (QAUTOVRT)	37
		Device Recovery Action (QDEVRCYACN)	38
		Disconnected Job Time-Out Interval (QDSCJOBTV)	38
		Remote Service Attribute (QRMTSRVATR)	39
		Secure Sockets Layer (SSL) cipher specification list (QSSLCSL)	39
		Secure Sockets Layer (SSL) cipher control (QSSLCSLCTL)	40
		Secure Sockets Layer (SSL) protocols (QSSLPCL)	40
		Security-related restore system values	41
		Verify Object on Restore (QVFYOBJRST)	41
		Force Conversion on Restore (QFRCCVNRST)	43
		Allow Restoring of Security-Sensitive Objects (QALWBJRST)	45
		System values that apply to passwords	46
		Block Password Change (QPWDCHGBLK)	47
		Password Expiration Interval (QPWDEXPITV)	47
		Password Expiration Warning (QPWDEXPWPN)	48
		Password Level (QPWDLVL)	48
		Minimum Length of Passwords (QPWDMINLEN)	50
		Maximum Length of Passwords (QPWDMAXLEN)	50
		Required Difference in Passwords (QPWDRQDDIF)	51
		Restricted Characters for Passwords (QPWDLMTCHR)	52
		Restriction of Consecutive Digits for Passwords (QPWDLMTAJC)	52
		Restriction of Repeated Characters for Passwords (QPWDLMTREP)	52
		Character Position Difference for Passwords (QPWDPOSDIF)	53
		Requirement for Numeric Character in Passwords (QPWDRQDDGT)	54
		Password Rules (QPWDRULES)	54
		Password Approval Program (QPWDVLDPGM)	60
		Using a password approval program	61
		System values that control auditing	65
		Auditing Control (QAUDCTL)	66
		Auditing End Action (QAUDENDACN)	66
What's new for IBM i 7.1	xiii		
Chapter 1. Introduction to System i security	1		
Physical security	2		
Keylock security	2		
Security level	2		
System values	3		
Signing	3		
Single sign-on enablement	3		
User profiles	4		
Group profiles	4		
Resource security	5		
Security audit journal	6		
Common Criteria security	6		
Independent disk pool	6		
Chapter 2. Using System Security (QSecurity) system value	9		
Security level 10	12		
Security level 20	12		
Changing to level 20 from level 10	12		
Changing to level 20 from a higher level	13		
Security level 30	13		
Changing to level 30 from a lower level	13		
Security level 40	14		
Preventing the use of unsupported interfaces	15		
Protecting job descriptions	16		
Signing on without a user ID and password	16		
Enhanced hardware storage protection	17		
Protecting a program's associated space	17		
Protecting a job's address space	17		
Validating parameters	17		
Validation of programs being restored	17		
Changing to security level 40	18		
Disabling security level 40	19		
Security level 50	19		
Restricting user domain objects	19		
Restricting message handling	20		
Preventing modification of internal control blocks	20		
Changing to security level 50	20		
Disabling security level 50	21		
Chapter 3. Security system values	23		
General security system values	24		
Allow User Domain Objects (QALWUSRDMN)	25		
Authority for New Objects (QCRTAUT)	26		
Display Sign-On Information (QDSPSGNINF)	26		
Inactive Job Time-Out Interval (QINACTITV)	27		
Inactive Job Time-Out Message Queue (QINACTMSGQ)	28		
Limit Device Sessions (QLMTDEVSSN)	29		

Auditing Force Level (QAUDFRCLVL)	67	User identification number	108
Auditing Level (QAUDLVL)	67	Group identification number	109
Auditing Level Extension (QAUDLVL2)	69	Home directory	109
Auditing for New Objects (QCRTOBJAUD)	71	EIM association	110
Chapter 4. User profiles	73	User expiration date	111
Roles of the user profile	73	User expiration interval	111
Group profiles	74	Authority	112
User-profile parameter fields	74	Object auditing	112
User profile name	75	Action auditing	113
Password	76	Additional information associated with a user profile	115
Set password to expired	77	Private authorities	115
Status	78	Primary group authorities	116
User class	79	Owned object information	116
Assistance level	80	Digital ID authentication	116
Current library	81	Working with user profiles	117
Initial program	81	Creating user profiles	117
Initial menu	82	Using the Work with User Profiles command	117
Limit capabilities	83	Using the Create User Profile command	118
Text	84	Using the Work with User Enrollment option	118
Special authority	84	Copying user profiles	119
*ALLOBJ special authority	85	Copying from the Work with User Profiles display	119
*SECADM special authority	85	Copying from the Work with User Enrollment display	120
*JOBCTL special authority	85	Copying private authorities	121
*SPLCTL special authority	86	Changing user profiles	122
*SAVSYS special authority	86	Deleting user profiles	122
*SERVICE special authority	86	Using the Delete User Profile command	122
Granting access to traces	87	Using the Remove User option	123
*AUDIT special authority	88	Working with Objects by Private Authorities	124
*IOSYSCFG special authority	88	Working with Objects by Primary Group	124
Special environment	88	Enabling a user profile	125
Display sign-on information	90	Listing user profiles	125
Password expiration interval	91	Displaying an individual profile	125
Block Password Change	92	Listing all profiles	125
Local password management	92	Types of user profile displays	126
Limit device sessions	93	Types of user profile reports	126
Keyboard buffering	93	Renaming a user profile	126
Maximum storage	94	Working with user auditing	127
Priority limit	95	Working with profiles in CL programs	128
Job description	96	User profile exit points	128
Group profile	96	IBM-supplied user profiles	128
Owner	97	Changing passwords for IBM-supplied user profiles	129
Group authority	98	Working with service tools user IDs	129
Group authority type	98	System password	130
Supplemental groups	99	Chapter 5. Resource security	131
Accounting code	100	Defining who can access information	131
Document password	100	Defining how information can be accessed	132
Message queue	101	Commonly used authorities	133
Delivery	101	Defining what information can be accessed	135
Severity	102	Library security	135
Print device	103	Library security and library lists	135
Output queue	103	Field authorities	136
Attention-Key-Handling program	104	Security and the System/38 Environment	137
Sort Sequence	104	Recommendation for System/38 Environment	137
Language identifier	105	Directory security	138
Country or region identifier	105	Authorization list security	138
Coded character set identifier	106		
Character identifier control	106		
Job attributes	107		
Locale	107		
User Options	108		

Authorization list management	138
Using authorization lists to secure IBM-supplied objects	139
Authority for new objects in a library	139
Create Authority (CRTAUT) risks.	140
Authority for new objects in a directory	140
Object ownership	142
Group ownership of objects	143
Primary group for an object	144
Default Owner (QDFTOWN) user profile	145
Assigning authority and ownership to new objects.	145
Objects that adopt the owner's authority	149
Adopted authority risks and recommendations	152
Programs that ignore adopted authority	152
Authority holders	153
Authority holders and System/36 Migration	154
Authority holder risks	154
Working with authority	154
Authority displays	154
Authority reports	157
Working with libraries	157
Creating objects	158
Working with individual object authority	159
Specifying user-defined authority.	160
Giving authority to new users.	160
Removing a user's authority	161
Working with authority for multiple objects	162
Working with object ownership	163
Working with primary group authority.	164
Using a referenced object	165
Copying authority from a user	165
Working with authorization lists	165
Advantages of using an authorization list	166
Creating an authorization list	166
Giving users authority to an authorization list	167
Securing objects with an authorization list	167
Setting up an authorization list	168
Deleting an authorization list	169
How the system checks authority.	169
Authority checking flowcharts.	169
Flowchart 1: Main authority checking process	170
Flowchart 2: Fast path for object authority checking	172
Flowchart 3: How user authority to an object is checked	174
Flowchart 4: How owner authority is checked	175
Flowchart 5: Fast path for user authority checking	176
Flowchart 6: How group authority is checked	179
Flowchart 7: How public authority is checked	181
Flowchart 8: How adopted authority is checked	182
Authority checking examples	186
Case 1: Using private group authority	186
Case 2: Using primary group authority.	187
Case 3: Using public authority.	189
Case 4: Using public authority without searching private authority	189

Case 5: Using adopted authority	189
Case 6: User and group authority	190
Case 7: Public authority without private authority	191
Case 8: Adopted authority without private authority	192
Case 9: Using an authorization list	193
Case 10: Using multiple groups	194
Case 11: Combining authorization methods	195
Authority cache	197

Chapter 6. Work management security 199

Job initiation	199
Starting an interactive job	199
Starting a batch job	200
Adopted authority and batch jobs	200
Workstations	201
Ownership of device descriptions	203
Signon screen display file	204
Changing the signon screen display	204
Display file source for the signon screen	204
Changing the signon display file	204
Subsystem descriptions	205
Controlling how jobs enter the system	205
Job descriptions	206
System operator message queue	207
Library lists	207
Security risks of library lists	208
Change in function	208
Unauthorized access to information	209
Recommendations for system portion of library list	209
Recommendations for product library	209
Recommendations for the current library	210
Recommendations for the user portion of the library list	210
Printing	211
Securing spooled files	211
Display Data (DSPDTA) parameter of output queue	211
Authority to Check (AUTCHK) parameter of output queue	212
Operator Control (OPRCTL) parameter of output queue	212
Output queue and parameter authorities required for printing	212
Examples: Output queue	213
Network attributes	214
Job Action (JOBACN) network attribute	214
Client Request Access (PCSACC) network attribute	215
Risks and recommendations	215
DDM Request Access (DDMACC) network attribute	216
Save and restore operations	216
Restricting save and restore operations	216
Example: Restricting save and restore commands	217
Performance tuning	217
Restricting jobs to batch	218

Chapter 7. Designing security 219

Overall recommendations for security design	220
Planning password level changes	221
Considerations for changing QPWDLVL from 0 to 1	222
Considerations for changing QPWDLVL from 0 or 1 to 2	222
Considerations for changing QPWDLVL from 2 to 3	223
Changing QPWDLVL to a lower password level	223
Planning libraries	225
Planning applications to prevent large profiles	226
Library lists	226
Controlling the user library list	226
Changing the system library list	227
Describing library security	228
Planning menus	228
Describing menu security	229
Using adopted authority in menu design	230
Ignoring adopted authority	232
System request menu	233
Planning command security	235
Planning file security	236
Securing logical files	236
Overriding files	239
File security and SQL	239
Planning group profiles	239
Considerations for primary groups for objects	240
Considerations for multiple group profiles	240
Accumulating special authorities for group profile members	240
Using an individual profile as a group profile	241
Comparison of group profiles and authorization lists	241
Planning security for programmers	242
Managing source files	242
Protecting Java class files and jar files in the integrated file system	243
Planning security for system programmers or managers	243
Using validation lists	243
Limit access to program function	244

Chapter 8. Backup and recovery of security information 245

How security information is stored	246
Saving security information	247
Recovering security information	248
Restoring user profiles	248
Restoring objects	249
Restoring authority	252
Restoring programs	252
Restoring licensed programs	253
Restoring authorization lists	254
Recovering the authorization list	254
Recovering the association of objects to the authorization list	255
Restoring the operating system	255
*SAVSYS special authority	255
Auditing save and restore operations	256

Chapter 9. Auditing security on System i 257

Checklist for security officers and auditors	257
Physical security	258
System values	258
IBM-supplied user profiles	258
Password control	259
User and group profiles	260
Authorization control	261
Unauthorized access	262
Unauthorized programs	262
Communications	262
Using the security audit journal	262
Planning security auditing	263
Planning the auditing of actions	263
Action auditing values	264
Security auditing journal entries	269
Planning the auditing of object access	286
Displaying object auditing	288
Setting default auditing for objects	288
Preventing loss of auditing information	288
Choosing not to audit QTEMP objects	289
Using CHGSECAUD to set up security auditing	290
Setting up security auditing	290
Managing the audit journal and journal receivers	292
Saving and deleting audit journal receivers	293
System-managed journal receivers	294
User-managed journal receivers	294
Stopping the audit function	294
Analyzing audit journal entries	295
Viewing audit journal entries	295
Analyzing audit journal entries with query or a program	296
Relationship of object Change Date/Time to audit records	298
Other techniques for monitoring security	299
Monitoring security messages	299
Using the history log	299
Using journals to monitor object activity	300
Analyzing user profiles	301
Printing selected user profiles	302
Examining large user profiles	302
Analyzing object and library authorities	303
Analyzing programs that adopt authority	303
Checking for objects that have been altered	304
Checking the operating system	304
Auditing the security officer's actions	305

Appendix A. Security commands 309

Authority holders commands	309
Authority lists commands	309
Object authority and auditing commands	310
Passwords commands	311
User profiles commands	311
Related user profile commands	312
Auditing commands	313
Document library objects commands	313
Server authentication entries commands	314
System distribution directory commands	314

Validation lists commands	315
Function usage information commands	315
Auditing security tools commands	315
Authority security tools commands	316
System security tools commands	316

Appendix B. IBM-supplied user profiles 319

Default values for user profiles	319
IBM-supplied user profiles	321

Appendix C. Commands shipped with public authority *EXCLUDE 327

Appendix D. Authority required for objects used by commands 339

Command usage assumptions	341
General rules for object authorities on commands	341
Common commands for most objects	343
Access path recovery commands	350
Advanced Function Presentation (AFP) commands	351
AF_INET sockets over SNA commands	352
Alerts commands	352
Application development commands	353
Authority holder commands	354
Authorization list commands	354
Binding directory commands	355
Change request description commands	355
Chart commands	356
Class commands	356
Class-of-service commands	356
Cluster commands	357
Command (*CMD) commands	361
Commitment control commands	362
Communications side information commands	362
Configuration commands	363
Configuration list commands	364
Connection list commands	364
Controller description commands	365
Cryptography commands	366
Data area commands	367
Data queue commands	368
Device description commands	368
Device emulation commands	370
Directory and directory shadowing commands	371
Directory server commands	371
Disk commands	372
Display station pass-through commands	372
Distribution commands	373
Distribution list commands	374
Document library object commands	374
Domain Name System commands	378
Double-byte character set commands	380
Edit description commands	380
Environment variable commands	380
Extended wireless LAN configuration commands	381
File commands	381
Filter commands	388
Finance commands	389
IBM i graphical operations commands	389

Graphics symbol set commands	390
Host server commands	390
Image catalog commands	390
Integrated file system commands	392
Interactive data definition commands	410
Internetwork Packet Exchange (IPX) commands	410
Information search index commands	411
IPL attribute commands	411
Java commands	411
Job commands	412
Job description commands	415
Job queue commands	416
Job schedule commands	417
Journal commands	417
Journal receiver commands	421
Kerberos commands	422
Language commands	424
Library commands	430
License key commands	434
Licensed program commands	435
Line description commands	435
Local Area Network (LAN) commands	437
Locale commands	437
Mail server framework commands	438
Media commands	438
Menu and panel group commands	439
Message commands	440
Message description commands	441
Message file commands	441
Message queue commands	441
Migration commands	442
Mode description commands	442
Module commands	443
NetBIOS description commands	443
Network commands	444
Network file system commands	445
Network interface description commands	446
Network server commands	446
Network server configuration commands	448
Network server description commands	448
Node list commands	449
Office services commands	449
Online education commands	450
Operational assistant commands	450
Optical commands	451
Output queue commands	454
Package commands	455
Performance commands	455
Print descriptor group commands	461
Print Services Facility configuration commands	461
Problem commands	462
Program commands	463
QSH shell interpreter commands	466
Query commands	466
Question and answer commands	468
Reader commands	469
Registration facility commands	469
Relational database commands	469
Resource commands	470
Remote Job Entry (RJE) commands	470
Security attributes commands	474

Server authentication entry commands	475
Service commands.	475
Spelling aid dictionary commands	480
Sphere of control commands	480
Spooled file commands	481
Subsystem description commands	483
System commands.	485
System reply list commands	485
System value commands	486
System/36 environment commands	486
Table commands	489
TCP/IP commands	489
Time zone description commands	490
User index, user queue, and user space commands	491
User-defined file system commands	491
User profile commands	492
Validation list commands	495
Workstation customization commands	496
Writer commands	496

Appendix E. Object operations and auditing 499

Operations common to all object types	499
Operations for Access Path Recovery Times	502
Operations for Alert Table (*ALRTBL)	503
Operations for Authorization List (*AUTL)	503
Operations for Authority Holder (*AUTHLR).	504
Operations for Binding Directory (*BNDDIR).	504
Operations for Configuration List (*CFGL)	505
Operations for Special Files (*CHRSF)	505
Operations for Chart Format (*CHTFMT)	505
Operations for C Locale Description (*CLD)	506
Operations for Change Request Description (*CRQD)	506
Operations for Class (*CLS)	507
Operations for Command (*CMD)	507
Operations for Connection List (*CNL)	508
Operations for Class-of-Service Description (*COSD)	509
Operations for Communications Side Information (*CSI)	509
Operations for Cross System Product Map (*CSPMAP)	509
Operations for Cross System Product Table (*CSPTBL)	510
Operations for Controller Description (*CTL)	510
Operations for Device Description (*DEVD)	511
Operations for Directory (*DIR)	512
Operations for Directory Server	514
Operations for Document Library Object (*DOC or *FLR)	516
Operations for Data Area (*DTAARA)	519
Operations for Interactive Data Definition Utility (*DTADCT)	520
Operations for Data Queue (*DTAQ)	520
Operations for Edit Description (*EDTD)	521
Operations for Exit Registration (*EXITRG)	521
Operations for Forms Control Table (*FCT)	522
Operations for File (*FILE)	522
Operations for First-in First-out Files (*FIFO).	525
Operations for Folder (*FLR)	525

Operations for Font Resource (*FNTRSC)	526
Operations for Form Definition (*FORMDF)	526
Operations for Filter Object (*FTR)	526
Operations for Graphics Symbols Set (*GSS)	527
Operations for Double-byte Character Set Dictionary (*IGCDCT)	527
Operations for Double-byte Character Set Sort (*IGCSRT)	528
Operations for Double-byte Character Set Table (*IGCTBL)	528
Operations for Job Description (*JOB)	528
Operations for Job Queue (*JOBQ)	529
Operations for Job Scheduler Object (*JOBSCD)	530
Operations for Journal (*JRN)	530
Operations for Journal Receiver (*JRNRCV)	532
Operations for Library (*LIB)	532
Operations for Line Description (*LIND)	533
Operations for Mail Services	534
Operations for Menu (*MENU)	535
Operations for Mode Description (*MODD)	535
Operations for Module Object (*MODULE)	535
Operations for Message File (*MSGF)	536
Operations for Message Queue (*MSGQ)	537
Operations for Node Group (*NODGRP)	538
Operations for Node List (*NODL)	538
Operations for NetBIOS Description (*NTBD)	538
Operations for Network Interface (*NWID)	539
Operations for Network Server Description (*NWS)	540
Operations for Output Queue (*OUTQ).	540
Operations for Overlay (*OVL)	541
Operations for Page Definition (*PAGDFN)	542
Operations for Page Segment (*PAGSEG)	542
Operations for Print Descriptor Group (*PDG)	542
Operations for Program (*PGM)	542
Operations for Panel Group (*PNLGRP)	544
Operations for Product Availability (*PRDAVL)	544
Operations for Product Definition (*PRDDFN)	545
Operations for Product Load (*PRDLOD)	545
Operations for Query Manager Form (*QMFORM)	545
Operations for Query Manager Query (*QMQR)	546
Operations for Query Definition (*QRYDFN)	546
Operations for Reference Code Translate Table (*RCT).	547
Operations for Reply List	547
Operations for Subsystem Description (*SBSD)	548
Operations for Information Search Index (*SCHIDX)	549
Operations for Local Socket (*SOCKET)	550
Operations for Spelling Aid Dictionary (*SPADCT)	552
Operations for Spooled Files	552
Operations for SQL Package (*SQLPKG)	554
Operations for Service Program (*SRVPGM)	554
Operations for Session Description (*SSND)	555
Operations for Server Storage Space (*SVRSTG)	555
Operations for Stream File (*STMF)	555
Operations for Symbolic Link (*SYMLNK).	557
Operations for S/36 Machine Description (*S36)	558
Operations for Table (*TBL)	559
Operations for User Index (*USRIDX)	559
Operations for User Profile (*USRPRF)	560

Operations for User Queue (*USRQ)	561
Operations for User Space (*USRSPC)	561
Operations for Validation List (*VLDL)	562
Operations for Workstation Customizing Object (*WSCST)	562

Appendix F. Layout of audit journal entries 563

Standard heading fields for audit journal entries	
QJORDJE5 Record Format (*TYPE5)	564
Standard heading fields for audit journal entries	
QJORDJE4 Record Format (*TYPE4)	565
Standard heading fields for audit journal entries	
QJORDJE2 Record Format (*TYPE2)	567
Audit Journal (QAUDJRN) entry types	568
AD (Auditing Change) journal entries	570
AF (Authority Failure) journal entries	573
AP (Adopted Authority) journal entries	579
AU (Attribute Changes) journal entries	579
CA (Authority Changes) journal entries	580
CD (Command String) journal entries	583
CO (Create Object) journal entries	584
CP (User Profile Changes) journal entries	586
CQ (*CRQD Changes) journal entries	589
CU (Cluster Operations) journal entries	589
CV (Connection Verification) journal entries	591
CY (Cryptographic Configuration) journal entries	593
DI (Directory Server) journal entries	596
DO (Delete Operation) journal entries	601
DS (IBM-Supplied Service Tools User ID Reset) journal entries	603
EV (Environment Variable) journal entries	604
GR (Generic Record) journal entries	605
GS (Give Descriptor) journal entries	610
IM (Intrusion Monitor) journal entries	611
IP (Interprocess Communication) journal entries	614
IR (IP Rules Actions) journal entries	615
IS (Internet Security Management) journal entries	617
JD (Job Description Change) journal entries	619
JS (Job Change) journal entries	620
KF (Key Ring File) journal entries	625
LD (Link, Unlink, Search Directory) journal entries	628
ML (Mail Actions) journal entries	630
NA (Attribute Change) journal entries	630
ND (APPN Directory Search Filter) journal entries	631
NE (APPN End Point Filter) journal entries	632
OM (Object Management Change) journal entries	632
OR (Object Restore) journal entries	636
OW (Ownership Change) journal entries	640
O1 (Optical Access) journal entries	642
O2 (Optical Access) journal entries	643
O3 (Optical Access) journal entries	644
PA (Program Adopt) journal entries	645
PG (Primary Group Change) journal entries	647
PO (Printer Output) journal entries	650
PS (Profile Swap) journal entries	651
PW (Password) journal entries	653
RA (Authority Change for Restored Object) journal entries	654
RJ (Restoring Job Description) journal entries	656

RO (Ownership Change for Restored Object) journal entries	657
RP (Restoring Programs that Adopt Authority) journal entries	659
RQ (Restoring Change Request Descriptor Object) journal entries	661
RU (Restore Authority for User Profile) journal entries	661
RZ (Primary Group Change for Restored Object) journal entries	662
SD (Change System Distribution Directory) journal entries	664
SE (Change of Subsystem Routing Entry) journal entries	665
SF (Action to Spooled File) journal entries	666
SG (Asynchronous Signals) journal entries	670
SK (Secure Sockets Connections) journal entries	671
SM (Systems Management Change) journal entries	673
SO (Server Security User Information Actions) journal entries	674
ST (Service Tools Action) journal entries	675
SV (Action to System Value) journal entries	680
VA (Change of Access Control List) journal entries	681
VC (Connection Start and End) journal entries	681
VF (Close of Server Files) journal entries	682
VL (Account Limit Exceeded) journal entries	683
VN (Network Log On and Off) journal entries	684
VO (Validation List) journal entries	685
VP (Network Password Error) journal entries	686
VR (Network Resource Access) journal entries	687
VS (Server Session) journal entries	688
VU (Network Profile Change) journal entries	689
VV (Service Status Change) journal entries	690
X0 (Network Authentication) journal entries	691
X1 (Identity Token) journal entries	695
XD (Directory Server Extension) journal entries	697
YC (Change to DLO Object) journal entries	698
YR (Read of DLO Object) journal entries	699
ZC (Change to Object) journal entries	700
ZR (Read of Object) journal entries	703
Numeric codes for access types	706

Appendix G. Commands and menus for security commands 707

Options on the Security Tools menu	707
How to use the Security Batch menu	709
Options on the security batch menu	711
Commands for customizing security	715
Values that are set by the Configure System Security command	716
Changing the program	718
What the Revoke Public Authority command does	718
Changing the program	719

Appendix H. Related information for IBM i security reference 721

Appendix I. Notices 725
Programming Interface Information 727
Trademarks 727

Terms and conditions. 727

Index 729

What's new for IBM i 7.1

Read about new or significantly changed information for the Security reference topic collection.

User profile expiration date parameter

The User expiration date field allows a security administrator to indicate that the user profile will expire on a specific date. If User expiration interval is used, this date is calculated by the system.

How to see what's new or changed

To help you see where technical changes have been made, the information center uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

In PDF files, you might see revision bars (| or +) in the left margin of new and changed information.

Chapter 1. Introduction to System i security

The IBM Systems family covers a wide range of users. Security on the System i[®] platform is flexible enough to meet the requirements of this wide range of users and situations.

A small system might have three to five users, and a large system might have several thousand users. Some installations have all their workstations in a single, relatively secure, area. Others have widely distributed users, including users who connect by dialing in and indirect users connected through personal computers or system networks. You need to understand the features and options available so that you can adapt them to your own security requirements.

System security has three important objectives:

Confidentiality:

- Protecting against disclosing information to unauthorized people
- Restricting access to confidential information
- Protecting against curious system users and outsiders

Integrity:

- Protecting against unauthorized changes to data
- Restricting manipulation of data to authorized programs
- Providing assurance that data is trustworthy

Availability:

- Preventing accidental changes or destruction of data
- Protecting against attempts by outsiders to abuse or destroy system resources

System security is often associated with external threats, such as hackers or business rivals. However, protection against system accidents by authorized system users is often the greatest benefit of a well-designed security system. In a system without good security features, pressing the wrong key might result in deleting important information. System security can prevent this type of accident.

The best security system functions cannot produce good results without good planning. Security that is set up in small pieces, without planning, can be confusing. It is difficult to maintain and to audit. Planning does not imply designing the security for every file, program, and device in advance. It does imply establishing an overall approach to security on the system and communicating that approach to application designers, programmers, and system users.

As you plan security on your system and decide how much security you need, consider these questions:

- Is there a company policy or standard that requires a certain level of security?
- Do the company auditors require some level of security?
- How important is your system and the data on it to your business?
- How important is the error protection provided by the security features?
- What are your company security requirements for the future?

To facilitate installation, many of the security capabilities on your system are not activated when your system is shipped. Recommendations are provided in this topic collection to bring your system to a reasonable level of security. Consider the security requirements of your own installation as you evaluate the recommendations.

Physical security

Physical security includes protecting the system unit, system devices, and backup media from accidental or deliberate damage. Most measures you take to ensure the physical security of your system are external to the system. However, the system is equipped with a keylock that prevents unauthorized functions at the system unit.

Note: You must order the keylock feature on some models.

Related information:

Planning physical security

Keylock security

You can retrieve and change the keylock position by using the Retrieve IPL Attributes (QWCRIPLA) API or the Change IPL Attributes (CHGIPLA) command.

The keylock on the 940x control panel controls access to various system control panel functions.

The keylock feature allows the remote user access to additional functions available at the control panel. For example, it controls where the machine will IPL from and to what environment, either IBM® i or Dedicated Service Tools (DST).

The IBM i system value, QRMTSRVATR, controls the remote access. This value is shipped defaulted to off which will not allow the keylock to be overridden. The system value can be changed to allow remote access, but does require *SECADM and *ALLOBJ special authorities to change.

Related reference:

“Remote Service Attribute (QRMTSRVATR)” on page 39

The Remote Service Attribute (QRMTSRVATR) controls the remote system service problem analysis ability. The value allows the system to be analyzed remotely.

Security level

The System i platform offers five levels of security. You can choose which level of security you want the system to enforce by setting the security level (QSECURITY) system value.

Level 10:

Level 10 is no longer supported.

Level 20:

The system requires a user ID and password for sign-on. All users are given access to all objects.

Level 30:

The system requires a user ID and password for sign-on. The security of resources is enforced.

Level 40:

The system requires a user ID and password for sign-on. The security of resources is enforced. Additional integrity protection features are also enforced.

Level 50:

The system requires a user ID and password for sign-on. The security of resources is enforced. Level 40 integrity protection and enhanced integrity protection are enforced. Security level 50 is intended for System i platforms with high security requirements, and it is designed to meet Common Criteria (CC) security requirements.

Related reference:

Chapter 2, “Using System Security (QSecurity) system value,” on page 9

You can choose how much security you want the system to enforce by setting the security level (QSECURITY) system value.

System values

System values provide customization on many characteristics of your System i platform. You can use system values to define system-wide security settings.

For example, you can specify the following settings:

- How many sign-on attempts you allow at a device.
- Whether the system automatically signs off an inactive workstation.
- How often passwords need to be changed.
- The length and composition of passwords.

Related concepts:

Chapter 3, "Security system values," on page 23

System values allow you to customize many characteristics of your system. A group of system values are used to define system-wide security settings.

Signing

You can reinforce integrity by signing software objects that you use.

A key component of security is *integrity*: being able to trust that objects on the system have not been tampered with or altered. Your System i operating system software is protected by digital signatures.

Signing your software object is particularly important if the object has been transmitted across the Internet or stored on media which you feel might have been modified. The digital signature can be used to detect if the object has been altered.

Digital signatures, and their use for verification of software integrity, can be managed according to your security policies using the Verify Object Restore (QVIFYOBJRST) system value, the Check Object Integrity (CHKOBJITG) command, and the Digital Certificate Manager tool. Additionally, you can choose to sign your own programs (all licensed programs shipped with the system are signed).

You can restrict adding digital signatures to a digital certificate store using the Add Verifier API and restrict resetting passwords on the digital certificate store. System Service Tools (SST) provides a new menu option, entitled "Work with system security" where you can restrict adding digital certificates.

Related information:

Using digital signatures to protect software integrity

Digital Certificate Manager

Single sign-on enablement

Single *sign-on* is an authentication process in which a user can access more than one system by entering a single user ID and password. In today's heterogeneous networks with partitioned systems and multiple platforms, administrators must cope with the complexities of managing identification and authentication for network users.

To enable a single sign-on environment, IBM provides two technologies that work together to enable users to sign in with their Windows user name and password and be authenticated to System i platforms in the network. Network Authentication Service (NAS) and Enterprise Identity Mapping (EIM) are the two technologies that an administrator must configure to enable a single sign-on environment. Windows 2000, Windows XP, AIX®, and z/OS® use Kerberos protocol to authenticate users to the network. A secure, centralized system, called a key distribution center, authenticates principals (Kerberos users) to the network.

While Network Authentication Service (NAS) allows a System i platform to participate in the Kerberos realm, EIM provides a mechanism for associating these Kerberos principals to a single EIM identifier that represents that user within the entire enterprise. Other user identities, such as an IBM i user name, can also be associated with this EIM identifier. When a user signs on to the network and accesses a System i platform, that user is not prompted for a user ID and password. If the Kerberos authentication is successful, applications can look up the association to the EIM identifier to find the IBM i user name. The user no longer needs a password to sign on to System i platform because the user is already authenticated through the Kerberos protocol. Administrators can centrally manage user identities with EIM while network users need only to manage one password. You can enable single sign-on by configuring Network Authentication Service (NAS) and Enterprise Identity Mapping (EIM) on your system.

Related information:

Scenario: Creating a single signon test environment

User profiles

On the IBM i operating system, every system user has a user profile.

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

The user profile is a powerful and flexible tool. It controls what the user can do and customizes the way the system appears to the user. The following list describes some of the important security features of the user profile:

Special authority

Special authorities determine whether the user is allowed to perform system functions, such as creating user profiles or changing the jobs of other users.

Initial menu and initial program

The initial menu and program determine what the user sees after signing on the system. You can limit a user to a specific set of tasks by restricting the user to an initial menu.

Limit capabilities

The limit capabilities field in the user profile determines whether the user can enter commands and change the initial menu or initial program when signing on.

Related concepts:

Chapter 4, "User profiles," on page 73

User profiles are a powerful and flexible tool. Designing them well can help you protect your system and customize it for your users.

Group profiles

A *group profile* is a special type of user profile. Rather than giving authority to each user individually, you can use a group profile to define authority for a group of users.

A group profile can own objects on the system. You can also use a group profile as a pattern when creating individual user profiles by using the copy profile function.

Related concepts:

"Planning group profiles" on page 239

A group profile is a useful tool when several users have similar security requirements. You can directly create group files or you can make an existing profile into a group profile. When you use group profiles, you can manage authority more efficiently and reduce the number of individual private authorities for objects.

"Group ownership of objects" on page 143

This topic provides detailed information about the group ownership of objects.

“Primary group for an object” on page 144

You can specify a primary group for an object.

“Copying user profiles” on page 119

You can create a user profile by copying another user profile or a group profile.

Resource security

The ability to access an object is called *authority*. Resource security on the IBM i operating system enables you to control object authorities by defining who can use which objects and how those objects can be used.

You can specify detailed authorities, such as adding records or changing records. Or you can use the system-defined subsets of authorities: *ALL, *CHANGE, *USE, and *EXCLUDE.

Files, programs, and libraries are the most common objects requiring security protection, but you can specify authority for any object on the system. The following list describes the features of resource security:

Group profiles

A group of similar users can share the same authority to use objects.

Authorization lists

Objects with similar security needs can be grouped in one list. Authority can be granted to the list rather than to the individual objects.

Object ownership

Every object on the system has an owner. Objects can be owned by an individual user profile or by a group profile. Correct assignment of object ownership helps you manage applications and delegate responsibility for the security of your information.

Primary group

You can specify a primary group for an object. The primary group’s authority is stored with the object. Using primary groups may simplify your authority management and improve authority checking performance.

Library authority

You can put files and programs that have similar protection requirements into a library and restrict access to that library. This is often easier than restricting access to each individual object.

Directory authority

You can use directory authority in the same way that you use library authority. You can group objects in a directory and secure the directory rather than the individual objects.

Object authority

In cases where restricting access to a library or directory is not specific enough, you can restrict authority to access individual objects.

Public authority

For each object, you can define what kind of access is available for any system user who does not have any other authority to the object. Public authority is an effective means for securing information and provides good performance.

Adopted authority

Adopted authority adds the authority of a program owner to the authority of the user running the program. Adopted authority is a useful tool when a user needs different authority for an object, depending on the situation.

Authority holder

An authority holder stores the authority information for a program-described database file. The

authority information remains, even when the file is deleted. Authority holders are commonly used when converting from the System/36, because System/36 applications often delete files and create them again.

Field level authority

Field level authorities are given to individual fields in a database file. You can use SQL statements to manage this authority.

Related concepts:

Chapter 5, "Resource security," on page 131

This section describes each of the components of resource security and how they work together to protect information about your system. It also explains how to use CL commands and displays to set up resource security on your system.

Security audit journal

You can use security audit journals to audit the effectiveness of security on your system.

The IBM i operating system provides the ability to log selected security-related events in a security audit journal. Several system values, user profile values, and object values control which events are logged.

Related concepts:

Chapter 9, "Auditing security on System i," on page 257

This section describes techniques for auditing the effectiveness of security on your system.

Common Criteria security

Common Criteria is a framework for independent assessment, analysis, and testing of products to a set of security requirements.

On August 10, 2005, IBM received Common Criteria certification of IBM i V5R3M0 at Evaluated Assurance Level (EAL) 4 augmented with ALC_FLR.2 of the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999. To order the evaluated system, order Common Criteria FC 1930 under 5722-SS1.

Only customers who must run within a Common Criteria configuration should order this feature number.

The product is posted on the Validated Products List page at the Common Criteria Evaluation and Validation SchemeWeb site (<http://www.niap-ccevs.org/cc-scheme/>).

Independent disk pool

Independent disk pools provide the ability to group together storage that can be taken offline or brought online independent of system data or other unrelated data. The terms *independent auxiliary storage pool* (iASP) and *independent disk pool* are synonymous.

An independent disk pool can be either switchable among multiple systems in a clustering environment or privately connected to a single system. As of V5R2, functional changes to independent disk pools have security implications on your system. For example, when you perform a CRTUSRPRF, you cannot 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.

Independent disk pools support many library-based objects and user-defined file systems. However, several objects are not allowed on independent disk pools. In IBM i V5R1, you can use independent disk pools only with user-defined file systems.

Related information:

Supported and unsupported object types

Chapter 2. Using System Security (QSecurity) system value

You can choose how much security you want the system to enforce by setting the security level (QSECURITY) system value.

Overview

Purpose:

Specify level of security to be enforced on the system.

How To:

WRKSYSVAL *SEC (Work with System Values command) or Menu SETUP, option 1 (Change System Options)

Authority:

*ALLOBJ and *SECADM

Journal Entry:

SV

Note: Before changing on a production system, read appropriate section on migrating from one level to another.

Levels of security

The system offers five levels of security:

10 No system-enforced security

Note: You cannot set the system value QSECURITY to security level 10.

20 Sign-on security

30 Sign-on and resource security

40 Sign-on and resource security; integrity protection

50 Sign-on and resource security; enhanced integrity protection.

Your system is shipped at level 40, which provides sign-on and resource security and provides integrity protection. For more information, see "Security level 40" on page 14.

If you want to change the security level, use the Work with System Values (WRKSYSVAL) command. The minimum security level you should use is 30. However, level 40 or higher is recommended. The change takes effect the next time you perform an initial program load (IPL). Table 1 compares the levels of security on the system:

Table 1. Security levels: function comparison

Function	Level 20	Level 30	Level 40	Level 50
User name required to sign on.	Yes	Yes	Yes	Yes
Password required to sign on.	Yes	Yes	Yes	Yes
Password security active.	Yes	Yes	Yes	Yes
Menu and initial program security active.	Yes ¹	Yes ¹	Yes ¹	Yes ¹
Limit capabilities support active.	Yes	Yes	Yes	Yes
Resource security active.	No	Yes	Yes	Yes

Table 1. Security levels: function comparison (continued)

Function	Level 20	Level 30	Level 40	Level 50
Access to all objects.	Yes	No	No	No
User profile created automatically.	No	No	No	No
Security auditing capabilities available.	Yes	Yes	Yes	Yes
Programs that contain restricted instructions cannot be created or recompiled.	Yes	Yes	Yes	Yes
Programs that use unsupported interfaces fail at run time.	No	No	Yes	Yes
Enhanced hardware storage protection is enforced for all storage.	No	No	Yes	Yes
Library QTEMP is a temporary object.	No	No	No	No
*USRSPC, *USRIDX, and *USRQ objects can be created only in libraries specified in the QALWUSRDMN system value.	Yes	Yes	Yes	Yes
Pointers used in parameters are validated for user domain programs running in system state.	No	No	Yes	Yes
Message handling rules are enforced between system and user state programs.	No	No	No	Yes
A program's associated space cannot be directly modified.	No	No	Yes	Yes
Internal control blocks are protected.	No	No	Yes	Yes ²
¹ When LMTCPB(*YES) is specified in the user profile. ² At level 50, more protection of internal control blocks is enforced than at level 40. See "Preventing modification of internal control blocks" on page 20.				

Default special authorities

The system security level determines what the default special authorities are for each user class. When you create a user profile, you can select special authorities based on the user class. Special authorities are also added and removed from user profiles when you change security levels.

These special authorities can be specified for a user:

*ALLOBJ

All-object special authority gives a user authority to perform all operations on objects.

*AUDIT

Audit special authority allows a user to define the auditing characteristics of the system, objects, and system users.

*IOSYSCFG

System configuration special authority allows a user to configure input and output devices on the system.

*JOBCTL

Job control special authority allows a user to control batch jobs and printing on the system.

*SAVSYS

Save system special authority allows a user to save and restore objects.

*SECADM

Security administrator special authority allows a user to work with user profiles on the system.

*SERVICE

Service special authority allows a user to perform software service functions on the system.

*SPLCTL

Spool control special authority allows unrestricted control of batch jobs and output queues on the system.

You can also restrict users with *SECADM and *ALLOBJ authorities from changing this security related system value with the CHGSYSVAL command. You can specify this restriction in the System Service Tools (SST) with the "Work with system security" option.

Note: This restriction applies to several other system values.

For details on how to restrict changes to security system values and a complete list of the affected system values, see Security system values.

Table 2 shows the default special authorities for each user class. The entries indicate that the authority is given at security levels 10 and 20 only, at all security levels, or not at all.

Table 2. Default special authorities for user classes by security level

Special authority	User classes				
	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	All	10 or 20	10 or 20	10 or 20	10 or 20
*AUDIT	All				
*IOSYSCFG	All				
*JOBCTL	All	10 or 20	10 or 20	All	
*SAVSYS	All	10 or 20	10 or 20	All	10 or 20
*SECADM	All	All			
*SERVICE	All				
*SPLCTL	All				

Note: The topics "User class" on page 79 and "Special authority" on page 84 provide more information about user classes and special authorities.

Considerations

Security level 30 or higher is recommended because the system does not automatically give users access to all resources. At lower security levels, all users are given *ALLOBJ special authority.

At security level 30 (or below), users can call system interfaces that exchange to QSECOFR user profile or allow users access to resources that they are not normally allowed to access. At security level 40, users are not allowed to directly call these interfaces. Therefore, security level 40 or higher is strongly recommended.

Security level 40 provides additional integrity protection without affecting system performance. Applications that do not run at security level 40 have a negative effect on performance at security level 30. They cause the system to respond to domain violations.

Security level 50 is intended for systems with very high security requirements. If you run your system at security level 50, you might notice some performance effect because of the additional checking that the system performs.

Even if you want to give all users access to all information, consider running your system at security level 30. You can use the public authority capability to give users access to information. Using security level 30 from the beginning gives you the flexibility of securing a few critical resources when you need to without having to test all of your applications again.

Related concepts:

“Security level” on page 2

The System i platform offers five levels of security. You can choose which level of security you want the system to enforce by setting the security level (QSECURITY) system value.

Related tasks:

“Disabling security level 50” on page 21

After changing to security level 50, you might find you need to move back to security level 30 or 40 temporarily. For example, you might need to test new applications for integrity errors; or you might discover integrity problems that did not appear at lower security levels.

Security level 10

At security level 10, you have no security protection. Therefore, security level 10 is not recommended.

Beginning in Version 4 Release 3, you cannot set your security level to 10. If your system is currently at level 10, your system will remain at level 10 when you install Version 4 Release 3. If you change the system level to some other value, you cannot change it back to level 10.

When a new user signs on, the system creates a user profile with the profile name equal to the user ID specified on the sign-on display. If the same user signs on later with a different user ID, a new user profile is created. Appendix B, “IBM-supplied user profiles,” on page 319 shows the default values that are used when the system automatically creates a user profile.

The system performs authority checking at all levels of security. Because all user profiles created at security level 10 are given *ALLOBJ special authority, users successfully pass almost every authority check and have access to all resources. If you want to test the effect of moving to a higher security level, you can remove *ALLOBJ special authority from user profiles and grant those profiles the authority to use specific resources. However, this does not give you any security protection. Anyone can sign on with a new user ID, and a new profile is created with *ALLOBJ special authority. You cannot prevent this at security level 10.

Security level 20

Security level 20 provides more security functions than level 10. However, because at security level 20 all profiles are created with *ALLOBJ special authority by default, security level 20 is not recommended either.

Security level 20 provides the following security functions:

- Both user ID and password are required to sign on.
- Only a security officer or someone with *SECADM special authority can create user profiles.
- The limit capabilities value specified in the user profile is enforced.

Changing to level 20 from level 10

When you change from level 10 to level 20, any user profiles that were automatically created at level 10 are preserved. The password for each user profile that was created at level 10 is the same as the user profile name. No changes are made to the special authorities in the user profiles.

Consider performing the following list of recommended activities if you plan to change from level 10 to level 20 after your system has been in production:

- List all the user profiles on the system using the Display Authorized User (DSPAUTUSR) command.
- Either create new user profiles with standardized names or copy the existing profiles and give them new, standardized names.
- Set the password to expired in each existing profile, forcing each user to assign a new password.

- Set password composition system values to prevent users from assigning trivial passwords.
- Review the default values in “Default values for user profiles” on page 319 in Appendix B, “IBM-supplied user profiles,” on page 319 for any changes you want to make to the profiles automatically created at security level 10.

Changing to level 20 from a higher level

When you change from a higher security level to level 20, special authorities are added to the user profiles. By doing this, the user has, at least, the default special authority for the user class.

When you change to level 20 from a higher security level, the system adds *ALLOBJ special authority to every user profile. This allows users to view, change, or delete any object on the system.

Refer to Table 2 on page 11 to see how special authorities differ between level 20 and higher security levels.

Security level 30

Security level 30 provides more security functions than security level 20.

Level 30 provides the following security functions, in addition to what is provided at level 20:

- Users must be specifically given authority to use resources on the system.
- Only user profiles created with the *SECOFR security class are given *ALLOBJ special authority automatically.

Changing to level 30 from a lower level

When you change to security level 30 from a lower security level, the system changes all user profiles to update special authorities the next time you perform an initial program load (IPL).

Special authorities that the user was given at 10 or 20, but didn't have at 30 or above, are removed. Special authorities that the user was given that are not associated with their user class are not changed. For example, *ALLOBJ special authority is removed from all user profiles except those with a user class of *SECOFR. See Table 2 on page 11 for a list of the default special authorities and the differences between level 10 or 20 and the higher security levels.

If your system has been running applications at a lower security level, you should set up and test resource security before changing to security level 30. Consider performing the following recommended activities:

- For each application, set the appropriate authorities for application objects.
- Test each application by using either actual user profiles or special test user profiles.
 - Remove *ALLOBJ special authority from the user profiles that are used for testing.
 - Grant appropriate application authorities to the user profiles.
 - Run the application using the user profiles.
 - Check for authority failures either by looking for error messages or by using the security audit journal.
- When all applications run successfully with the test profiles, grant appropriate authorities for application objects to the production user profiles that should have access to the application.
- If the QLMTSECOFR (limit security officer) system value is 1 (Yes), users with *ALLOBJ or *SERVICE special authority must be specifically authorized to devices at security level 30 or higher. You can give these users *CHANGE authority to selected devices, give QSECOFR *CHANGE authority to the devices, or change the QLMTSECOFR system value to 0.
- Change the security level on your system and perform an initial program load (IPL).

If you want to change to level 30 without defining individual object authorities, make the public authority for application objects high enough to run the application. Run application tests to make sure no authority failures occur.

Related reference:

“Defining how information can be accessed” on page 132

You can define what operations can be preformed on objects, data, and fields.

Security level 40

Security level 40 prevents potential integrity or security risks from programs that can circumvent security in special cases. Security level 50 provides enhanced integrity protection for installations with strict security requirements.

Table 3 compares how security functions are supported at levels 30, 40, and 50.

Table 3. Comparison of security levels 30, 40, and 50

Scenario description	Level 30	Level 40	Level 50
A program attempts to access objects using interfaces that are not supported.	AF journal entry ¹	AF journal entry ¹ ; operation fails.	AF journal entry ¹ ; operation fails.
A program attempts to use a restricted instruction.	AF journal entry ¹ ; operation fails.	AF journal entry ¹ ; operation fails.	AF journal entry ¹ ; operation fails.
The user submitting a job does not have *USE authority to the user profile specified in the job description.	AF journal entry ¹	AF journal entry ¹ ; job does not run.	AF journal entry ¹ ; job does not run.
A user attempts default sign-on without a user ID and a password.	AF journal entry ¹	AF journal entry ¹ ; sign-on is not successful.	AF journal entry ¹ ; sign-on is not successful.
A *USER state program attempts to write to the system area of disk that is defined as read-only or no access.	Attempt may succeed.	AF journal entry; ¹ operation fails.	AF journal entry; ¹ operation fails.
An attempt is made to restore a program that does not have a validation value. ²	No validation is performed. Program must be converted before it can be used.	No validation is performed. Program must be converted before it can be used.	No validation is performed. Program must be converted before it can be used.
An attempt is made to restore a program that has a validation value.	Program validation is performed.	Program validation is performed.	Program validation is performed.
An attempt is made to change a program’s associated space.	Attempt is successful.	AF journal entry; ¹ operation fails.	AF journal entry; ¹ operation fails.
An attempt is made to change a job’s address space.	Attempt is successful.	AF journal entry; ¹ operation fails.	AF journal entry; ¹ operation fails.
A user state program attempts to call or transfer control to a system domain program.	Attempt is successful.	AF journal entry; ¹ operation fails.	AF journal entry; ¹ operation fails.
An attempt is made to create a user domain object of type *USRSPC, *USRIDX, or *USRQ in a library not included in the QALWUSRDMN system value.	Operation fails.	Operation fails.	Operation fails.
A user state program sends an exception message to a system state program that is not immediately above it in the call stack.	Attempt is successful.	Attempt is successful.	Operation fails.
A parameter is passed to a user domain program running in the system state.	Attempt is successful.	Parameter validation is performed.	Parameter validation is performed.

Table 3. Comparison of security levels 30, 40, and 50 (continued)

Scenario description	Level 30	Level 40	Level 50
An IBM-supplied command is changed to run a different program using the CHGCMD command. The command is changed again to run the original IBM-supplied program, which is a system domain program. A user attempts to run the command.	Attempt is successful.	AF journal entry; ^{1, 3} operation fails. ³	AF journal entry; ^{1, 3} operation fails. ³
¹	An authority failure (AF) type entry is written to the audit (QAUDJRN) journal, if the auditing function is active. See Chapter 9, "Auditing security on System i," on page 257 for more information about the audit function.		
²	Programs created before Version 1 Release 3 do not have a validation value.		
³	When you change an IBM-supplied command, it can no longer call a system domain program.		

If you use the auditing function at lower security levels, the system logs journal entries for most of the actions shown in Table 3 on page 14, except those detected by the enhanced hardware protection function. You receive warnings in the form of journal entries for potential integrity violations. At level 40 and higher, integrity violations cause the system to fail the attempted operation.

Preventing the use of unsupported interfaces

At security level 40 or higher, the system prevents attempts to directly call system programs that are not documented as call-level interfaces.

For example, directly calling the command processing program for the SIGNOFF command fails.

The system uses the domain attribute of an object and the state attribute of a program to enforce this protection.

- **Domain:**

Every object belongs to either the *SYSTEM domain or the *USER domain. *SYSTEM domain objects can be accessed only by *SYSTEM state programs or by *INHERIT state programs that are called by *SYSTEM state programs.

You can display the domain of an object by using the Display Object Description (DSPOBJD) command and specifying DETAIL(*FULL). You can also use the following commands:

- Display Program (DSPPGM) to display the domain of a program
- Display Service Program (DSPSRVPGM) to display the domain of a service program

- **State:**

Programs are either *SYSTEM state, *INHERIT state, or *USER state. The *USER state programs can directly access only *USER domain objects. You can access objects that are *SYSTEM domain by using the appropriate command or application programming interface (API). The *SYSTEM and *INHERIT states are reserved for IBM-supplied programs.

You can display the state of a program by using the Display Program (DSPPGM) command. You can display the state of a service program by using the Display Service Program (DSPSRVPGM) command.

Table 4 shows the domain and state access rules:

Table 4. Domain and state access

Program state	Object domain	
	*USER	*SYSTEM
*USER	YES	NO ¹

Table 4. Domain and state access (continued)

Program state	Object domain	
	*USER	*SYSTEM
*SYSTEM	YES	YES
¹ A domain or state violation causes the operation to fail at security level 40 and higher. At all security levels, an AF type entry is written to the audit journal if the auditing function is active.		

Journal entry:

When the following conditions are met, an authority failure (AF) entry, violation type D or R, is written to the QAUDJRN journal:

- The auditing function is active
- The QAUDLVL system value includes *PGMFAIL
- An attempt is made to use an unsupported interface

Protecting job descriptions

If a user profile name is used as the value for the User field in a job description, any jobs submitted with the job description can run under that user profile. Thus an unauthorized user might submit a job to run under the user profile specified in the job description.

At security level 40 and higher, the job will fail unless the user submitting the job has *USE authority to both the job description and the user profile specified in the job description. At security level 30, the job runs if the submitter has *USE authority to the job description.

Journal entry:

When the following conditions are met, an AF entry, violation type J, is written to the QAUDJRN journal:

- The auditing function is active
- The QAUDLVL system value includes *AUTFAIL
- A user submits a job, while the user is not authorized to the user profile in the job description

Signing on without a user ID and password

Your security level determines how the system controls signing on without a user ID and password.

At security level 30 and below, signing on by pressing the Enter key without a user ID and password is possible with certain subsystem descriptions. At security level 40 and higher, the system stops any attempt to sign on without a user ID and password.

Journal entry:

When the following conditions are met, an AF entry, violation type S, is written to the QAUDJRN journal:

- The auditing function is active
- The QAUDLVL system value includes *AUTFAIL
- A user attempts to sign on without entering a user ID and password and the subsystem description allows it

Note that the attempt fails at security level 40 and higher.

Related concepts:

“Subsystem descriptions” on page 205

The subsystem descriptions perform several functions on the system.

Enhanced hardware storage protection

Enhanced hardware storage protection allows blocks of system information that are located on the memory to be defined as read-write, read-only, or no access.

At security level 40 and higher, the system controls how *USER state programs access these protected blocks.

Enhanced hardware storage protection is supported on all System i models.

Journal entry:

When the following conditions are met, an AF entry, violation type R, is written to the QAUDJRN journal:

- The auditing function is active
- The QAUDLVL system value includes *PGMFAIL
- A program attempts to write to an area of memory protected by the enhanced hardware storage protection feature

Protecting a program's associated space

For original program model (OPM) programs, at security level 40 and higher, the associated space of a program object cannot be directly changed by user state programs. For integrated language environment (ILE) programs, the associated space of a program object cannot be changed by user state programs at any security level.

Protecting a job's address space

At security level 50, a user state program cannot obtain the address for another job on the system. Therefore, a user state program cannot directly manipulate objects associated with another job.

Validating parameters

Interfaces to the IBM i operating system are system state programs in the user domain. When parameters are passed between user state and system state programs, those parameters must be checked to prevent any unexpected values from jeopardizing the integrity of the operating system.

When you run your system at security level 40 or 50, the system specifically checks every parameter passed between a user state program and a system state program in the user domain. This is required for your system to separate the system and user domain, and to meet the requirements of a Common Criteria level of security. You might notice some performance effect because of this additional checking.

Validation of programs being restored

When a program is created, the system calculates a validation value, which is stored with the program. When the program is restored, the validation value is calculated again and compared to the validation value that is stored with the program.

If the validation values do not match, the system takes action according to the Force Conversion on Restore (QFRCCVNRST) and Allow Object Restore (QALWOBJRST) system values.

In addition to a validation value, a program might optionally have a digital signature that can be verified on restore. Any system actions related to digital signatures are controlled by the QVIFYOBJRST and QFRCCVNRST system values. The three system values, Verify Object on Restore (QVIFYOBJRST), QFRCCVNRST and QALWOBJRST, act as a series of filters to determine whether a program will be restored without change, whether it will be re-created (converted) as it is restored, or whether it will not be restored to the system.

Note: System state programs must have a valid IBM digital signature. Otherwise, they cannot be restored, no matter how the system values are set

The first filter is the QVIFYOBRST system value. It controls the restore operation on some objects that can be digitally signed. After an object is successfully checked and is validated by this system value, the object proceeds to the second filter, the QFRCCVNRST system value. With this system value you specify whether to convert programs, service programs, or module objects during a restore operation. This system value also prevents certain objects from being restored. Only when the objects have passed the first two filters do they proceed to the final filter, the QALWOBRST system value. This system value controls whether objects with security sensitive attributes can be restored.

Notes:

1. Programs created for the IBM i operating system can contain information that allows the program to be re-created at restore time, without requiring the program source.
2. Programs created for IBM i Version 5, Release 1 and later, contain the information needed for re-creation even when the observability of the program is removed.
3. Programs created for releases before Version 5, Release 1 can only be re-created at restore time if the observability of the program has not been deleted.

Related reference:

“Security-related system values” on page 36

This topic introduces the security-related system values on your IBM i operating system.

Changing to security level 40

Before migrating to level 40, make sure that all of your applications run successfully at security level 30. Security level 30 gives you the opportunity to test resource security for all of your applications.

Follow these steps to migrate to security level 40:

1. Activate the security auditing function, if you have not already done so. The topic “Setting up security auditing” on page 290 gives complete instructions for setting up the auditing function.
2. Make sure that the QAUDLVL system value includes *AUTFAIL and *PGMFAIL. *PGMFAIL logs journal entries for any access attempts that violate the integrity protection at security level 40.
3. Monitor the audit journal for *AUTFAIL and *PGMFAIL entries while running all of your applications at security level 30. Pay particular attention to the following detailed entries in AF type entries:

- C Object validation failure
- D Unsupported interface (domain) violation
- J Job-description and user-profile authorization failure
- R Attempt to access protected area of disk (enhanced hardware storage protection)
- S Default sign-on attempt

These codes indicate the presence of integrity exposures in your applications. At security level 40, these programs fail.

4. If you have any programs that were created before Version 1 Release 3, use the CHGPGM command with the FRCCRT parameter to create validation values for those programs. At security level 40, the system translates any program that is restored without a validation value. This can add considerable time to the restore process. See the topic “Validation of programs being restored” on page 17 for more information about program validation.

Note: Restore program libraries as part of your application test. Check the audit journal for validation failures.

5. Based on the entries in the audit journal, take steps to correct your applications and prevent program failures.

6. Change the QSECURITY system value to 40 and perform an IPL.

Disabling security level 40

You might want to move back to level 30 from level 40 temporarily because you need to test new applications for integrity errors. Or, you might discover you did not test well enough before changing to security level 40.

You can change from security level 40 to level 30 without jeopardizing your resource security. No changes are made to special authorities in user profiles when you move from level 40 to level 30. After you have tested your applications and resolved any errors in the audit journal, you can move back to level 40.

Attention: If you move from level 40 to level 20, some special authorities are added to all user profiles. (See Table 2 on page 11.) This removes resource security protection.

Security level 50

Security level 50 is designed to meet some of the requirements defined by the Controlled Access Protection Profile (CAPP) for Common Criteria (CC) compliance. Security level 50 provides enhanced integrity protection, in addition to what is provided by security level 40, for installations with strict security requirements.

The security functions included for security level 50 are described in the topics that follow:

- Restricting user domain object types (*USRSPC, *USRIDX, and *USRQ)
- Restricting message handling between user and system state programs
- Preventing modification of all internal control blocks

Restricting user domain objects

Most objects are created in the system domain. When you run your system at security level 40 or 50, system domain objects can be accessed only by using the commands and APIs provided.

These object types can be either system or user domain:

- User space (*USRSPC)
- User index (*USRIDX)
- User queue (*USRQ)

Objects of type *USRSPC, *USRIDX, and *USRQ in user domain can be manipulated directly without using system-provided APIs and commands. This allows a user to access an object without creating an audit record.

Note: Objects of type *PGM, *SRVPGM and *SQLPKG can also be in the user domain. Their contents cannot be manipulated directly, and they are not affected by the restrictions.

At security level 50, a user must not be permitted to pass security-relevant information to another user without the ability to write an audit record. To enforce this:

- At security level 50, no job can get addressability to the QTEMP library for another job. Therefore, if user domain objects are stored in the QTEMP library, they cannot be used to pass information to another user.
- To provide compatibility with existing applications that use user domain objects, you can specify additional libraries in the QALWUSRDMN system value. The QALWUSRDMN system value is enforced at all security levels. See “Allow User Domain Objects (QALWUSRDMN)” on page 25 for more information.

Related tasks:

“Changing to security level 50”

If your current security level is 10 or 20, change the security level to 40 before you change it to 50. If your current security level is 30 or 40, you need to evaluate the QALWUSRDMN value and recompile some programs to prepare for security level 50.

Restricting message handling

Messages sent between programs provide the potential for integrity exposures.

At security level 50, you are able to restrict the messages sent between programs to protect the integrity of your system.

The following applies to message handling at security level 50:

- Any user state program can send a message of any type to any other user state program.
- Any system state program can send a message of any type to any user or system state program.
- A user state program can send a non-exception message to any system state program.
- A user state program can send an exception type message (status, notify, or escape) to a system state program if one of the following is true:
 - The system state program is a request processor.
 - The system state program called a user state program.

Note: The user state program sending the exception message does not need to be the program called by the system state program. For example, in this call stack, an exception message can be sent to Program A by Program B, C, or D:

Program A	System state
Program B	User state
Program C	User state
Program D	User state

- When a user state program receives a message from an external source (*EXT), any pointers in the message replacement text are removed.

Preventing modification of internal control blocks

At security level 40, some internal control blocks, such as the work control block, cannot be modified by a user state program. At security level 50, no system internal control blocks can be modified. This includes the open data path (ODP), the spaces for CL commands and programs, and the S/36 environment job control block.

Changing to security level 50

If your current security level is 10 or 20, change the security level to 40 before you change it to 50. If your current security level is 30 or 40, you need to evaluate the QALWUSRDMN value and recompile some programs to prepare for security level 50.

Most of the additional security measures that are enforced at security level 50 do not cause audit journal entries at lower security levels. Therefore, an application cannot be tested for all possible integrity error conditions before changing to security level 50.

The actions that cause errors at security level 50 are uncommon in normal application software. Most software that runs successfully at security level 40 also runs at security level 50.

If you are currently running your system at security level 30, complete the steps described in “Changing to security level 40” on page 18 to prepare for changing to security level 50.

If you are currently running your system at security level 30 or 40, do the following to prepare for security level 50:

- Evaluate the QALWUSRDMN system value. Controlling user domain objects is important to system integrity.
- Recompile any COBOL programs that assign the device in the SELECT clause to WORKSTATION if the COBOL programs were compiled using a pre-V2R3 compiler.
- Recompile any S/36 environment COBOL programs that were compiled using a pre-V2R3 compiler.
- Recompile any RPG/400® or System/38 environment RPG* programs that use display files if they were compiled using a pre-V2R2 compiler.

You can go directly from security level 30 to security level 50. Running at security level 40 as an intermediate step does not provide significant benefits for testing.

If you are currently running at security level 40, you can change to security level 50 without extra testing. Security level 50 cannot be tested in advance. The additional integrity protection that is enforced at security level 50 does not produce error messages or journal entries at lower security levels.

Related concepts:

“Restricting user domain objects” on page 19

Most objects are created in the system domain. When you run your system at security level 40 or 50, system domain objects can be accessed only by using the commands and APIs provided.

Disabling security level 50

After changing to security level 50, you might find you need to move back to security level 30 or 40 temporarily. For example, you might need to test new applications for integrity errors; or you might discover integrity problems that did not appear at lower security levels.

You can change from security level 50 to level 30 or 40 without jeopardizing your resource security. No changes are made to special authorities in user profiles when you move from level 50 to level 30 or 40. After you have tested your applications and resolved any errors in the audit journal, you can move back to level 50.

Attention: If you move from level 50 to level 20, some special authorities are added to all user profiles. This removes resource security protection.

Related reference:

Chapter 2, “Using System Security (QSecurity) system value,” on page 9

You can choose how much security you want the system to enforce by setting the security level (QSECURITY) system value.

Chapter 3. Security system values

System values allow you to customize many characteristics of your system. A group of system values are used to define system-wide security settings.

You can restrict users from changing the security-related system values. System service tools (SST) and dedicated service tools (DST) provide an option to lock these system values. By locking the system values, you can prevent even a user with *SECADM and *ALLOBJ authority from changing these system values with the CHGSYSVAL command. In addition to restricting changes to these system values, you can also restrict adding digital certificates to digital certificate store with the Add Verifier API and restrict password resetting on the digital certificate store.

Note: If you lock the security-related system values and need to perform a restore operation as part of a system recovery, be aware that you need to unlock the system values to complete the restore operation. This ensures that the system values are free to be changed during the initial program load (IPL).

You can restrict the following system values by using the lock option:

Table 5. System values that can be locked

QALWJOBITP	QAUTORMT	QLMTDEVSSN	QPWDLMTREP	QRETSVRSEC
QALWOBJRST	QAUTOVRT	QLMTSECOFR	QPWDLVL	QRMTSIGN
QALWUSRDMN	QCRTAUT	QMAXSGNACN	QPWDMAXLEN	QRMTSRVATR
QAUDCTL	QCRTOBJAUD	QMAXSIGN	QPWDMINLEN	QSCANFS
QAUDENDACN	QDEVRCYACN	QPWDCHGBLK	QPWDPOSDIF	QSCANFCTL
QAUDFRCLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QSECURITY
QAUDLVL	QDSCJOBITV	QPWDEXPWRN	QPWDRQDDIF	QSHRMEMCTL
QAUDLVL2	QFRCCVNRST	QPWDLMTAJC	QPWDRULES	QUSEADPAUT
QAUTOCFG	QINACTMSGQ	QPWDLMTCHR	QPWDVLDPGM	QVFOBJRST

You can use system service tools (SST) or dedicated service tools (DST) to lock and unlock the security-related system values. However, you must use DST if you are in recovery mode because SST is not available during this mode. Otherwise, use SST to lock or unlock the security-related system values.

To lock or unlock security-related system values with the Start System Service Tools (STRSST) command, follow these steps:

Note: You must have a service tools user ID and password to lock or unlock the security-related system values.

1. Open a character-based interface.
2. On the command line, type STRSST.
3. Type your service tools user ID and password.
4. Select option 7 (Work with system security).
5. Type 1 to unlock security-related system values or 2 to lock security-related system values in the **Allow system value security changes** parameter.

To lock or unlock security-related system values using dedicated service tools (DST) during an attended IPL of a system recovery, follow these steps:

1. From the IPL or Install the System display, select option 3 (Use Dedicated Service Tools).

Note: This step assumes that you are in recovery mode and are performing an attended IPL.

2. Sign on to DST using your service tools user ID and password.
3. Select option 13 (Work with system security).
4. Type 1 to unlock security-related system values or 2 to lock security-related system values in the **Allow system value security changes** parameter.

Related concepts:

“System values” on page 3

System values provide customization on many characteristics of your System i platform. You can use system values to define system-wide security settings.

General security system values

This topic introduces the general system values that you can use to control security on your IBM i operating system.

Overview:

General security system values allow you to set security function to support the decisions you made when developing your security policy. For example, in your security policy you state that systems containing confidential information, such as customer accounts or payroll inventories, need a stricter level of security than systems used for testing applications that are developed within your company. You can then plan and set a security level on these systems that corresponds with the decisions you made while developing your security policy.

Purpose:

Specify system values that control security on the system.

How To:

WRKSYSVAL *SEC (Work with System Values command)

Authority:

*ALLOBJ and *SECADM

Journal Entry:

SV

Note: Changes take effect immediately. IPL is required only when changing the security level (QSECURITY system value) or password level (QPWDLVL system value).

General system values that control security on your system are as follows:

QALWUSRDMN

Allow user domain objects in the libraries

QCRTAUT

Create default public authority

QDSPSGNINF

Display sign-on information

QFRCCVNRST

Force conversion on restore

QINACTITV

Inactive job time-out interval

QINACTMSGQ

Inactive job message queue

- QLMTDEVSSN**
Limit device sessions
- QLMTSECOFR**
Limit security officer
- QMAXSIGN**
Maximum sign-on attempts
- QMAXSGNACN**
Action when maximum sign-on attempts exceeded
- QRETSVRSEC**
Retain Server Security
- QRMTSIGN**
Remote sign-on requests
- QSCANFS**
Scan file systems
- QSCANFCTL**
Scan file systems control
- QSECURITY**
Security level
- QSHRMEMCTL**
Shared memory control
- QUSEADPAUT**
Use Adopted Authority
- QVFYOBJRST**
Verify object on restore

Allow User Domain Objects (QALWUSRDMN)

All objects are assigned a domain attribute when they are created. A domain is a characteristic of an object that controls how programs can access the object. The Allow User Domain Objects (QALWUSRDMN) system value specifies which libraries are allowed to contain user domain objects of type *USRSPC, *USRIDX, and *USRQ.

Systems with high security requirements require the restriction of user *USRSPC, *USRIDX, *USRQ objects. The system cannot audit the movement of information to and from user domain objects. The restriction does not apply to user domain objects of type program (*PGM), server program (*SRVPGM), and SQL packages (*SQLPKG).

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 6. Possible values for the QALWUSRDMN system value:

*ALL	User domain objects are allowed in all libraries and directories on the system. This is the shipped value.
*DIR	User domain objects are allowed in all directories on the system.
<i>library- name</i>	The names of up to 50 libraries that can contain user domain objects of type *USRSPC, *USRIDX, and *USRQ. If individual libraries are listed, the library QTEMP <i>must</i> be included in the list.

Recommended value: For most systems, the recommended value is *ALL. If your system has a high security requirement, you should allow user domain objects only in the QTEMP library.

Some systems have application software that relies on object types *USRSPC, *USRIDX, or *USRQ. For those systems, the list of libraries for the QALWUSRDMN system value should include the libraries that are used by the application software. The public authority of any library placed in QALWUSRDMN, except QTEMP, should be set to *EXCLUDE. This limits the number of users that can use MI interface to read or change the data in user domain objects in these libraries without being audited.

Note: If you run the Reclaim Storage (RCLSTG) command, user domain objects might need to be moved in and out of the QRCL (reclaim storage) library. To run the RCLSTG command successfully, you might need to add the QRCL library to the QALWUSRDMN system value. To protect system security, set the public authority to the QRCL library to *EXCLUDE. Remove the QRCL library from the QALWUSRDMN system value when you have finished running the RCLSTG command.

Authority for New Objects (QCRTAUT)

The Authority for New Objects (QCRTAUT) system value specifies the public authority for a newly created object.

The QCRTAUT system value is used to determine the public authority for a newly created object if the following conditions are met:

- The create authority (CRTAUT) for the library of the new object is set to *SYSVAL.
- The new object is created with public authority (AUT) of *LIBCRTAUT.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 7. Possible values for the QCRTAUT system value:

*CHANGE	The public can change newly created objects.
*USE	The public may view, but not change, newly created objects.
*ALL	The public may perform any function on new objects.
*EXCLUDE	The public is not allowed to use new objects.

Recommended value:

*CHANGE

The QCRTAUT system value is not used for objects created in directories in the enhanced file system.

Attention: Several IBM-supplied libraries, including QSYS, have a CRTAUT value of *SYSVAL. If you change the QCRTAUT system value to something other than *CHANGE, you might encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than *CHANGE, make sure that all device descriptions and their associated message queues have a PUBLIC authority of *CHANGE. One way to accomplish this is to change the CRTAUT value for library QSYS to *CHANGE from *SYSVAL.

Display Sign-On Information (QDSPGNINF)

The Display Sign-On Information (QDSPGNINF) system value determines whether the Sign-on Information display is shown after signing on.

The Sign-on Information display shows:

- Date of last sign-on
- Any password verifications that were not valid
- The number of days until the password expires (if the password is due to expire within the password expiration warning days (QPWDEXPWRN))

```

                Sign-on Information
                System:
Previous sign-on . . . . . : 10/30/91 14:15:00
Password verifications not valid . . . . . : 3
Days until password expires . . . . . : 5

```

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 8. Possible values for the QDSPSGNINF system value:

<u>0</u>	Display is not shown.
1	Display is shown.

Recommended value: 1 (Display is shown) is recommended so that users can monitor attempted use of their profiles and know when a new password is needed.

Note: Display sign-on information can also be specified in individual user profiles.

Inactive Job Time-Out Interval (QINACTIV)

The Inactive Job Time-Out Interval (QINACTIV) system value specifies in minutes how long the system allows a job to be inactive before taking action.

A workstation is considered inactive if it is in display wait (DSPW) status, or if it is waiting for message input with no user interaction. Some examples of user interaction are:

- Using the Enter key
- Using the paging function
- Using function keys
- Using the Help key

Emulation sessions through System i Access are included. Local jobs that are signed on to a remote system are excluded. Jobs that are connected by file transfer protocol (FTP) are excluded. To control the time-out of FTP connections, change the INACTTIMO parameter on the Change FTP Attribute (CHGFTP) command. To control the time-out of telnet sessions before V4R2, use the Change Telnet Attribute (CHGTELNA) command.

The following examples show how the system determines which jobs are inactive:

- A user uses the system request function to start a second interactive job. A system interaction, such as the Enter key, on either job causes both jobs to be marked as active.
- A System i Access job might appear inactive to the system if the user is performing PC functions, such as editing a document, without interacting with the system.

The QINACTMSGQ system value determines what action the system takes when an inactive job exceeds the specified interval.

When the system is started, it checks for inactive jobs at the interval specified by the QINACTIV system value. For example, if the system is started at 9:46 in the morning and the QINACTIV system value is 30 minutes, it checks for inactive jobs at 10:16, 10:46, 11:16, and so on. If it discovers a job that has been

inactive for 30 minutes or more, it takes the action specified by the QINACTMSGQ system value. In this example, if a job becomes inactive at 10:17, it will not be acted on until 11:16. At the 10:46 check, it has been inactive for only 29 minutes.

The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed on. An inactive workstation might allow an unauthorized person access to the system.

Table 9. Possible values for the QINACTITV system value:

*NONE:	The system does not check for inactive jobs.
<i>interval-in-minutes</i>	Specify a value of 5 through 300. When a job has been inactive for that number of minutes, the system takes the action specified in QINACTMSGQ.

Recommended value: 60 minutes

Inactive Job Time-Out Message Queue (QINACTMSGQ)

The Inactive Job Time-Out Message Queue (QINACTMSGQ) system value specifies what action the system takes when the inactive job time-out interval for a job has been reached.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 10. Possible values for QINACTMSGQ system value:

*ENDJOB	Inactive jobs are ended. If the inactive job is a group job, ¹ all jobs associated with the group are also ended. If the job is part of a secondary job, ¹ both jobs are ended. The action taken by *ENDJOB is equal to running the command ENDJOB JOB(name) OPTION (*IMMED) ADLINTJOBS(*ALL) against the inactive job.
*DSCJOB	The inactive job is disconnected, as are any secondary or group jobs ¹ associated with it. The disconnected job time-out interval (QDSCJOBITV) system value controls whether the system eventually ends disconnected jobs. See “Disconnected Job Time-Out Interval (QDSCJOBITV)” on page 38 for more information. Attention: The system cannot disconnect some jobs, such as PC Organizer and PC text-assist function (PCTA). If the system cannot disconnect an inactive job, it ends the job instead.
<i>message-queue-name</i>	Message CPI1126 is sent to the specified message queue when the inactive job time-out interval is reached. This message states: Job &3/&2/&1; has not been active. The message queue must exist before it can be specified for the QINACTMSGQ system value. This message queue is automatically cleared during an IPL. If you assign QINACTMSGQ as the user's message queue, all messages in the user's message queue are lost during each IPL.
¹ The Work management topic describes group jobs and secondary jobs.	

Recommended value: *DSCJOB is recommended unless your users run System i Access jobs. Using *DSCJOB when some System i Access jobs are running is the equivalent of ending the jobs. It can cause significant loss of information. Use the *message-queue* option if you have the System i Access licensed program. The CL Programming topic shows an example of writing a program to handle messages.

Using a message queue: A user or a program can monitor the message queue and take action as needed, such as ending the job or sending a warning message to the user. Using a message queue allows you to

make decisions about particular devices and user profiles, rather than treating all inactive devices in the same way. This method is recommended when you use the System i Access licensed program.

If a workstation with two secondary jobs is inactive, two messages are sent to the message queue (one for each secondary job). A user or program can use the End Job (ENDJOB) command to end one or both secondary jobs. If an inactive job has one or more group jobs, a single message is sent to the message queue. Messages continue to be sent to the message queue for each interval that the job is inactive.

Limit Device Sessions (QLMTDEVSSN)

The Limit Device Sessions (QLMTDEVSSN) system value specifies whether the number of device sessions allowed for a user is limited.

This value does not restrict the System Request menu or a second sign-on from the same device. If a user has a disconnected job, the user is allowed to sign on to the system with a new device session.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 11. Possible values for the QLMTDEVSSN system value:

<u>0</u>	The user is not limited to a specific number of device sessions.
1	The user is limited to a single device session.
2 - 9	The user is limited to the specified number of device sessions.

Recommended value: 1 (Yes) is recommended because limiting users to a single device reduces the likelihood of sharing passwords and leaving devices unattended.

Note: Limiting device sessions can also be specified in individual user profiles.

Limit Security Officer (QLMTSECOFR)

The Limit Security Officer (QLMTSECOFR) system value controls whether a user with all-object (*ALLOBJ) or service (*SERVICE) special authority can sign on to any workstation. Limiting powerful user profiles to certain well-controlled workstations provides security protection.

The QLMTSECOFR system value is only enforced at security level 30 and higher. "Workstations" on page 201 provides more information about the authority required to sign on at a workstation.

You can always sign on at the console with the QSECOFR, QSRV, and QSRVBAS profiles, no matter how the QLMTSECOFR value is set.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 12. Possible values for the QLMTSECOFR system value:

<u>1</u>	A user with *ALLOBJ or *SERVICE special authority can sign on at a workstation only if that user is specifically authorized (that is, given *CHANGE authority) to the workstation or if user profile QSECOFR is authorized (given *CHANGE authority) to the workstation. This authority cannot come from public authority.
0	Users with *ALLOBJ or *SERVICE special authority can sign on at any workstation for which they have *CHANGE authority. They can receive *CHANGE authority through private or public authority or because they have *ALLOBJ special authority.

Recommended value: 1 (Yes)

Maximum Sign-On Attempts (QMAXSIGN)

The Maximum Sign-On Attempts (QMAXSIGN) system value controls the number of consecutive sign-on or password verification attempts that are not correct by local and remote users.

Incorrect sign-on or password verification attempts can be caused by a user ID that is not correct, a password that is not correct, or inadequate authority to use the workstation.

When the maximum number of sign-on or password verification attempts is reached, the QMAXSGNACN system value is used to determine the action to be taken. A CPF1393 message is sent to the QSYSOPR message queue (and QSYSMSG message queue if it exists in library QSYS) to notify the security officer of a possible intrusion.

If you create the QSYSMSG message queue in the QSYS library, messages about critical system events are sent to that message queue as well as to QSYSOPR. The QSYSMSG message queue can be monitored separately by a program or a system operator. This provides additional protection of your system resources. Critical system messages in QSYSOPR are sometimes missed because of the volume of messages sent to that message queue.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 13. Possible values for the QMAXSIGN system value:

<u>3</u>	A user can try a maximum of 3 sign-on or password verification attempts.
*NOMAX	The system allows an unlimited number of incorrect sign-on or password verification attempts. This gives a potential intruder unlimited opportunities to guess a valid user ID and password combination.
<i>limit</i>	Specify a value from 1 through 25. The recommended number of sign-on or password verification attempts is three. Typically, three attempts are enough to correct typing errors but low enough to help prevent unauthorized access.

Recommended value: 3

Action When Sign-On Attempts Reached (QMAXSGNACN)

The Action When Sign-On Attempts Reached (QMAXSGNACN) system value determines what the system does when the maximum number of sign-on or password verification attempts is reached at a workstation.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 14. Possible values for the QMAXSGNACN system value:

<u>3</u>	Disable both the user profile and device.
1	Disable the device only.
2	Disable the user profile only.

The system disables a device by varying it off. The device is disabled only if the sign-on attempts that are not valid are consecutive on the same device. One valid sign-on resets the count of incorrect sign-on attempts for the device.

The system disables a user profile by changing the *Status* parameter to *DISABLED. The user profile is disabled when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same or different devices. One valid sign-on or password verification resets the count of incorrect sign-on attempts in the user profile.

If you create the QSYSMSG message queue in QSYS, the message sent (CPF1397) contains the user and device name. Therefore, it is possible to control the disabling of the device based on the device being used.

“Maximum Sign-On Attempts (QMAXSIGN)” on page 30 provides more information about the QSYSMSG message queue.

If the QSECOFR profile is disabled, you may sign on as QSECOFR at the console and enable the profile. If the console is varied off and no other user can vary it on, you must IPL the system to make the console available.

Recommended value: 3

Retain Server Security (QRETSVRSEC)

The Retain Server Security (QRETSVRSEC) system value determines whether decryptable authentication information associated with user profiles or validation list (*VLDL) entries can be retained on the host system. This does not include the System i user profile password.

If you change the value from 1 to 0, the system disables access to the authentication information. If you change the value back to 1, the system reenables access to the authentication information.

The authentication information can be removed from the system by setting the QRETSVRSEC system value to 0 and running the Clear Server Security Data (CLRSVRSEC) command. If you have a large number of user profiles or validation lists on your system the **CLRSVRSEC** command might run for an extensive period of time.

The encrypted data field of a validation list entry is typically used to store authentication information. Applications specify whether to store the encrypted data in a decryptable or non-decryptable form. If the applications choose a decryptable form and the QRETSVRSEC value is changed from 1 to 0, the encrypted data field information is not accessible from the entry. If the encrypted data field of a validation list entry is stored in a non-decryptable form, it is not affected by the QRETSVRSEC system value.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 15. Possible values for the QRETSVRSEC system value:

<u>0</u>	Server security data is not retained.
1	Server security data is retained.

Recommended value: 0

Related concepts:

“Using validation lists” on page 243

Validation list objects provide a method for applications to securely store user-authentication information.

Remote power-on and restart (QRMTIPL)

One part of your system security plan is to determine whether you will allow remote users to power-on and restart the system. The Remote power-on and restart (QRMTIPL) system value provides you the ability to start the remote system by using your telephone and a modem or the SPCN signal.

When QRMTIPL is set to 1 (Yes), any telephone call causes the system to restart. Even though this system value deals with restart options of your system, it has security implications. Obviously you do not want someone inadvertently restarting your systems. However, if you use a remote system to administer your system you will need to allow remote restart.

Table 16. Possible values for the remote power-on and restart system value (QRMTIPL)

<u>0</u>	Do not allow remote power-on and restart
1	Allow remote power-on and restart

Related information:

Restart system values: Allow remote power-on and restart

Remote Sign-On Control (QRMTSIGN)

The Remote Sign-On Control (QRMTSIGN) system value specifies how the system handles remote sign-on requests.

Examples of remote sign-on are display station pass-through from another system, the workstation function of the System i Access licensed program, and TELNET access.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 17. Possible values for the QRMTSIGN system value:

*FRCSIGNON	Remote sign-on requests must go through the normal sign-on process.
*SAMEPRF	When the source and target user profile names are the same, the sign-on display can be bypassed if automatic sign-on is requested. Password verification occurs before the target pass-through program is used. If a password that is not valid is sent on an automatic sign-on attempt, the pass-through session always ends and an error message is sent to the user. However, if the profile names are different, *SAMEPRF indicates that the session ends with a security failure even if the user entered a valid password for the remote user profile. The sign-on display appears for pass-through attempts not requesting automatic sign-on.
*VERIFY	The *VERIFY value allows you to bypass the sign-on display of the target system if valid security information is sent with the automatic sign-on request. If the password is not valid for the specified target user profile, the pass-through session ends with a security failure. If the target system has a QSECURITY value of 10, any automatic sign-on request is allowed. The sign-on display appears for pass-through attempts not requesting automatic sign-on.
*REJECT	No remote sign-on is permitted.
	For TELNET access, there is no action for *REJECT.
<i>program-name library-name</i>	The program specified runs at the start and end of every pass-through session.

Recommended value: *REJECT is recommended if you do not want to allow any pass-through or System i Access access. If you do allow pass-through or System i Access access, use *FRCSIGNON or *SAMEPRF.

The Remote Workstation Support  book contains detailed information about the QRMTSIGN system value. It also contains the requirements for a remote sign-on program and an example.

Scan File Systems (QSCANFS)

The Scan File Systems (QSCANFS) system value allows you the option to specify the integrated file system in which objects will be scanned.

For example, you can use this option to scan for a virus. Integrated file system scanning is enabled when exit programs are registered with any of the integrated file system scan-related exit points. The QSCANFS system value specifies the integrated file systems in which objects will be scanned when exit programs are registered with any of the integrated file system scan-related exit points.

The integrated file system scan-related exit points are:

- QIBM_QP0L_SCAN_OPEN — Integrated file system scan on open exit.
- QIBM_QP0L_SCAN_CLOSE — Integrated file system scan on close exit.

For more information about integrated file systems, see the Integrated file system topic.

Table 18. Possible values for the QSCANFS system value:

*NONE	No integrated file system objects will be scanned.
*ROOTOPNUD	Objects of type *STMF that are in *TYPE2 directories in the "root" (/), QOpenSys, and user-defined file systems will be scanned.

Recommended value: The recommended value is *ROOTOPNUD so that the "root" (/), QOpenSys and user-defined file systems are scanned when anyone registers exit programs with the integrated file system scan-related exit points.

Related reference:

“Scan File Systems Control (QSCANFSCTL)”

The Scan File Systems Control (QSCANFSCTL) system value controls the integrated file system scanning that is enabled when exit programs are registered with any of the integrated file system scan-related exit points.

Related information:

*TYPE2 directories

Scan File Systems Control (QSCANFSCTL)

The Scan File Systems Control (QSCANFSCTL) system value controls the integrated file system scanning that is enabled when exit programs are registered with any of the integrated file system scan-related exit points.

QSCANFSCTL works with the scan file systems system value to provide granular controls on how and what is scanned in the integrated file system. You can choose different scanning options or you can select to use default scan options. Also, you can select several scan options which control how and what the registered exit programs will scan. These options are described in following table:

Table 19. Possible values for the QSCANFSCTL system value:

*NONE	No controls are being specified for the integrated file system scan-related exit points.
-------	--

Table 19. Possible values for the QSCANFCTL system value: (continued)

*ERRFAIL	If there are errors when calling the exit program (for example, program not found or the exit program signals an error), the system will fail the request which triggered the exit program call. If this is not specified, the system will skip the exit program and treat it as if the object was not scanned.
*FSVROLY	Only accesses through the file servers will be scanned. For example, accesses through Network File System will be scanned as well as other file server methods. If this is not specified, all accesses will be scanned.
*NOFAILCLO	The system will not fail the close requests with an indication of scan failure, even if the object failed a scan which was done as part of the close processing. Also, this value will override the *ERRFAIL specification for the close processing, but not for any other scan-related exit points.
*NOPOSTRST	<p>After objects are restored, they will not be scanned just because they were restored. If the object attribute is that "the object will not be scanned", the object will not be scanned at any time. If the object attribute is that "the object will be scanned only if it has been modified since the last time it was scanned", the object will only be scanned if it is modified after being restored.</p> <p>If *NOPOSTRST is not specified, objects will be scanned at least once after being restored. If the object attribute is that "the object will not be scanned", the object will be scanned once after being restored. If the object attribute is that "the object will be scanned only if it has been modified since the last time it was scanned", the object will be scanned after being restored because the restore will be treated as a modification to the object.</p> <p>In general, it may be dangerous to restore objects without scanning them at least once. It is best to use this option only when you know that the objects were scanned before they were saved or they came from a trusted source.</p>
*NOWRTUPG	The system will not attempt to upgrade the access for the scan descriptor passed to the exit program to include write access. If this is not specified, the system will attempt to do the write access upgrade.
*USEOCOATR	The system will use the specification of the "object change only" attribute to only scan the object if it has been modified (not also because scan software has indicated an update). If this is not specified, this "object change only" attribute will not be used, and the object will be scanned after it is modified and when scan software indicates an update.

Recommended value: If you want the most restrictive values specified for integrated file system scanning, then the recommended settings are *ERRFAIL and *NOWRTUPG. This ensures that any failure from the scan exit programs prevent the associated operations, as well as not give the exit program additional access levels. However, the *NONE value is a good option for most users. When installing code that is shipped from a trusted source, it is recommended that *NOPOSTRST be specified during that install time period.

Related reference:

“Scan File Systems (QSCANFS)” on page 33

The Scan File Systems (QSCANFS) system value allows you the option to specify the integrated file system in which objects will be scanned.

Share Memory Control (QSHRMEMCTL)

The Share Memory Control (QSHRMEMCTL) system value defines which users are allowed to use shared memory or mapped memory that has write capability.

Your environment may contain applications, each running different jobs, but sharing pointers within these applications. Using these APIs provides for better application performance and streamlines the application development by allowing shared memory and stream files among these different applications

and jobs. However, use of these APIs might potentially pose a risk to your system and assets. A programmer can have write access and can add, change, and delete entries in the shared memory or stream file.

To change this system value, users must have `*ALLOBJ` and `*SECADM` special authorities. A change to this system value takes effect immediately.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 20. Possible values for the QSHRMEMCTL system value:

0	<p>Users cannot use shared memory, or use mapped memory that has write capability.</p> <p>This value means that users cannot use shared-memory APIs (for example, <code>shmat()</code> — Shared Memory Attach API), and cannot use mapped memory objects that have write capability (for example, <code>mmap()</code> — Memory Map a File API provides this function).</p> <p>Use this value in environments with higher security requirements.</p>
<u>1</u>	<p>Users can use shared memory or mapped memory that has write capability.</p> <p>This value means that users can use shared-memory APIs (for example, <code>shmat()</code> — Shared Memory Attach API), and can use mapped memory objects that have write capability (for example, <code>mmap()</code> — Memory Map a File API provides this function).</p>

Recommended value: 1

Use Adopted Authority (QUSEADPAUT)

The Use Adopted Authority (QUSEADPAUT) system value defines which users can create programs with the use adopted authority (`*USEADPAUT(*YES)`) attribute.

All users authorized by the QUSEADPAUT system value can create or change programs and service programs to use adopted authority if the user has the necessary authority to the program or service program.

The system value can contain the name of an authorization list. The user's authority is checked against this list. If the user has at least `*USE` authority to the named authorization list, the user can create, change, or update programs or service programs with the `USEADPAUT(*YES)` attribute. The authority to the authorization list cannot come from adopted authority.

If an authorization list is named in the system value and the authorization list is missing, the function being attempted will not complete. A message is sent indicating this.

However, if the program is created with the `QPRCRTPG` API, and the `*NOADPAUT` value is specified in the option template, the program creates successfully even if the authorization list does not exist.

If more than one function is requested on the command or API, and the authorization list is missing, the function is not performed.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 21. Possible values for the QUSEADPAUT system value:

<i>authorization list name</i>	A diagnostic message is signaled to indicate that the program is created with USEADPAUT(*NO) if all of the following are true: <ul style="list-style-type: none"> • The user does not have authority to the specified authorization list. • There are no other errors when the program or service program is created.
*NONE¹	All users can create, change, or update programs and service programs to use the authority of the program which called them if the user has the necessary authority to the program or service program.
¹	*NONE indicates that no authorization list is used and by default all users will be allowed to access programs that use adopted authority.

Recommended value: For production machines, create an authorization list with authority of *PUBLIC(*EXCLUDE). Specify this authorization list for the QUSEADPAUT system value. This prevents anyone from creating programs that use adopted authority.

You should carefully consider the security design of your application before creating the authorization list for QUSEADPAUT system value. This is especially important for application development environments.

Security-related system values

This topic introduces the security-related system values on your IBM i operating system.

Overview:

Purpose:

Specify system values that relate to security on the system.

How To:

WRKSYSVAL (Work with System Values command)

Authority:

*ALLOBJ and *SECADM

Journal Entry:

SV

Note: Changes take effect immediately. IPL is not required.

The following information are descriptions of additional system values that relate to security on your system. These system values are not included in the *SEC group on the Work with System Values display.

QAUTOCFG

Automatic device configuration

QAUTOVRT

Automatic configuration of virtual devices

QDEVRCYACN

Device recovery action

QDSCJOBIV

Disconnected job time-out interval

Note: This system value is also discussed in the Jobs system values: Time-out interval for disconnected jobs topic.

QRMTSRVATR

Remote service attribute

QSSLCSL

Secure Sockets Layer (SSL) cipher specification list

QSSLCSLCTL

Secure Sockets Layer (SSL) cipher control

QSSLPCL

Secure Sockets Layer (SSL) protocols

Related concepts:

“Validation of programs being restored” on page 17

When a program is created, the system calculates a validation value, which is stored with the program. When the program is restored, the validation value is calculated again and compared to the validation value that is stored with the program.

Automatic Device Configuration (QAUTOCFG)

The Automatic Device Configuration (QAUTOCFG) system value automatically configures locally attached devices. The value specifies whether devices that are added to the system are configured automatically.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 22. Possible values for the QAUTOCFG system value:

<u>0</u>	Automatic configuration is off. You must configure manually any new local controllers or devices that you add to your system.
1	Automatic configuration is on. The system automatically configures any new local controllers or devices that you add to your system. The operator receives a message that indicates the changes to the system's configuration.

Recommended value: When initiating system setup or when adding many new devices, the system value should be set to 1. At all other times the system value should be set at 0.

Automatic Configuration of Virtual Devices (QAUTOVRT)

The Automatic Configuration of Virtual Devices (QAUTOVRT) system value specifies whether pass-through virtual devices and TELNET full screen virtual devices (as opposed to the workstation function virtual device) are automatically configured.

A *virtual device* is a device description that does not have hardware associated with it. It is used to form a connection between a user and a physical workstation attached to a remote system.

Allowing the system to automatically configure virtual devices makes it easier for users to break into your system using pass-through or telnet. Without automatic configuration, a user attempting to break in has a limited number of attempts at each virtual device. The limit is defined by the security officer using the QMAXSIGN system value. With automatic configuration active, the actual limit is higher. The system sign-on limit is multiplied by the number of virtual devices that can be created by the automatic configuration support. This support is defined by the QAUTOVRT system value.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 23. Possible values for the QAUTOVRT system value:

<u>0</u>	No virtual devices are created automatically.
----------	---

Table 23. Possible values for the QAUTOVRT system value: (continued)

number-of- virtual- devices	Specify a value 1 through 32500. If fewer than the specified number of devices are attached to a virtual controller and no device is available when a user attempts pass-through or full screen TELNET, the system configures a new device.
-----------------------------	---

Recommended value: 0

Related information:



Remote Workstation Support

TCP/IP setup

Device Recovery Action (QDEVRCYACN)

The Device Recovery Action (QDEVRCYACN) system value specifies what action to take when an I/O error occurs for an interactive job's workstation.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 24. Possible values for the QDEVRCYACN system value:

*DSCMSG	Disconnects the job. When signing on again, an error message is sent to the user's application program.
*MSG	Signals the I/O error message to the user's application program. The application program performs error recovery.
*DSCENDRQS	Disconnects the job. When signing on again, a cancel request function is performed to return control of the job back to the last request level.
*ENDJOB	Ends the job. A job log is produced for the job. A message indicating that the job ended because of the device error is sent to the job log and the QHST log. To minimize the performance effect of the ending job, the job's priority is lowered by 10, the time slice is set to 100 milliseconds and the purge attribute is set to yes.
*ENDJOBNOLIST	Ends the job. A job log is not produced for the job. A message is sent to the QHST log indicating that the job ended because of the device error.

When a value of *MSG or *DSCMSG is specified, the device recovery action is not performed until the job performs the next I/O operation. In an LAN/WAN environment, this allows one device to disconnect and another to connect, using the same address, before the next I/O operation for the job occurs. The job can recover from the I/O error message and continue running to the second device. To avoid this, specify a device recovery action of *DSCENDRQS, *ENDJOB, or *ENDJOBNOLIST. These device recovery actions are performed immediately when an I/O error, such as a power-off operation, occurs.

Recommended value: *DSCMSG

Note: *ALLOBJ and *SECADM special authorities are not required to change this value.

Disconnected Job Time-Out Interval (QDSCJOBTV)

The Disconnected Job Time-Out Interval (QDSCJOBTV) system value determines if and when the system ends a disconnected job. The interval is specified in minutes.

If you set the QINACTMSGQ system value to disconnect inactive jobs (*DSCJOB), you should set the QDSCJOBTV to end the disconnected jobs eventually. A disconnected job uses up system resources, as well as retaining any locks on objects.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 25. Possible values for the QDSCJOBTV system value:

<u>240</u>	The system ends a disconnected job after 240 minutes.
*NONE	The system does not automatically end a disconnected job.
<i>time-in-minutes</i>	Specify a value between 5 and 1440.

Recommended value: 120

Remote Service Attribute (QRMTSRVATR)

The Remote Service Attribute (QRMTSRVATR) controls the remote system service problem analysis ability. The value allows the system to be analyzed remotely.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

The values allowed for the QRMTSRVATR system value are:

Table 26. Possible values for the QRMTSRVATR system value:

<u>0</u>	Remote service attribute is off.
<u>1</u>	Remote service attribute is on.

Recommended value: 0

Related concepts:

“Keylock security” on page 2

You can retrieve and change the keylock position by using the Retrieve IPL Attributes (QWCRIPLA) API or the Change IPL Attributes (CHGIPLA) command.

Secure Sockets Layer (SSL) cipher specification list (QSSLCSL)

The Secure Sockets Layer cipher specification list (QSSLCSL) system value determines what cipher specification list will be supported by System SSL.

System SSL uses the sequence of the values in QSSLCSL to order the System SSL default cipher specification list. The default cipher specification list entries are system defined and can be changed on release boundaries. If a default cipher suite is removed from the QSSLCSL system value, it is also removed from the default cipher specification list. The default cipher suite is added back to the default cipher specification list when the cipher suite is added back into the QSSLCSL system value. You cannot add other cipher suites to the default cipher specification list beyond the system defined set for the release. Besides, a cipher suite cannot be added to QSSLCSL if the required SSL protocol value for the cipher suite is not set for the QSSLPCL (SSL protocol list) system value.

The values of the QSSLCSL system value are read-only unless the SSL cipher control (QSSLCSLCTL) system value is set to *USRDFN.

The values allowed for the QSSLCSL system value are as follows:

- *RSA_AES_128_CBC_SHA
- | • *RSA_AES_128_CBC_SHA256
- | • *RSA_AES_256_CBC_SHA256
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5

- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_EXPORT_RC4_40_MD5
- *RSA_NULL_SHA256
- *RSA_NULL_SHA
- *RSA_NULL_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_DES_CBC_MD5

Note: You must have *IOSYSCFG, *ALLOBJ, and *SECADM special authorities to change this system value.

You can refer to the Secure Sockets Layer cipher specification list topic in the System values topic collection for more information about the shipped values.

Related information:

Security system values: Secure Sockets Layer cipher specification list
System SSL Properties

Secure Sockets Layer (SSL) cipher control (QSSLCSLCTL)

The Secure Sockets Layer cipher control (QSSLCSLCTL) system value specifies whether the system or the user controls the Secure Sockets Layer cipher specification list (QSSLCSL) system value.

The values allowed for the QSSLCSLCTL system value are as follows:

- *OPSYS
- *USRDFN

Note: You must have *IOSYSCFG, *ALLOBJ, and *SECADM special authorities to change this system value.

You can refer to the Secure Sockets Layer cipher control topic in the System values topic collection for more information about the shipped values.

Related information:

Security system values: Secure Sockets Layer cipher control

Secure Sockets Layer (SSL) protocols (QSSLPCL)

The Secure Sockets Layer protocols (QSSLPCL) system value specifies the Secure Sockets Layer (SSL) protocols supported by the System SSL.

The values allowed for the QSSLPCL system value are as follows:

- *OPSYS
- *TLSV1.2
- *TLSV1.1
- *TLSV1
- *SSLV2
- *SSLV3

Note: You must have *IOSYSCFG, *ALLOBJ, and *SECADM special authorities to change this system value.

You can refer to the Secure Sockets Layer protocols topic in the System values topic collection for more information about the shipped values.

Related information:

Security system values: Secure Sockets Layer protocols

Security-related restore system values

This topic introduces the security-related restore system values on your IBM i operating system.

Overview:

Purpose:

Controls how and which security-related objects are restored on the system.

How To:

WRKSYSVAL*SEC (Work with System Values command)

Authority:

*ALLOBJ and *SECADM

Journal Entry:

SV

Note: Changes take effect immediately. IPL is not required.

The following information are descriptions of system values that relate to restoring security-related objects on the system which should be considered when restoring objects as well. See Table 19 on page 33 for more information about the QSCANFSTL *NOPOSTRST system value.

QVfyOBRST

Verify object on restore

QFRCCVNRST

Force conversion on restore

QALWOBJRST

Allow restoring of security sensitive objects

Descriptions of these system values follow. For each value, the possible choices are shown. The choices that are underlined> are the system-supplied defaults.

Related concepts:

“Restoring programs” on page 252

Restoring programs to your system that are obtained from an unknown source poses a security exposure. This topic provides information about the factors that should be taken into consideration when restoring programs.

Verify Object on Restore (QVfyOBRST)

The Verify Object on Restore (QVfyOBRST) system value determines whether objects are required to have digital signatures in order to be restored to your system.

You can prevent anyone from restoring an object, unless that object has a correct digital signature from a trusted software provider. This value applies to objects of types: *PGM, *SRVPGM, *SQLPKG, *CMD and *MODULE. It also applies to *STMF objects which contain Java™ programs.

When an attempt is made to restore an object onto the system, three system values work together as filters to determine if the object is allowed to be restored. The first filter is the Verify Object on Restore (QVfyOjRst) system value. It is used to control the restore of some objects that can be digitally signed. The second filter is the Force Conversion on Restore (QFRCCVnrst) system value. This system value allows you to specify whether to convert programs, service programs, SQL packages, and module objects during the restore. It can also prevent some objects from being restored. Only objects that can get past the first two filters are processed by the third filter. The third filter is the Allow Object on Restore (QALWObjRst) system value. It specifies whether objects with security-sensitive attributes can be restored.

If Digital Certificate Manager (IBM i option 34) is not installed on the system, all objects except those signed by a system trusted source are treated as unsigned when determining the effects of the QVfyOjRst system value during a restore operation.

Program, service program and module objects that are created or converted on a system with a release before V6R1 are treated as unsigned when they are restored to a V6R1 or later system. Likewise, program, service program and module objects that are created or converted on a V6R1 or later release are treated as unsigned when they are restored to a system before V6R1.

A change to this system value takes effect immediately.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. Objects that have the system-state attribute and objects that have the inherit-state attribute are required to have a valid signature from a system-trusted source. Objects in Licensed Internal Code PTFs are also required to have a valid signature from a system-trusted source. If these objects do not have a valid signature, they cannot be restored, regardless of the value of the QVfyOjRst system value.

Attention: When your system is shipped, the QVfyOjRst system value is set to 3. If you change the value of QVfyOjRst, it is important to set the QVfyOjRst value to 3 or lower before installing a new release of the IBM i operating system.

Table 27. Possible values for the QVfyOjRst system value:

1	<p>Do not verify signatures on restore. Restore all user-state objects regardless of their signature.</p> <p>Do not use this value unless you have signed objects to restore which will fail their signature verification for some acceptable reason.</p>
2	<p>Verify objects on restore. Restore unsigned commands and user-state objects. Restore signed commands and user-state objects, even if the signatures are not valid.</p> <p>Use this value only if certain objects that you want to restore contain signatures that are not valid. In general, it is not recommended to restore objects with signatures that are not valid on your system.</p>
3	<p>Verify signatures on restore. Restore unsigned commands and user-state objects. Restore signed commands and user-state objects only if the signatures are valid.</p> <p>Use this value for normal operations, when you expect some of the objects you restore to be unsigned, but you want to ensure that all signed objects have signatures that are valid. Commands and programs you have created or purchased before digital signatures were available will be unsigned. This value allows those commands and programs to be restored. This is the default value.</p>

Table 27. Possible values for the QVFYOBJRST system value: (continued)

4	<p>Verify signatures on restore. Do not restore unsigned commands and user-state objects. Restore signed commands and user-state objects, even if the signatures are not valid.</p> <p>Use this value only if certain objects that you want to restore contain signatures that are not valid, but you do not want the possibility of unsigned objects being restored. In general, it is not recommended to restore objects with signatures that are not valid on your system.</p>
5	<p>Verify signatures on restore. Do not restore unsigned commands and user-state objects. Restore signed commands and user-state objects only if the signatures are valid.</p> <p>This value is the most restrictive value and should be used when the only objects you want to be restored are those which have been signed by trusted sources</p>

Some commands use a signature that does not include all parts of the object. Some parts of the command are not signed while other parts are only signed when they contain a non-default value. This type of signature allows some changes to be made to the command without invalidating its signature. Examples of changes that will not invalidate these types of signatures include:

- Changing command defaults.
- Adding a validity checking program to a command that does not have one.
- Changing the "where allowed to run" parameter.
- Changing the "allow limited user" parameter.

If you like, you can add your own signature to these commands that includes these areas of the command object.

Recommended value: 3

Force Conversion on Restore (QFRCCVNRST)

The Force Conversion on Restore (QFRCCVNRST) system value can force the conversion of some object types during a restore. This system value can also prevent some objects from being restored.

The QFRCCVNRST system value specifies whether to convert the following object types during a restore:

- program (*PGM)
- service program (*SRVPGM)
- SQL Package (*SQLPKG)
- module (*MODULE)

An object which is specified to be converted by the system value, but cannot be converted because it does not contain sufficient creation data, will not be restored.

The *SYSVAL value for the FRCOBJCVN parameter on the restore commands (RST, RSTLIB, RSTOBJ, RSTLICPGM) uses the value of this system value. Therefore, you can turn on and turn off conversion for the entire system by changing the QFRCCVNRST value. However, the FRCOBJCVN parameter overrides the system value in some cases. Specifying *YES and *ALL on the FRCOBJCVN will override all settings of the system value. Specifying *YES and *RQD on the FRCOBJCVN parameter is the same as specifying '2' for this system value and can override the system value when it is set to 0 or 1.

QFRCCVNRST is the second of three system values that work consecutively as filters to determine if an object is allowed to be restored, or if it is converted during the restore. The first filter, Verify Object on Restore (QVFYOBJRST) system value, controls the restore of some objects that can be digitally signed.

Only objects that can get past the first two filters are processed by the third filter, the Allow Object Restore (QALWOBJRST) system value, which specifies whether objects with security-sensitive attributes can be restored.

If Digital Certificate Manager (i5/OS option 34) is not installed on the system, all objects except those signed by a system trusted source are treated as unsigned when determining the effects of the QFRCCVNRST system value during a restore operation.

Program, service program and module objects that are created or converted on a system with a release before V6R1 are treated as unsigned when they are restored to a V6R1 or later system. Likewise, program, service program and module objects that are created or converted on a V6R1 or later release are treated as unsigned when they are restored to a system before V6R1.

The shipped value of QFRCCVNRST is 1. For all values of QFRCCVNRST an object which should be converted but cannot be converted will not be restored. Objects digitally signed by a system trusted source are restored without conversion for all values of this system value.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

The following table summarizes the allowed values for QFRCCVNRST:

Table 28. QFRCCVNRST values

0	Do not convert anything. Do not prevent anything from being restored.
1	Objects with validation errors will be converted.
2	Objects will be converted if their conversion is required for the current operating system or the current machine, or if they have a validation error.
3	Objects which are suspected of having been tampered with, objects which contain validation errors, and objects which require conversion to be used on the current version of the operating system or on the current machine will be converted.
4	Objects which contain sufficient creation data to be converted and do not have valid digital signatures will be converted. An object that does not contain sufficient creation data will be restored without conversion. Note: Objects (signed and unsigned) that have validation errors, are suspected of having been tampered with, or require conversion to be used on the current version of the operating system or on the current machine will be converted; or will fail to restore if they do not convert.
5	Objects that contain sufficient creation data will be converted. An object that does not contain sufficient creation data to be converted will be restored. Note: Objects that have validation errors, are suspected of having been tampered with, or require conversion to be used on the current version of the operating system or on the current machine that cannot be converted will not restore.
6	All objects which do not have a valid digital signature will be converted. Note: An object with a valid digital signature that also has a validation error or is suspected of having been tampered with will be converted, or if it cannot be converted, it will not be restored.
7	Every object will be converted.

When an object is converted, its digital signature is discarded. The state of the converted object is user state. Converted objects will have a good validation value and are not suspected of having been tampered with.

Recommended value: 3 or higher

Allow Restoring of Security-Sensitive Objects (QALWOBJRST)

The Allow Restoring of Security-Sensitive Objects (QALWOBJRST) system value determines whether objects that are security-sensitive may be restored to your system.

When an attempt is made to restore an object onto the system, three system values work together as filters to determine if the object is allowed to be restored, or if it is converted during the restore. The first filter is the Verify Object on Restore (QVFYOBJRST) system value. It is used to control the restore of some objects that can be digitally signed. The second filter is the Force Conversion on Restore (QFRCCVNRST) system value. This system value allows you to specify whether to convert programs, service programs, SQL packages, and module objects during the restore. It can also prevent some objects from being restored. Only objects that can get past the first two filters are processed by the third filter. The third filter is the Allow Object on Restore (QALWOBJRST) system value. It specifies whether objects with security-sensitive attributes can be restored. You can use it to prevent anyone from restoring a system state object or an object that adopts authority.

When your system is shipped, the QALWOBJRST system value is set to *ALL. This value is necessary to install your system successfully.

ATTENTION: It is important to set the QALWOBJRST value to *ALL before performing some system activities, such as:

- Installing a new release of the IBM i licensed program.
- Installing new licensed programs.
- Recovering your system.

These activities may fail if the QALWOBJRST value is not *ALL. To ensure system security, return the QALWOBJRST value to your normal setting after completing the system activity.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

You can specify multiple values for the QALWOBJRST system value, unless you specify *ALL or *NONE.

Table 29. Possible values for the QALWOBJRST system value:

*ALL	Any object can be restored to your system by a user with the correct authority.
*NONE	Security-sensitive objects, such as system state programs or programs that adopt authority, cannot be restored to the system.
*ALWYSSTT	System and inherit state objects can be restored to the system.
*ALWPGMADP	Objects that adopt authority can be restored to the system.
*ALWPTF	System and inherit state objects, objects that adopt authority, objects that have the S_ISUID(set-user-ID) attribute enabled, and objects that have S_ISGID (set-group-ID) attribute enabled can be restored to the system during PTF install.
*ALWSETUID	Allow restore of files that have the S_ISUID (set-user-ID) attribute enabled.
*ALWSETGID	Allow restore of files that have the S_ISGID (set-group-ID) attribute enabled.
*ALWVLDERR	Allow restore of objects that do not pass the object validation tests. If the setting of QFRCCVNRST system value causes the object to be converted, its validation errors will have been corrected.

Recommended value: The QALWOBJRST system value provides a method to protect your system from programs that may cause serious problems. For normal operations, consider setting this value to *NONE.

Remember to change it to *ALL before performing the activities listed previously. If you regularly restore programs and applications to your system, you might need to set the QALWOBJRST system value to *ALWPGMADP.

System values that apply to passwords

This topic describes the system values that apply to passwords. These system values require users to change passwords regularly and help prevent users from assigning trivial, easily guessed passwords. They can also make sure passwords meet the requirements of your communications network.

Overview:

Purpose:

Specify system values to set requirements for the passwords users assign.

How To:

WRKSYSVAL *SEC (Work with System Values command)

Authority:

*ALLOBJ and *SECADM

Journal Entry:

SV

Note: Changes take effect immediately (except for QPWDLVL). IPL is not required.

The system values control passwords:

QPWDCHGBLK

Block password change

QPWDEXPITV

Expiration interval

QPWDEXPWRN

Password expiration warning

QPWDLVL

Password level

QPWDLMTCHR

Restricted characters

QPWDLMTAJC

Restrict adjacent characters

QPWDLMTREP

Restrict repeating characters

QPWDMINLEN

Minimum length

QPWDMAXLEN

Maximum length

QPWDPOSDIF

Character position difference

QPWDRQDDIF

Required difference

QPWDRQDDGT

Require numeric character

QPWDRULES

Password rules

QPWDVLDPGM

Password validation program

The password-composition system values are enforced only when the password is changed using the **CHGPWD** command, the ASSIST menu option to change a password, or the QSYCHGPW application programming interface (API). They are not enforced when the password is set using the **CRTUSRPRF** or **CHGUSRPRF** command.

The system prevents a user from setting the password equal to the user profile name using the **CHGPWD** command, the ASSIST menu, or the QSYCHGPW API in any of the following conditions.

- The Password Rules (QPWDRULES) system value has a value of *PWDSYSVAL and the Password Minimum Length (QPWDMINLEN) system value has a value other than 1.
- The Password Rules (QPWDRULES) system value has a value of *PWDSYSVAL and the Password Maximum Length (QPWDMAXLEN) system value has a value other than 10.
- The Password Rules (QPWDRULES) system value has a value of *PWDSYSVAL and you change any of the other password-control system values from the defaults.

If a password is forgotten, the security officer can use the Change User Profile (**CHGUSRPRF**) command to set the password equal to the profile name or to any other value. The Set password to expired field in the user profile can be used to require that a password be changed the next time the user signs on.

Related information:

System values: Password overview

Block Password Change (QPWDCHGBLK)

The Block Password Change (QPWDCHGBLK) system value specifies the time period during which a password is blocked from being changed after the prior successful password change operation.

A change to this system value takes effect immediately.

Note: This system value is a restricted value. Refer to the Security System Values topic for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 30. Possible values for the QPWDCHGBLK system value:

<u>*NONE</u>	The password can be changed at any time.
1 - 99	A password cannot be changed within the specified number of hours after the prior successful password changed operation.

Password Expiration Interval (QPWDEXPITV)

The Password Expiration Interval (QPWDEXPITV) system value controls the number of days allowed before a password must be changed.

If a user attempts to sign on after the password has expired, the system shows a display requiring that the password be changed before the user is allowed to sign on.

Sign-on Information

System:

Password has expired. Password must be changed to continue sign-on request.

Previous sign-on : 10/30/99 14:15:00

Sign-on attempts not valid : 3

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 31. Possible values for the QPWDEXPITV system value:

*NOMAX	Users are not required to change their passwords.
limit-in-days	Specify a value from 1 through 366.

Recommended value: 30 to 90

Note: A password expiration interval can also be specified in individual user profiles.

Password Expiration Warning (QPWDEXPWRN)

The Password Expiration Warning (QPWDEXPWRN) system value specifies the number of days before a password expiration to begin displaying the password expiration warning messages when a user signs on.

A change to this system value takes effect immediately.

Note: This system value is a restricted value. Refer to the Security System Values topic for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 32. Possible values for the QPWDEXPWRN system value:

7	Specifies that the password expiration warning message should start to be displayed 7 days before the password expiration.
1 - 99	Specifies the number of days before the password expiration to begin displaying the password expiration warning message.

Recommended value: 14 (days)

Password Level (QPWDLVL)

The password level of the system can be set to allow for user profile passwords from 1-10 characters or to allow for user profile passwords from 1-128 characters.

The password level can be set to allow a passphrase as the password value. The term *passphrase* is sometimes used in the computer industry to describe a password value which can be very long and has few, if any, restrictions on the characters used in the password value. Blanks can be used between letters in a passphrase, which allows you to have a password value that is a sentence or sentence fragment. The only restrictions on a passphrase are that it cannot start with an asterisk (*) and trailing blanks will be removed. Before changing the password level of your system, review the section Planning password level changes.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 33. Possible values for the QPWDLVL system value:

0	<p>The system supports user profile passwords with a length of 1-10 characters. The allowable characters are A-Z, 0-9 and characters \$, @, # and underline.</p> <ul style="list-style-type: none"> • QPWDLVL 0 should be used if your system communicates with other System i platforms in a network and those systems are running with either a QPWDLVL value of 0 or an operating system release less than V5R1M0. • QPWDLVL 0 should be used if your system communicates with any other system that limits the length of passwords from 1-10 characters. • QPWDLVL 0 must be used if your system communicates with the IBM i Support for Windows Network Neighborhood IBM i NetServer) product and your system communicates with other systems using passwords from 1-10 characters. <p>When the QPWDLVL value of the system is set to 0, the operating system will create the encrypted password for use at QPWDLVL 2 and 3. The password value that can be used at QPWDLVL 2 and 3 will be the same password as is being used at QPWDLVL 0 or 1.</p>
1	<p>QPWDLVL 1 is the equivalent support of QPWDLVL 0 with the following exception: IBM i NetServer passwords for Windows 95/98/ME clients will be removed from the system.</p> <p>Note: The IBM i NetServer product will work with Windows NT/2000/XP/Vista clients when the password level is 1 or 3.</p> <p>Unless the Windows 95/98/ME clients are configured to use NTLMv2 passwords, you cannot use QPWDLVL value 1 to connect those clients to the IBM i NetServer product. QPWDLVL 1 improves the security of System i platforms by removing all LAN manager passwords from the system.</p>
2	<p>The system supports user profile passwords from 1-128 characters. Upper and lower case characters are allowed. Passwords can consist of any character and the password will be case sensitive. QPWDLVL 2 is viewed as a compatibility level. This level allows for a move back to QPWDLVL 0 or 1 as long as the password created on QPWDLVL 2 or 3 meets the length and syntax requirements of a password valid on QPWDLVL 0 or 1.</p> <ul style="list-style-type: none"> • QPWDLVL 2 can be used if your system communicates with the IBM i Support for Windows Network Neighborhood IBM i NetServer) product as long as your password is 1-14 characters in length. • QPWDLVL 2 cannot be used if your system communicates with other System i platforms in a network and those systems are running with either a QPWDLVL value of 0 or 1 or an operating system release less than V5R1M0. • QPWDLVL 2 cannot be used if your system communicates with any other system that limits the length of passwords from 1-10 characters. <p>No encrypted passwords are removed from the system when QPWDLVL is changed to 2.</p>

Table 33. Possible values for the QPWDLVL system value: (continued)

3	<p>The system supports user profile passwords from 1-128 characters. Upper and lower case characters are allowed. Passwords can consist of any character and the password will be case sensitive.</p> <ul style="list-style-type: none"> • QPWDLVL 3 cannot be used if your system communicates with other System i platforms in a network and those systems are running with either a QPWDLVL value of 0 or 1 or an operating system release less than V5R1M0. • QPWDLVL 3 cannot be used if your system communicates with any other system that limits the length of passwords from 1-10 characters. • QPWDLVL 3 cannot be used if your system communicates with the IBM i Support for Windows Network Neighborhood IBM i NetServer product. <p>Note: The IBM i Netserver product will work with Windows NT/2000/XP/Vista clients when the password level is 1 or 3. All user profile passwords that are used at QPWDLVL 0 and 1 are removed from the system when QPWDLVL is 3. Changing from QPWDLVL 3 back to QPWDLVL 0 or 1 requires a change to QPWDLVL 2 before going to 0 or 1. QPWDLVL 2 allows for the creation of user profile passwords that can be used at QPWDLVL 0 or 1 as long as the length and syntax requirements for the password meet the QPWDLVL 0 or 1 rules.</p>
----------	--

Changing the password level of the system from 1-10 character passwords to 1-128 character passwords requires careful consideration. If your system communicates with other systems in a network, then all systems must be able to handle the longer passwords.

A change to this system value takes effect at the next IPL. To see the current and pending password level values, use the Display Security Attributes (**DSPSECA**) command .

Minimum Length of Passwords (QPWDMINLEN)

The Minimum Length of Passwords (QPWDMINLEN) system value controls the minimum number of characters in a password.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value is any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 34. Possible values for the QPWDMINLEN system value:

6	A minimum of six characters are required for passwords.
<i>minimum-number-of-characters</i>	Specify a value of 1 through 10 when the password level (QPWDLVL) system value is 0 or 1. Specify a value of 1 through 128 when the password level (QPWDLVL) system value is 2 or 3.

Recommended value: 6 is recommended to prevent users from assigning passwords that are easily guessed, such as initials or a single character.

Maximum Length of Passwords (QPWDMAXLEN)

The Maximum Length of Passwords (QPWDMAXLEN) system value controls the maximum number of characters in a password.

This provides additional security by preventing users from specifying passwords that are too long and need to be recorded somewhere because they cannot be easily remembered. Some communications networks require a password that is 8 characters or less. Use this system value to ensure that passwords meet the requirements of your network.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 35. Possible values for the QPWDMAXLEN system value:

<u>8</u>	A maximum of eight characters for a password are allowed.
<i>maximum-number-of-characters</i>	Specify a value of 1 through 10 when the password level (QPWDLVL) system value is 0 or 1. Specify a value of 1 through 128 when the password level (QPWDLVL) system value is 2 or 3.

Recommended value: 8

Required Difference in Passwords (QPWDRQDDIF)

The Required Difference in Passwords (QPWDRQDDIF) system value controls whether the password must be different from previous passwords.

This value provides additional security by preventing users from specifying passwords that were used previously. It also prevents a user whose password has expired from changing it and then immediately changing it back to the old password.

Note: The value of the QPWDRQDDIF system value determines how many of these previous passwords are checked for a duplicate password. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 36. Possible values for the QPWDRQDDIF system value:

<i>Value</i>	<i>Number of previous passwords checked for duplicates</i>
<u>0</u>	0 Duplicate passwords are allowed.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Recommended value: Select a value of 5 or less to prevent the use of repeated passwords. Use a combination of the Required Difference in Passwords (QPWDRQDDIF) system value and the Password Expiration Interval (QPWDEXPITV) system value to prevent a password from being reused for at least 6 months. For example, set the QPWDEXPITV system value to 30 (days) and the QPWDRQDDIF system

value to 5 (10 unique passwords). This means a typical user, who changes passwords when warned by the system, will not repeat a password for approximately 9 months.

Restricted Characters for Passwords (QPWDLMTCHR)

The Restricted Characters for Passwords (QPWDLMTCHR) system value limits the use of certain characters in a password.

This value provides additional security by preventing users from using specific characters, such as vowels, in a password. Restricting vowels prevents users from forming actual words for their passwords.

The QPWDLMTCHR system value is not enforced when the password level (QPWDLVL) system value has a value of 2 or 3. The QPWDLMTCHR system value can be changed at QPWDLVL 2 or 3, but will not be enforced until QPWDLVL is changed to a value of 0 or 1.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 37. Possible values for the QPWDLMTCHR system value:

*NONE	There are no restricted characters for passwords.
<i>restricted-characters</i>	Specify up to 10 restricted characters. The valid characters are A through Z, 0 through 9, and special characters pound (#), dollar (\$), at (@), and underline (_).

Recommended value: A, E, I, O, or U. You might also want to prevent special characters (#, \$, and @) for compatibility with other systems.

Restriction of Consecutive Digits for Passwords (QPWDLMTAJC)

The Restriction of Consecutive Digits for Passwords (QPWDLMTAJC) system value limits the use of numeric characters next to each other (adjacent) in a password.

This value provides additional security by preventing users from using birthdays, telephone numbers, or a sequence of numbers as passwords.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 38. Possible values for the QPWDLMTAJC system value:

0	Numeric characters are allowed next to each other in passwords.
1	Numeric characters are not allowed next to each other in passwords.

Restriction of Repeated Characters for Passwords (QPWDLMTREP)

The Restriction of Repeated Characters for Passwords (QPWDLMTREP) system value limits the use of repeating characters in a password.

This value provides additional security by preventing users from specifying passwords that are easy to guess, such as the same character repeated several times.

When the password level (QPWDLVL) system value has a value of 2 or 3, the test for repeated characters is case sensitive. This means that a lowercase 'a' is not the same as an uppercase 'A'.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 39. Possible values for the QPWDLMTREP system value:

<u>0</u>	The same characters can be used more than once in a password.
1	The same character cannot be used more than once in a password.
2	The same character cannot be used consecutively in a password.

Table 40 shows examples of what passwords are allowed based on the QPWDLMTREP system value.

Table 40. Passwords with repeating characters with QPWLVL 0 or 1

Password example	QPWDLMTREP value of 0	QPWDLMTREP value of 1	QPWDLMTREP value of 2
A11111	Allowed	Not allowed	Not allowed
BOBBY	Allowed	Not allowed	Not allowed
AIRPLANE	Allowed	Not allowed	Allowed
N707UK	Allowed	Not allowed	Allowed

Table 41. Passwords with repeating characters with QPWLVL 2 or 3

Password example	QPWDLMTREP value of 0	QPWDLMTREP value of 1	QPWDLMTREP value of 2
j22222	Allowed	Not allowed	Not allowed
ReallyFast	Allowed	Not allowed	Not allowed
Mom'sApPlePie	Allowed	Not allowed	Allowed
AaBbCcDdEe	Allowed	Allowed	Allowed

Character Position Difference for Passwords (QPWDPOSDIF)

The Character Position Difference for Passwords (QPWDPOSDIF) system value controls each position in a new password.

This system value provides additional security by preventing users from using the same character (alphabetic or numeric) in a position corresponding to the same position in the previous password.

When the password level (QPWDLVL) system value has a value of 2 or 3, the test for the same character is case sensitive. This means that a lowercase 'a' is not the same as an uppercase 'A'.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 42. Possible values for the QPWDPOSDIF system value:

<u>0</u>	The same characters can be used in a position corresponding to the same position in the previous password.
1	The same character cannot be used in a position corresponding to the same position in the previous password.

Requirement for Numeric Character in Passwords (QPWDRQDDGT)

The Requirement for Numeric Character in Passwords (QPWDRQDDGT) system value controls whether a numeric character is required in a new password. This value provides additional security by preventing users from using all alphabetic characters.

Notes:

1. This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.
2. If the QPWDRULES system value specifies any value other than *PWDSYSVAL, this system value cannot be changed and its value will be ignored when new passwords are checked to see if they are formed correctly.

Table 43. Possible values for the QPWDRQDDGT system value:

<u>0</u>	Numeric characters are not required in new passwords.
1	One or more numeric characters are required in new passwords.

Recommended value: 1

Password Rules (QPWDRULES)

The Password Rules (QPWDRULES) system value specifies the rules used to check whether a password is formed correctly. You can specify more than one value for the QPWDRULES system value, unless you specify *PWDSYSVAL.

Changes made to this system value take effect the next time a password is changed.

Note: This system value is a restricted value. Refer to the Security System Values topic for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 44. Possible values for the QPWDRULES system value:

<p>*PWDSYSVAL</p>	<p>This value specifies that the QPWDRULES system value is ignored and the other password system values are used to check whether a password is formed correctly. These other password system values include QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF, and QPWDQDDGT.</p> <p>Note: If any value other than *PWDSYSVAL is specified for QPWDRULES, the QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF, and QPWDQDDGT system values are ignored when a new password is checked to see if it is formed correctly. In addition, any attempt to change these system values will be rejected as long as the QPWDRULES system value contains a value other than *PWDSYSVAL.</p>
<p>*CHRLMTAJC</p>	<p>The value specifies that a password cannot contain 2 or more occurrences of the same character that are positioned adjacent to each other. This value performs the same function as specifying a value of 2 for the QPWDLMTREP system value. If the *CHRLMTAJC value was specified, this value cannot be specified.</p> <p>Examples:</p> <pre>Better.test not valid - tt fix11bugs not valid - 11 @12/A78 valid A1234A1234 valid</pre>
<p>*CHRLMTREP</p>	<p>The value specifies that a password cannot contain 2 or more occurrences of the same character. This value performs the same function as specifying a value of 1 for the QPWDLMTREP system value. If the *CHRLMTAJC value was specified, this value cannot be specified.</p> <p>Examples:</p> <pre>John.Jones not valid - J o n THISONEOK not valid - 0 @12/A78 valid AaCcEeFfGg valid</pre>
<p>*DGLMTAJC</p>	<p>The value specifies that a password cannot contain 2 or more adjacent digit characters.</p> <p>Examples:</p> <pre>@12/A78 not valid !@#%a1234. not valid THISONEOK valid A1B2C3DE5 valid</pre>
<p>*DGLMTFST</p>	<p>The value specifies that the first character of a password cannot be a digit character. If *LTRLMTFST and *SPCCHRLMTFST values were specified, this value cannot be specified. If the system is operating at password level 0 or 1, the system functions like the *DGLMTFST value is specified.</p> <p>Examples:</p> <pre>16ST-SW-Roch not valid - 1 99BottlesOfBeer not valid - 9 @12/A78 valid Allow-this.1 valid</pre>

Table 44. Possible values for the QPWDRULES system value: (continued)

<p>*DGTMLTLST</p>	<p>The value specifies that the last character of the password cannot be a digit character. If *LTRLMTLST and *SPCCHRLMTLFST values were specified, this value cannot be specified.</p> <p>Examples:</p> <pre>John.doe12 not valid - 2 @12/A78 not valid - 8 THISONEOK valid A1234b123. valid</pre>
<p>*DGTMAXn</p>	<p>The value specifies the maximum number of digit characters that can occur in the password. The n is a number from 0 to 9.</p> <p>Only one *DGTMAXn value can be specified. If a *DGTMINn value is also specified, the n value specified for *DGTMAXn must be greater than or equal to the n value specified for *DGTMINn.</p> <p>Examples: for *DGTMAX2</p> <pre>Q12345678 not valid - 6 digits too many 3-2-1->Go not valid - 1 digit too many Rick1 valid Ed1-Jeff3 valid</pre>
<p>*DGTMINn</p>	<p>The value specifies the minimum number of digit characters that must occur in the password. The n is a number from 0 to 9.</p> <p>Only one *DGTMINn value can be specified. If a *DGTMAXn value is also specified, the n value specified for *DGTMAXn must be greater than or equal to the n value specified for *DGTMINn.</p> <p>Examples: for *DGTMIN3</p> <pre>Rick1 not valid - only 1 digit Ed1-Jeff3 not valid - only 2 digits 3-2-1->Go valid Q12345678 valid</pre>
<p>*LMTSAMPOS</p>	<p>The same character cannot be used in a position corresponding to the same position in the previous password. This value performs the same function as the QPWDPOSDIF system value.</p> <p>When the password is set by the Change User Profile (CHGUSRPRF) or Create User Profile (CRTUSRPRF) command, this password rule cannot be checked because the previous password value is not supplied.</p> <p>Examples: for *LMTSAMPOS when Vote4Me was previous password:</p> <pre>Victory1 not valid - V in position 1 Mine2love not valid - e in position 4 v0TE-mE valid (case is different) Allisgood valid</pre>
<p>*LMTPRFNAME</p>	<p>The uppercase password value cannot contain the complete user profile name in consecutive positions.</p> <p>Examples: for *LMTPRFNAME with profile name is JOHNB:</p> <pre>bigJOHNB9 not valid - positions 4-8 JohnB78 not valid - positions 1-5 J_ohn_B234 valid john_b valid</pre>

Table 44. Possible values for the QPWDRULES system value: (continued)

*LTRLMTAJC	<p>The value specifies a password cannot contain 2 or more adjacent letter characters.</p> <p>Examples:</p> <pre>John.Smith not valid THISONEOK not valid @12/A78 valid A1234b1234 valid</pre>
*LTRLMTFST	<p>The value specifies the first character of the password cannot be a letter character. If *DGLMTFST and *SPCCHRLMTFST values were specified, this value cannot be specified. If the system is operating with a QPWDLVL value of 0 or 1, *LTRLMTFST and *SPCCHRLMTFST cannot both be specified.</p> <p>Examples:</p> <pre>John.Smith not valid - J THISONEOK not valid - T @12/A78 valid 16ST-SW-Roch valid</pre>
*LTRLMTLST	<p>The value specifies the last character of the password cannot be a letter character. If *DGLMTLST and *SPCCHRLMTLST values were specified, this value cannot be specified</p> <p>Examples:</p> <pre>John.Smith not valid - h 1Allow.It not valid - t @12/A78 valid (pay*rate) valid</pre>
*LTRMAXn	<p>The value specifies the maximum number of letter characters that can occur in the password. The n is a number from 0 to 9.</p> <p>Only one *LTRMAXn value can be specified. If a *LTRMINn value is also specified, the n value specified for *LTRMAXn must be greater than or equal to the n value specified for *LTRMINn.</p> <p>If a *MIXCASEn value is also specified, the n value specified for *LTRMAXn must be greater than or equal to 2 times the n value specified for *MIXCASEn.</p> <p>Examples: for *LTRMAX4</p> <pre>THISONEOK not valid - 5 letters too many John.Smith1 not valid - 5 letters too many John1423 valid A1b2.#456 valid</pre>
*LTRMINn	<p>The value specifies the minimum number of letter characters that must occur in the password. The n is a number from 0 to 9.</p> <p>Only one *LTRMINn value can be specified. If a *LTRMAXn value was specified, the n value specified for *LTRMAXn must be greater than or equal to the n value specified for *LTRMINn.</p> <p>Examples: for *LTRMIN2</p> <pre>@12/A78 not valid - only 1 letter !@#%a1234 not valid - only 1 letter THISONEOK valid A1234b1234 valid</pre>

Table 44. Possible values for the QPWDRULES system value: (continued)

<p>*MAXLENnnn</p>	<p>The value specifies the maximum number of characters in a password. The nnn is a number from 1 to 128 (without leading zeros). This value performs the same function as the QPWDMAXLEN system value.</p> <p>If the system is operating at QPWDLVL 0 or 1, the valid range is from 1 to 10. If the system is operating at QPWDLVL 2 or 3, the valid range is from 1 to 128.</p> <p>The nnn value specified must be large enough to accommodate all *MIXCASEn, *DGTMAXn, *LTRMAXn, *SPCCHRMAXn, first and last character restrictions, and non-adjacent character requirements.</p> <p>If *MINLENnnn is also specified, the nnn value specified for *MAXLENnnn must be greater than or equal to the nnn value specified for *MINLENnnn.</p> <p>If no *MAXLENnnn value is specified, a value of *MAXLEN10 is assumed if the system is operating with a QPWDLVL value of 0 or 1 or a value of *MAXLEN128 is assumed if the system is operating with a QPWDLVL value of 2 or 3.</p>
<p>*MINLENnnn</p>	<p>The value specifies the minimum number of characters in a password. The nnn is a number from 1 to 128 (without leading zeros).</p> <p>If the system is operating at QPWDLVL 0 or 1, the valid range is from 1 to 10. If the system is operating at QPWDLVL 2 or 3, the valid range is from 1 to 128.</p> <p>If *MAXLENnnn is also specified, the nnn value specified for *MAXLENnnn must be greater than or equal to the nnn value specified for *MINLENnnn.</p> <p>If no *MINLENnnn value is specified, a value of *MINLEN1 is assumed.</p>
<p>*MIXCASEn</p>	<p>The value specifies a password must contain at least n uppercase and n lowercase letters. The n is a number from 0 to 9. This value is rejected if the system is operating with a QPWDLVL value of 0 or 1 because passwords are required to be uppercase.</p> <p>Only one *MIXCASEn value can be specified.</p> <p>If a *LTRMAXn value was specified, the n value specified for *LTRMAXn must be greater than or equal to two times the n value specified for *MIXCASEn.</p> <p>Examples: for *MIXCASE2</p> <pre>@12/A78bC not valid - missing 1 lowercase THISONEOK not valid - missing 2 lowercase ThisIs0kay valid Allow-It valid</pre>

Table 44. Possible values for the QPWDRULES system value: (continued)

<p>*REQANY3</p>	<p>The value specifies a password must contain characters from at least three of the following four types of characters.</p> <ul style="list-style-type: none"> • Uppercase letters • Lowercase letters • Digits • Special characters <p>When the system is operating with a QPWDLVL of 0 or 1, *REQANY3 has the same effect as if *DGTMIN1, *LTRMIN1, and *SPCCHRMIN1 were all specified.</p> <p>Examples:</p> <pre>THISONEOK not valid - only 1 type @12/-78 not valid - only 2 types A1234b1234 valid - upper, lower, digit John.Smith valid - upper, lower, special peter(21) valid - lower, special, digit</pre>
<p>*SPCCHRLMTAJC</p>	<p>The value specifies a password cannot contain 2 or more adjacent (consecutive) special characters. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.</p> <p>Examples:</p> <pre>Big//Box not valid this->way not valid @12/A78 valid John.Smith valid</pre>
<p>*SPCCHRLMTFST</p>	<p>The value specifies the first character of the password cannot be a special character. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.</p> <p>If *DGTLMTFST and *LTRLMTFST values were specified, this value cannot be specified. If the system is operating with a QPWDLVL value of 0 or 1, *LTRLMTFST and *SPCCHRLMTFST cannot both be specified.</p> <p>Examples:</p> <pre>(2+2equals4) not valid - (#fred/#charlie not valid - # 1Good->one12 valid A1234b1234 valid</pre>
<p>*SPCCHRLMTLST</p>	<p>The value specifies the last character of the password cannot be a special character. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.</p> <p>If *DGTLMTLST and *LTRLMTLST values were specified, this value cannot be specified.</p> <p>Examples:</p> <pre>A1234b123. not valid - . >John.Doe< not valid - < THISONEOK valid @12/A78 valid</pre>

Table 44. Possible values for the QPWDRULES system value: (continued)

<p>*SPCCHRMAXn</p>	<p>The value specifies the maximum number of special characters that may occur in the password. The n is a number from 0 to 9. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.</p> <p>Only one *SPCCHRMAXn value can be specified. If a *SPCCHRMINn value was specified, the n value specified for *SPCCHRMAXn must be greater than or equal to the n value specified for *SPCCHRMINn.</p> <p>Examples: for *SPCCHRMAX3</p> <pre>@12/A78.b# not valid - 1 too many !@#\$\$%a1234 not valid - 2 too many THISONEOK valid A1234b-234 valid</pre>
<p>*SPCCHRMINn</p>	<p>The value specifies the minimum number of special characters that must occur in the password. The n is a number from 0 to 9. A character is considered as a special character if its equivalent unicode character has the property of not being a letter nor a digit.</p> <p>Only one *SPCCHRMINn value can be specified. If a *SPCCHRMAXn value was specified, the n value specified for *SPCCHRMAXn must be greater than or equal to the n value specified for *SPCCHRMINn.</p> <p>Examples: for *SPCCHRMIN4</p> <pre>Su@us.ibm.com not valid - 1 too few 123+45=168 not valid - 2 too few A.B@us.ibm.com valid (24/8=3) valid</pre>

Password Approval Program (QPWDVLDPGM)

You can specify the Password Approval Program (QPWDVLDPGM) to control the validation of new passwords.

If *REGFAC or a program name is specified in the QPWDVLDPGM system value, the system runs one or more programs after the new password has passed any validation tests you specify in the password-control system values. You can use the programs to do additional checking of user-assigned passwords before they are accepted by the system.

A password approval program must be in the system auxiliary storage pool (ASP) or a basic user ASP.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 45. Possible values for the QPWDVLDPGM system value:

<p>*NONE</p>	<p>No user-written program is used. This includes any password approval programs registered in the exit registration facility.</p>
<p>*REGFAC</p>	<p>The validation program is retrieved from the registration facility, exit point QIBM_QSY_VLD_PASSWRD. More than one validation program can be specified in the registration facility. Each program will be called until one of them indicates that the password should be rejected or all of them have indicated the password is valid.</p>

Table 45. Possible values for the QPWDVLDPGM system value: (continued)

<i>program-name</i>	Specify the name of the user-written validation program, from 1 through 10 characters. A program name cannot be specified when the current or pending value of the password level (QPWDLVL) system value is 2 or 3.
<i>library-name</i>	Specify the name of the library where the user-written program is located. If the library name is not specified, the library list (*LIBL) of the user changing the system value is used to search for the program. QSYS is the recommended library.

Using a password approval program

If *REGFAC or a program name is specified in the QPWDVLDPGM system value, one or more programs are called by the Change Password (CHGPWD) command or Change Password (QSYCHGPW) API. The programs are called only if the new password has passed all other tests specified in the password-control system values.

In case it is necessary to recover your system from a disk failure, place the password approval program in library QSYS. This way the password approval program is loaded when you restore library QSYS.

If a program name is specified in the QPWDVLDPGM system value, the system passes the following parameters to the password approval program:

Table 46. Parameters for password approval program

Position	Type	Length	Description
1	*CHAR	10	The new password entered by the user.
2	*CHAR	10	The user's old password.
3	*CHAR	1	Return code: 0 for valid password; not 0 for incorrect password.
4 ¹	*CHAR	10	The name of the user.
1	Position 4 is optional.		

If *REGFAC is specified in the QPWDVLDPGM system value, refer to the Security Exit Program information in the System API manual for information about the parameters passed to the validation program.

If your program determines that the new password is not valid, you can either send your own exception message (using the SNDPGMMSG command) or set the return code to a value other than 0 and let the system display an error message. Exception messages that are signaled by your program must be created with the DMPLST(*NONE) option of the Add Message Description (ADDMSGD) command.

The new password is accepted only if the user-written program ends with no escape message and a return code of 0. Because the return code is initially set for passwords that are not valid (not zero), the approval program must set the return code to 0 before the password can be changed.

Attention: The current and new password are passed to the validation program without encryption. The validation program can store passwords in a database file and compromise security on the system. Make sure the functions of the validation program are reviewed by the security officer and that changes to the program are strictly controlled.

The following control language (CL) program is an example of a password approval program when a program name is specified for QPWDVLDPGM. This example checks to make sure the password is not changed more than once in the same day. Additional calculations can be added to the program to check other criteria for passwords:

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

```

/*****/
/* NAME:      PWDVALID - Password Validation */
/*          */
/* FUNCTION:  Limit password change to one per */
/*          day unless the password is expired */
/*****/
PGM (&NEW &OLD &RTNCD &USER)
DCL VAR(&NEW)      TYPE(*CHAR) LEN(10)
DCL VAR(&OLD)      TYPE(*CHAR) LEN(10)
DCL VAR(&RTNCD)    TYPE(*CHAR) LEN(1)
DCL VAR(&USER)     TYPE(*CHAR) LEN(10)
DCL VAR(&JOBDATE)  TYPE(*CHAR) LEN(6)
DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
DCL VAR(&PWDEXP)   TYPE(*CHAR) LEN(4)
/* Get the current date and convert to YMD format */
RTVJOBA    DATE(&JOBDATE)
CVTDAT    DATE(&JOBDATE) TOVAR(&JOBDATE) +
          TOFMT(*YMD)    TOSEP(*NONE)
/* Get date password last changed and whether */
/* password is expired from user profile */
RTVUSRPRF  USRPRF(&USER) PWDCHGDAT(&PWDCHGDAT)+
          PWDEXP(&PWDEXP)
/* Compare two dates */
/* if equal and password not expired */
/* then send *ESCAPE message to prevent change */
/* else set return code to allow change */
IF (&JOBDATE=&PWDCHGDAT *AND &PWDEXP='*NO ') +
  SNDPGMMSG MSGID(CPF9898) MSGF(QCPFMSG) +
  MSGDTA('Password can be changed only +
         once per day') +
  MSGTYPE(*ESCAPE)
ELSE CHGVAR &RTNCD '0'
ENDPGM

```

The following control language (CL) program is an example of a password approval program when *REGFAC is specified for QPWDVLDLVL.

This example checks to make sure the new password is in CCSID 37 (or if it is in CCSID 13488 it converts the new password to CCSID 37), that the new password does not end in a numeric character, and that the new password does not contain the user profile name. The example assumes that a message file (PWDERRORS) has been created and message descriptions (PWD0001 and PWD0002) have been added to the message file. Additional calculations can be added to the program to check other criteria for passwords:

```

/*****/
/*          */
/* NAME:      PWDEXITPGM1 - Password validation exit 1 */
/*          */
/* Validates passwords when *REGFAC is specified for */
/* QPWDVLDLPGM. Program is registered using the ADDEXITPGM*/
/* CL command for the QIBM_QSY_VLD_PASSWRD exit point. */
/*          */
/*          */
/* ASSUMPTIONS: If CHGPWD command was used, password */
/* CCSID will be job default (assumed to be CCSID 37). */
/* If QSYCHGPW API was used, password CCSID will be */
/* UNICODE CCSID 13488. */
/*****/

PGM  PARM(&EXINPUT &RTN)
DCL &EXINPUT  *CHAR 1000
DCL &RTN      *CHAR 1

```

```

DCL &UNAME      *CHAR 10
DCL &NEWPW      *CHAR 256
DCL &NPOFF      *DEC 5 0
DCL &NPLEN      *DEC 5 0
DCL &INDX       *DEC 5 0
DCL &INDX2      *DEC 5 0
DCL &INDX3      *DEC 5 0
DCL &UNLEN      *DEC 5 0

DCL &XLTCHR2    *CHAR 2 VALUE(X'0000')
DCL &XLTCHR     *DEC 5 0
DCL &XLATEU     *CHAR 255 VALUE('..... +
!"#%&'()*+,-./0123456789:;<=>?+
@ABCDEFGHIJKLMN OPQRSTUVWXYZ[\]^_+
`ABCDEFGHIJKLMN OPQRSTUVWXYZ{|}~.+
.....+
.....+
.....+
.....+')

DCL &XLATEC     *CHAR 255 VALUE('.....+
.....+
.....+
.....+
.ABCDEFGHI.....JKLMN OPQR.....+
..STUVWXYZ.....+
.....+
.....+')

/*****/
/* FORMAT OF EXINPUT IS: */
/* */
/* POSITION DESCRIPTION */
/* 001 - 020 EXIT POINT NAME */
/* 021 - 028 EXIT POINT FORMAT NAME */
/* 029 - 032 PASSWORD LEVEL (binary) */
/* 033 - 042 USER PROFILE NAME */
/* 043 - 044 RESERVED */
/* 045 - 048 OFFSET TO OLD PASSWORD (binary) */
/* 049 - 052 LENGTH OF OLD PASSWORD (binary) */
/* 053 - 056 CCSID OF OLD PASSWORD (binary) */
/* 057 - 060 OFFSET TO NEW PASSWORD (binary) */
/* 061 - 064 LENGTH OF NEW PASSWORD (binary) */
/* 065 - 068 CCSID OF NEW PASSWORD (binary) */
/* ??? - ??? OLD PASSWORD */
/* ??? - ??? NEW PASSWORD */
/* */
/*****/

/*****/
/* Establish a generic monitor for the program. */
/*****/

MONMSG CPF0000
/* Assume new password is valid */
CHGVAR &RTN VALUE('0') /* accept */
/* Get new password length, offset and value. Also get user name */
CHGVAR &NPLEN VALUE(%BIN(&EXINPUT 61 4))
CHGVAR &NPOFF VALUE(%BIN(&EXINPUT 57 4) + 1)
CHGVAR &UNAME VALUE(%SST(&EXINPUT 33 10))
CHGVAR &NEWPW VALUE(%SST(&EXINPUT &NPOFF &NPLEN))
/* If CCSID is 13488, probably used the QSYCHGPW API which converts */
/* the passwords to UNICODE CCSID 13488. So convert to CCSID 37, if */
/* possible, else give an error */
IF COND(%BIN(&EXINPUT 65 4) = 13488) THEN(DO)
    CHGVAR &INDX2 VALUE(1)

```

```

CHGVAR &INDX3 VALUE(1)
CVT1:
CHGVAR &XLTCHR VALUE(%BIN(&NEWPW &INDX2 2))
IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
  CHGVAR &RTN VALUE('3') /* reject */
  SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
  GOTO DONE
ENDDO
CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEU &XLTCHR 1))
CHGVAR &INDX2 VALUE(&INDX2 + 2)
CHGVAR &INDX3 VALUE(&INDX3 + 1)
IF COND(&INDX2 *GT &NPLEN) THEN(GOTO ECVT1)
GOTO CVT1
ECVT1:
CHGVAR &NPLEN VALUE(&INDX3 - 1)
CHGVAR %SST(&EXINPUT 65 4) VALUE(X'00000025')
ENDDO

/* Check the CCSID of the new password value - must be 37 */
IF COND(%BIN(&EXINPUT 65 4) *NE 37) THEN(DO)
  CHGVAR &RTN VALUE('3') /* reject */
  SNDPGMMSG MSG('CCSID OF NEW PASSWORD MUST BE 37')
  GOTO DONE
ENDDO

/* UPPERCASE NEW PASSWORD VALUE */
CHGVAR &INDX2 VALUE(1)
CHGVAR &INDX3 VALUE(1)
CVT4:
CHGVAR %SST(&XLTCHR2 2 1) VALUE(%SST(&NEWPW &INDX2 1))
CHGVAR &XLTCHR VALUE(%BIN(&XLTCHR2 1 2))
IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
  CHGVAR &RTN VALUE('3') /* reject */
  SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
  GOTO DONE
ENDDO
IF COND(%SST(&XLATEC &XLTCHR 1) *NE '.' ) +
THEN(CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEC &XLTCHR 1)))
CHGVAR &INDX2 VALUE(&INDX2 + 1)
CHGVAR &INDX3 VALUE(&INDX3 + 1)
IF COND(&INDX2 *GT &NPLEN) THEN(GOTO ECVT4)
GOTO CVT4
ECVT4:

/* CHECK IF LAST POSITION OF NEW PASSWORD IS NUMERIC */
IF COND(%SST(&NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
IF COND(%SST(&NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)

/* CHECK IF PASSWORD CONTAINS USER PROFILE NAME */
CHGVAR &UNLEN VALUE(1)
LOOP2: /* FIND LENGTH OF USER NAME */
IF COND(%SST(&UNAME &UNLEN 1) *NE ' ') THEN(DO)
  CHGVAR &UNLEN VALUE(&UNLEN + 1)
  IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
  GOTO LOOP2
ENDDO
ELOOP2:
CHGVAR &UNLEN VALUE(&UNLEN - 1)

```

```

/* CHECK FOR USER NAME IN NEW PASSWORD          */
IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
CHGVAR &INDX VALUE(1)
LOOP3:
  IF COND(%SST(&NEWPW &INDX &UNLEN) = %SST(&UNAME 1 &UNLEN)) +
    THEN(GOTO ERROR2)
  IF COND((&INDX + &UNLEN + 1) *LT 128) THEN(DO)
    CHGVAR &INDX VALUE(&INDX + 1)
    GOTO LOOP3
  ENDDO
ELOOP3:

/* New Password is valid                        */
GOTO DONE

ERROR1: /* NEW PASSWORD ENDS IN NUMERIC CHARACTER */
CHGVAR &RTN VALUE('3') /* reject */
SNDPGMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
GOTO DONE

ERROR2: /* NEW PASSWORD CONTAINS USER NAME */
CHGVAR &RTN VALUE('3') /* reject */
SNDPGMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
GOTO DONE

DONE:
ENDPGM

```

System values that control auditing

Auditing system activity is an important part of system security, as it can help detect system misuse and intrusions. You can use specific systems values to control auditing on the IBM i operating system.

Overview:

Purpose:

Specify system values to control security auditing on the system.

How To:

WRKSYSVAL *SEC (Work with System Values command)

Authority:

*AUDIT

Journal Entry:

SV

Note: Changes take effect immediately. IPL is not required.

These system values control auditing on the system:

QAUDCTL

Auditing control

QAUDENDACN

Auditing end action

QAUDFRCLVL

Auditing force level

QAUDLVL

Auditing level

QAUDLVL2

Auditing level extension

QCRTOBJAUD

Create default auditing

Auditing Control (QAUDCTL)

The Auditing Control (QAUDCTL) system value determines whether auditing is performed.

This system value functions like an on and off switch for the following operations:

- The QAUDLVL and QAUDLVL2 system values
- The auditing defined for objects using the Change Object Auditing (**CHGOBJAUD**), Change Auditing Value (**CHGAUD**), and Change DLO Auditing (**CHGDLOAUD**) commands
- The auditing defined for users using the Change User Audit (**CHGUSRAUD**) command

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

You can specify more than one value for the QAUDCTL system value, unless you specify *NONE.

Table 47. Possible values for the QAUDCTL system value

*NONE	No auditing is performed for user actions and objects.
*NOTAVL	This value is displayed to indicate that the system value is unavailable to the user because the user has neither *AUDIT nor *ALLOBJ special authority. You cannot set the system value to this value.
*OBJAUD	Auditing is performed for objects that have been selected using the CHGOBJAUD , CHGDLOAUD , or CHGAUD commands.
*AUDLVL	Auditing is performed for any functions selected on the QAUDLVL and QAUDLVL2 system values and on the AUDLVL parameter of individual user profiles. The audit level for a user is specified using the Change User Audit (CHGUSRAUD) command.
*NOQTEMP	Auditing is not performed for most actions if the object is in QTEMP library. See Chapter 9, "Auditing security on System i," on page 257 for more details. You must specify this value with either *OBJAUD or *AUDLVL.
	See "Planning security auditing" on page 263 for a complete description of the process for controlling auditing on your system.

Auditing End Action (QAUDENDACN)

The Auditing End Action (QAUDENDACN) system value determines what action the system takes if auditing is active and the system is unable to write entries to the audit journal.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 48. Possible values for the QAUDENDACN system value:

*NOTAVL	This value is displayed to indicate that the system value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The system value cannot be set to this value.
*NOTIFY	Message CPI2283 is sent to the QSYSOPR message queue and the QSYSMSG message queue (if it exists) every hour until auditing is successfully restarted. The system value QAUDCTL is set to *NONE to prevent the system from attempting to write additional audit journal entries. Processing on the system continues. If an IPL is performed before auditing is restarted, message CPI2284 is sent to the QSYSOPR and QSYSMSG message queues during the IPL.

Table 48. Possible values for the QAUDENDACN system value: (continued)

*PWRDWSYS	If the system is unable to write an audit journal entry, the system powers down immediately. The system unit displays system reference code (SRC) B900 3D10. When the system is powered on again, it is in a restricted state. This means the controlling subsystem is in a restricted state, no other subsystems are active, and sign-on is allowed only at the console. The QAUDCTL system value is set to *NONE. The user who signs on the console to complete the IPL must have *ALLOBJ and *AUDIT special authority.
-----------	---

Recommended value: For most installations, *NOTIFY is the recommended value. If your security policy requires that no processing be performed on the system without auditing, then you must select *PWRDWSYS.

Only very unusual circumstances cause the system to be unable to write audit journal entries. However, if this does happen and the QAUDENDACN system value is *PWRDWSYS, your system ends abnormally. This might cause a lengthy initial program load (IPL) when your system is powered on again.

Auditing Force Level (QAUDFRCLVL)

The Auditing Force Level (QAUDFRCLVL) system value determines how often new audit journal entries are forced from memory to auxiliary storage. This system value controls the amount of auditing data that may be lost if the system ends abnormally.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 49. Possible values for the QAUDFRCLVL system value

*NOTAVL	This value is displayed to indicate that the system value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The system value cannot be set to this value.
*SYS	The system determines when journal entries are written to auxiliary storage based on internal system performance.
<i>number-of- records</i>	Specify a number between 1 and 100 to determine how many audit entries can accumulate in memory before they are written to auxiliary storage. The smaller the number, the greater the effect on system performance.

Recommended value: *SYS provides the best auditing performance. However, if your installation requires that no audit entries be lost when your system ends abnormally, you must specify 1. Specifying 1 might impair performance.

Auditing Level (QAUDLVL)

The Auditing Level (QAUDLVL) system value along with the QAUDLVL2 system value determines which security-related events are logged to the security audit journal (QAUDJRN) for all system users.

You can specify more than one value for the QAUDLVL system value, unless you specify *NONE.

For the QAUDLVL system value to take effect, the QAUDCTL system value must include *AUDLVL.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 50. Possible values for the QAUDLVL system value

*NONE	No events controlled by the QAUDLVL or QAUDLVL2 system values are logged. Events are logged for individual users based on the AUDLVL values of user profiles.
*NOTAVL	This value is displayed to indicate that the system value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The system value cannot be set to this value.
*AUDLVL2	Both QAUDLVL and QAUDLVL2 system values will be used to determine the security actions to be audited.
*ATNEVT	Attention events are logged.
*AUTFAIL	Authority failure events are logged.
*CREATE	Object create operations are logged.
*DELETE	Object delete operations are logged.
*JOBBAS	Job base functions are audited.
*JOBCHGUSR	Changes to a thread's active user profile or its group profiles are audited.
*JOBDTA	Actions that affect a job are logged. *JOBDTA is composed of two values, which are *JOBBAS and *JOBCHGUSR, to enable you to better customize your auditing. If both of the values are specified, you will get the same auditing as if just *JOBDTA is specified.
*NETBAS	Network base functions are audited.
*NETCLU	Cluster and cluster resource group operations are audited.
*NETCMN	Network and communication functions are audited. *NETCMN is composed of several values to enable you to better customize your auditing. The following values make up *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Network failures are audited.
*NETSCK	Socket tasks are audited.
*OBJMGT	Object move and rename operations are logged.
*OFCSRVR	Changes to the system distribution directory and office mail actions are logged.
*OPTICAL	Use of Optical Volumes is logged.
*PGMADP	Obtaining authority from a program that adopts authority is logged.
*PGMFAIL	System integrity violations are logged.
*PRTDTA	Printing a spooled file, sending output directly to a printer, and sending output to a remote printer are logged.
*SAVRST	Save and restore operations are logged.
*SECCFG	Security configuration is audited.
*SECDIRSRV	Changes or updates when doing directory service functions are audited.
*SECIPC	Changes to interprocess communications are audited.
*SECNAS	Network authentication service actions are audited.
*SECRUN	Security run time functions are audited.
*SECSCKD	Socket descriptors are audited.

Table 50. Possible values for the QAUDLVL system value (continued)

*SECURITY	Security-related functions are logged. *SECURITY is composed of several values to enable you to better customize your auditing. The following values make up *SECURITY: *SECCFG *SEC DIRSRV *SECIPC *SECNAS *SECRUN *SECCKD *SECVFY *SECVLDL
*SECVFY	Use of verification functions are audited.
*SECVLDL	Changes to validation list objects are audited.
*SERVICE	Using service tools is logged.
*SPLFDTA	Actions performed on spooled files are logged.
*SYSMGT	Use of systems management functions is logged.

Related reference:

“Planning the auditing of actions” on page 263

The QAUDCTL (audit control) system value, the QAUDLVL (audit level) system value, the QAUDLVL2 (audit level extension) system value, and the AUDLVL (action auditing) parameter in user profiles work together to control action auditing.

Auditing Level Extension (QAUDLVL2)

The Auditing Level Extension (QAUDLVL2) system value is required when more than sixteen auditing values are needed.

Specifying *AUDLVL2 as one of the values in the QAUDLVL system value will cause the system to also look for auditing values in the QAUDLVL2 system value. You can specify more than one value for the QAUDLVL2 system value, unless you specify *NONE. For the QAUDLVL2 system value to take effect, the QAUDCTL system value must include *AUDLVL and the QAUDLVL system value must include *AUDLVL2.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 51. Possible values for the QAUDLVL2 system value

*NONE	No auditing values are contained in this system value.
*NOTAVL	This value is displayed to indicate that the system value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The system value cannot be set to this value.
*ATNEVT	Attention events are logged.
*AUTFAIL	Authority failure events are logged.
*CREATE	Object create operations are logged.
*DELETE	Object delete operations are logged.
*JOBBAS	Job base functions are audited.
*JOBCHGUSR	Changes to a thread's active user profile or its group profiles are audited.

Table 51. Possible values for the QAUDLVL2 system value (continued)

*JOBDTA	<p>Actions that affect a job are logged.</p> <p>*JOBDTA is composed of two values, which are *JOBBAS and *JOBCHGUSR, to enable you to better customize your auditing. If both of the values are specified, you will get the same auditing as if just *JOBDTA is specified.</p>
*NETBAS	Network base functions are audited.
*NETCLU	Cluster and cluster resource group operations are audited.
*NETCMN	<p>Network and communication functions are audited.</p> <p>*NETCMN is composed of several values to allow you to better customize your auditing. The following values make up *NETCMN:</p> <p>*NETBAS *NETCLU *NETFAIL *NETSCK</p>
*NETFAIL	Network failures are audited.
*NETSCK	Socket tasks are audited.
*OBJMGT	Object move and rename operations are logged.
*OFCSRVR	Changes to the system distribution directory and office mail actions are logged.
*OPTICAL	Use of Optical Volumes is logged.
*PGMADP	Obtaining authority from a program that adopts authority is logged.
*PGMFAIL	System integrity violations are logged.
*PRTDTA	Printing a spooled file, sending output directly to a printer, and sending output to a remote printer are logged.
*SAVRST	Restore operations are logged.
*SECCFG	Security configuration is audited.
*SECDIRSRV	Changes or updates when doing directory service functions are audited.
*SECIPC	Changes to interprocess communications are audited.
*SECNAS	Network authentication service actions are audited.
*SECRUN	Security run time functions are audited.
*SECCKD	Socket descriptors are audited.
*SECURITY	<p>Security-related functions are logged.</p> <p>*SECURITY is composed of several values to allow you to better customize your auditing. The following values make up *SECURITY:</p> <p>*SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECCKD *SECVFY *SECVLDL</p>
*SECVFY	Use of verification functions are audited.
*SECVLDL	Changes to validation list objects are audited.
*SERVICE	Using service tools is logged.
*SPLFDTA	Actions performed on spooled files are logged.

Table 51. Possible values for the QAUDLVL2 system value (continued)

*SYSMGT	Use of systems management functions is logged.
---------	--

Related reference:

“Planning the auditing of actions” on page 263

The QAUDCTL (audit control) system value, the QAUDLVL (audit level) system value, the QAUDLVL2 (audit level extension) system value, and the AUDLVL (action auditing) parameter in user profiles work together to control action auditing.

Auditing for New Objects (QCRTOBJAUD)

The Auditing for New Objects (QCRTOBJAUD) system value is used to determine the auditing value for a new object, if the create object auditing default for the library or directory of the new object is set to *SYSVAL.

The QCRTOBJAUD system value is also the default object auditing value for new folderless documents.

For example, the CRTOBJAUD value for the CUSTLIB library is *SYSVAL. The QCRTOBJAUD value is *CHANGE. If you create a new object in the CUSTLIB library, its object auditing value is automatically set to *CHANGE. You can change the object auditing value using the **CHGOBJAUD** or **CHGAUD** command.

Note: This system value is a restricted value. See Security system values for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 52. Possible values for the QCRTOBJAUD system value:

*NONE	No auditing is done for the object.
*NOTAVL	This value is displayed to indicate that the system value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The system value cannot be set to this value.
*USRPRF	Auditing of the object is based on the value in the profile of the user accessing the object.
*CHANGE	An audit record is written whenever a security relevant change is made to the object.
*ALL	An audit record is written for any security relevant action that affects the contents of the object. An audit record is also written if a security relevant change is made to the object.

Recommended value: The value you select depends on the auditing requirements of your installation. “Planning the auditing of object access” on page 286 provides more information about methods for setting up object auditing on your system. You can control the auditing value at the directory level with the CRTOBJAUD parameter on the Make Directory (**CRTDIR**) command, and the *CRTOBJAUD value on the Change Attribute (**CHGATR**) command. You can also control the auditing value at the library level with the CRTOBJAUD parameter with the **CRTLIB** command and the **CHGLIB** command.

Chapter 4. User profiles

User profiles are a powerful and flexible tool. Designing them well can help you protect your system and customize it for your users.

Overview:

Purpose:

Create and maintain user profiles and group profiles on the system

How To:

Work with User Profiles (**WRKUSRPRF**) command

Change User Audit (**CHGUSRAUD**) command

Authority:

*SECADM special authority

*AUDIT special authority to change user auditing

Journal Entry:

AD for changes to user auditing

CO for creation of a user profile

CP for changes to users profiles

DO for deletion of a user profile

ZC for changes to a user profile that are not relevant to security

Related concepts:

“User profiles” on page 4

On the IBM i operating system, every system user has a user profile.

Roles of the user profile

A user profile contain a user's passwords, the list of special authorities assigned to a user, and the objects the user owns.

A user profile has several roles on the system:

- It contains security-related information that controls how the user signs on the system, what the user is allowed to do after signing on, and how the user's actions are audited.
- It contains information that is designed to customize the system and adapt it to the user.
- It is a management and recovery tool for the operating system. The user profile contains information about the objects owned by the user and all the private authorities to objects.
- The user profile name identifies the user's jobs and printer output.

If the security level (QSECURITY) system value on your system is 10, the system automatically creates a user profile when someone signs on with a user ID that does not already exist on the system. “Default values for user profiles” on page 319 in Appendix B, “IBM-supplied user profiles,” on page 319 shows the values assigned when the system creates a user profile.

If the QSECURITY system value on your system is 20 or higher, a user profile must exist before a user can sign on.

Group profiles

A group profile is a special type of user profile that provides the same authority to a group of users.

A group profile serves two purposes on the system:

Security tool

A group profile provides a method for organizing authorities on your system and sharing them among users. You can define object authorities or special authorities for group profiles rather than for each individual user profile. A user can be a member of up to 16 group profiles.

Customizing tool

A group profile can be used as a pattern for creating individual user profiles. Most people who are part of the same group have the same customizing needs, such as the initial menu and the default printer. You can define these things in the group profile and then copy the group profile to create individual user profiles.

You create group profiles in the same way that you create individual profiles. The system recognizes a group profile when you add the first member to it. At that point, the system sets information in the profile indicating that it is a group profile. The system also generates a group identification number (gid) for the profile. You can also designate a profile as a group profile at the time when you create it by specifying a value in the gid parameter. "Planning group profiles" on page 239 shows an example of setting up a group profile.

User-profile parameter fields

This topic describes detailed information about the parameter fields for user profiles shown on the Create User Profile command prompt.

When you create a user profile, the system gives these authorities to the profile: *OBJMGT, *CHANGE. These authorities are necessary for system functions and should not be removed.

Many system displays have different versions, called *assistance levels*, to meet the needs of different users:

- Basic assistance level, which contains less information and does not use technical terminology.
- Intermediate assistance level, which shows more information and uses technical terms.
- Advanced assistance level, which uses technical terms and shows the maximum amount of data by not always displaying function key and option information.

The following sections show what the user profile fields are called on both the basic assistance level and the intermediate assistance level displays.

Field title

The title of the section shows how the field name appears on the Create User Profile command prompt. The title displays when you create a user profile with intermediate assistance level or the Create User Profile (CRTUSRPRF) command.

Add User prompt:

This shows how the field name appears on the Add User display and other user-profile displays that use basic assistance level. The basic assistance level displays show a subset of the fields in the user profile. *Not shown* means the field does not appear on the basic assistance level display. When you use the Add User display to create a user profile, default values are used for all fields that are not shown.

CL parameter:

You use the CL parameter name for a field in a CL program or when you enter a user profile command without prompting.

Length:

If you use the Retrieve User Profile (RTVUSRPRF) command in a CL program, this is the length you should use to define the field associated with the parameter.

Authority:

If a field refers to a separate object, such as a library or a program, you are told the authority requirements for the object. To specify the object when you create or change a user profile, you need the corresponding authority listed. To sign on using the profile, the user needs the authority listed. For example, if you create user profile USERA with job description JOBD1, you must have *USE authority to JOBD1. USERA must have *USE authority to JOBD1 to successfully sign on with the profile.

In addition, each section describes the possible values for the field and a recommended value.

User profile name

The user profile name identifies the user to the system. This user profile name is also known as the user ID. It is the name the user types in the User prompt on the Sign On display.

Add User prompt:

User

CL parameter:

USRPRF

Length:

10

The user profile name can be a maximum of 10 characters. The characters can be:

- Any letter (A through Z)
- Any number (0 through 9)
- These special characters: pound (#), dollar (\$), underline (_), at (@).

The user profile name cannot begin with a number.

Notes:

- The Add User display allows only an eight-character user name.
- It is possible to create a user profile so that when a user signs on, the user ID is only numerals. To create a profile like this, specify a Q as the first character, such as Q12345. A user can then sign on by entering 12345 or Q12345 for the *User* prompt on the Sign On display.

For more information about specifying names on the system, see the CL programming topic.

Recommendations for naming user profiles: Consider these things when deciding how to name user profiles:

- A user profile name can be up to 10 characters long. Some communications methods limit the user ID to eight characters. The Add User display also limits the user profile name to eight characters.
- Use a naming scheme that makes user IDs easy to remember.
- The system does not distinguish between uppercase and lowercase letters in a user profile name. If you enter lowercase alphabetic characters at your workstation, the system translates them to uppercase characters.
- The displays and lists that you use to manage user profiles show the user profiles in alphabetical order by user profile name.
- Avoid using special characters in user profile names. Special characters might cause problems with keyboard mapping for certain workstations or with national language versions of the IBM i licensed program.

One technique for assigning user profile names is to use the first seven characters of the family name followed by the first character of the first name. For example:

User name	User profile name
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Harrisburg, Keith	HARRISBK
Jones, Sharon	JONESS
Jones, Keith	JONESK

Recommendations for naming group profiles: To easily identify group profiles on the system, use a naming convention. Begin all group profile names with the same characters, such as GRP (for group) or DPT (for department).

Password

The password is used to verify a user's authority to sign on the system. A user ID and a password must be specified to sign on when password security is active (QSECURITY system value is 20 or higher).

Add User prompt:

Password

CL parameter:

PASSWORD

Length:

128

Passwords can be a maximum of 10 characters when the QPWDLVL system value is set to 0 or 1.
 Passwords can be a maximum of 128 characters when the QPWDLVL system value is set to 2 or 3.

When the Password Level (QPWDLVL) system value is 0 or 1, the rules for specifying passwords are the same as those used for user profile names. When the first character of the password is a Q and the second character is a numeric character, the Q can be omitted on the sign-on display. If a user specifies Q12345 as the password on the Change Password display, the user can specify either 12345 or Q12345 as the password on the sign-on display. When QPWDLVL is 2 or 3, the user must specify the password as Q12345 on the sign-on display if the user profile was created with a password of Q12345. An all numeric password is allowed when QPWDLVL is 2 or 3, but the user profile password must be created as all numeric.

When the Password Level (QPWDLVL) system value is 2 or 3, the password is case-sensitive and can contain any character including blank characters. However, the password cannot begin with an asterisk character (*), and trailing blank characters in the password are removed.

Note: Passwords can be created using double-byte characters. However, a password containing double-byte characters cannot be used to sign on via the system sign-on screen. Passwords containing double byte characters can be created by the CRTUSRPRF and CHGUSRPRF commands and can be passed to the system APIs that support the password parameter.

One-way encryption is used to store the password on the system. If a password is forgotten, the security officer can use the Change User Profile (CHGUSRPRF) command to assign a temporary password and set that password to expired, requiring the user to assign a new password at the next sign-on.

You can set system values to control the passwords that users assign. The password composition system values apply only when a user changes a password using the Change Password (CHGPWD) command,

the Change password option from the ASSIST menu, or the QSYCHGPW API. A user cannot set the password equal to the user profile name using the CHGPWD command, the ASSIST menu, or the QSYCHGPW API in any of the following conditions.

- The QPWDRULES system value is *PWDSYSVAL and the Password Minimum Length (QPWDMINLEN) system value is not 1.
- The QPWDRULES system value is *PWDSYSVAL and the Password Maximum Length (QPWDMAXLEN) system value is not 10.
- The QPWDRULES system value is *PWDSYSVAL and any of the other password composition system values have been changed from the default values.

See the topic “System values that apply to passwords” on page 46 for information about setting the password composition system values.

Table 53. Possible values for PASSWORD:

*USRPRF	The password for this user is the same as the user profile name. When the Password Level (QPWDLVL) system value is 2 or 3, the password is the uppercased value of the user profile name. For profile JOHNDOE, the password is JOHNDOE, not johndoe.
*NONE	No password is assigned to this user profile. Sign-on is not allowed with this user profile. You can submit a batch job using a user profile with password *NONE if you have correct authority to the user profile.
<i>user- password</i>	A character string (128 characters or less).

Recommendations for passwords:

- Set the password for a group profile to *NONE. This prevents anyone from signing on with the group profile.
- When creating an individual user profile, set the password to an initial value and require a new password to be assigned when the user signs on (set password expired to *YES). The default password when creating a user profile is the same as the user profile name.
- If you use a trivial or default password when creating a new user profile, make sure the user intends to sign on immediately. If you expect a delay before the user signs on, set the status of the user profile to *DISABLED. Change the status to *ENABLED when the user is ready to sign on. This protects a new user profile from being used by someone who is not authorized.
- Use the password composition system values to prevent users from assigning trivial passwords.
- Some communications methods send passwords between systems and limit the length of password and the characters that passwords can contain. If your system communicates with other systems, use the QPWDMAXLEN or QPWDRULES system value to limit the passwords length. At password levels 0 and 1, the QPWDLMTCHR system value can be used to specify characters that cannot be used in passwords.

Set password to expired

The *Set password to expired* field allows a security administrator to indicate in the user profile that the user’s password is expired and must be changed the next time the user signs on.

Add User prompt:

Not shown

CL parameter:

PWDEXP

Length:

4

This value is reset to *NO when the password is changed. You can change the password by using either the CHGPWD or CHGUSRPRF command, or the QSYCHGPW API, or as part of the next sign-on process.

This field can be used when a user cannot remember the password and a security administrator must assign a new one. Requiring the user to change the password assigned by the security administrator prevents the security administrator from knowing the new password and signing on as the user.

When a user's password has expired, the user receives a message at sign-on (see "Password expiration interval" on page 91). The user can either press the Enter key to assign a new password or press F3 (Exit) to cancel the sign-on attempt without assigning a new password. If the user chooses to change the password, the Change Password display is shown and password validation is run for the new password.

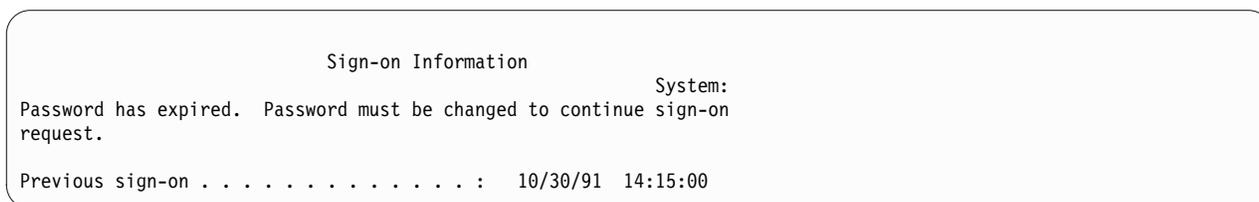


Figure 1. Password expiration message

Table 54. Possible values for PWDEXP:

*NO:	The password is not set to expired.
*YES:	The password is set to expired.

Recommendations: Set the password to expired whenever you create a new user profile or assign a temporary password to a user.

Status

The value of the *Status* field indicates if the profile is valid for sign-on. If the profile status is enabled, the profile is valid for sign-on. If the profile status is disabled, an authorized user has to enable the profile again to make it valid for sign-on.

Add User prompt:
Not shown

CL parameter:
STATUS

Length:
10

You can use the CHGUSRPRF command to enable a profile that has been disabled. You must have *SECADM special authority and *OBJMGT and *USE authority to the profile to change its status. "Enabling a user profile" on page 125 shows an example of an adopted authority program to allow a system operator to enable a profile.

The system can disable a profile after a certain number of incorrect password verification attempts with that profile, depending on the settings of the QMAXSIGN and QMAXSGNACN system values.

You can always sign on with the QSECOFR (security officer) profile at the console, even if the status of QSECOFR is *DISABLED. If the QSECOFR user profile becomes disabled, sign on as QSECOFR at the console and type CHGUSRPRF QSECOFR STATUS(*ENABLED).

Table 55. Possible values for STATUS:

*ENABLED	The profile is valid for sign-on.
*DISABLED	The profile is not valid for sign-on until an authorized user enables it again.

Recommendations: Set the status to *DISABLED if you want to prevent sign-on with a user profile. For example, you can disable the profile of a user who will be away from the business for an extended period.

User class

User class is used to control what menu options are shown to the user on IBM i menus. This helps control user access to some system functions.

Add User prompt:

Type of User

CL parameter:

USRCLS

Length:

10

This does not necessarily limit the use of commands. The *Limit capabilities* field controls whether the user can enter commands. User class may not affect what options are shown on menus provided by other licensed programs.

If no special authorities are specified when a user profile is created, the user class and the security level (QSECURITY) system value are used to determine the special authorities for the user.

Possible values for USRCLS: Table 56 shows the possible user classes and what the default special authorities are for each user class. The entries indicate that the authority is given at security levels 10 and 20 only, at all security levels, or not at all.

The default value for user class is ***USER**.

Table 56. Default special authorities by user class

Special authority	User classes				
	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	All	10 or 20	10 or 20	10 or 20	10 or 20
*SECADM	All	All			
*JOBCTL	All	10 or 20	10 or 20	All	
*SPLCTL	All				
*SAVSYS	All	10 or 20	10 or 20	All	10 or 20
*SERVICE	All				
*AUDIT	All				
*IOSYSCFG	All				

Recommendations: Most users do not need to perform system functions. Set the user class to *USER, unless a user specifically needs to use system functions.

Assistance level

The *Assistance level* field in the user profile specifies the default assistance level for the user when the profile is created. The System i platform provides three levels of assistance: basic, intermediate, and advanced.

Add User prompt:
Not shown

CL parameter:
ASTLVL

Length:
10

For each user, the system keeps track of the last assistance level used for every system display that has more than one assistance level. That level is used the next time the user requests that display. During an active job, a user can change the assistance level for a display or group of related displays by pressing F21 (Select assistance level). The new assistance level for that display is stored with the user information.

Specifying the assistance level (ASTLVL) parameter on a command does not change the assistance level that is stored for the user for the associated display.

If the assistance level in the user profile is changed using the CHGUSRPRF or the Change Profile (CHGPRF) command, the assistance levels stored for all displays for that user are reset to the new value.

For example, assume the user profile for USERA is created with the default assistance level (basic). Table 57 shows whether USERA sees the Work with User Profiles display or the Work with User Enrollment display when using different options. The table also shows whether the system changes the version for the display that is stored with USERA's profile.

Table 57. How assistance levels are stored and changed

Action taken	Version of display shown	Version of display stored
Use WRKUSRPRF command	Work with User Enrollment display	No change (basic assistance level)
From Work with User Enrollment display, press F21 and select intermediate assistance level.	Work with User Profiles display	Changed to intermediate assistance level
Use WRKUSRPRF command	Work with User Profiles display	No change (intermediate)
Select the work with user enrollment option from the SETUP menu.	Work with User Profiles display	No change (intermediate)
Type CHGUSRPRF USERA ASTLVL(*BASIC)		Changed to basic assistance level
Use WRKUSRPRF command	Work with User Enrollment display	No change (basic)
Type WRKUSRPRF ASTLVL(*INTERMED)	Work with User Profiles display	No change (basic)

Note: The *User option* field in the user profile also affects how system displays are shown. This field is described on page "User Options" on page 108.

Table 58. Possible Values for ASTLVL

*SYSVAL	The assistance level specified in the QASTLVL system value is used.
*BASIC	The Operational Assistant user interface is used.
*INTERMED	The system interface is used.

Table 58. Possible Values for ASTLVL (continued)

*ADVANCED	The expert system interface is used. To allow for more list entries, the option numbers and the function keys are not always displayed. If a command does not have an advanced (*ADVANCED) level, the intermediate (*INTERMED) level is used.
-----------	---

Current library

The *current library* is the library that is specified to be the first user library searched for objects requested by a user. If the user creates objects and specifies *CURLIB, the objects are put in the current library.

Add User prompt:

Default library

CL parameter:

CURLIB

Length:

10

Authority

*USE

The current library is automatically added to the user's library list when the user signs on. It does not need to be included in the initial library list in the user's job description.

The user cannot change the current library if the *Limit capabilities* field in the user profile is *YES or *PARTIAL.

The topic "Library lists" on page 207 provides more information about using library lists and the current library.

Table 59. Possible values for CURLIB:

*CRTDFT	This user has no current library. If objects are created using *CURLIB on a create command, the library QGPL is used as the default current library.
<i>current-library-name</i>	The name of a library.

Recommendations: Use the *Current library* field to control where users are allowed to put new objects, such as Query programs. Use the *Limit capabilities* field to prevent users from changing the current library.

Initial program

You can specify the name of a program to call when a user signs on. Such a program is called an initial program. An initial program runs before the initial menu, if any, is displayed.

Add User prompt:

Sign on program

CL parameter:

INLPGM

Length:

10 (program name) 10 (library name)

Authority:

*USE for program *EXECUTE for library

If the *Limit capabilities* field in the user's profile is *YES or *PARTIAL, the user cannot specify an initial program on the Sign On display.

The initial program is called only if the user's routing program is QCMD or QCL. See "Starting an interactive job" on page 199 for more information about the processing sequence when a user signs on.

Initial programs are used for two main purposes:

- To restrict a user to a specific set of functions.
- To perform some initial processing, such as opening files or establishing the library list, when the user first signs on.

Parameters cannot be passed to an initial program. If the initial program fails, the user is not able to sign on.

Table 60. Possible values for INLPGM:

*NONE	No program is called when the user signs on. If a menu name is specified on the initial menu (INLMNU) parameter, that menu is displayed.
<i>program-name</i>	The name of the program that is called when the user signs on.

Table 61. Possible values for INLPGM library:

*LIBL	The library list is used to locate the program. If the job description for the user profile has an initial library list, that list is used. If the job description specifies *SYSVAL for the initial library list, the QUSRLIBL system value is used.
*CURLIB	The current library specified in the user profile is used to locate the program. If no current library is specified, QGPL is used.
<i>library-name</i>	The library where the program is located.

Initial menu

You can specify the name of a menu to be shown when the user signs on. The initial menu is displayed after the user's initial program runs. The initial menu is called only if the user's routing program is QCMD or QCL.

Add User prompt:

First menu

CL parameter:

INLMNU

Length:

10 (menu name) 10 (library name)

Authority

*USE for menu *EXECUTE for library

If you want the user to run only the initial program, you can specify *SIGNOFF for the initial menu.

If the Limit capabilities field in the user's profile is *YES, the user cannot specify a different initial menu on the Sign On display. If a user is allowed to specify an initial menu on the Sign On display, the menu specified overrides the menu in the user profile.

Table 62. Possible values for MENU:

MAIN	The System i Main Menu is shown.
*SIGNOFF	The system signs off the user when the initial program completes. Use this to limit users to running a single program.
<i>menu-name</i>	The name of the menu that is called when the user signs on.

Table 63. Possible values for MENU library:

*LIBL	The library list is used to locate the menu. If the initial program adds entries to the library list, those entries are included in the search, because the menu is called after the initial program has completed.
*CURLIB	The current library for the job is used to locate the menu. If no current library entry exists in the library list, QGPL is used.
<i>library-name</i>	The library where the menu is located.

Limit capabilities

You can use the Limit capabilities field to limit the user's ability to enter commands and to override the initial program, initial menu, current library, and attention-key-handling program specified in the user profile. This field is a tool for preventing users from experimenting on the system.

Add User prompt:

Restrict command line use

CL parameter:

LMTCPB

Length:

10

A user with limited capabilities can only run commands that are defined as being allowed to be used by limited users. The following commands are shipped by IBM with ALWLMTUSR(*YES):

- Sign off (SIGNOFF)
- Send message (SNDMSG)
- Display messages (DSPMSG)
- Display job (DSPJOB)
- Display job log (DSPJOBLOG)
- Start PC Organizer (STRPCO)
- Work with Messages (WRKMSG)

The Limit capabilities field in the user profile and the ALWLMTUSR parameter on commands apply only to commands that are run from the command line, the Command Entry display, FTP, REXEC, using the QCAPCMD API, or an option from a command grouping menu. Users are not restricted to perform the following actions:

- Run commands in CL programs that are running a command as a result of taking an option from a menu
- Run remote commands through applications

You can allow the limited capability user to run additional commands, or remove some of these commands from the list, by changing the ALWLMTUSR parameter for a command. Use the Change Command (CHGCMD) command. If you create your own commands, you can specify the ALWLMTUSR parameter on the Create Command (CRTCMD) command.

Possible values: Table 64 shows the possible values for the Limit capabilities field and what functions are allowed for each value.

Table 64. Functions allowed for limit capabilities values

Function	*YES	*PARTIAL	*NO
Change initial program	No	No	Yes
Change initial menu	No	Yes	Yes

Table 64. Functions allowed for limit capabilities values (continued)

Function	*YES	*PARTIAL	*NO
Change current library	No	No	Yes
Change attention program	No	No	Yes
Enter commands	A few ¹	Yes	Yes
¹ These commands are allowed by default: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. The user cannot use F9 to display a command line from any menu or display.			

Recommendations: Using an initial menu, restricting command line use, and providing access to the menu allow you to set up an environment for a user who does not need or want to access system functions.

Related concepts:

“Planning menus” on page 228

Menus are a good method for providing controlled access on your system. You can use menus to restrict a user to a set of strictly controlled functions by specifying limited capabilities and an initial menu in the user profile.

Text

The text in the user profile is used to describe the user profile or what it is used for.

Add User prompt:

User description

CL parameter:

TEXT

Length:

50

For user profiles, the text should have identifying information, such as the user’s name and department. For group profiles, the text should identify the group, such as what departments the group includes.

Table 65. Possible values for text:

*BLANK:	No text is specified.
<i>description</i>	Specify no more than 50 characters.

Recommendations: The *Text* field is truncated on many system displays. Put the most important identifying information at the beginning of the field.

Special authority

Special authority is used to specify the types of actions a user can perform on system resources. A user can be given one or more special authorities.

Add User prompt:

Not shown

CL parameter:

SPCAUT

Length:

100 (10 characters per special authority)

Authority:

To give a special authority to a user profile, you must have that special authority.

Table 66. Possible values for SPCAUT:

*USRCLS	Special authorities are granted to this user based on the user class (USRCLS) field in the user profile and the security level (QSECURITY) system value. If *USRCLS is specified, no additional special authorities can be specified for this user. If you specify *USRCLS when you create or change a user profile, the system puts the correct special authorities in the profile as if you had entered them. When you display profiles, you cannot tell whether special authorities were entered individually or entered by the system based on the user class. Table 56 on page 79 shows the default special authorities for each user class.
*NONE	No special authority is granted to this user.
<i>special-authority-name</i>	Specify one or more special authorities for the user.

***ALLOBJ special authority**

All-object (*ALLOBJ) special authority allows the user to access any resource on the system whether private authority exists for the user.

Even if the user has *EXCLUDE authority to an object, *ALLOBJ special authority still allows the user to access the object.

Risks: *ALLOBJ special authority gives the user extensive authority over all resources on the system. The user can view, change, or delete any object. The user can also grant to other users the authority to use objects.

A user with *ALLOBJ authority cannot directly perform operations that require another special authority. For example, *ALLOBJ special authority does not allow a user to create another user profile, because creating user profiles requires *SECADM special authority. However, a user with *ALLOBJ special authority can submit a batch job to run using a profile that has the needed special authority. Giving *ALLOBJ special authority essentially gives a user access to all functions on the system.

***SECADM special authority**

Security administrator (*SECADM) special authority allows a user to create, change, and delete user profiles.

A user with *SECADM special authority can:

- Add users to the system distribution directory.
- Display authority for documents or folders.
- Add and remove access codes to the system.
- Give and remove a user's access code authority.
- Give and remove permission for users to work on another user's behalf.
- Delete documents and folders.
- Delete document lists.
- Change distribution lists created by other users.

Only a user with *SECADM and *ALLOBJ special authority can give *SECADM special authority to another user.

***JOBCTL special authority**

The Job control (*JOBCTL) special authority allows a user to change the priority of jobs and of printing, end a job before it has finished, or delete output before it has printed. *JOBCTL special authority can also give a user access to confidential spooled output, if output queues are specified OPRCTL(*YES).

Job control (*JOBCTL) special authority allows the user to perform the following actions:

- Change, delete, hold, and release all files on any output queues specified as OPRCTL(*YES).
- Display, send, and copy all files on any output queues specified as DSPDTA(*YES or *NO) and OPRCTL(*YES).
- Hold, release, and clear job queues specified as OPRCTL(*YES).
- Hold, release, and clear output queues specified as OPRCTL(*YES).
- Hold, release, change, and cancel other users' jobs.
- Start, change, end, hold, and release writers, if the output queue is specified as OPRCTL(*YES).
- Change the running attributes of a job, such as the printer for a job.
- Stop subsystems.
- Perform an initial program load (IPL).

Securing printer output and output queues is discussed in "Printing" on page 211.

You can change the job priority (JOBPTY) and the output priority (OUTPTY) of your own job without job control special authority. You must have *JOBCTL special authority to change the run priority (RUNPTY) of your own job.

Changes to the output priority and job priority of a job are limited by the priority limit (PTYLMT) in the profile of the user making the change.

Risks: A user who abuses *JOBCTL special authority can cause negative effect on individual jobs and on overall system performance.

***SPLCTL special authority**

Spool control (*SPLCTL) special authority allows the user to perform all spool control functions, such as changing, deleting, displaying, holding and releasing spooled files.

The user can perform these functions on all output queues, regardless of any authorities for the output queue or the OPRCTL parameter for the output queue. *SPLCTL special authority also allows the user to manage job queues, including holding, releasing, and clearing the job queue. The user can perform these functions on all job queues, regardless of any authorities for the job queue or the OPRCTL parameter for the job queue.

Risks: The user with *SPLCTL special authority can perform any operation on any spooled file in the system. Confidential spooled files cannot be protected from a user with *SPLCTL special authority.

***SAVSYS special authority**

Save system (*SAVSYS) special authority gives the user the authority to save, restore, and free storage for all objects on the system, regardless of whether the user has object existence authority to the objects.

Risks: The user with *SAVSYS special authority can:

- Save an object and take it to another system to be restored.
- Save an object and display the tape to view the data.
- Save an object and free storage, thus deleting the data portion of the object.
- Save a document and delete it.

***SERVICE special authority**

Service (*SERVICE) special authority allows the user to start system service tools using the STRSST command. This special authority allows the user to debug a program with only *USE authority to the program and perform the display and alter service functions. It also allows the user to perform trace functions.

The dump function can be performed without *SERVICE authority.

Risks: A user with *SERVICE special authority can display and change confidential information using service functions. The user must have *ALLOBJ special authority to change the information using service functions.

To minimize the risk for trace commands, users can be given authorization to perform service tracing without the *SERVICE special authority. In this way, only specific users have the ability to perform a trace command, which can grant them access to sensitive data. The user must be authorized to the command and have either *SERVICE special authority, or be authorized to the Service Trace function of i5/OS through Application Administration in System i Navigator. The Change Function Usage (CHGFCNUSG) command, with the function ID of QIBM_SERVICE_TRACE, can also be used to change the list of users that are allowed to perform trace operations.

The commands to which access can be granted in this way include:

STRCMNTRC	Start Communications Trace
ENDCMNTRC	End Communications Trace
PRTCMNTRC	Print Communications Trace
DLTCMNTRC	Delete Communications Trace
CHKCMNTRC	Check Communications Trace
TRCCNN	Trace Connection (see "Granting access to traces")
TRCINT	Trace Internal
STRTRC	Start Job Trace
ENDTRC	End Job Trace
PRTTRC	Print Job Trace
DLTRC	Delete Job Trace
TRTCPAPP	Trace TCP/IP Application
WRKTRC	Work with Traces

Note: You need *ALLOBJ to change data using service functions.

Granting access to traces:

Trace commands, such as TRCCNN (Trace Connection) are powerful commands that should not be granted to all users who need access to other service and debug tools.

Complete the following steps to limit who can access these trace commands without having *SERVICE authority:

1. In System i Navigator, open Users and Groups.
2. Select **All Users** to view a list of user profiles.
3. Right-click the user profile to be altered.
4. Select **Properties**.
5. Click **Capabilities**.
6. Open the Applications tab.
7. Select **Access for**.
8. Select **Host Applications**.
9. Select **Operating System**.
10. Select **Service**.

11. Use the check box to grant or revoke access to trace command.

Alternatively, the Change Function Usage (CHGFCNUSG) command can be used to grant users access to the trace commands. Enter CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(user-profile) USAGE(*ALLOWED).

***AUDIT special authority**

Audit (*AUDIT) special authority gives the user the ability to view and change auditing characteristics.

A user can perform the following tasks with the *AUDIT special authority:

- Change and display the system values that control auditing.
- Use the CHGOBJAUT, CHGDLOAUD, and CHGAUD commands to change auditing for objects.
- Use the CHGUSRAUD command to change auditing for a user.
- Display an object's auditing values.
- Display a user profile's auditing values.
- Run some of the security tool commands, such as PRTADPOBJ.

Risks: A user with *AUDIT special authority can stop and start auditing on the system or prevent auditing of particular actions. If having an audit record of security-relevant events is important for your system, carefully control and monitor the use of *AUDIT special authority.

To prevent general users from viewing auditing information, restrict general users' access to the following information:

- The security audit journal (QAUDJRN)
- Other journals that contain auditing data
- Save files, outfiles, spool files, and printed output that contain auditing information

Note: Only a user with *ALLOBJ, *SECADM, and *AUDIT special authorities can give another user *AUDIT special authority.

***IOSYSCFG special authority**

System configuration (*IOSYSCFG) special authority gives the user the ability to change how the system is configured. Users with this special authority can add or remove communications configuration information, work with TCP/IP servers, and configure the internet connection server (ICS). Most commands for configuring communications require *IOSYSCFG special authority.

Recommendations for special authorities: Giving special authorities to users represents a security exposure. For each user, carefully evaluate the need for any special authorities. Keep track of which users have special authorities and periodically review their requirement for the authority.

In addition, you should control the following situations for user profiles and programs:

- Whether user profiles with special authorities can be used to submit jobs
- Whether programs created by these users can run using the authority of the program owner

Programs adopt the *ALLOBJ special authority of the owner if:

- The programs are created by users who have *ALLOBJ special authority
- The user specifies USRPRF(*OWNER) parameter on the command that creates the program

Special environment

The user can operate in the IBM i, the System/36, or the System/38 environment. When the user signs on, the system uses the routing program and the special environment in the user's profile to determine the user's environment.

Add User prompt:
Not shown

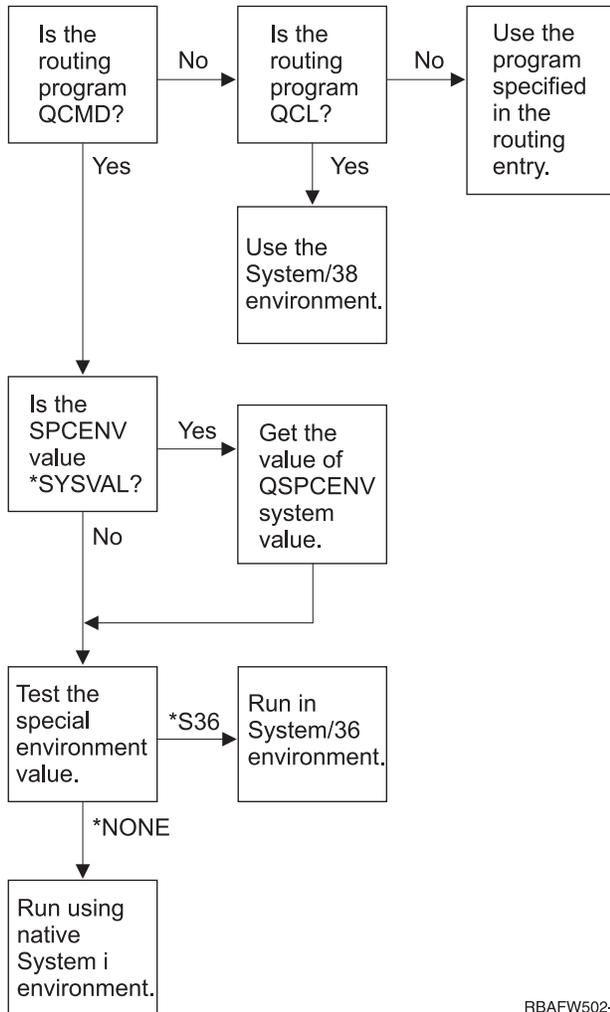
CL parameter:
SPCENV

Length:
10

Table 67. Possible values for SPCENV:

*SYSVAL	The QSPCENV system value is used to determine the environment when the user signs on, if the user's routing program is QCMD.
*NONE	The user operates in the IBM i environment.
*S36	The user operates in the System/36 environment if the user's routing program is QCMD.

Recommendations: If the user runs a combination of System i and System/36 applications, use the Start System/36 (STRS36) command before running System/36 applications rather than specifying the System/36 environment in the user profile. This provides better performance for the System i applications.



RBAFW502-2

Figure 2. Description of special environment

Description of special environment in Figure 2

The system determines if the routing program is QCMD. If it is not, then the system checks to see if the routing program is QCL. If the routing program is QCL, then the system will use the System/38 special environment. If the routing program is not QCL, then the system uses the program specified in the routing entry.

If the routing program is QCMD, then the system determines if the SPCENV system value is set. If it is set, then the system retrieves the value for QSPCENV system value and the system tests the special environment value. If SPCENV system value is not set, then the system tests the special environment value.

If the special environment value is set to *S36, the system runs the System/36 special environment. If the special environment value is set to *NONE, then the system runs the integrated IBM i environment.

Display sign-on information

The Sign-on Information display is a tool for users to monitor their profiles and to detect attempted misuse. The Display sign-on information field specifies whether the Sign-on Information display is shown when the user signs on.

Add User prompt:

Not shown

CL parameter:

DSPSGNINF

Length:

7

Figure 3 shows the display. Password expiration information is only shown if the password expires within the password expiration warning days.

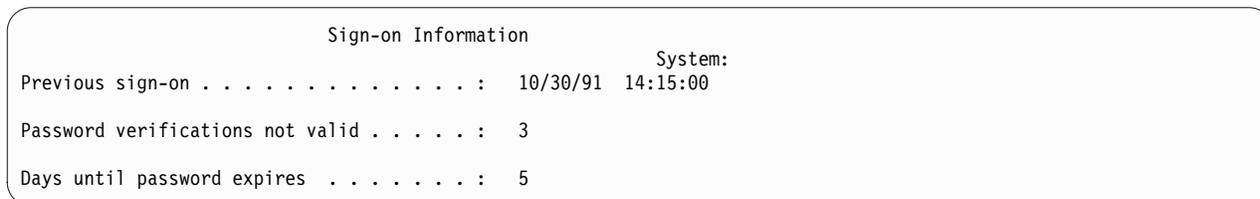


Figure 3. Sign-On Information Display

Table 68. Possible values for DSPSGNINF:

*SYSVAL	The QDSPSGNINF system value is used.
*NO	The Sign-on Information display is not shown when the user signs on.
*YES	The Sign-on Information display is shown when the user signs on.

Recommendations: Having all users see this display is recommended. Users with special authority or authority to critical objects should be encouraged to use the display to make sure no one attempts to use their profiles.

Password expiration interval

The password expiration interval controls the number of days that a valid password can be used before it must be changed.

Add User prompt:

Not shown

CL parameter:

PWDEXPITV

Length:

5,0

When a user’s password has expired, the user receives a message at sign-on. The user can either press the Enter key to assign a new password or press F3 (Exit) to cancel the sign-on attempt without assigning a new password. If the user chooses to change the password, the Change Password display is shown and full password validation is run for the new password. “Password expiration interval” shows an example of the password expiration message.

Table 69. Possible values for PWDEXPITV:

*SYSVAL	The QPWDEXPITV system value is used.
*NOMAX	The system does not require the user to change the password.
<i>password- expiration- interval</i>	Specify a number from 1 through 366.

Recommendations: Set the QPWDEXPITV system value for an appropriate interval, such as 60 to 90 days. Use the Password expiration interval field in the user profile to require users with *SERVICE, *SAVSYS, *SECADM, or *ALLOBJ special authorities to change passwords more frequently than other users.

Block Password Change

The block password change parameter specifies the time period during which a password is blocked from being changed after the prior successful password change operation.

Add User prompt:

Not shown

CL parameter:

PWDCHGBLK

Length:

10

This parameter value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command. In addition, this parameter value is not enforced if the set password to expired (PWDEXP) field in the user profile has a value of *YES. This enables a security administrator to create a user profile with an expired password and still permit the user to sign-on and change the password (once) without being restricted by the block password change system value.

Table 70. Possible values for PWDCHGBLK:

*SYSVAL	The QPWDCHGBLK system value is used.
*NONE	The password can be changed at any time.
1 - 99	A password cannot be changed within the specified number of hours after the prior successful password changed operation.

Recommendation: Set the parameter to *SYSVAL unless you notice unusual password change activity for a specific user. In this case, you can use a value, such as 2, to limit the user's password change frequency.

Local password management

The Local password management (LCLPWDMGT) parameter controls whether the user profile password is managed locally. When the password is not management locally, users cannot access the system by direct sign-on, but through other platforms.

If the password is managed locally, then the password is stored locally with the user profile. This is the traditional method of storing the password.

Add User prompt:

Not shown

CL parameter:

LCLPWDMGT

Length:

10

If the password is not being managed locally, then the local IBM i password is set to *NONE. The password value specified in the password parameter will be sent to other IBM products that do password synchronization, such as IBM i Integration for Windows Server. Users will not be able to change their passwords using the Change Password (CHGPWD) command. In addition, users will not be able to sign on to the system directly. Specifying this value will affect other IBM products that do password synchronization, such as IBM i Integration for Windows Server.

This parameter should not be set to *NO unless the user only needs to access the system through some other platform, such as Windows Server.

Table 71. Possible values for LCLPDMGT:

*YES	The password is managed locally.
*NO	The password is not managed locally.

Limit device sessions

The Limit device sessions field controls whether the number of device sessions allowed for a user is limited. The value does not restrict the use of the System Request menu or a second sign-on from the same device.

Add User prompt:

Not shown

CL parameter:

LMTDEVSSN

Length:

7

Table 72. Possible values for LMTDEVSSN:

*SYSVAL	The QLMTDEVSSN system value is used.
*NO	The user may be signed on to more than one device at the same time.
*YES	The user may not be signed on to more than one device at the same time.
0	The user is not limited to a specific number of device sessions. This value has the same meaning as *NO.
1	The user is limited to a single device session. This value has the same meaning as *YES.
2 - 9	The user is limited to the specified number of device sessions.

Recommendations: Limiting users to one workstation at a time is one way to discourage sharing user profiles. Set the QLMTDEVSSN system value to 1 (YES). If some users have a requirement to sign on at multiple workstations, use the Limit device sessions field in the user profile for those users.

Keyboard buffering

This parameter specifies the keyboard buffering value used when a job is initialized for this user profile. The new value takes effect the next time the user signs on.

Add User prompt:

Not shown

CL parameter:

KBDBUF

Length:

10

The keyboard buffering field controls two functions:

Type-ahead:

Lets the user type data faster than it can be sent to the system.

Attention key buffering:

If attention key buffering is on, the Attention key is treated like any other key. If attention key buffering is not on, pressing the Attention key results in sending the information to the system even when other workstation input is inhibited.

Table 73. Possible values for KBDBUF:

*SYSVAL	The QKBDBUF system value is used.
*NO	The type-ahead feature and Attention-key buffering option are not active for this user profile.
*TYPEAHEAD	The type-ahead feature is active for this user profile.
*YES	The type-ahead feature and Attention-key buffering option are active for this user profile.

Maximum storage

You can specify the maximum amount of auxiliary storage that the system uses to store permanent objects that a user profile owns. This includes objects that the system places in the temporary library (QTEMP) during a job.

Add User prompt:

Not shown

CL parameter:

MAXSTG

Length:

11,0

If the storage needed is greater than the maximum amount specified when the user attempts to create an object, the object is not created.

The maximum storage value is independently applied to each independent auxiliary storage pool (ASP) on the system. Therefore, specifying a value of 5000 means that the user profile can use the following size of auxiliary storage:

- 5000 KB of auxiliary storage in the system ASP and basic user ASPs.
- 5000 KB of auxiliary storage in independent ASP 00033 (if it exists).
- 5000 KB of auxiliary storage in independent ASP 00034 (if it exists).

This provides a total of 15 000 KB of auxiliary storage from the whole system.

When planning maximum storage for user profiles, consider the following system functions, which can affect the maximum storage needed by a user:

- A restore operation first assigns the storage to the user doing the restore operation, and then transfers the objects to the OWNER. Users who do large restore operations should have MAXSTG(*NOMAX) in their user profiles.
- The user profile that owns a journal receiver is assigned the storage as the receiver size grows. If new receivers are created, the storage continues to be assigned to the user profile that owns the active journal receiver. Users who own active journal receivers should have MAXSTG(*NOMAX) in their user profiles.
- If a user profile specifies OWNER(*GRPPRF), ownership of any object created by the user is transferred to the group profile after the object is created. However, the user creating the object must have adequate storage to contain any created object before the object ownership is transferred to the group profile.

- The system assigns storage for the descriptions of objects that are placed in a library to the owner of that library. This is true even if the objects are owned by another user profile. Examples of such descriptions are text and program references.
- The system assigns storage to the user profile for temporary objects that are used during job processing. Examples of such objects are commitment control blocks, file editing spaces, and documents.

Table 74. Possible values for MAXSTG:

*NOMAX	As much storage as required can be assigned to this profile.
<i>maximum- KB</i>	Specify the maximum amount of storage in kilobytes (1 kilobyte equals 1024 bytes) that can be assigned to this user profile.

Priority limit

The priority limit in the user profile determines the maximum scheduling priorities (job priority and output priority) that are allowed for any jobs the user submits. Priority limit controls the job's priority when it is submitted. It also controls any changes made to the job's priority while the job is waiting in the queue, or when the job runs.

Add User prompt:

Not shown

CL parameter:

PTYLMT

Length:

1

A batch job has three different priority values:

Run priority:

Determines how the job competes for machine resources when the job is running. Run priority is determined by the job's class.

Job priority:

Determines the scheduling priority for a batch job when the job is in the job queue. You can set the job's priority in the job description or by using the submit command.

Output priority:

Determines the scheduling priority for any output created by the job on the output queue. You can set the output priority in the job description or when you use the submit command.

The priority limit also limits changes that a user with *JOBCTL special authority can make to another user's job. You cannot give someone else's job a higher priority than the limit specified in your own user profile.

If a batch job runs under a different user profile than the user submitting the job, the priority limits for the batch job are determined by the profile the job runs under. If a requested scheduling priority on a submitted job is higher than the priority limit in the user profile, the priority of the job is reduced to the level permitted by the user profile.

Table 75. Possible values for PTYLMT:

3	The default priority limit for user profiles is 3. The default priority for both job priority and output priority on job descriptions is 5. Setting the priority limit for the user profile at 3 gives the user the ability to move some jobs ahead of others on the queues.
<i>priority- limit</i>	Specify a value, 1 through 9. The highest priority is 1; the lowest priority is 9.

Recommendations: Using the priority values in job descriptions and on the submit job commands is often a better way to manage the use of system resources than changing the priority limit in user profiles.

Use the priority limit in the user profile to control changes that users can make to submitted jobs. For example, system operators may need a higher priority limit so that they can move jobs in the queues.

Job description

A job description contains a specific set of job-related attributes, such as which job queue to use, scheduling priority, routing data, message queue severity, library list and output information. The attributes determine how each job is run on the system.

Add User prompt:
Not shown

CL parameter:
JOBDB

Length
10 (job description name) 10 (library name)

Authority:
*USE for job description, *READ and *EXECUTE for library

When a user signs on, the system looks at the workstation entry in the subsystem description to determine what job description to use for the interactive job. If the workstation entry specifies *USRPRF for the job description, the job description in the user profile is used.

The job description for a batch job is specified when the job is started. It can be specified by name, or it can be the job description from the user profile under which the job runs.

See the Work management topic for more information about job descriptions and their uses.

Table 76. Possible values for JOBDB:

QDFTJOBDB	The system-supplied job description found in library QGPL is used. You can use the Display Job Description (DSPJOBDB) command to see the attributes contained in this job description.
<i>job- description- name</i>	Specify the name of the job description, 10 characters or less.

Table 77. Possible values for JOBDB Library:

*LIBL	The library list is used to locate the job description.
*CURLIB	The current library for the job is used to locate the job description. If no current library entry exists in the library list, QGPL is used.
<i>library- name</i>	Specify the library where the job description is located, 10 characters or less.

Recommendations: For interactive jobs, the job description is a good method of controlling library access. You can use a job description for an individual to specify a unique library list, rather than using the QUSRLIBL (user library list) system value.

Group profile

The group profile (GRPPRF) parameter specifies if the user is a member of a group profile. The group profile can provide the user with authority to use objects for which the user does not have specific authority. You may specify up to 15 additional groups for the user in the Supplemental group profile (SUPGRPPRF) parameter.

Add User prompt:
User Group

CL parameter:
GRPPRF

Length:
10

Authority:
To specify a group when creating or changing a user profile, you must have *OBJMGT, *OBJOPR, *READ, *ADD, *UPD, and *DLT authority to the group profile.

Note: Adopted authority is not used to check for *OBJMGT authority to the group profile. For more information about adopted authority, see “Objects that adopt the owner’s authority” on page 149.

When a group profile is specified in a user profile, the user is automatically granted *OBJMGT, *OBJOPR, *READ, *ADD, *UPD, and *DLT authorities to the group profile, if the group profile is not already one of the user's group profiles. These authorities are necessary for system functions and should not be removed.

If a profile specified in the GRPPRF parameter is not already a group profile, the system sets information in the profile marking it as a group profile. The system also generates a gid for the group profile, if it does not already have one.

When the GRPPRF value is changed, the change takes effect the next time the user signs on or the next time a job swaps to the user profile using a profile handle or profile token, which was obtained after the change occurred.

See “Planning group profiles” on page 239 for more information about using group profiles.

Table 78. Possible values for GRPPRF

*NONE	No group profile is used with this user profile.
<i>user-profile-name</i>	Specify the name of a group profile of which this user profile is a member.

Owner

If the user is a member of a group, you can use the owner parameter in the user profile to specify who owns any new objects created by the user. Objects can be owned either by the user or by the user’s first group (the value of the GRPPRF parameter). You can specify the Owner field only if you have specified a value other than *NONE for the Group profile field.

Add User prompt:
Not shown

CL parameter:
OWNER

Length:
10

When the Owner value is changed, the change takes effect the next time the user signs on or the next time a job swaps to the user profile using a profile handle or profile token obtained after the change has occurred.

Table 79. Possible values for Owner:

*USRPRF	This user profile is the Owner of any new objects it creates.
----------------	---

Table 79. Possible values for Owner: (continued)

*GRPPRF	<p>The group profile is made the Owner of any objects created by the user and is given all (*ALL) authority to the objects. The user profile is not given any specific authority to new objects it creates. If *GRPPRF is specified, you must specify a group profile name in the GRPPRF parameter, and the GRPAUT parameter must be *NONE.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If you give ownership to the group, all members of the group can change, replace, and delete the object. 2. The *GRPPRF parameter is ignored for all file systems except QSYS.LIB. In cases where the parameter is ignored, the user retains ownership of the object.
---------	--

Group authority

If the user profile is a member of a group and OWNER(*USRPRF) is specified, the Group authority field controls what authority is given to the group profile for any objects created by this user.

Add User prompt:

Not shown

CL parameter:

GRPAUT

Length:

10

Group authority can be specified only when GRPPRF is not *NONE and OWNER is *USRPRF. Group authority applies to the profile specified in the GRPPRF parameter. It does not apply to supplemental group profiles specified in the SUPGRPPRF parameter.

When the GRPAUT value is changed, the change takes effect the next time the user signs on or the next time a job swaps to the user profile using a profile handle or profile token obtained after the change has occurred.

Table 80. Possible values for GRPAUT:

*NONE	No specific authority is given to the group profile when this user creates objects.
*ALL	The group profile is given all management and data authorities to any new objects the user creates.
*CHANGE	The group profile is given the authority to change any objects the user creates.
*USE	The group profile is given authority to view any objects the user creates.
*EXCLUDE	The group profile is specifically denied access to any new objects created by the user.

Related reference:

“Defining how information can be accessed” on page 132

You can define what operations can be performed on objects, data, and fields.

Group authority type

When a user creates a new object, the Group authority type parameter in the user’s profile determines what type of authority the user’s group receives to the new object.

Add User prompt:

Not shown

CL parameter:
GRPAUTYP

Length:
10

The GRPAUTYP parameter works with the OWNER, GRPPRF, and GRPAUT parameters to determine the group's authority to a new object.

When the GRPAUTYP value is changed, the change takes effect the next time the user signs on or the next time a job swaps to the user profile using a profile handle or profile token obtained after the change has occurred.

Table 81. Possible values for GRPAUTYP: ¹

*PRIVATE	The authority defined in the GRPAUT parameter is assigned to the group profile as a private authority.
*PGP	The group profile defined in the GRPPRF parameter is the primary group for the newly created object. The primary group authority for the object is the authority specified in the GRPAUT parameter. This value can be specified only when GRPAUT is not *NONE.
¹	Private authority and primary group authority provide the same access to the object for members of the group, but they might have different performance characteristics. "Primary group for an object" on page 144 explains how primary group authority works.

Recommendations: Specifying *PGP is a method for beginning to use primary group authority. Consider using GRPAUTYP(*PGP) for users who frequently create new objects that must be accessed by members of the group profile.

Supplemental groups

You can specify supplemental groups when creating or changing a user profile. The user cannot have supplemental group profiles if the GRPPRF parameter is *NONE.

Add User prompt:
Not shown

CL parameter:
SUPGRPPRF

Length:
150

Authority:
To specify supplemental groups when creating or changing a user profile, you must have *OBJMGT, *OBJOPR, *READ, *ADD, *UPD, and *DLT authority to each group profile.

Note: *OBJMGT authority cannot come from adopted authority. For more information, see "Objects that adopt the owner's authority" on page 149.

You can specify the names of up to 15 profiles from which this user is to receive authority. The user becomes a member of each supplemental group profile.

When supplemental group profiles are specified in a user profile, the user is automatically granted *OBJMGT, *OBJOPR, *READ, *ADD, *UPD, and *DLT authorities to each group profile, if the group profile is not already one of the user's group profiles. These authorities are necessary for system functions and should not be removed. If a profile specified in the SUPGRPPRF parameter is not already a group profile, the system marks it as a group profile. The system also generates a group identification number (gid) for the group profile, if it does not already have one.

When the SUPGRPPRF value is changed, the change takes effect the next time the user signs on or the next time a job swaps to the user profile using a profile handle or profile token obtained after the change has occurred.

See “Planning group profiles” on page 239 for more information about using group profiles.

Table 82. Possible values for SUPGRPPRF

*NONE	No supplemental groups are used with this user profile.
<i>group- profile- name</i>	Specify up to 15 names of group profiles to be used with this user profile. These profiles, in addition to the profile specified in the GRPPRF parameter, are used to give the user access to objects. The profile name specified for GRPPRF can also be specified as one of the 15 supplemental group profiles.

Accounting code

Specifying the accounting code allows you to gather information about the system resources used by a job.

Add User prompt:

Not shown

CL parameter:

ACGCDE

Length:

15

Job accounting is an optional function used to gather information about the use of system resources. The accounting level (QACGLVL) system value determines whether job accounting is active. The accounting code for a job comes from either the job description or the user profile. The accounting code can also be specified when a job is running using the Change Accounting Code (CHGACGCDE) command.

When the *accounting code* value is changed, the change takes effect the next time the user signs on or the next time a job, which runs using the user profile's accounting code value, is started.

See the Work management topic for more information about job accounting.

Table 83. Possible values for ACGCDE:

*BLANK	An accounting code of 15 blanks is assigned to this user profile.
<i>accounting-code</i>	Specify a 15-character accounting code. If less than 15 characters are specified, the string is padded with blanks on the right.

Document password

A document password controls the accessibility and distribution of personal mail when viewed by people who are working on behalf of the user. The document password is supported by some Document Interchange Architecture (DIA) products, such as the Displaywriter.

Add User prompt:

Not shown

CL parameter:

DOCPWD

Table 84. Possible values for DOCPWD:

*NONE	No document password is used by this user.
--------------	--

Table 84. Possible values for DOCPWD: (continued)

<i>document- password</i>	Specify a document password for this user. The password must consist of from 1 through 8 characters (letters A through Z and numbers 0 through 9). The first character of the document password must be alphabetic; the remaining characters can be alphanumeric. Embedded blanks, leading blanks, and special characters are not allowed.
---------------------------	--

Message queue

A *message queue* is an object on which messages are placed when they are sent to a person or a program. A message queue is used when a user sends or receives messages.

Add User prompt:

Not shown

CL parameter:

MSGQ

Length:

10 (message queue name) 10 (library name)

Authority:

*USE for message queue, if it exists. *EXECUTE for the message queue library.

If the message queue does not exist, it is created when the profile is created or changed. The message queue is owned by the profile being created or changed. The user creating the profile is given *ALL authority to the message queue.

If the message queue for a user profile is changed using the Change User Profile (CHGUSRPRF) command, the previous message queue is not automatically deleted by the system.

Table 85. Possible values for MSGQ:

*USRPRF	A message queue with the same name as the user profile name is used as the message queue for this user. If the message queue does not exist, it is created in library QUSRSYS.
<i>message- queue-name</i>	Specify the message queue name that is used for this user. If you specify a message queue name, you must specify the library parameter.

Table 86. Possible values for MSGQ Library:

*LIBL	The library list is used to locate the message queue. If the message queue does not exist, you cannot specify *LIBL.
*CURLIB	The current library for the job is used to locate the message queue. If no current library entry exists in the library list, QGPL is used. If the message queue does not exist, it is created in the current library or QGPL.
<i>library- name</i>	Specify the library where the message queue is located. If the message queue does not exist, it is created in this library.

Recommendations: Give each user profile a unique message queue, preferably with the same name as the user profile.

Delivery

The delivery mode of a message queue determines whether the user is interrupted when a new message arrives on the queue.

Add User prompt:

Not shown

CL parameter:

DLVRY

Length:

10

The delivery mode specified in the user profile applies to the user's personal message queue. If you change the message queue delivery in the user profile and the user is signed on, the change takes effect the next time the user signs on. You can also change the delivery of a message queue with the Change Message Queue (CHGMSGQ) command.

Table 87. Possible values for DLVRY:

*NOTIFY	The job to which the message queue is assigned is notified when a message arrives at the message queue. For interactive jobs at a workstation, the audible alarm sounds and the message-waiting light turns on. The type of delivery cannot be changed to *NOTIFY if the message queue is also being used by another user.
*BREAK	The job that the message queue is assigned to is interrupted when a message arrives at the message queue. If the job is an interactive job, the audible alarm sounds (if the alarm is installed). The type of delivery cannot be changed to *BREAK if the message queue is also being used by another user.
*HOLD	The messages are held in the message queue until they are requested by the user or program.
*DFT	Messages requiring replies are answered with their default reply; information-only messages are ignored.

Severity

If a message queue is in *BREAK or *NOTIFY mode, the severity code determines the lowest-level messages that are delivered to the user. Messages whose severity is lower than the specified severity code are held in the message queue without the user being notified.

Add User prompt:

Not shown

CL parameter:

SEV

Length:

2,0

If you change the message queue severity in the user profile and the user is signed on, the change takes effect the next time the user signs on. You can also change the severity of a message queue with the CHGMSGQ command.

Table 88. Possible values for SEV:

00:	If a severity code is not specified, 00 is used. The user is notified of all messages, if the message queue is in *NOTIFY or *BREAK mode.
<i>severity- code</i>	Specify a value, 00 through 99, for the lowest severity code that causes the user to be notified. Any 2-digit value can be specified, even if no severity code has been defined for it (either defined by the system or by the user).

Print device

You can specify the printer used to print the output for this user. Spooled files are placed on an output queue with the same name as the printer when the output queue (OUTQ) is specified as the print device (*DEV).

Add User prompt:
Default printer

CL parameter:
PRTDEV

Length:
10

The print device and output queue information from the user profile are used only if the printer file specifies *JOB and the job description specifies *USRPRF. For more information about directing printer output, see the Basic printing topic.

Table 89. Possible values for PRTDEV:

*WRKSTN	The printer assigned to the user's workstation (in the device description) is used.
*SYSVAL	The default system printer specified in the QPRTDEV system value is used.
<i>print- device- name</i>	Specify the name of the printer that is used to print the output for this user.

Output queue

Both interactive and batch processing can result in spooled files that are to be sent to a printer. Spooled files are placed on an output queue. The system can have many different output queues.

Add User prompt:
Not shown

CL parameter:
OUTQ

Length:
10 (output queue name) 10 (library name)

Authority:
*USE for output queue *EXECUTE for library

An output queue does not need to be attached to a printer to receive new spooled files.

The print device and output queue information from the user profile are used only if the printer file specifies *JOB and the job description specifies *USRPRF. For more information about directing printer output, see the Advanced Function Presentation topic.

Table 90. Possible values for OUTQ:

*WRKSTN	The output queue assigned to the user's workstation (in the device description) is used.
*DEV	An output queue with the same name as the print device specified on the PRTDEV parameter is used.
<i>output- queue- name</i>	Specify the name of the output queue that is to be used. The output queue must already exist. If an output queue is specified, the library must be specified also.

Table 91. Possible values for OUTQ library:

*LIBL	The library list is used to locate the output queue.
--------------	--

Table 91. Possible values for OUTQ library: (continued)

*CURLIB	The current library for the job is used to locate the output queue. If no current library entry exists in the library list, QGPL is used.
<i>library- name</i>	Specify the library where the output queue is located.

Attention-Key-Handling program

The Attention-key-handling program (ATNPGM) is the program that is called when the user presses the Attention (ATTN) key during an interactive job.

Add User prompt:

Not shown

CL parameter:

ATNPGM

Length:

10 (program name) 10 (library name)

Authority:

*USE for program

*EXECUTE for library

The ATNPGM is activated only if the user's routing program is QCMD. The ATNPGM is activated before the initial program is called. If the initial program changes the ATNPGM, the new ATNPGM remains active only until the initial program ends. If the Set Attention-Key-Handling Program (SETATNPGM) command is run from a command line or an application, the new ATNPGM specified overrides the ATNPGM from the user profile.

Note: See "Starting an interactive job" on page 199 for more information about the processing sequence when a user signs on.

The *Limit capabilities* field determines if a different Attention-key-handling program can be specified by the user with the Change Profile (CHGPRF) command.

Table 92. Possible values for ATNPGM:

*SYSVAL	The QATNPGM system value is used.
*NONE	No Attention-key-handling program is used by this user.
*ASSIST	Operational Assistant Attention Program (QEZMAIN) is used.
<i>program- name</i>	Specify the name of the Attention-key-handling program. If a program name is specified, a library must be specified.

Table 93. Possible values for ATNPGM Library:

*LIBL	The library list is used to locate the Attention-key-handling program.
*CURLIB	The current library for the job is used to locate the Attention-key-handling program. If no current library entry exists in the library list, QGPL is used.
<i>library- name:</i>	Specify the library where the Attention-key-handling program is located.

Sort Sequence

Sort sequence is used for this user's output. You can use system-provided sort tables or create your own. A sort table can be associated with a particular language identifier on the system.

Add User prompt:

Not shown

CL parameter:

SRTSEQ

Length:

10 (value or table name) 10 (library name)

Authority:

*USE for table *EXECUTE for library

Table 94. Possible values for SRTSEQ:

*SYSVAL	The QSRTSEQ system value is used.
*HEX	The standard hexadecimal sort sequence is used for this user.
*LANGIDSHR	The sort sequence table associated with the user's language identifier is used. The table can contain the same weight for multiple characters.
*LANGIDUNQ	The sort sequence table associated with the user's language identifier is used. The table must contain a unique weight for each character in the code page.
<i>table-name</i>	Specify the name of the sort sequence table for this user.

Table 95. Possible values for SRTSEQ Library:

*LIBL	The library list is used to locate the table specified for the SRTSEQ value.
*CURLIB	The current library for the job is used to locate the table specified for the SRTSEQ value. If no current library entry exists in the library list, QGPL is used.
<i>library- name</i>	Specify the library where the sort sequence table is located.

Language identifier

You can specify the language identifier to be used by the system for the user.

Add User prompt:

Not shown

CL parameter:

LANGID

Length:

10

To see a list of language identifiers, press F4 (prompt) on the language identifier parameter from the Create User Profile display or the Change User Profile display.

Table 96. Possible values for LANGID:

*SYSVAL:	The system value QLANGID is used to determine the language identifier.
<i>language- identifier</i>	Specify the language identifier for this user.

Country or region identifier

You can specify the country or region identifier to be used by the system for the user.

Add User prompt:

Not shown

CL parameter:

CNTRYID

Length:
10

To see a list of country or region identifiers, press F4 (prompt) on the country or region identifier parameter from the Create User Profile display or the Change User Profile display.

Table 97. Possible values for CNTRYID:

*SYSVAL	The system value QCNTYID is used to determine the country or region identifier.
<i>country or region identifier</i>	Specify the country or region identifier for this user.

Coded character set identifier

You can specify the coded character set identifier to be used by the system for the user.

Add User prompt:
Not shown

CL parameter:
CCSID

Length:
5,0

To see a list of coded character set identifiers, press F4 (prompt) on the coded character set identifier parameter from the Create User Profile display or the Change User Profile display.

Table 98. Possible values for CCSID:

*SYSVAL	The QCCSID system value is used to determine the coded character set identifier.
<i>coded-character- set-identifier</i>	Specify the coded character set identifier for this user.

Character identifier control

The *CHRIDCTL* attribute controls the type of coded character set conversion that occurs for display files, printer files and panel groups.

Add User prompt:
Not shown

CL parameter:
CHRIDCTL

Length:
10

The character identifier control information from the user profile is used only if the *CHRIDCTL special value is specified on the CHRID command parameter on the create, change, or override commands for display files, printer files, and panel groups.

Table 99. Possible values for CHRIDCTL:

*SYSVAL	The system value QCHRIDCTL is used to determine the character identifier control.
*DEVD	The CHRID of the device is used to represent the CCSID of the data. No conversions occur, since the CCSID of the data is always the same as the CHRID of the device.

Table 99. Possible values for CHRIDCTL: (continued)

*JOBCCSID	Character conversion occurs when a difference exists between the device CHRID, job CCSID, or data CCSID values. On input, character data is converted from the device CHRID to the job CCSID when it is necessary. On output, character data is converted from the job CCSID to the device CHRID when it is necessary. On output, character data is converted from the file or panel group CCSID to the device CHRID when it is necessary.
-----------	--

Job attributes

The SETJOBATR field specifies which job attributes are to be taken at job initiation from the locale specified in the LOCALE parameter.

Add User prompt:

Not shown

CL parameter:

SETJOBATR

Length:

160

Table 100. Possible values for SETJOBATR:

*SYSVAL	The system value QSETJOBATR is used to determine which job attributes are to be taken from the locale.
*NONE	No job attributes are to be taken from the locale.
*CCSID	The coded character set identifier (CCSID) from the locale is used. The CCSID value from the locale will override the user profile CCSID.
*DATFMT	The date format from the locale is used.
*DATSEP	The date separator from the locale is used.
*DECfmt	The decimal format from the locale is used.
*SRTSEQ	The sort sequence from the locale is used. The sort sequence from the locale will override the user profile sort sequence.
*TIMSEP	The time separator from the locale is used.

Any combination of the following values can be specified:

- *CCSID
- *DATFMT
- *DATSEP
- *DECfmt
- *SRTSEQ
- *TIMSEP

Locale

The Locale field specifies the path name of the locale that is assigned to the LANG environment variable for this user.

Add User prompt:

Not shown

CL parameter:

LOCALE

Table 101. Possible values for LOCALE:

*SYSVAL	The system value QLOCALE is used to determine the locale path name to be assigned for this user.
*NONE	No locale is assigned for this user.
*C	The C locale is assigned for this user.
*POSIX	The POSIX locale is assigned for this user.
<i>locale path name</i>	The path name of the locale to be assigned to this user.

User Options

The User options field allows you to customize certain system displays and functions for the user. You can specify multiple values for the user option parameter.

Add User prompt:

Not shown

CL parameter:

USROPT

Length:

240 (10 characters each)

Table 102. Possible values for USROPT:

*NONE	No special options are used for this user. The standard system interface is used.
*CLKWD	Keywords are shown instead of the possible parameter values when a control language (CL) command is prompted. This is equivalent to pressing F11 from the normal control language (CL) command prompting display.
*EXPERT	When the user views displays that show object authority, such as the Edit Object Authority display or the Edit Authorization List display, detailed authority information is shown without the user having to press F11 (Display detail). "Authority displays" on page 154 shows an example of the expert version of the display.
*HLPFULL	The user sees full display help information instead of a window.
*PRTMSG	A message is sent to the user's message queue when a spooled file is printed for this user.
*ROLLKEY	The actions of the Page Up and Page Down keys are reversed.
*NOSTMSG	Status messages typically shown at the bottom of the display are not shown to the user.
*STSMG	Status messages are displayed when sent to the user.

User identification number

The integrated file system uses the user identification number (uid) to identify a user and verify the user's authority. Every user on the system must have a unique uid.

Add User prompt:

Not shown

CL parameter:

UID

Length:

10,0

Table 103. Possible values for UID:

<u>*GEN</u>	The system generates a unique uid for this user. The generated uid will be greater than 100.
<i>uid</i>	A value from 1 to 4294967294 to be assigned as the uid for this user. The uid must not be already assigned to another user.

Recommendations: For most installations, let the system generate a uid for new users by specifying UID(*GEN). However, if your system is part of a network, you may need to assign uids to match those assigned on other systems in the network. Consult your network administrator.

Group identification number

The integrated file system uses the group identification number (gid) to identify this profile as a group profile. A profile that is used as a group profile must have a gid.

Add User prompt:

Not shown

CL parameter:

GID

Length:

10,0

Table 104. Possible values for GID:

<u>*NONE</u>	This profile does not have a gid. This value must be specified if the user profile is a member of a group (GRPPRF is not *NONE).
<u>*GEN</u>	The system generates a unique gid for this profile. The generated gid will be greater than 100.
<i>gid</i>	A value from 1 to 4294967294 to be assigned as the gid for this profile. The gid must not be already assigned to another profile.

Recommendations: For most installations, let the system generate a gid for new group profiles by specifying GID(*GEN). However, if your system is part of a network, you might need to assign gids to match those assigned on other systems in the network. Consult your network administrator.

Do not assign a gid to a user profile that you do not plan to use as a group profile. In some environments, a user who is signed on and has a gid is restricted from performing certain functions.

Home directory

The home directory is the user's initial working directory for the integrated file system. The home directory is the user's current directory if a different current directory has not been specified.

Add User prompt:

Not shown

CL parameter:

HOMEDIR

If the home directory specified in the profile does not exist when the user signs on, the user's home directory is the "root" (/) directory.

Table 105. Possible values for HOMEDIR:

<u>*USRPRF</u>	The home directory assigned to the user is /home/xxxxx, where xxxxx is the user's profile name.
----------------	---

Table 105. Possible values for HOMEDIR: (continued)

<i>home-directory</i>	The name of the home directory to assign to this user.
-----------------------	--

EIM association

The EIM association specifies whether an Enterprise Identity Mapping (EIM) association should be added to an EIM identifier for this user. Optionally, the EIM identifier can also be created if it does not already exist.

Add User prompt:

Not shown

CL parameter:

EIMASSOC

Notes:

1. The EIM association information is not stored in the user profile. This information is not saved or restored with the user profile.
2. If this system is not configured for EIM, then no processing is done. Not being able to perform EIM operations does not cause the command to fail.

Table 106. Possible values for EIMASSOC, single values:

Single values	
*NOCHG	EIM association will not be added.

Table 107. Possible values for EIMASSOC, element 1:

Element 1: EIM identifier	
Specifies the EIM identifier for this association.	
*USRPRF	The name of the EIM identifier is the same name as the user profile.
<i>character-value</i>	Specifies the name of the EIM identifier.

Table 108. Possible values for EIMASSOC, element 2:

Element 2: Association type	
Specifies the type of association. It is recommended that a target association is added for an IBM i user.	
Target associations are primarily used to secure existing data. They are found as the result of a mapping lookup operation (for example, <code>eimGetTargetFromSource()</code>), but cannot be used as the source identity for a mapping lookup operation.	
Source associations are primarily used for authentication purposes. They can be used as the source identity of a mapping lookup operation, but will not be found as the target of a mapping lookup operation.	
Administrative associations are used to show that an identity is associated with an EIM identifier, but cannot be used as the source for, and will not be found as the target of, a mapping lookup operation.	
*TARGET	Process a target association.
*SOURCE	Process a source association.
*TGTSRC	Process both a target and a source association.
*ADMIN	Process an administrative association.
*ALL	Process all association types.

Table 109. Possible values for EIMASSOC, element 3:

Element 3: Association action	
*REPLACE	Associations of the specified type will be removed from all EIM identifiers that have an association for this user profile and local EIM registry. A new association will be added to the specified EIM identifier.
*ADD	Add an association.
*REMOVE	Remove an association.

Table 110. Possible values for EIMASSOC, element 4:

Element 4: Create EIM identifier	
Specifies whether the EIM identifier should be created if it does not already exist.	
*NOCRTEIMID	EIM identifier does not get created.
*CRTEIMID	EIM identifier gets created if it does not exist.

User expiration date

The User expiration date can be used to specify the date at which the user profile is automatically disabled.

Add User prompt:

Not shown

CL parameter:

USREXPDATE

Length:

6

The User expiration date field allows a security administrator to indicate that the user profile will expire on a specific date. If User expiration interval is used, this date is calculated by the system.

Table 111. Possible values for USREXPDATE:

*NONE	The user profile does not have an expiration date.
*USREXPITV	The user expiration date is to be calculated using the value specified in the User expiration interval (USREXPITV) parameter.
<i>user-expiration-date</i>	Specifies the date when the user profile expires. The date must be specified in the job date format.

User expiration interval

The User expiration interval controls the number of days before the user profile is automatically disabled.

Add User prompt:

Not shown

CL parameter:

USREXPITV

Length:

5,0

The User expiration interval field allows a security administrator to indicate in the user profile the number of days before the user profile will expire and be automatically disabled. If a value is specified

for User expiration interval when a user profile is created or when an expired user profile is re-enabled, the User expiration date is generated by the system using the expiration interval.

Table 112. Possible values for USREXPITV:

<i>user-expiration-interval</i>	Specify a number from 1 through 366.
---------------------------------	--------------------------------------

Authority

The Authority field specifies the public authority to the user profile.

Add User prompt:

Not shown

CL parameter:

AUT

The authority to a profile controls many functions associated with the profile, such as:

- Changing the profile
- Displaying the profile
- Deleting the profile
- Submitting a job using the profile
- Specifying the profile in a job description
- Transferring object ownership to the profile
- Adding members, if the profile is a group profile

Table 113. Possible values for AUT:

*EXCLUDE	The public is specifically denied access to the user profile.
*ALL	The public is given all management and data authorities to the user profile.
*CHANGE	The public is given the authority to change the user profile.
*USE	The public is given authority to view the user profile.

See “Defining how information can be accessed” on page 132 for a complete explanation of the authorities that can be granted.

Recommendations: To prevent misuse of user profiles that have authority to critical objects, make sure the public authority to the profiles is *EXCLUDE. Possible misuses of a profile include submitting a job that runs under that user profile or changing a program to adopt the authority of that user profile.

Object auditing

The object auditing value for a user profile works with the object auditing value for an object to determine whether the user’s access of an object is audited.

Add User prompt:

Not shown

CL parameter:

OBJAUD

Length:

10

Object auditing for a user profile cannot be specified on any user profile commands. Use the CHGUSRAUD command to specify object auditing for a user. Only a user with *AUDIT special authority can use the CHGUSRAUD command.

Table 114. Possible values for OBJAUD:

*NONE	The OBJAUD value for objects determines whether object auditing is done for this user.
*ALL	If the OBJAUD value for an object specifies *USRPRF, an audit record is written when this user changes or reads the object.
*CHANGE	If the OBJAUD value for an object specifies *USRPRF, an audit record is written when this user changes the object.
*NOTAVL	This value is displayed to indicate that the parameter value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The parameter value cannot be set to this value.

Table 115 shows how the OBJAUD values for the user and the object work together:

Table 115. Auditing performed for object access

OBJAUD value for object	OBJAUD value for user		
	*NONE	*CHANGE	*ALL
*ALL	Change and Use	Change and Use	Change and Use
*CHANGE	Change	Change	Change
*NONE	None	None	None
*USRPRF	None	Change	Change and Use

Related tasks:

“Planning the auditing of object access” on page 286

The i5/OS operating system provides the ability to log accesses to an object in the security audit journal by using system values and the object auditing values for users and objects. This is called *object auditing*.

Action auditing

For an individual user, you can specify which security-relevant actions should be recorded in the audit journal. The actions specified for an individual user apply in addition to the actions specified for all users by the QAUDLVL and QAUDLVL2 system values.

Add User prompt:

Not shown

CL parameter:

AUDLVL

Length:

640

Action auditing for a user profile cannot be specified on any user profile displays. It is defined using the CHGUSRAUD command. Only a user with *AUDIT special authority can use the CHGUSRAUD command.

Table 116. Possible values for AUDLVL:

*NONE	The QAUDLVL system value controls action auditing for this user. No additional auditing is done.
*NOTAVL	This value is displayed to indicate that the parameter value is not available to the user because the user does not have either *AUDIT or *ALLOBJ special authority. The parameter value cannot be set to this value.
*AUTFAIL	Authorization failures are audited.

Table 116. Possible values for AUDLVL: (continued)

*CMD	Command strings are logged. *CMD can be specified only for individual users. Command string auditing is not available as a system-wide option using the QAUDLVL system value.
*CREATE	Object create operations are logged.
*DELETE	Object delete operations are logged.
*JOBBAS	Job base functions are audited.
*JOBCHGUSR	Changes to a thread's active user profile or its group profiles are audited.
*JOBDTA ¹	Job changes are logged.
*OBJMGT	Object move and rename operations are logged.
*OFCSRVR	Changes to the system distribution directory and office mail actions are logged.
*NETBAS	Network base functions are audited.
*NETCLU	Cluster or cluster resource group operations are audited.
*NETCMN ³	Networking and communications functions are audited.
*NETFAIL	Network failures are audited.
*NETSCK	Sockets tasks are audited.
*OPTICAL	All optical functions are audited.
*PGMADP	Obtaining authority to an object through a program that adopts authority is logged.
*PGMFAIL	Program failures are audited.
*PRDTA	Printing functions with parameter SPOOL(*NO) are audited.
*SAVRST	Save and restore operations are logged.
*SECCFG	Security configuration is audited.
*SECDIRSRV	Changes or updates when doing directory service functions are audited.
*SECIPC	Changes to interprocess communications are audited.
*SECNAS	Network authentication service actions are audited.
*SECRUN	Security run time functions are audited.
*SECSCKD	Socket descriptors are audited.
*SECURITY ²	Security-related functions are logged.
*SECVFY	Use of verification functions are audited.
*SECVLDL	Changes to validation list objects are audited.
*SERVICE	Using service tools is logged.
*SPLFDTA	Actions performed on spooled files are logged.
*SYSMGT	Use of systems management functions is logged.

Table 116. Possible values for AUDLVL: (continued)

1	<p>*JOBDDTA includes two values that are *JOBDBAS and *JOBCHGUSR, which enable you to better customize your auditing. If both of the values are specified, you will get the same auditing as if just *JOBDDTA is specified.</p>
2	<p>*SECURITY is composed of several values to enable you to better customize your auditing. If all of the values are specified, you will get the same auditing as if just *SECURITY is specified. These values are as follows.</p> <ul style="list-style-type: none">• *SECCFG• *SEC_DIRSRV• *SECIPC• *SECNAS• *SECRUN• *SECSCKD• *SECVFY• *SECVLDL
3	<p>*NETCMN is composed of several values to enable you to better customize your auditing. If all of the values are specified, you will get the same auditing as if just *NETCMN is specified. These values are as follows.</p> <ul style="list-style-type: none">• *NETBAS• *NETCLU• *NETFAIL• *NETSCK

Related reference:

“Planning the auditing of actions” on page 263

The QAUDCTL (audit control) system value, the QAUDLVL (audit level) system value, the QAUDLVL2 (audit level extension) system value, and the AUDLVL (action auditing) parameter in user profiles work together to control action auditing.

Additional information associated with a user profile

This topic discusses the private authorities, owned object information, and primary group object information that are associated with a user profile.

Related reference:

“How security information is stored” on page 246

Planning adequate backup and recovery procedures for security information requires understanding how the information is stored and saved.

Private authorities

All of the private authorities that a user has to objects are stored with the user profile. When a user needs authority to an object, the user’s private authorities might be searched.

“Flowchart 3: How user authority to an object is checked” on page 174 provides more information about authority checking.

You can display a user’s private authorities to library-based objects by using the Display User Profile command:

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

You can work with a user's private authorities to library- and directory-based objects using the Work with Objects by Private Authority (WRKOBJPVT) command. To change a user's private authorities, you can use the commands that work with object authorities, such as Edit Object Authority (EDTOBJAUT).

You can copy all of the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command. See "Copying authority from a user" on page 165 for more information.

Primary group authorities

The names of all of the objects for which the profile is the primary group are stored with the group profile.

You can display the library-based objects for which the profile is the primary group using the DSPUSRPRF command:

```
DSPUSRPRF group-profile-name TYPE(*OBJPGP)
```

You can also use the Work with Objects by Primary Group (WRKOBJPGP) command.

Owned object information

Because the size of a user profile can affect your performance, it is suggested that you do not assign all (or nearly all) objects to only one owning profile.

Private authority information for an object is stored with the user profile that owns the object. This information is used to build system displays that work with object authority. If a profile owns a large number of objects that have many private authorities, the performance of building object authority displays for these objects can be affected. The size of an owner profile affects performance when displaying and working with the authority to owned objects, and when saving or restoring profiles. System operations can also be impacted. To prevent impacts to either performance or system operations, distribute ownership of objects to multiple profiles.

Digital ID authentication

The digital certificates allow users to secure communications and ensure message integrity. The System i security infrastructure allows x.509 digital certificates to be used for identification.

The digital ID APIs create, distribute, and manage digital certificates associated with user profiles. See Digital certificate management APIs for details about the following APIs:

- Add User Certificate (QSYADDUC)
- Remove User Certificate (QSYRMVUC)
- List User Certificate (QSYLSTUC)
- Find Certificate User (QSYFNDUC)
- Add Validation List Certificate (QSYADDVC)
- Remove Validation List Certificate (QSYRMVVC)
- List Validation List Certificate (QSYLSTVC)
- Check Validation List Certificate (QSYCHKVC)
- Parse Certificate (QSYPARSC)

Working with user profiles

This topic describes the commands and displays you use to create, change, and delete user profiles on the IBM i operating system.

You must have *SECADM special authority to create, change, or delete user profiles.

Creating user profiles

You can create a user profile by using the Work with User Profiles (WRKUSRPRF) list display, using the Create User Profile (CRTUSRPRF) command, using the Work with User Enrollment option from the SETUP menu or using System i Navigator .

The user who creates the user profile owns it and is given *ALL authority to it. The user profile is given *OBJMGT and *CHANGE authority to itself. These authorities are necessary for normal operations and should not be removed.

A user profile cannot be created with more authorities or capabilities than those of the user who creates the profile.

Note: You cannot use the Create User Profile(CRTUSRPRF) command to create a user profile 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.

Using the Work with User Profiles command

You can enter a specific profile name, a generic profile set, or *ALL on the Work with User Profiles (WRKUSRPRF) command.

The assistance level determines which list display you see. When you use the WRKUSRPRF command with *BASIC assistance level, you will access the Work with User Enrollment display. If *INTERMED assistance level is specified, you will access the Work with User Profiles display.

You can specify the ASTLVL (assistance level) parameter on the command. If you do not specify ASTLVL, the system uses the assistance level stored with your user profile.

On the Work with User Profiles display, type 1 and the name of the profile you want to create:

```
Work with User Profiles

Type options, press Enter.
1=Create  2=Change  3=Copy  4=Delete  5=Display
12=Work with objects by owner

      User
Opt  Profile      Text
1   NEWUSER
—   DPTSM         Sales and Marketing Departme
—   DPTWH         Warehouse Department
```

You see the Create User Profile display:

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile	NEWUSER	Name
User password	*NONE	Character value, *USRPRF...
Set password to expired	*YES	*NO, *YES
Status	*ENABLED	*ENABLED, *DISABLED
User class	*USER	*USER, *SYSOPR, *PGMR...
Assistance level	*SYSVAL	*SYSVAL, *BASIC, *INTERMED...
Current library	*CRTDFT	Name, *CRTDFT
Initial program to call	*NONE	Name, *NONE
Library		Name, *LIBL, *CURLIB
Initial menu	MAIN	Name, *SIGNOFF
Library	QSYS	Name, *LIBL, *CURLIB
Limit capabilities	*NO	*NO, *PARTIAL, *YES
Text 'description'	*BLANK	

The Create User Profile display shows all of the fields in the user profile. Use F10 (Additional parameters) and page down to enter more information. Use F11 (Display keywords) to see the parameter names.

The Create User Profile display does not add the user to the system directory.

Using the Create User Profile command

You can use the (Create User Profile) CRTUSRPRF command to create a user profile. You can enter parameters with the command, or you can request prompting (F4) and see the Create User Profile display.

Using the Work with User Enrollment option

You can use the Work with User Enrollment option to add users to the system.

Select the Work with User Enrollment option from the SETUP menu. The assistance level stored with your user profile determines whether you see the Work with User Profiles display or the Work with User Enrollment display. You can use F21 (Select assistance level) to change levels.

On the Work with User Enrollment display, use option 1 (Add) to add a new user to the system.

Work with User Enrollment

Type options below, then press Enter.

1=Add 2=Change 3=Copy 4=Remove 5=Display

Opt	User	Description
1	NEWUSER	
-	DPTSM	Sales and Marketing Departme
-	DPTWH	Warehouse Department

You see the Add User display:

```

                                Add User

Type choices below, then press Enter.

User . . . . . NEWUSER      Name
User description . . . . .
Password . . . . . NEWUSER
Type of user . . . . . *USER      Type, F4 for list
User group . . . . . *NONE      Name, F4 for list

Restrict command line use  N      Y=Yes, N=No

Default library . . . . .      Name
Default printer . . . . . *WRKSTN  Name, *WRKSTN, F4 for list
Sign on program . . . . . *NONE    Name, *NONE
  Library . . . . .      Name

First menu . . . . .      Name
  Library . . . . .      Name

F1=Help  F3=Exit  F5=Refresh  F12=Cancel

```

The Add User display is designed for a security administrator without a technical background. It does not show all of the fields in the user profile. Default values are used for all fields that are not shown.

Note: If you use the Add User display, you are limited to eight-character user profile names.

Page down to see the second display:

```

                                Add User

Type choices below, then press Enter.

Attention key program . . *SYSVAL
  Library . . . . .

```

The Add user display automatically adds an entry in the system directory with the same user ID as the user profile name (the first eight characters) and an address of the system name.

Copying user profiles

You can create a user profile by copying another user profile or a group profile.

You might want to set up one profile in a group as a pattern. Copy the first profile in the group to create additional profiles.

You can copy a profile interactively from either the Work with User Enrollment display or the Work with User Profiles display. No command exists to copy a user profile.

Related concepts:

“Group profiles” on page 4

A *group profile* is a special type of user profile. Rather than giving authority to each user individually, you can use a group profile to define authority for a group of users.

Copying from the Work with User Profiles display

You can copy the information of a user profile from the Work with User Profiles display.

On the Work with User Profiles display, type 3 in front of the profile you want to copy. You see the Create User Profile display:

```

                                Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . .
User password . . . . . > *USRPRF      Name
Set password to expired . . . . . > *NO      *NO, *YES
Status . . . . . > *ENABLED      *ENABLED,
User class . . . . . > *USER      *USER,
Assistance level . . . . . > *SYSVAL      *SYSVAL,
Current library . . . . . > DPTWH      Name,
Initial program to call . . . . . > *NONE      Name,
Library . . . . .
Initial menu . . . . . > ICMAIN      Name,
Library . . . . . > ICPGMLIB      Name,
Limit capabilities . . . . . > *NO      *NO,
Text 'description' . . . . . > 'Warehouse Department '

```

All of the values from the copy-from user profile are shown on the Create User Profile display, except the following fields:

User profile

Blank. Must be filled in.

Password

CRTUSRPRF command default

Document password

*NONE

Message queue

*USRPRF

Locale job attributes

*SYSVAL

Locale

*SYSVAL

User Identification Number

*GEN

Group Identification Number

*NONE

Home directory

*USRPRF

EIM Association

*NOCHG

Authority

*EXCLUDE

You can change any fields on the Create User Profile display. Private authorities of the copy-from profile are not copied. In addition, internal objects containing user preferences and other information about the user are not copied.

Copying from the Work with User Enrollment display

You can also copy user profiles from the Work with User Enrollment display.

On the Work with User Enrollment display, type 3 in front of the profile you want to copy. You see the Copy User display:

```
Copy User
Copy from user . . . . . : DPTWH
Type choices below, then press Enter.
User . . . . .
User description . . . . : Warehouse Department
Password . . . . .
Type of user . . . . . : USER
User group . . . . .
Restrict command line use : N
Default library . . . . . : DPTWH
Default printer . . . . . : PRT04
Sign on program . . . . . : *NONE
Library . . . . .
```

All of values from the copy-from profile appear on the Add User display, except the following values:

User Blank. Must be filled in. Limited to 8 characters.

Password

Blank. If you do not enter a value, the profile is created with the password equal to the default value specified for the PASSWORD parameter of the CRTUSRPRF command.

You can change any fields on the Copy User display. User profile fields that do not appear on the basic assistance level version are still copied from the copy-from profile, with the following exceptions:

Message queue

*USRPRF

Document password

*NONE

User Identification Number

*GEN

Group Identification Number

*NONE

EIM Association

*NOCHG

Authority

*EXCLUDE

Private authorities of the copy-from profile are not copied.

Copying private authorities

You can copy the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command.

This should not be used in place of group profiles or authorization lists. Copying authorities does not help you manage similar authorities in the future, and it can cause performance problems on your system.

Related concepts:

“Copying authority from a user” on page 165

You can copy all the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command.

Changing user profiles

You can change a user profile using option 2 (Change) from either the Work with User Profiles display or the Work with User Enrollment display. You can also use the Change User Profile (**CHGUSRPRF**) command.

Users who are allowed to enter commands can change some parameters of their own profiles using the Change Profile (**CHGPRF**) command.

A user cannot change a user profile to have more special authorities or capabilities than the user who changes the profile.

Deleting user profiles

You cannot delete a user profile that owns objects. Before you can delete such user profiles, you must delete any objects owned by the profile or transfer ownership of those objects to another profile.

You cannot delete a user profile if it is the primary group for any objects. When you use the intermediate assistance level to delete a user profile, you can change or remove the primary group for objects. You can use the WRKOBJPGP command to list any objects for which a profile is the primary group.

When you delete a user profile, the user is removed from all distribution lists and from the system directory.

You do not need to change ownership of or delete the user’s message queue. The system automatically deletes the message queue when the profile is deleted.

You cannot delete a group profile that has members. To list the members of a group profile, type `DSPUSRPRF group-profile-name *GRPMBR`. Change the GRPPRF or SUPGRPPRF field in each member profile before deleting the group profile.

Using the Delete User Profile command

To delete a user profile, you can enter the Delete User Profile (DLTUSRPRF) command directly, or you can use option 4 (Delete) from the Work with User Profiles display.

The DLTUSRPRF command has parameters allowing you to handle:

- All objects owned by the profile
- All objects for which the profile is the primary group
- EIM associations

```

Delete User Profile (DLTUSRPRF)

Type choices, press Enter.

User profile . . . . . > HOGANR      Name
Owned object option:
Owned object value . . . . . *CHGOWN  *NODLT, *DLT, *CHGOWN
User profile name if *CHGOWN  WILLISR  Name
Primary group option:
Primary group value . . . . . *NOCHG  *NOCHG, *PGP
New primary group . . . . .
New primary group authority .
EIM association . . . . . *DLT      *DLT, *NODLT

```

You can delete all the owned objects or transfer them to a new owner. If you want to handle owned objects individually, you can use the Work with Objects by Owner (WRKOBJOWN) command. You can change the primary group for all objects for which the group profile is the primary group. If you want to handle objects individually, you can use the Work with Objects by Primary Group (WRKOBJPGP) command. The displays for both commands are similar:

```

Work with Objects by Owner

User profile . . . . . : HOGANR

Type options, press Enter.
2=Edit authority      4=Delete  5=Display author
8=Display description 9=Change owner

Opt Object      Library      Type      Attribute      ASP
 4 HOGANR      QUSRSYS     *MSGQ     *SYSBAS
 9 QUERY1      DPTWH       *PGM      *SYSBAS
 9 QUERY2      DPTWH       *PGM      *SYSBAS

```

Using the Remove User option

You can use the Remove User option on the Work with User Enrollment display to delete a user profile. From the Work with User Enrollment display, type 4 (Remove) in front of the profile you want to delete. You see the Remove User display:

```

Remove User

User . . . . . : HOGANR
User description . . . . . : Sales and Marketing Department

To remove this user type a choice below, then press Enter.

1. Give all objects owned by this user to a new owner
2. Delete or change owner of specific objects owned by this user.

```

To change the ownership of all objects before deleting the profile, select option 1. You see a display prompting you for the new owner.

To handle the objects individually, select option 2. You see a detailed Remove User display:

```

                                Remove User
User . . . . . : HOGANR
User description . . . . . : Hogan, Richard - Warehouse DPT

New owner . . . . . Name, F4 for list

To remove this user, delete or change owner of all objects.
Type options below and press Enter.
  2=Change to new owner  4=Delete  5=Display details

Opt Object      Library      Description
  4 HOGANR      QUSRSYS     HOGANR message queue
  2 QUERY1     DPTWH       Inventory Query, on-hand report
  2 QUERY2     DPTWH       Inventory Query, on-order report

```

Use the options on the display to delete objects or transfer them to a new owner. When all objects have been removed from the display, you can delete the profile.

Notes:

1. You can use F13 to delete all the objects owned by the user profile.
2. Spooled files do not appear on the Work with Objects by Owner display. You can delete a user profile even though that profile still owns spooled files. After you have deleted a user profile, use the Work with Spooled Files (WRKSPLF) command to locate and delete any spooled files owned by the user profile, if they are no longer needed.
3. Any objects for which the deleted user profile was the primary group will have a primary group of *NONE.

Working with Objects by Private Authorities

You can use the Work with Objects by Private Authorities (WRKOBJPVT) command to display and work with objects for which a profile has private authority.

Working with Objects by Primary Group

You can use the Work with Objects by Primary Group (WRKOBJPGP) command to display and work with objects for which a profile is the primary group.

You can use this display to change an object's primary group to another profile or to set its primary group to *NONE.

```

                                Work with Objects by Primary Group
Primary group . . . . . : DPTAR

Type options, press Enter.
  2=Edit authority      4=Delete  5=Display authority
  8=Display description 9=Change primary group

Opt Object      Library      Type  Attribute  Device
  CUSTMAST  CUSTLIB     *FILE *SYSBAS
  CUSTWRK   CUSTLIB     *FILE *SYSBAS
  CUSTLIB   QSYS        *LIB  *SYSBAS

```

Enabling a user profile

If the QMAXSIGN and QMAXSGNACN system values on your system are set up to disable a user profile after too many password verification attempts, you might need to enable the profile by changing the profile status to *ENABLED.

To enable a user profile, you must have *SECADM special authority, *OBJMGT authority, and *USE authority to the user profile. Normally, a system operator does not have *SECADM special authority. A solution is to use a simple program which adopts authority:

1. Create a CL program owned by a user who has *SECADM special authority, *OBJMGT authority, and *USE authority to the user profiles on the system. Adopt the authority of the owner when the program is created by specifying USRPRF(*OWNER).
2. Use the **EDTOBJAUT** command to make the public authority to the program *EXCLUDE and give the system operators *USE authority.
3. The operator enables the profile by entering `CALL ENABLEPGM profile-name`.
4. The main part of the ENABLEPGM program looks like this:

```
PGM &PROFILE
DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
ENDPGM
```

Listing user profiles

You can display and print information about user profiles in a variety of formats.

Displaying an individual profile

To display the values for an individual user profile, use option 5 (Display) from either the Work with User Enrollment display or the Work with User Profiles display. Or, you can use the Display User Profile (DSPUSRPRF) command.

Listing all profiles

You can use the Display Authorized Users (DSPAUTUSR) command to either print or display all the user profiles on the system.

The sequence (SEQ) parameter on the command allows you to sort the list either by profile name or by group profile.

Display Authorized Users				
Group Profile	User Profile	Password		Text
		Last Changed	No Password	
DPTSM	ANDERSR	08/04/0x		Anders, Roger
	VINCENT	09/15/0x		Vincent, Mark
DPTWH	ANDERSR	08/04/0x		Anders, Roger
	HOGANR	09/06/0x		Hogan, Richard
	QUINN	09/06/0x		Quinn, Rose
QSECOFR	JONESS	09/20/0x		Jones, Sharon
	HARRISON	08/29/0x		Harrison, Ken
*NO GROUP	DPTSM	09/05/0x	X	Sales and Marketing
	DPTWH	09/18/0x	X	Warehouse

By pressing F11, you are able to see which user profiles have passwords defined for use at the various password levels.

Display Authorized Users						
User Profile	Group Profile	Password Last Changed	Level 0 or 1 Password	Level 2 or 3 Password	Netserver Password	Local Pwd Mgt
ANGELA		04/21/0x	*YES	*NO	*YES	*YES
ARTHUR		07/07/0x	*YES	*YES	*YES	*YES
CAROL1		05/15/0x	*YES	*YES	*YES	*YES
CAROL2		05/15/0x	*NO	*NO	*NO	*NO
CHUCKE		05/18/0x	*YES	*NO	*YES	*YES
DENNISS		04/20/0x	*YES	*NO	*YES	*YES
DPORTER		03/30/0x	*YES	*NO	*YES	*YES
GARRY		08/04/0x	*YES	*YES	*YES	*YES
JANNY		03/16/0x	*YES	*NO	*YES	*YES

Types of user profile displays

The Display User Profile (DSPUSRPRF) command provides several types of displays and listings.

- Some displays and listings are available only for individual profiles. Others can be printed for all profiles or a generic set of profiles.
- You can create an output file from some displays by specifying output (*OUTFILE). Use a query tool or program to produce customized reports from the output file. “Analyzing user profiles” on page 301 gives suggestions for reports.

Types of user profile reports

You can generate user profile reports by using the Print User Profile (PRTUSRPRF) command or the Analyze Default Password (ANZDFTPWD) command.

- Print User Profile (PRTUSRPRF)

This command generates reports that contain information about the user profiles on the system. Four different variations of this report can be printed. One contains authority type information, one contains environment type information, one contains password type information, and one contains password level type information.

- Analyze Default Password (ANZDFTPWD)

This command generates a report about all of the user profiles on the system that have a default password and allows you to take an action against the profiles. A profile has a default password when the user profile name matches the profile's password.

User profiles on the system that have a default password can be disabled and their passwords can be set to expired.

Renaming a user profile

The system does not provide a direct method for renaming a user profile. A new profile can be created with the same authorities for a user with a new name.

Some information, however, cannot be transferred to the new profile. The following are examples of information that cannot be transferred:

- Spool files.
- Internal objects containing user preferences and other information about the user will be lost.
- Digital certificates that contain the user name will be invalidated.
- The uid and gid information retained by the integrated file system cannot be changed.
- You might not be able to change the information that is stored by applications that contain the user name.

Applications that are run by the user can have application profiles. Creating a new IBM i user profile to rename a user does not rename any application profiles the user might have. A Lotus® Notes® profile is one example of an application profile.

The following example shows how to create a new profile for a user with a new name and the same authorities. The old profile name is SMITHM, while the new user profile name is JONESM:

1. Copy the old profile (SMITHM) to a new profile (JONESM) using the copy option from the Work with User Enrollment display.

2. Give JONESM all the private authorities of SMITHM using the Grant User Authority (**GRTUSRAUT**) command:

```
GRTUSRAUT JONESM REFUSER(SMITHM)
```

3. Change the primary group of all objects that SMITHM is the primary group of using the Work with Objects by Primary Group (**WRKOBJPGP**) command:

```
WRKOBJPGP PGP(SMITHM)
```

Enter option 9 on all objects that need their primary group changed and enter NEWPGP (JONESM) on the command line.

Note: JONESM must have a gid assigned using the GID parameter on the Create or Change User Profile (**CRTUSRPRF** or **CHGUSRPRF**) command.

4. Display the SMITHM user profile using the Display User Profile (**DSPUSRPRF**) command:

```
DSPUSRPRF USRPRF(SMITHM)
```

Write down the uid and gid for SMITHM.

5. Transfer ownership of all other owned objects to JONESM and remove the SMITHM user profile, using option 4 (Remove) from the Work with User Enrollment display.
6. Change the uid and the gid of JONESM to the uid and gid that belonged to SMITHM by using the Change User Profile (**CHGUSRPRF**) command:

```
CHGUSRPRF USRPRF(JONESM) UID(uid from SMITHM)
GID(gid from SMITHM)
```

If JONESM owns objects in a directory, the **CHGUSRPRF** command cannot be used to change the uid and gid. Use the QSYCHGID API to change the uid and gid of user profile JONESM.

Working with user auditing

You can use the Change User Auditing (CHGUSRAUD) command to set the audit characteristics for users.

To use this command, you must have *AUDIT special authority.

Change User Audit (CHGUSRAUD)

Type choices, press Enter.

User profile	HOGANR
+ for more values	JONESM
Object auditing value	*SAME
User action auditing	*CMD
+ for more values	*SERVICE

You can specify the auditing characteristics for more than one user at a time by listing user profile names.

The AUDLVL (user action auditing) parameter can have more than one value. The values that you specify are not added to the current AUDLVL values for the users but rather they replace the current AUDLVL values.

If you have either *ALLOBJ or *AUDIT special authority, you can use the Display User Profile (DSPUSRPRF) command to see audit characteristics for a user.

Working with profiles in CL programs

You can work with user profiles within a CL program.

You may want to retrieve information about the user profile from within a CL program. You can use the Retrieve User Profile (RTVUSRPRF) command in your CL program. The command returns the requested attributes of the profile to variables you associate with the user profile field names. The descriptions of user profile fields in this section show the field lengths expected by the RTVUSRPRF command. In some cases, a decimal field can also have a value that is not numeric. For example, the maximum storage field (MAXSTG) is defined as a decimal field, but it can have a value of *NOMAX. Online information for the RVTUSRPRF command describes the values that are returned in a decimal field for values that are not numeric.

The sample program in “Using a password approval program” on page 61 shows an example of using the RTVUSRPRF command.

You may also want to use the CRTUSRPRF or CHGUSRPRF command within a CL program. If you use variables for the parameters of these commands, define the variables as character fields to match the Create User Profile prompt display. The variable sizes do not need to match the field sizes.

You cannot retrieve a user’s password, because the password is stored with one-way encryption. If you want the user to enter the password again before accessing critical information, you can use the Check Password (CHKPWD) command in your program. The system compares the password entered to the user’s password and sends an escape message to your program if the password is not correct.

User profile exit points

You can write your own exit programs to perform specific user profile functions. When you register your exit programs with any of the user profile exit points, you are notified when a user profile is created, changed, deleted, or restored.

At the time of notification, your exit program can perform any of the following operations:

- Retrieve information about the user profile.
- Enroll the user profile that was just created in the system directory.
- Create necessary objects for the user profile.

Note: All adopted authority will be suppressed before the exit programs are called. This means that the exit program may not have authority to access the user profile object.

Related information:

Exit programs

IBM-supplied user profiles

A number of user profiles are shipped with your system software. These IBM-supplied user profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

To allow you to install your system the first time, the password for the security officer (QSECOFR) profile is the same for every system that is shipped. However, the password for QSECOFR is shipped as expired. For new systems, you are required to change the password the first time you sign on as QSECOFR.

When you install a new release of the operating system, passwords for IBM-supplied profiles are not changed. If profiles such as QPGMR and QSYSOPR have passwords, those passwords are not set to *NONE automatically.

Appendix B, "IBM-supplied user profiles," on page 319 contains a complete list of all the IBM-supplied user profiles and the field values for each profile.

Note: All IBM-supplied user profiles except for QSECOFR are shipped with a password of *NONE and are not intended for sign-on. These profiles are used by the IBM i operating system. Therefore, signing on with these profiles or using the profiles to own user (non-IBM supplied) objects is not recommended.

Related concepts:

"IBM-supplied user profiles" on page 258

You can perform auditing tasks on IBM-supplied user profiles by verifying their passwords.

Changing passwords for IBM-supplied user profiles

If you need to sign on with one of the IBM-supplied profiles, you can change the password using the **CHGUSRPRF** command. You can also change these passwords using an option from the SETUP menu.

To protect your system, you should leave the password set to *NONE for all IBM-supplied profiles except QSECOFR. Do not allow trivial passwords for the QSECOFR profile.

```
Change Passwords for IBM-Supplied

Type new password below for IBM-supplied user,
type password again to verify change, then
press Enter.

New security officer (QSECOFR) password . . . . .
New password (to verify) . . . . .

New system operator (QSYSOPR) password . . . . .
New password (to verify) . . . . .

New programmer (QPGMR) password . . . . .
New password (to verify) . . . . .

New user (QUSER) password . . . . .
New password (to verify) . . . . .

New service (QSRV) password . . . . .
New password (to verify) . . . . .
```

Page down to change additional passwords:

```
Change Passwords for IBM-Supplied

Type new password below for IBM-supplied user, type
change, then press Enter.

New basic service (QSRVBAS) password . . . . .
New password (to verify) . . . . .
```

Working with service tools user IDs

There are several enhancements and additions to service tools that make them easier to use and understand.

- **System service tools (SST)**

You can now manage and create service tools user IDs from system service tools (SST) by selecting option 8 (Work with service tools user IDs) from the main SST display. You no longer need to go into dedicated service tools (DST) to reset passwords, grant or revoke privileges, or create service tools user IDs. **Note:** Information regarding Service tools has been moved to the information center.

- **Password management enhancements**

The server is shipped with limited ability to change default and expired passwords. This means that you cannot change service tools user IDs that have default and expired passwords through the Change Service Tools User ID (QSYCHGDS) API, nor can you change their passwords through SST. You can only change a service tools user ID with a default and expired password through DST. And, you can change the setting to allow default and expired passwords to be changed. Also, you can use the new Start service tools (STRSST) privilege to create a service tools user ID that can access DST, but can be restricted from accessing SST.

- **Terminology changes**

The textual data and other documentation have been changed to reflect the new service tools terminology. Specifically, the term service tools user IDs replaces previous terms, such as DST user profiles, DST user IDs, service tools user profiles, or variations of these names.

Related concepts:

“IBM-supplied user profiles” on page 258

You can perform auditing tasks on IBM-supplied user profiles by verifying their passwords.

Related information:

Managing service tools user IDs

System password

The system password is used to authorize system model changes, certain service conditions, and ownership changes. If these changes have occurred on your system, you may be prompted for the system password when you perform an IPL.

Chapter 5. Resource security

This section describes each of the components of resource security and how they work together to protect information about your system. It also explains how to use CL commands and displays to set up resource security on your system.

Resource security defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects.

Chapter 7, “Designing security,” on page 219 discusses techniques for designing resource security, including how it affects both application design and system performance.

The topic “How the system checks authority” on page 169 provides detailed flowcharts and notes about how the system checks authority. You might find it useful to consult this information as you read the explanations that follow.

Related concepts:

“Resource security” on page 5

The ability to access an object is called *authority*. Resource security on the IBM i operating system enables you to control object authorities by defining who can use which objects and how those objects can be used.

“Overall recommendations for security design” on page 220

Keeping your security design as simple as possible makes it easier to manage and audit security. It also improves application performance and backup performance.

Defining who can access information

You can give authority to individual users, groups of users, and the public.

Note: In some environments, a user's authority is referred to as a **privilege**.

You define who can use an object in several ways:

Public authority:

The **public authority** consists of anyone who is authorized to sign on to your system. Public authority is defined for every object on the system, although the public authority for an object can be *EXCLUDE. Public authority to an object is used if no other specific authority is found for the object.

Private authority:

You can define specific authority to use (or not use) an object. You can grant authority to an individual user profile or to a group profile. An object has **private authority** if any authority other than public authority, object ownership, or primary group authority is defined for the object.

User authority:

Individual user profiles can be given authority to use objects on the system. This is one type of private authority.

Group authority:

Group profiles can be given authority to use objects on the system. A member of the group gets the group's authority unless an authority is specifically defined for that user. Group authority is also considered private authority.

Object ownership:

Every object on the system has an owner. The owner has *ALL authority to the object by default. However, the owner's authority to the object can be changed or removed. The owner's authority to the object is not considered private authority.

Primary group authority:

You can specify a primary group for an object and the authority the primary group has to the object. Primary group authority is stored with the object and can provide better performance than private authority granted to a group profile. Only a user profile with a group identification number (gid) can be the primary group for an object. Primary group authority is not considered private authority.

Defining how information can be accessed

You can define what operations can be preformed on objects, data, and fields.

Authority means the type of access allowed to an object. Different operations require different types of authority.

Note: In some environments, the authority associated with an object is called the object's **mode of access**.

Authority to an object is divided into three categories:

1. **Object authority** defines what operations can be performed on the object as a whole.
2. **Data authority** defines what operations can be performed on the contents of the object.
3. **Field authority** defines what operations can be performed on the data fields.

Table 117 describes the types of authority available and lists some examples of how the authorities are used. In most cases, accessing an object requires a combination of object, data, field authorities. Appendix D, "Authority required for objects used by commands," on page 339 provides information about the authority that is required to perform a specific function.

Table 117. Description of authority types

Authority	Name	Functions allowed
<i>Object Authorities:</i>		
*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.
*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 .

Table 117. Description of authority types (continued)

Authority	Name	Functions allowed
<i>Data Authorities:</i>		
*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.
<i>Field Authorities:</i>		
*MGT	Management	Specify the security for the field.
*ALTER	Alter	Change the attributes of the field.
*REF	Reference	Specify the field as part of the parent key in a referential constraint.
*READ	Read	Access the contents of the field. For example, display the contents of the field.
*ADD	Add	Add entries to data, such as adding information to a specific field.
*UPDATE	Update	Change the content of existing entries in the field.
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	See the topic "Authorization list management" on page 138 for more information.	

Related tasks:

"Changing to level 30 from a lower level" on page 13

When you change to security level 30 from a lower security level, the system changes all user profiles to update special authorities the next time you perform an initial program load (IPL).

Related reference:

"Group authority" on page 98

If the user profile is a member of a group and OWNER(*USRPRF) is specified, the Group authority field controls what authority is given to the group profile for any objects created by this user.

Commonly used authorities

You can specify certain sets of objects and data authorities.

Certain sets of object and data authorities are commonly required to perform operations on objects. You can specify these system-defined sets of authority (*ALL, *CHANGE, *USE) instead of individually defining the authorities needed for an object. *EXCLUDE authority is different than having no authority. *EXCLUDE authority specifically denies access to the object. Having no authority means you use the public authority defined for the object. Table 118 on page 134 shows the system-defined authorities available using the object authority commands and displays.

Table 118. System-defined authority

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

Table 119 shows additional system-defined authorities that are available using the WRKAUT and CHGAUT commands:

Table 119. System-defined authority

Authority	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Object Authorities</i>							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
<i>Data Authorities</i>							
*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

The LAN Server licensed program uses access control lists to manage authority. A user's authorities are called **permissions**. Table 120 shows how the LAN Server permissions map to object and data authorities:

Table 120. LAN server permissions

Authority	LAN server permissions
*EXCLUDE	None
<i>Object Authorities</i>	
*OBJOPR	See note 1
*OBJMGT	Permission
*OBJEXIST	Create, Delete
*OBJALTER	Attribute

Table 120. LAN server permissions (continued)

Authority	LAN server permissions
*OBJREF	No equivalent
<i>Data Authorities</i>	
*READ	Read
*ADD	Create
*UPD	Write
*DLT	Delete
*EXECUTE	Execute

¹ Unless NONE is specified for a user in the access control list, the user is implicitly given *OBJOPR.

Defining what information can be accessed

You can define resource security for individual objects on the system. You can also define security for groups of objects using either library security or an authorization list.

Library security

You can use library security to protect information.

Most objects on the system reside in libraries. To access an object, you need authority both to the object itself and the library in which the object resides. For most operations, including deleting an object, *USE authority to the object library is sufficient (in addition to the authority required for the object). Creating a new object requires *ADD authority to the object library. Appendix D, "Authority required for objects used by commands," on page 339 shows what authority is required by CL commands for objects and the object libraries.

Using library security is one technique for protecting information while maintaining a simple security scheme. For example, to secure confidential information for a set of applications, you can do the following actions:

- Use a library to store all confidential files for a particular group of applications.
- Ensure that public authority is sufficient for all objects (in the library) that are used by applications (*USE or *CHANGE).
- Restrict public authority to the library itself (*EXCLUDE).
- Give selected groups or individuals authority to the library (*USE, or *ADD if the applications require it).

Although library security is a simple, effective method for protecting information, it might not be adequate for data with high security requirements. Highly sensitive objects should be secured individually or with an authorization list, rather than relying on library security.

Related concepts:

"Planning libraries" on page 225

A library is like a directory used to locate the objects in the library. Many factors affect how you choose to group your application information into libraries and manage libraries.

Library security and library lists

When a library is added to a user's library list, the authority the user has to the library is stored with the library list information.

The user's authority to the library remains for the entire job, even if the user's authority to the library is revoked while the job is active.

When access to an object is requested and *LIBL is specified for the object, the library list information is used to check authority for the library. If a qualified name is specified, the authority for the library is specifically checked, even if the library is included in the user's library list.

Attention: If a user is running under adopted authority when a library is added to the library list, the user remains authorized to the library even when the user is no longer running under adopted authority. This represents a potential security exposure. Any entries added to a user's library list by a program running under adopted authority should be removed before the adopted authority program ends.

In addition, applications that use library lists rather than qualified library names have a potential security exposure. A user who is authorized to the commands to work with library lists can potentially run a different version of a program.

Related reference:

"Library lists" on page 207

The **library list** for a job indicates which libraries are to be searched and the order in which they are to be searched.

Field authorities

You can specify field authorities for database files.

Field authorities are supported for database files. Authorities supported are Management, Alter, Reference, Read, Add, and Update. You can only administer these authorities through the SQL statements, GRANT and REVOKE. You can display these authorities through the Display Object Authority (DSPOBJAUT) and the Edit Object Authority (EDTOBJAUT) commands. You can only display the field authorities with the EDTOBJAUT command; you cannot edit them.

```

                                Display Object Authority

Object . . . . . : PLMITXT      Owner . . . . . : PGMR1
Library. . . . . : RLN          Primary group . . . : DPTAR
Object type. . . . : *FILE      ASP Device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object Authority  Read  Add  Update  Delete  Execute
*PUBLIC   *PUBLIC   *CHANGE  X     X   X       X       X
PGMR1     *PUBLIC   *ALL     X     X   X       X       X
USER1     *PUBLIC   *USE     X                       X       X
USER2     *PUBLIC   USER DEF X                       X       X
USER3     *PUBLIC   USER DEF X                       X       X

Press Enter to continue

F3=Exit  F11=Nondisplay detail  F12=Cancel  F16=Display field authorities

```

Figure 4. Display Object Authority display showing F16=Display field authorities. This function key will be displayed when a database file has field authorities.

```

                                Display Field Authority
Object . . . . . : PLMITXT      Owner . . . . . : PGMRI
Library . . . . . : RLN        Primary group . . . : *NONE
Object type . . . . : *FILE

Field      User      Object      -----Field Authorities-----
Field3    PGMRI     *ALL       Mgt  Alter Ref  Read  Add  Update
          USER1    *Use              X      X  X      X      X
          USER2    USER DEF          X      X  X      X      X
          USER3    USER DEF          X      X  X      X      X
          *PUBLIC  *CHANGE          X      X  X      X      X
Field4    PGMRI     *ALL       X      X      X      X  X      X
          USER1    *Use              X      X  X      X      X
          USER2    USER DEF          X      X  X      X      X
          USER3    USER DEF          X      X  X      X      X
          *PUBLIC  *CHANGE          X      X  X      X      X
                                     More
Press Enter to continue.

F3=Exit F5=Refresh F12=Cancel F16=Repeat position to F17=Position to

```

Figure 5. Display Field Authority display. When "F17=Position to" is pressed, the Position List prompt will be displayed. If F16 is pressed, the previous position to operation will be repeated.

Field authorities include the following options:

- The Print Private Authority (PRTPVTAUT) command has a field that indicates when a file has field authorities.
- The Display Object Authority (DSPOBJAUT) command has an Authority Type parameter to allow display of object authorities, field authorities, or all authorities. If the object type is not *FILE, you can display only object authorities.
- Information provided by List Users Authorized to Object (QSYLUSRA) API indicates if a file has field authorities.
- The Grant User Authority (GRTUSRAUT) command will not grant a user's field authorities.
- When a grant with reference object is performed using the GRTOBJAUT command and both objects (the one being granted to and the referenced one) are database files, all field authorities will be granted where the field names match.
- If a user's authority to a database file is removed, any field authorities for the user are also removed.

Security and the System/38 Environment

This section provides information about security in the System/38 Environment.

The System/38 Environment and CL programs of type CLP38 represent a potential security exposure. When a non-library qualified command is entered from the System/38 Command Entry screen, or invoked by any CLP38 CL program, library QUSER38 (if it exists) is the first library searched for that command. Library QSYS38 is the second library searched. A programmer or other knowledgeable user might place another CL command in either of these libraries and cause that command to be used instead of one from a library in the library list.

Library QUSER38 is not shipped with the operating system. However, it can be created by anyone with enough authority to create a library.

Related information:

 System/38 Environment Programming

Recommendation for System/38 Environment

This topic includes a list of recommendations for the System/38 Environment.

Use these measures to protect your system for the System/38 Environment and CL programs of type CLP38:

- Check the public authority of the QSYS38 library, and if it is *ALL or *CHANGE then change it to *USE.
- Check the public authority of the QUSER38 library, and if it is *ALL or *CHANGE then change it to *USE.
- If the QUSER38 and QSYS38 do not exist, then create them and set them to public *USE authority. This will prevent anyone else from creating it at a later time and giving themselves or the public too much authority to it.

Directory security

You can use directory security to protect information.

When accessing an object in a directory, you must have authority to all the directories in the path containing the object. You must also have the necessary authority to the object to perform the operation you requested.

You might want to use directory security in the same way that you use library security. Limit access to directories and use public authority to the objects within the directory. Limiting the number of private authorities defined for objects improves the performance of the authority checking process.

Authorization list security

You can group objects with similar security requirements using an authorization list.

An authorization list, conceptually, contains a list of users and the authorities that the users have for the objects secured by the list. Each user can have a different authority to the set of objects the list secures. When you give a user authority to the authorization list, the operating system actually grants a **private authority for that user** to the authorization list.

You can also use an authorization list to define public authority for the objects in the list. If the public authority for an object is set to *AUTL, the object gets its public authority from its authorization list.

The authorization list object is used as a management tool by the system. It actually contains a list of all objects that are secured by the authorization list. This information is used to build displays for viewing or editing the authorization list objects.

You cannot use an authorization list to secure a user profile or another authorization list. Only one authorization list can be specified for an object.

Only the owner of the object, a user with all object (*ALLOBJ) special authority, or a user with all (*ALL) authority to the object, can add or remove the authorization list for an object.

Objects in the system library (QSYS) can be secured with an authorization list. However, the name of the authorization list that secures an object is stored with the object. In some cases, when you install a new release of the operating system, all the objects in the QSYS library are replaced. The association between the objects and your authorization list will be lost.

See the topic “Advantages of using an authorization list” on page 166 for examples of how to use authorization lists.

Authorization list management

You can grant a special operational authority called Authorization List Management (*AUTLMGT) for authorization lists.

Users with *AUTLMGT authority are allowed to add and remove the users' authority to the authorization list and change the authorities for those users. *AUTLMGT authority, by itself, does not give authority to secure new objects with the list or to remove objects from the list.

A user with *AUTLMGT authority can give only the same or less authority to others. For example, assume that USERA has *CHANGE and *AUTLMGT authority to authorization list CPLIST1. USERA can add USERB to CPLIST1 and give USERB *CHANGE authority or less. USERA cannot give USERB *ALL authority to CPLIST1, because USERA does not have *ALL authority.

A user with *AUTLMGT authority can remove the authority for a user if the *AUTLMGT user has equal or greater authority to the list than the user profile name being removed. If USERC has *ALL authority to CPLIST1, then USERA cannot remove USERC from the list, because USERA has only *CHANGE and *AUTLMGT.

Using authorization lists to secure IBM-supplied objects

You can use authorization lists to secure IBM-supplied objects. For example, you might want to restrict the use of a group of commands to a few users.

Objects in IBM-supplied libraries, other than the QUSRSYS and QGPL libraries, are replaced whenever you install a new release of the operating system. Therefore, the link between objects in IBM-supplied libraries and authorization lists is lost. Also, if an authorization list secures an object in QSYS and a complete system restore is required, the link between the objects in QSYS and the authorization list is lost. After you install a new release or restore your system, use the EDTOBJAUT or GRTOBJAUT command to re-establish the link between the IBM-supplied object and the authorization list.

Authority for new objects in a library

You can specify the authority for new objects in a library.

Every library has a parameter called CRTAUT (create authority). This parameter determines the default public authority for any new object that is created in that library. When you create an object, the AUT parameter on the create command determines the public authority for the object. If the AUT value on the create command is *LIBCRTAUT, which is the default for most commands, the public authority for the object is set to the CRTAUT value for the library.

For example, assume that library CUSTLIB has a CRTAUT value of *USE. Both of the commands below create a data area called DTA1 with public authority *USE:

- Specifying the AUT parameter:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +  
  TYPE(*CHAR) AUT(*LIBCRTAUT)
```

- Allowing the AUT parameter to default. *LIBCRTAUT is the default:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +  
  TYPE(*CHAR)
```

The default CRTAUT value for a library is *SYSVAL. Any new objects created in the library using AUT(*LIBCRTAUT) have public authority set to the value of the QCRTAUT system value. The QCRTAUT system value is shipped as *CHANGE. For example, assume that the ITEMLIB library has a CRTAUT value of *SYSVAL. This command creates the DTA2 data area with public authority of change:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +  
  TYPE(*CHAR) AUT(*LIBCRTAUT)
```

“Assigning authority and ownership to new objects” on page 145 shows more examples of how the system assigns ownership and authority to new objects.

The CRTAUT value for a library can also be set to an authorization list name. Any new object created in the library with AUT(*LIBCRTAUT) is secured by the authorization list. The public authority for the object is set to *AUTL.

The CRTAUT value of the library is not used during a move (MOV OBJ), create duplicate (CRTDUPOBJ), or restore of an object into the library. The public authority of the existing object is used.

If the REPLACE (*YES) parameter is used on the create command, then the authority of the existing object is used instead of the CRTAUT value of the library.

Create Authority (CRTAUT) risks

You need to consider the risks when you change the Create Authority (CRTAUT) for an application library.

If your applications use default authority for new objects created during application processing, you should control who has authority to change the library descriptions. Changing the CRTAUT authority for an application library might allow unauthorized access to new objects created in the library.

Authority for new objects in a directory

You can specify the authority for new objects in a directory.

When you create a new directory using the CRTDIR (Make Directory), MD (Make Directory) or MKDIR (Make Directory) commands, you specify the data authority and object authority that the public receives for the new directory. If you use the default *INDIR option, the authority for the created directory is determined from its parent directory. Otherwise, you can specify the specific required authority.

When you create a new directory using the mkdir()--Make Directory API, the owner, primary group, and public object authorities for the created directory are determined from the directory in which it is being created while the owner, primary group, and public data authorities are determined by the mode that is specified on the API call.

The following two examples show different results when you create a new directory with various options.

The first example creates a new directory in the "root"(/) file system using the CRTDIR command and specify *PUBLIC authority.

Starting conditions: Authorities on parent directory:

```

                                     Display Authority
Object . . . . . : /sandersonmytest
Owner . . . . . : SANDERS
Primary group . . . . . : SANDERSGP3
Authorization list . . . . . : *NONE

User      Data      -----Object Authorities-----
Authority Exist  Mgt  Alter  Ref
*PUBLIC  *RWX      X    X    X    X
SANDERS  *RW
SANDERSGP3 *RX
QPGMR    *RWX
QTCM     *RWX      X    X    X    X
```

User SANDERS issues the following command:

```
CRTDIR DIR('/sandersonmytest/deletemepub') DTAAUT(*R) OBJAUT(*NONE)
```

Results: Authorities on created directory:

```

                                     Display Authority
Object . . . . . : /sandersonmytest/deletemepub
Owner . . . . . : SANDERS
Primary group . . . . . : SANDERSGP3
Authorization list . . . . . : *NONE

User      Data      -----Object Authorities-----
Authority Exist  Mgt  Alter  Ref
*PUBLIC  *R
SANDERS  *RWX
SANDERSGP3 *RX
```

Notes:

1. The *PUBLIC data and object authorities are set based on the DTAAUT and OBJAUT parameters.
2. The owner's (SANDERS) data authorities are set to *RWX but the object authorities are inherited from the parent directory's owner. This means that the owner of this directory has no object authorities to the new directory because the owner of the parent directory has no object authorities to the parent directory.
3. The new directory has a primary group profile of SANDERSGP3 because the parent directory has SANDERSGP3 as its primary group profile.

The second example shows how all authorities are inherited from the parent directory when you create a new directory in the "root" (/) file system using the CRTDIR command .

Starting conditions: Authorities on parent directory:

```

                                     Display Authority
Object . . . . . : /sandersonmytest
Owner . . . . . : SANDERS
Primary group . . . . . : SANDERSGP3
Authorization list . . . . . : *NONE

User      Data      -----Object Authorities-----
Authority Exist  Mgt  Alter  Ref
*PUBLIC  *RWX      X    X    X    X
SANDERS  *RW
SANDERSGP3 *RX
QPGMR    *RWX
QTCM    *RWX      X    X    X    X
```

User SANDERSUSR issues the following command:
CRTDIR DIR('/sandersonmytest/deletemepub')

Results: Authorities on created directory:

```

                                     Display Authority
Object . . . . . : /sandersonmytest/deletemepub
Owner . . . . . : SANDERSUSR
Primary group . . . . . : SANDERSGP3
Authorization list . . . . . : *NONE

User      Data      -----Object Authorities-----
Authority Exist  Mgt  Alter  Ref
*PUBLIC  *RWX      X    X    X    X
SANDERSUSR *RWX
SANDERSGP3 *RX
QPGMR    *RWX
QTCM    *RWX      X    X    X    X
SANDERS  *RW
```

Notes:

1. The *PUBLIC data and object authorities are inherited from the parent directory; therefore, the data authority is set to *RWX with all object authorities.
2. The owner's (SANDERSUSR) data authorities are set to *RWX but the object authorities are inherited from the parent directory's owner. This means that the owner of this directory has no object authorities to the new directory because the owner of the parent directory has no object authorities to the parent directory.
3. The new directory has a primary group profile of SANDERSGP3 because the parent directory has SANDERSGP3 as its primary group profile.
4. All users who are privately authorized to the parent directory (QPGMR, QTCM), and the owner of the parent directory (SANDERS), are granted the same private authority to the new directory.

Object ownership

This topic describes object ownership and its functions in the system.

Each object is assigned to an owner when it is created. The owner is either the user who creates the object or the group profile if the member user profile has specified that the group profile should be the owner of the object. When the object is created, the owner is given all the object and data authorities to the object. “Assigning authority and ownership to new objects” on page 145 shows examples of how the system assigns ownership to new objects.

The owner of an object always has all the authorities for the object unless any or all authorities is removed specifically. As an object owner, you might choose to remove some specific authority as a precautionary measure provided you do not have *ALLOBJ special authority. For example, if a file exists that contains critical information, you might remove your object existence authority to prevent yourself from accidentally deleting the file. However, as object owner, you can grant any object authority to yourself at any time. The owner of a newly created integrated file system object has the same object authorities for that integrated file system object as the owner of the parent directory has to the parent directory. Check the Planning and setting up system security topic to see whether the rules for object authorities apply to all file systems or only to certain ones.

Ownership of an object can be transferred from one user to another. Ownership can be transferred to an individual user profile or a group profile. A group profile can own objects, whether the group has members.

The following paragraphs apply to both library- and directory-based objects.

When changing an object’s owner, you have the option to keep or revoke the former owner’s authority.

You cannot delete a profile that owns objects. Ownership of objects must be transferred to a new owner or the objects must be deleted before the profile can be deleted. The Delete User Profile (DLTUSRPRF) command allows you to handle owned objects when you delete the profile.

Object ownership is used as a management tool by the system. The owner profile for an object contains a list of all users who have private authority to the object. This information is used to build displays for editing or viewing object authority.

Profiles that own many objects with many private authorities can become very large. The size of a profile that owns many objects affects performance when displaying and working with the authority to objects it owns and when saving or restoring profiles. System operations can also be impacted. To prevent impacts on either performance or system operations, do not assign objects to only one owner profile for your entire IBM i environment. Each application and the application objects should be owned by a separate profile. Also, IBM-supplied user profiles should not own user data or objects.

The owner of an object also needs sufficient storage for the object. See “Maximum storage” on page 94 for more information.

Group ownership of objects

This topic provides detailed information about the group ownership of objects.

When an object is created, the system looks at the profile of the user creating the object to determine object ownership. If the user is a member of a group profile, the OWNER field in the user profile specifies whether the user or the group should own the new object.

If the group owns the object (OWNER is *GRPPRF), the user creating the object is not automatically given any specific authority to the object. The user gets authority to the object through the group. If the user owns the object (OWNER is *USRPRF), the group's authority to the object is determined by the GRPAUT field in the user profile. Objects created into directories do not use the OWNER and GRPAUT values to determine ownership or group authority. The object will always be owned by the creator of the object.

The *group authority type* (GRPAUTTY) field in the user profile determines whether the group (1) becomes the primary group for the object or (2) is given private authority to the object. “Assigning authority and ownership to new objects” on page 145 shows several examples.

If the user who owns the object changes to a different user group, the original group profile still retains authority to any objects created.

Even if the *Owner* field in a user profile is *GRPPRF, the user must still have sufficient storage to hold a new object while it is being created. After it is created, ownership is transferred to the group profile. The MAXSTG parameter in the user profile determines how much auxiliary storage a user is allowed.

Evaluate the objects a user might create, such as query programs, when choosing between group and individual user ownership:

- If the user moves to a different department and a different user group, should the user still own the objects?
- Is it important to know who creates objects? The object authority displays show the object owner, not the user who created the object.

Note: The Display Object Description display shows the object creator.

If the audit journal function is active, a Create Object (CO) entry is written to the QAUDJRN audit journal at the time an object is created. This entry identifies the creating user profile. The entry is written only if the QAUDLVL system value includes *CREATE and the QAUDCTL system value includes *AUDLVL.

Related concepts:

“Group profiles” on page 4

A *group profile* is a special type of user profile. Rather than giving authority to each user individually, you can use a group profile to define authority for a group of users.

Primary group for an object

You can specify a primary group for an object.

The name of the primary group profile and the primary group's authority to the object are stored with the object. Using primary group authority might provide better performance than using private group authority when checking authority to an object.

A profile must be a group profile (have a gid) to be assigned as the primary group for an object. The same profile cannot be the owner of the object and its primary group.

When a user creates a new object, parameters in the user profile control whether the user's group is given authority to the object and the type of authority given. The *Group authority type* (GRPAUTTY) parameter in a user profile can be used to make the user's group the primary group for the object. “Assigning authority and ownership to new objects” on page 145 shows examples of how authority is assigned when new objects are created. For a directory-based object in some file systems, the object inherits the primary group of its parent directory. For example, if the parent directory has a primary group of FRED, then FRED will have problems trying to create anything in that parent directory. That is because the same profile cannot be both the owner and the primary group profile for the same object.

You can change the primary group for a library- or directory-based object using any of the following commands:

- Change Object Primary Group (**CHGOBJPGP**) command
- Change Primary Group (**CHGPGP**) command
- Option 9 on the Work with Objects by Primary Group (**WRKOBJPGP**) command

You can change the authority of the primary group using the Edit Object Authority (**EDTOBJAUT**) command or the grant and revoke authority commands. You can change the primary group's authority for a library- or directory-based object using the Change Authority (**CHGAUT**) command or the Work with Authority (**WRKAUT**) command.

Related concepts:

“Group profiles” on page 4

A *group profile* is a special type of user profile. Rather than giving authority to each user individually, you can use a group profile to define authority for a group of users.

Default Owner (QDFTOWN) user profile

The Default Owner (QDFTOWN) user profile is an IBM-supplied user profile that is used when an object has no owner or when object ownership might pose a security exposure.

The following situations cause ownership of an object to be assigned to the QDFTOWN profile:

- If an owning profile becomes damaged and is deleted, its objects no longer have an owner. Using the Reclaim Storage (RCLSTG) command assigns ownership of these objects to the default owner (QDFTOWN) user profile.
- If an object is restored and the owner profile does not exist.
- If a program that needs to be created again is restored, but the program creation is not successful. See the topic “Validation of programs being restored” on page 17 for more information about which conditions cause ownership to be assigned to QDFTOWN.
- If the maximum storage limit is exceeded for the user profile that owns an authority holder that has the same name as a file being moved, renamed, or whose library is being renamed.

The system supplies the QDFTOWN user profile because all objects must have an owner. When the system is shipped, only a user with *ALLOBJ special authority can display and access this user profile and transfer ownership of objects associated with the QDFTOWN user profile. You can grant other users authority to the QDFTOWN profile. QDFTOWN user profile is intended for system use only. You should not design your security such that QDFTOWN normally owns objects.

Assigning authority and ownership to new objects

You can assign authority and ownership to new objects on the system.

The system uses several values to assign authority and ownership when a new object is created on the system:

- Parameters on the CRTxxx command
- The QCRTAUT system value
- The CRTAUT value of the library
- Values in the user profile of the creator

Figure 6 on page 146 through Figure 9 on page 149 show several examples of how these values are used:

QCRTAUT system value:
*CHANGE

CRTAUT library parameter:
*USE

Values in USERA (Creator) Profile:

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTYP:
*PRIVATE

Command Used to Create Object:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
          TYPE(*CHAR) AUT(*LIBCRTAUT)
```

or

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
          TYPE(*CHAR)
```

Values for New Object:

Public authority:
*USE

Owner authority:
USERA *ALL

Primary group authority:
None

Private authority:
DPT806 *CHANGE

Note:

*LIBCRTAUT is the default value for the AUT parameter on most CRTxxx commands.

Figure 6. New object example: Public authority from library, group given private authority

QCRTAUT system value:

*CHANGE

CRTAUT library parameter:

*SYSVAL

Values in USERA (Creator) Profile:

GRPPRF:

DPT806

OWNER:

*USRPRF

GRPAUT:

*CHANGE

GRPAUTTYP:

*PRIVATE

Command Used to Create Object:

CRTDTAARA DTAARA(CUSTLIB/DTA1)
TYPE(*CHAR) AUT(*LIBCRTAUT)

Values for New Object:

Public authority:

*CHANGE

Owner authority:

USERA *ALL

Primary group authority:

None

Private authority:

DPT806 *CHANGE

Figure 7. New object example: Public authority from system value, group given private authority

QCRTAUT system value:
*CHANGE

CRTAUT library parameter:
*USE

Values in USERA (Creator) Profile:

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PGP

Command Used to Create Object:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)  
TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Values for New Object:

Public authority:
*USE

Owner authority:
USERA *ALL

Primary group authority:
DPT806 *CHANGE

Private authority:
None

Figure 8. New object example: Public authority from library, group given primary group authority

QCRTAUT system value:

*CHANGE

CRTAUT library parameter:

*USE

Values in USERA (Creator) Profile:

GRPPRF:

DPT806

OWNER:

*GRPPRF

GRPAUT:

GRPAUTYP:

Command Used to Create Object:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
          TYPE(*CHAR) AUT(*CHANGE)
```

Values for New Object:

Public authority:

*CHANGE

Owner authority:

DPT806 *ALL

Primary group authority:

None

Private authority:

None

Figure 9. New object example: Public authority specified, group owns object

Objects that adopt the owner's authority

You can assign adopted authority to a user program to allow the user to change a customer file.

Sometimes a user needs different authorities to an object or an application, depending on the situation. For example, a user might be allowed to change the information in a customer file when using application programs providing that function. However, the same user should be allowed to view, but not change, customer information when using a decision support tool, such as SQL.

A solution to this situation is to 1) give the user *USE authority to customer information to allow querying the files and 2) use adopted authority in the customer maintenance programs to allow the user to change the files.

When an object uses the owner's authority, this is called *adopted authority*. Objects of type *PGM, *SRVPGM, *SQLPKG and Java programs can adopt authority.

When you create a program, you specify a user profile (USRPRF) parameter on the CRTxxxPGM command. This parameter determines whether the program uses the authority of the owner of the program in addition to the authority of the user running the program.

Consult the Limit the use of adopted authority topic concerning security considerations and adopted authority when using SQL packages.

The following description applies to adopted authority:

- Adopted authority is added to any other authority found for the user.
- Adopted authority is checked only if the authority that the user, the user's group, or the public has to an object is not adequate for the requested operation.
- The special authorities (such as *ALLOBJ) in the owner's profile are used.
- If the owner profile is a member of a group profile, the group's authority is *not* used for adopted authority.
- Public authority is *not* used for adopted authority. For example, USER1 runs the program LSTCUST, which requires *USE authority to the CUSTMST file:
 - Public authority to the CUSTMST file is *USE.
 - USER1's authority is *EXCLUDE.
 - USER2 owns the LSTCUST program, which adopts owner authority.
 - USER2 does not own the CUSTMST file and has no private authority to it.
 - Although public authority is sufficient to give USER2 access to the CUSTMST file, USER1 does not get access. Owner authority, primary group authority, and private authority are used for adopted authority.
 - Only the authority is adopted. No other user profile attributes are adopted. For example, the limited capabilities attributes are not adopted.
- Adopted authority is active as long as the program using adopted authority remains in the call stack. For example, assume that PGMA uses adopted authority:
 - If PGMA starts PGMB using the CALL command, these are the call stacks before and after the CALL command:

Table 121. Adopted authority and the CALL command

Call stack before CALL command:	Call stack after CALL command:
QCMD • • • PGMA	QCMD • • • PGMA PGMB

Because PGMA remains in the call stack after PGMB is called, PGMB uses the adopted authority of PGMA. (The use adopted authority (USEADPAUT) parameter can override this. See “Programs that ignore adopted authority” on page 152 for more information about the USEADPAUT parameter.)

- If PGMA starts PGMB using the Transfer Control (TFRCTL) command, the call stacks look like this:

Table 122. Adopted authority and the TFRCTL command

Call stack before TFRCTL command:	Call stack after TFRCTL command:
QCMD • • • PGMA	QCMD • • • PGMB

PGMB does not use the adopted authority of PGMA, because PGMA is no longer in the call stack.

- If the program running under adopted authority is interrupted, the use of adopted authority is suspended. The following functions do not use adopted authority:
 - System request

- Attention key (If a Transfer to Group Job (TFRGRPJOB) command is running, adopted authority is not passed to the group job.)
- Break-message-handling program
- Debug functions

Note: Adopted authority is immediately interrupted by the attention key or a group job request. The user must have authority to run the attention-key-handling program or the group job initial program, or the attempt fails.

For example, USERA runs the program PGM1, which adopts the authority of USERB. PGM1 uses the SETATNPGM command and specifies PGM2. USERB has *USE authority to PGM2. USERA has *EXCLUDE authority to PGM2. The SETATNPGM function is successful because it is run using adopted authority. USERA receives an authority error when attempting to use the attention key because USERB's authority is no longer active.

- If a program that uses adopted authority submits a job, that submitted job does not have the adopted authority of the submitting program.
- When a trigger program or exit point program is called, adopted authority from previous programs in the call stack will not be used as a source of authority for the trigger program or exit point program.
- Adopted authority is not used by the integrated file systems, including the "root" (/), QOpenSys, QDLS, and user-defined file systems.
- The program adopt function is not used when you use the Change Job (CHGJOB) command to change the output queue for a job. The user profile making the change must have authority to the new output queue.
- Any objects created, including spooled files that might 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.
- Adopted authority can be specified either on the command that creates the program (CRTxxxPGM) or on the Change Program (CHGPGM) or Change Service Program (CHGSRVPGM) command.
- If a program is created using REPLACE(*YES) on the CRTxxxPGM command, the new copy of the program has the same USRPRF, USEADPAUT, and AUT values as the replaced program. The USRPRF and AUT parameters specified on the CRTxxxPGM parameter are ignored.
- Only the owner of the program can specify REPLACE(*YES) on the CRTxxxPGM command when USRPRF(*OWNER) is specified on the original program.
- Only a user who owns the program or has *ALLOBJ and *SECADM special authorities can change the value of the USRPRF parameter.
- You must be signed on as a user with *ALLOBJ and *SECADM special authorities to transfer ownership of an object that adopts authority.
- If someone other than the program's owner or a user with *ALLOBJ and *SECADM special authorities restores a program that adopts authority, all private and public authorities to the program are revoked to prevent a possible security exposure.

The Display Program (DSPPGM) and Display Service Program (DSPSRVPGM) commands show whether a program adopts authority (*User profile* prompt) and whether it uses adopted authority from previous programs in the call stack (*Use adopted authority* prompt). The Display Program Adopt (DSPPGMADP) command shows all the objects that adopt the authority of a specific user profile. The Print Adopting Objects (PRTADPOBJ) command provides a report with more information about objects that adopt authority. This command also provides an option to print a report for objects that have been changed since the last time the command was run.

“Flowchart 8: How adopted authority is checked” on page 182 provides more information about adopted authority. The topic “Using adopted authority in menu design” on page 230 shows an example of how to use adopted authority in an application.

Adopted authority and bound programs:

An ILE* program (*PGM) is an object that contains one or more modules. It is created by an ILE* compiler. An ILE program can be bound to one or more service programs (*SRVPGM).

To activate an ILE program successfully, the user must have *EXECUTE authority to the ILE program and to all service programs to which it is bound. If an ILE program uses adopted authority from a program higher in the program call stack, that adopted authority is used to check authority to all service programs to which the ILE program is bound. If the ILE program adopts authority, the adopted authority will not be checked when the system checks the user's authority to the service programs at program activation time.

Adopted authority risks and recommendations

You should use adopted authorities with care to prevent possible security risks.

Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user will not normally have. Adopted authority provides an important tool for meeting diverse authority requirements, but it should be used with care:

- Adopt the minimum authority required to meet the application requirements. Adopting the authority of an application owner is preferable to adopting the authority of QSECOFR or a user with *ALLOBJ special authority.
- Carefully monitor the function provided by programs that adopt authority. Make sure that these programs do not provide a means for the user to access objects outside the control of the program, such as command entry capability.
- Make sure that programs that adopt authority and call other programs perform library qualified calls. Do not use the library list (*LIBL) on the call.
- Control which users are permitted to call programs that adopt authority. Use menu interfaces and library security to prevent these programs from being called without sufficient control.

Programs that ignore adopted authority

You can specify the use adopted authority (USEADPAUT) parameter to control whether a program uses the adopted authority.

You might not want some programs to use the adopted authority of previous programs in the call stack. For example, if you use an initial menu program that adopts owner authority, you might not want some of the programs called from the menu program to use that authority.

The use adopted authority (USEADPAUT) parameter of a program determines whether the system uses the adopted authority of previous programs in the stack when checking authority for objects.

When you create a program, the default is to use adopted authority from previous programs in the stack. If you do not want the program to use adopted authority, you can change the program with the Change Program (CHGPGM) command or Change Service Program (CHGSRVPGM) command to set the USEADPAUT parameter to *NO. If a program is created using REPLACE(*YES) on the CRTxxxPGM command, the new copy of the program has the same USRPRF, USEADPAUT, and AUT values as the replaced program.

The topic "Ignoring adopted authority" on page 232 shows an example of how to use this parameter in menu design. See "Use Adopted Authority (QUSEADPAUT)" on page 35 for information about the QUSEADPAUT system value.

Attention: In some situations, you can use the MODINVAU MI instruction to prevent passing adopted authority to called functions. The MODINVAU instruction can be used to prevent passing any adopted authority from C and C++ programs to called functions in another program or service program. This might be useful when you do not know the USEADPAUT setting of the function that is called.

Related concepts:

“Ignoring adopted authority” on page 232

The technique of using adopted authority in menu design requires the user to return to the initial menu before running queries. If you want to provide the convenience of starting query from application menus as well as from the initial menu, you can set up the QRYSTART program to ignore adopted authority.

Authority holders

An authority holder is a tool for keeping the authorities for a program-described database file that does not currently exist on the system.

The primary use of an authority holder is for System/36 environment applications, which often delete program-described files and create them again.

An authority holder can be created for a file that already exists or for a file that does not exist, using the Create Authority Holder (CRTAUTHLR) command. The following descriptions apply to authority holders:

- Authority holders can only secure files in the system auxiliary storage pool (ASP) or a basic user ASP. They cannot secure files in an independent ASP.
- The authority holder is associated with a specific file and library. It has the same name as the file.
- Authority holders can be used only for program-described database files and logical files.
- After the authority holder is created, you add private authorities for it like a file. Use the commands to grant, revoke, and display object authorities, and specify object type *FILE. On the object authority displays, the authority holder is indistinguishable from the file itself. The displays do not indicate whether the file exists; nor do they show that the file has an authority holder.
- If a file is associated with an authority holder, the authorities defined for the authority holder are used during authority checking. Any private authorities defined for the file are ignored.
- Use the Display Authority Holder (DSPAUTHLR) command to display or print all the authority holders on the system. You can also use it to create an output file (OUTFILE) for processing.
- If you create an authority holder for a file that exists:
 - The user creating the authority holder must have *ALL authority to the file.
 - The owner of the file becomes the owner of the authority holder regardless of the user creating the authority holder.
 - The public authority for the authority holder comes from the file. The public authority (AUT) parameter on the CRTAUTHLR command is ignored.
 - The existing file's authority is copied to the authority holder.
- If you create a file and an authority holder for that file already exists:
 - The user creating the file must have *ALL authority to the authority holder.
 - The owner of the authority holder becomes the owner of the file regardless of the user creating the file.
 - The public authority for the file comes from the authority holder. The public authority (AUT) parameter on the CRTPF or CRTLF command is ignored.
 - The authority holder is linked to the file. The authority specified for the authority holder is used to secure the file.
- If an authority holder is deleted, the authority information is transferred to the file itself.

- If a file is renamed and the new file name matches an existing authority holder, the authority and ownership of the file are changed to match the authority holder. The user renaming the file needs *ALL authority to the authority holder.
- If a file is moved to a different library and an authority holder exists for that file name and the target library, the authority and ownership of the file are changed to match the authority holder. The user moving the file must have *ALL authority to the authority holder.
- Ownership of the authority holder and the file always match. If you change the ownership of the file, ownership of the authority holder also changes.
- When a file is restored, if an authority holder exists for that file name and the library to which it is being restored, it is linked to the authority holder.
- Authority holders cannot be created for files in these libraries: QSYS, QRCL, QRECOVERY, QSPL, QTEMP, and QSPL0002 – QSPL0032.

Authority holders and System/36 Migration

The System/36 Migration Aid creates an authority holder for every file that is migrated. It also creates an authority holder for entries in the System/36 resource security file if no corresponding file exists on the System/36.

You need authority holders only for files that are deleted and re-created by your applications. Use the Delete Authority Holder (DLTAUTHLR) command to delete any authority holders that you do not need.

Authority holder risks

You should take security into consideration when using an authority holder.

An authority holder provides the capability of defining authority for a file before that file exists. Under certain circumstances, this can allow an unauthorized user to gain access to information. If a user knew that an application creates, moves, or renames a file, the user can create an authority holder for the new file. The user thus gains access to the file.

To limit this exposure, the CRTAUTHLR command is shipped with public authority *EXCLUDE. Only users with *ALLOBJ authority can use the command, unless you grant authority to others.

Working with authority

This topic describes commonly-used methods for setting up, maintaining, and displaying authority information about your system.

Appendix A, “Security commands,” on page 309 provides a complete list of the commands available for working with authority. The descriptions that follow do not discuss all the parameters for commands or all the fields on the displays. Consult online information for complete details.

Authority displays

This section describes some characteristics of the displays that show object authorities.

Four displays show object authorities:

- Display Object Authority display
- Edit Object Authority display
- Display Authority display
- Work with Authority display

Figure 10 on page 155 shows the basic version of the Display Object Authority display:

```

                                Display Object Authority
Object . . . . . : CUSTNO   Owner . . . . . : PGMR1
  Library. . . . . : CUSTLIB  Primary group . . . : DPTAR
Object type . . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
*PUBLIC
PGMR1
DPTAR
DPTSM
F3=Exit F11=Display detail object authorities F12=Cancel F17=Top

```

Figure 10. Display Object Authority display

The system-defined names of the authorities are shown on this display. F11 acts as a toggle between this and two other versions of the display. One shows detailed object authorities:

```

                                Display Object Authority
Object . . . . . : CUSTNO   Owner . . . . . : PGMR1
  Library. . . . . : CUSTLIB  Primary group . . . : DPTAR
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object -----Object-----
Authority Opr Mgt Exist Alter Ref
*PUBLIC
PGMR1
DPTAR
DPTSM
:
:
F3=Exit F11=Display data authorities F12=Cancel F17=Top F18=Bottom

```

The other shows data authorities:

```

                                Display Object Authority
Object . . . . . : CUSTNO   Owner . . . . . : PGMR1
  Library. . . . . : CUSTLIB  Primary group . . . : DPTAR
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Object secured by authorization list. . . . . : *NONE

User      Group      Object -----Data-----
Authority Read Add Update Delete Execute
*PUBLIC
PGMR1
DPTAR
DPTSM

```

If you have *OBJMGT authority to an object, you see all private authorities for that object. If you do not have *OBJMGT authority, you see only your own sources of authority for the object.

For example, if USERA displays authority for the CUSTNO data area, only public authority is shown.

If USERB, who is a member of the DPTAR group profile, displays the authority for the CUSTNO data area, it looks like this:

```

                Display Object Authority
Object . . . . . : CUSTNO      Owner . . . . . : PGMR1
  Library. . . . . : CUSTLIB   Primary group . . . : DPTAR
Object type. . . . : *DTAARA   ASP device . . . . : *SYSBAS

Object secured by authorization list. . . . . : *NONE

User      Group      Object
*GROUP    DPTAR      *CHANGE
  
```

If USERB runs a program that adopts the authority of PGMR1 and displays the authority for the CUSTNO data area, it looks like this:

```

                Display Object Authority
Object . . . . . : CUSTNO      Owner . . . . . : PGMR1
  Library . . . . . : CUSTLIB   Primary group . . . : DPTAR
Object type. . . . : *DTAARA   ASP device . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
*ADOPTED          USER DEF
*PUBLIC           *EXCLUDE
PGMR1             *ALL
*GROUP    DPTAR   *CHANGE
DPTSM           *USE
  
```

The *ADOPTED authority indicates only the additional authority received from the program owner. USERB receives from PGMR1 all the authorities that are not included in *CHANGE. The display shows all private authorities because USERB has adopted *OBJMGT. The detailed display looks like this:

```

                Display Object Authority
Object . . . . . : CUSTNO      Owner . . . . . : PGMR1
  Library. . . . . : CUSTLIB   Primary group . . . : DPTAR
Object type. . . . : *DTAARA   ASP device . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object      -----Object-----
Authority  Opr  Mgt  Exist  Alter  Ref
*ADOPTED          USER DEF      X    X    X    X
*PUBLIC           *EXCLUDE
PGMR1             *ALL      X    X    X    X
*GROUP    DPTAR   *CHANGE      X
DPTSM           *USE      X

F3=Exit F11=Display data authorities F12=Cancel F17=Top F18=Bottom
  
```

If the user option (USROPT) field in USERB's user profile includes *EXPERT, this is how the display looks:

```

                                Display Object Authority
Object . . . . . : CUSTNO   Owner . . . . . : PGMR1
Library. . . . . : CUSTLIB  Primary group . . . : DPTAR
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User   Group   OBJECT Authority  ----Object-----  -----Data-----
*ADOPTED          USER DEF      0  M  E  A  R      R  A  U  D  E
*PUBLIC           *EXCLUDE
PGMR1             *ALL          X  X  X  X  X      X  X  X  X  X
*GROUP DPTAR     *CHANGE       X                    X  X  X  X  X
DPTSM            *USE          X                    X                    X

```

Authority reports

Several reports are available to help you monitor your security implementation.

For example, you can monitor objects with *PUBLIC authority other than *EXCLUDE and objects with private authorities with the following commands:

- Print Public Authority (PRTPUBAUT)
- Print Private Authority (PRTPVTAUT)

Related information:

System security tools

Working with libraries

You can specify the authority for libraries and new objects created in the libraries.

Two parameters on the Create Library (CRTLIB) command affect authority:

Authority (AUT): The AUT parameter can be used to specify either of the following authorities:

- The public authority for the library
- The authorization list that secures the library.

The AUT parameter applies to the library itself, not to the objects in the library. If you specify an authorization list name, the public authority for the library is set to *AUTL.

If you do not specify AUT when you create a library, *LIBCRTAUT is the default. The system uses the CRTAUT value from the QSYS library, which is shipped as *SYSVAL.

Create Authority (CRTAUT): The CRTAUT parameter determines the default authority for any new objects that are created in the library. CRTAUT can be set to one of the system-defined authorities (*ALL, *CHANGE, *USE, or *EXCLUDE), to *SYSVAL (the QCRTAUT system value), or to the name of an authorization list.

Note: You can change the CRTAUT value for a library using the Change Library (CHGLIB) command.

If user PGMR1 enters this command:

```
CRTLIB TESTLIB AUT(LIBLST) CRTAUT(OBJLST)
```

the authority for the library looks like this:

```

                                Display Object Authority
Object . . . . . : TESTLIB      Owner . . . . . : PGMR1
  Library. . . . . : QSYS        Primary group . . . : *NONE
Object type. . . . : *LIB        ASP device . . . . . : *SYSBAS

Object secured by authorization list. . . . . : LIBLST

User      Group      Object
*PUBLIC   Group      Authority
PGMR1     *PUBLIC   *AUTL
           PGMR1     *ALL
  
```

- Because an authorization list was specified for the AUT parameter, public authority is set to *AUTL.
- The user entering the CRTLIB command owns the library, unless the user's profile specifies OWNER(*GRPPRF). The owner is automatically given *ALL authority.
- The CRTAUT value is not shown on the object authority displays. Use the Display Library Description (DSPLIBD) command to see the CRTAUT value for a library.

```

                                Display Library Description
Library . . . . . : TESTLIB

Type . . . . . : PROD
ASP number . . . . . : 1
ASP device . . . . . : *SYSBAS
Create authority . . . . . : OBJLST
Create object auditing . . . . . : *SYSVAL
Text description . . . . . : Customer Rec
  
```

Creating objects

You can specify the authority of a new object.

When you create a new object, you can either specify the authority (AUT) or use the default, *LIBCRTAUT. If PGMR1 enters this command:

```

CRTDTAARA (TESTLIB/DTA1) +
  TYPE(*CHAR)
  
```

the authority for the data area looks like this:

```

                                Display Object Authority
Object . . . . . : DTA1        Owner . . . . . : PGMR1
  Library. . . . . : TESTLIB    Primary group . . . : *NONE
Object type. . . . : *DTAARA    ASP device . . . . . : *SYSBAS

Object secured by authorization list. . . . . : OBJLST

User      Group      Object
*PUBLIC   Group      Authority
PGMR1     *PUBLIC   *AUTL
           PGMR1     *ALL
  
```

The authorization list (OBJLST) comes from the CRTAUT parameter that was specified when TESTLIB was created.

If PGMR1 enters this command:

```
CRTDTAARA (TESTLIB/DTA2) AUT(*CHANGE) +
  TYPE(*CHAR)
```

the authority for the data area looks like this:

```
Display Object Authority
Object . . . . . : DTA2      Owner . . . . . : PGMR1
Library . . . . . : TESTLIB  Primary group . . . . : *NONE
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
*PUBLIC   Group      Authority
PGMR1    *CHANGE
          *ALL
```

Working with individual object authority

You can change the authority for an object.

To change the authority for an object, you must have one of the following authorities:

- *ALLOBJ authority or membership in a group profile that has *ALLOBJ special authority.

Note: The group's authority is not used if you have private authority to the object.

- Ownership of the object. If a group profile owns the object, any member of the group can act as the object owner, unless the member has been given specific authority that does not meet the requirements for changing the object's authority.
- *OBJMGT authority to the object and any authorities being granted or revoked (except *EXCLUDE). Any user who is allowed to work with the object's authority can grant or revoke *EXCLUDE authority.

The easiest way to change authority for an individual object is with the Edit Object Authority display. This display can be called directly by using the Edit Object Authority (EDTOBJAUT) command or selected as an option from the Work with Objects by Owner, Work with Objects by Private Authority, Work with Objects by Primary Group, or Work with Objects display.

```
Edit Object Authority
Object. . . . . : DTA1      Owner . . . . . : PGMR1
Library . . . . . : TESTLIB  Primary group . . . . : *NONE
Object type. . . . : *DTAARA  ASP device . . . . . : *SYSBAS

Type changes to current authorities, press Enter.

Object secured by authorization list . . . . . : OBJLST

User      Group      Object
*PUBLIC   Group      Authority
PGMR1    *AUTL
          *ALL
```

You can also use these commands to change object authority:

- Change Authority (CHGAUT)
- Work with Authority (WRKAUT)
- Grant Object Authority (GRTOBJAUT)
- Revoke Object Authority (RVKOBJAUT)

To specify the generic authority subsets, such as Read/Write (*RX) or Write/Execute (*WX), you must use the CHGAUT or WRKAUT commands.

Specifying user-defined authority

This topic provides information about specifying user-defined authorities.

The Object Authority column on the Edit Object Authority display allows you to specify any of the system-defined sets of authorities (*ALL, *CHANGE, *USE, *EXCLUDE). If you want to specify authority that is not a system-defined set, use F11 (Display detail).

Note: If the *User options* (USROPT) field in your user profile is set to *EXPERT, you always see this detailed version of the display without having to press F11.

For example, PGMR1 removes *OBJEXIST authority to the CONTRACTS file, to prevent accidentally deleting the file. Because PGMR1 has a combination of authorities that is not one of the system-defined sets, the system puts *USER DEF* (user-defined) in the Object Authority column:

```

                                Edit Object Authority
Object . . . . . : CONTRACTS  Owner . . . . . : PGMR1
Library . . . . . : TESTLIB   Primary group . . . . . : *NONE
Object type . . . . . : *FILE   ASP device . . . . . : *SYSBAS

Type changes to current authorities, press Enter.

Object secured by authorization list. . . . . : LIST2

User      Group      Object Authority  Opr  Mgt  Exist  Alter  Ref
*PUBLIC
PGMR1      USER DEF      X    X           X    X

```

You can press F11 (Display data authorities) to view or change the data authorities:

```

                                Edit Object Authority
Object . . . . . : CONTRACTS  Owner . . . . . : PGMR1
Library . . . . . : TESTLIB   Primary group . . . . . : *NONE
Object type . . . . . : *FIL    ASP device . . . . . : *SYSBAS

Type changes to current authorities, press Enter.

Object secured by authorization list. . . . . : LIST2

User      Group      Object Authority  Read  Add  Update  Delete  Execute
*PUBLIC
PGMR1      USER DEF      X    X    X       X       X

```

Giving authority to new users

You can grant authority to new users.

To give authority to additional users, press F6 (Add new users) from the Edit Object Authority display. You see the Add New Users display, which allows you to define authority for multiple users:

```

                                Add New Users

Object . . . . . : DTA1
Library . . . . . : TESTLIB

Type new users, press Enter.

User      Object
USER1     *USE
USER2     *CHANGE
PGMR2     *ALL

```

Removing a user's authority

You can also remove a user's authority for an object.

Removing a user's authority for an object is different from giving the user *EXCLUDE authority. *EXCLUDE authority means the user is specifically not allowed to use the object. Only *ALLOBJ special authority and adopted authority override *EXCLUDE authority.

Note: *EXCLUDE authority for a group profile can be overridden if the user has another group profile with private authority to the object.

Removing a user's authority means the user has no specific authority to the object. The user can gain access through a group profile, an authorization list, public authority, *ALLOBJ special authority, or adopted authority.

You can remove a user's authority using the Edit Object Authority display. Type blanks in the Object Authority field for the user and press the Enter key. The user is removed from the display. You can also use the Revoke Object Authority (RVKOBJAUT) command. Either revoke the specific authority the user has or revoke *ALL authority for the user.

Note: The RVKOBJAUT command revokes only the authority you specify. For example, USERB has *ALL authority to FILEB in library LIBB. You revoke *CHANGE authority:

```

RVKOBJAUT OBJ(LIBB/FILEB) OBJTYPE(*FILE) +
USER(*USERB) AUT(*CHANGE)

```

After the command, USERB's authority to FILEB looks like this:

```

                                Display Object Authority

Object . . . . . : FILEB   Owner . . . . . : PGMR1
Library . . . . . : LIBB   Primary group . . . : *NONE
Object type . . . : *FILE  ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

      Object
User  Group Authority Opr Mgt Exist Alter Ref
USERB      USER DEF      X  X      X      X

```

```

                                Display Object Authority
Object . . . . . : FILEB      Owner . . . . . : PGMR1
  Library. . . . . : LIBB      Primary group . . . : *NONE
Object type . . . : *FILE     ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . *NONE

User      Group      Object      -----Data-----
USERB                                Authority Read Add Update Delete Execute
USER DEF

```

Working with authority for multiple objects

Learn how to make authority changes to more than one object at a time.

The Edit Object Authority display allows you to interactively work with the authority for one object at a time. The Grant Object Authority (GRTOBJAUT) command allows you to make authority changes to more than one object at a time. You can use the GRTOBJAUT authority command interactively or in batch. You can also call it from a program.

Following are examples of using the GRTOBJAUT command, showing the prompt display. When the command runs, you receive a message for each object indicating whether the change was made. Authority changes require an exclusive lock on the object and cannot be made when an object is in use. Print your job log for a record of changes attempted and made.

- To give all the objects in the TESTLIB library a public authority of *USE:

```

                                Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.
Object . . . . . *ALL
Library . . . . . TESTLIB
Object type . . . . *ALL
ASP device . . . . . *
Users . . . . . *PUBLIC
+ for more values
Authority . . . . . *USE

```

This example for the GRTOBJAUT command gives the authority you specify, but it does not remove any authority that is greater than you specified. If some objects in the TESTLIB library have public authority *CHANGE, the command just shown will not reduce their public authority to *USE. To make sure that all objects in TESTLIB have a public authority of *USE, use the GRTOBJAUT command with the REPLACE parameter.

```
GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
          USER(*PUBLIC) REPLACE(*YES)
```

The REPLACE parameter indicates whether the authorities you specify replaces the existing authority for the user. The default value of REPLACE(*NO) gives the authority that you specify, but it does not remove any authority that is greater than the authority you specify, unless you are granting *EXCLUDE authority.

These commands set public authority only for objects that currently exist in the library. To set the public authority for any new objects that are created later, use the CRTAUT parameter on the library description.

- To give *ALL authority to the work files in the TESTLIB library to users AMES and SMITHR. In this example, work files all start with the characters WRK:

```

Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.

Object . . . . . WRK*
Library . . . . . TESTLIB
Object type . . . . . *FILE
ASP device . . . . . *
Users . . . . . AMES
      + for more values SMITHR
Authority . . . . . *ALL

```

This command uses a generic name to specify the files. You specify a generic name by typing a character string followed by an asterisk (*). Online information tells which parameters of a command allow a generic name.

- To secure all the files starting with the characters AR* using an authorization list called ARLST1 and have the files get their public authority from the list, use the following two commands:
 1. Secure the files with the authorization list using the GRTOBJAUT command:

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
Library . . . . . TESTLIB
Object type . . . . . *FILE
ASP device . . . . . *
:
:
Authorization list . . . . . ARLST1

```

2. Set public authority for the files to *AUTL, using the GRTOBJAUT command:

```

Grant Object Authority

Type choices, press Enter.

Object . . . . . AR*
Library . . . . . TESTLIB
Object type . . . . . *FILE
ASP device . . . . . *
Users . . . . . *PUBLIC
      + for more values
Authority . . . . . *AUTL

```

Working with object ownership

You can change the ownership of an object in several ways.

To change ownership of an object, use one of the following commands:

- The Change Object Owner (CHGOBJOWN) command
- The Work with Objects by Owner (WRKOBJOWN) command
- The Change Owner (CHGOWN) command

The Work with Objects by Owner display shows all the objects owned by a profile. You can assign individual objects to a new owner. You can also change ownership for more than one object at a time by using the NEWOWN (new owner) parameter at the bottom of the display:

```

Work with Objects by Owner

User profile . . . . . : OLDDOWNER

Type options, press Enter.
 2=Edit authority      4=Delete   5=Display author
 8=Display description 9=Change owner

Opt Object      Library      Type      Attribute      ASP
  Device
 9  COPGMSG     COPGMLIB   *MSGQ
 9  CUSTMAS     CUSTLIB    *FILE
 9  CUSTMSGQ    CUSTLIB    *MSGQ
    ITEMMSGQ    ITEMLIB    *MSGQ
    *SYSBAS
    *SYSBAS
    *SYSBAS
    *SYSBAS

Parameters or command
====> NEWOWN (OWNIC)
F3=Exit  F4=Prompt  F5=Refresh  F9=Retrieve
F18=Bottom

```

When you change ownership using either method, you can choose to remove the previous owner's authority to the object. The default for the CUROWNAUT (current owner authority) parameter is *REVOKE.

To transfer ownership of an object, you must have:

- Object existence authority for the object
- *ALL authority or ownership, if the object is an authorization list
- Add authority for the new owner's user profile
- Delete authority for the present owner's user profile

You cannot delete a user profile that owns objects. The topic “Deleting user profiles” on page 122 shows methods for handling owned objects when deleting a profile.

The Work with Objects by Owner display includes integrated file system objects. For these objects, the *Object* column on the display shows the first 18 characters of the path name. If the path name is longer than 18 characters, a greater than symbol (>) appears at the end of the path name. To see the absolute path name, place your cursor anywhere on the path name and press the F22 key.

Working with primary group authority

You can change the primary group or primary group's authority to an object.

To change the primary group or primary group's authority to an object, use one of the following commands:

- Change Object Primary Group (**CHGOBJPGP**)
- Work with Objects by Primary Group (**WRKOBJPGP**)
- Change Primary Group (**CHGPGP**)

When you change an object's primary group, you specify what authority the new primary group has. You can also revoke the old primary group's authority. If you do not revoke the old primary group's authority, it becomes a private authority.

The new primary group cannot be the owner of the object.

To change an object's primary group, you must have all of the following authorities:

- *OBJEXIST authority for the object.
- If the object is a file, library, or subsystem description, *OBJOPR and *OBJEXIST authority.
- If the object is an authorization list, *ALLOBJ special authority or the owner of the authorization list.
- If revoking authority for the old primary group, *OBJMGT authority.
- If a value other than *PRIVATE is specified, *OBJMGT authority and all the authorities being given.

Using a referenced object

Both the Edit Object Authority display and the **GRTOBJAUT** command allow you to give authority to an object (or group of objects) based on the authority of a referenced object.

This is a useful tool in some situations, but you should also evaluate the use of an authorization list to meet your requirements. See “Advantages of using an authorization list” on page 166 for information about the advantages of using authorization lists.

Copying authority from a user

You can copy all the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command.

This method can be useful in certain situations. For example, the system does not allow you to rename a user profile. To create an identical profile with a different name involves several steps, including copying the original profile's authorities. “Renaming a user profile” on page 126 shows an example of how to do this.

The GRTUSRAUT command copies private authorities only. It does not copy special authorities; nor does it transfer object ownership.

The GRTUSRAUT command should not be used in place of creating group profiles. GRTUSRAUT creates a duplicate set of private authorities, which increases the time it takes to save the system and makes authority management more difficult. GRTUSRAUT copies authorities as they exist at a particular moment. If authority is required to new objects in the future, each profile must be granted authority individually. The group profile provides this function automatically.

To use the GRTUSRAUT command, you must have all the authorities being copied. If you do not have an authority, that authority is not granted to the target profile. The system issues a message for each authority that is granted or not granted to the target user profile. Print the job log for a complete record. To avoid having a partial set of authorities copied, the GRTUSRAUT command should be run by a user with *ALLOBJ special authority.

Related tasks:

“Copying private authorities” on page 121

You can copy the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command.

Working with authorization lists

This section introduces the steps for creating an authorization list.

Setting up an authorization list requires three steps:

1. Creating the authorization list.
2. Adding users to the authorization list.
3. Securing objects with the authorization list.

Steps 2 and 3 can be done in any order.

Advantages of using an authorization list

You can use authorization lists to protect objects on your system.

An authorization list has these advantages:

- Authorization lists simplify managing authorities. User authority is defined for the authorization list, not for the individual objects on the list. If a new object is secured by the authorization list, the users on the list gain authority to the object.
- One operation can be used to give a user authority to all the objects on the list.
- Authorization lists reduce the number of private authorities on the system. Each user has a private authority to one object, the authorization list. This gives the user authority to all the objects on the list. Reducing the number of private authorities in the system has the following advantages:
 - Reduces the size of user profiles.
 - Improves the performance when saving the system (SAVSYS) or saving the security data (SAVSECDTA).
- Authorization lists provide a good way to secure files. If you use private authorities, each user will have a private authority for each file member. If you use an authorization list, each user will have only one authority. Also, files that are open cannot have authority granted to the file or revoked from the file. If you secure the file with an authorization list, you can change the authorities, even when the file is open.
- Authorization lists provide a way to remember authorities when an object is saved. When an object is saved that is secured by an authorization list, the name of the authorization list is saved with the object. If the object is deleted and restored to the same system, it is automatically linked to the authorization list again. If the object is restored on a different system, the authorization list is not linked, unless ALWOBJDIF(*ALL), ALWOBJDIF(*AUTL), or ALWOBJDIF(*COMPATIBLE) is specified on the restore command.
- From a security management view, an authorization list is the preferred method to manage objects that have the same security requirements. Even when there are only a few objects that are secured by the list, there is still an advantage of using an authorization list over using private authorities on the object. Because the authorities are in one place (the authorization list), it is easier to change who is authorized to the objects. It is also easier to secure any new objects with the same authorities as the existing objects.

Creating an authorization list

Use the Create Authorization List (**CRTAUTL**) command to create an authorization list.

You do not need any authority to the QSYS library to create an authorization list into that library. Use the Create Authorization List (**CRTAUTL**) command:

```
                Create Authorization List (CRTAUTL)

Type choices, press Enter.

Authorization list . . . . .  custlst1      Name
Text 'description' . . . . .  Files cleared at month-end

                Additional Parameters

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

The AUT parameter sets the public authority for any objects secured by the list. The public authority from the authorization list is used only when the public authority for an object secured by the list is *AUTL.

Giving users authority to an authorization list

Use the Edit Authorization List (EDTAUTL) display to give users authority to the authorization list you have created.

To work with the authority that users have for the authorization list, you must have *AUTLMGT (authorization list management) authority, as well as the specific authorities you are granting. See the topic “Authorization list management” on page 138 for a complete description.

You can use the Edit Authorization List (EDTAUTL) display to change user authority to the authorization list or to add new users to the list:

```
                                Edit Authorization List
Object . . . . . : CUSTLST1      Owner . . . . . : PGMRI
Library . . . . . : QSYS         Primary group . . . : *NONE

Type changes to current authorities, press Enter.

User      Object  List
          Authority Mgt
*PUBLIC   *USE
PGMR1     *ALL    X
```

To give new users authority to the authorization list, press F6 (Add new users):

```
                                Add New Users
Object . . . . . : CUSTLST1      Owner . . . : PGMRI
Library . . . . . : QSYS

Type new users, press Enter.

User      Object  List
          Authority Mgt
AMES      *CHANGE
SMITHR    *CHANGE
```

Each user's authority to the list is actually stored as a private authority in that user's profile. You can also use commands to work with authorization list users, either interactively or in batch:

- Add Authorization List Entry (ADDAUTLE) to define authority for additional users.
- Change Authorization List Entry (CHGAUTLE) to change authority for users who are already authorized to the list.
- Remove Authorization List Entry (RMVAUTLE) to remove a user's authority to the list.
- Work with Authority (WRKAUT) to show the list of authorized users of an object.
- Change Authority (CHGAUT) to change a user's authority for the object.

Securing objects with an authorization list

To secure an object with an authorization list, you must own the object, have *ALL authority to it, or have *ALLOBJ special authority.

Use the Edit Object Authority display, the **GRTOBJAUT** command, the **WRKAUT** command, or the **CHGAUT** command to secure an object with an authorization list:

```

                                Edit Object Authority
Object . . . . . : ARWRK1      Owner . . . . . : PGMR1
  Library . . . . : TESTLIB    Primary group. . . . : *NONE
Object type . . . : *FILE      ASP device . . . . . : *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list . . . . . ARLST1

User      Object
*PUBLIC   Authority
PGMR1     *AUTL
          *ALL

```

Set the public authority for the object to *AUTL if you want public authority to come from the authorization list.

On the Edit Authorization List display, you can use F15 (Display authorization list objects) to list all of the objects secured by the list:

```

                                Display Authorization List Objects
Authorization list . . . . . : CUSTLST1
  Library . . . . . : CUSTLIB
Owner . . . . . : OWNAR
Primary group . . . . . : DPTAR

Object      Library  Type   Owner   Primary
CUSTMAS    CUSTLIB *FILE  OWNAR   group
CUSTADDR   CUSTLIB *FILE  OWNAR   Text

```

This is an information list only. You cannot add or remove objects from the list. You can also use the Display Authorization List Objects (**DSPAUTOBJ**) command to view or print a list of all objects secured by the list.

Setting up an authorization list

The setup of an authorization list makes it easier to change who is authorized to the objects, and easier to secure any new objects with the same authorities as the existing objects.

At the JKL Toy Company, an authorization list is used to secure all the work files used in month-end inventory processing. These work files are cleared, which requires *OBJMGT authority. As application requirements change, more work files may be added to the application. Also, as job responsibilities change, different users run month-end processing. An authorization list makes it simpler to manage these changes.

Follow these steps to set up the authorization list.

1. Create the authorization list:
CRTAUTL ICLIST1
2. Secure all the work files with the authorization list:
GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +
 OBJTYP(*FILE) AUTL(ICLIST1)
3. Add users to the list who perform month-end processing:
ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)

If you use authorization lists, then you should not have private authorities on the object. Two searches of the user's private authorities are required during the authority checking if the object has private authorities and the object is also secured by an authorization list. The first search is for the private authorities on the object; the second search is for the private authorities on the authorization list. Two searches require use of system resources; therefore, the performance can be impacted. If you use only the authorization list, only one search is performed. Also, because of the use of authority caching with the authorization list, the performance for the authority check will be the same as it is for checking only private authorities on the object.

Deleting an authorization list

You might also want to delete the authorization list that you have created.

You cannot delete an authorization list if it is used to secure any objects. Use the **DSPAUTOBJ** command to list all of the objects secured by the list. Use either the Edit Object Authority display, Change Authority (**CHGAUT**), or the Revoke Object Authority (**RVKOBJAUT**) command to change the authority for each object. When the authorization list no longer secures any objects, use the Delete Authorization List (**DLTAUTL**) command to delete it.

How the system checks authority

When a user attempts to perform an operation on an object, the system verifies that the user has adequate authority for the operation.

The system first checks authority to the library or directory path that contains the object. If the authority to the library or directory path is adequate, the system checks authority to the object itself. In the case of database files, authority checking is done at the time the file is opened, not when each individual operation to the file is performed.

During the authority-checking process, when any authority is found (even if it is not adequate for the requested operation) authority checking stops and access is granted or denied. The adopted authority function is the exception to this rule. Adopted authority can override any specific (and inadequate) authority found. See the topic "Objects that adopt the owner's authority" on page 149 for more information about adopted authority.

The system verifies a user's authority to an object in the following order:

1. Object's authority - fast path
2. User's *ALLOBJ special authority
3. User's specific authority to the object
4. User's authority on the authorization list securing the object
5. Groups' *ALLOBJ special authority
6. Groups' authority to the object
7. Groups' authority on the authorization list securing the object
8. Public authority specified for the object or for the authorization list securing the object
9. Program owner's authority, if adopted authority is used

Note: Authority from one or more of the user's groups might be accumulated to find sufficient authority for the object being accessed.

Authority checking flowcharts

This section introduces the flowcharts, descriptions, and examples of how authority is checked.

Use them to answer specific questions about whether a particular authority scheme will work or diagnose problems with your authority definitions. The charts also highlight the types of authority that cause the greatest performance effect.

The process of checking authority is divided into a primary flowchart and several smaller flowcharts showing specific parts of the process. Depending on the combination of authorities for an object, the steps in some flowcharts might be repeated several times.

The numbers at the upper left of figures on the flowcharts are used in the examples following the flowcharts.

The steps representing the search of a profile's private authorities are highlighted:

- Step 6 in Figure 13 on page 174
- Step 6 in Figure 16 on page 180
- Step 2 in Figure 19 on page 185

Repeating these steps is likely to cause performance problems in the authority checking process.

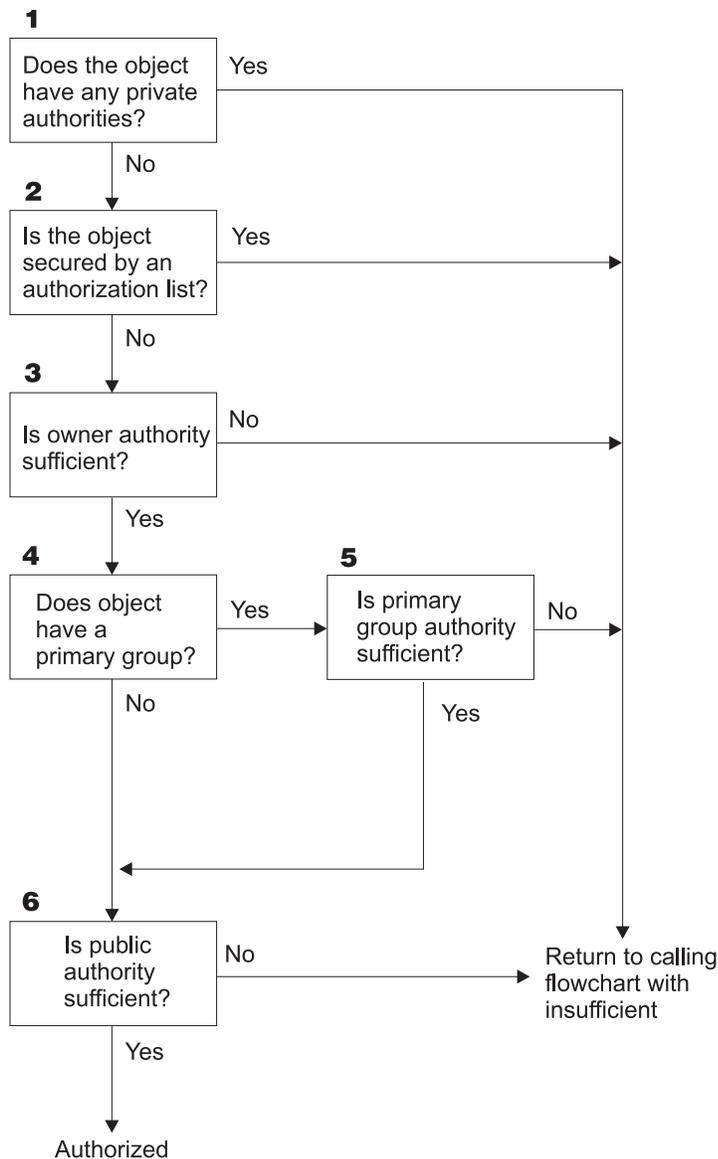
Flowchart 1: Main authority checking process

The steps in Flowchart 1 show the main process the system follows in checking authority for an object.

1. The system checks the object's authority. (Refer to Flowchart 2: Fast Path for Object Authority Checking.) If the system finds that authority is insufficient, it proceeds to Step 2.
2. The system checks the user's authority to the object. (Refer to Flowchart 3: How User Authority to an Object Is Checked.) If the system determines that the user does not have authority to the object, it proceeds to Step 3. If the system finds that the user's authority is insufficient, it proceed to Step 6.
3. The system checks whether the user profile belongs to any groups. If it does, the system proceeds to Step 4. If it does not, the system proceeds to Step 5.
4. The system determines the group authority. (Refer to Flowchart 6). If the system determines that there is no group authority to the object, it proceeds to Step 5. If the system determines that the group authority to the object is not sufficient, it proceeds to Step 6.
5. The system checks the public authority of the object. (Refer to Flowchart 7.) If the system determines that the public authority is insufficient, it proceeds to Step 6.
6. The system checks the adopted authority of the object. (Refer to Flowchart 8.)

Flowchart 2: Fast path for object authority checking

The steps in Flowchart 2 are performed using information stored with the object. This is the fastest method for authorizing a user to an object.



RBAFW522-0

Figure 12. Flowchart 2: Fast path for object authority

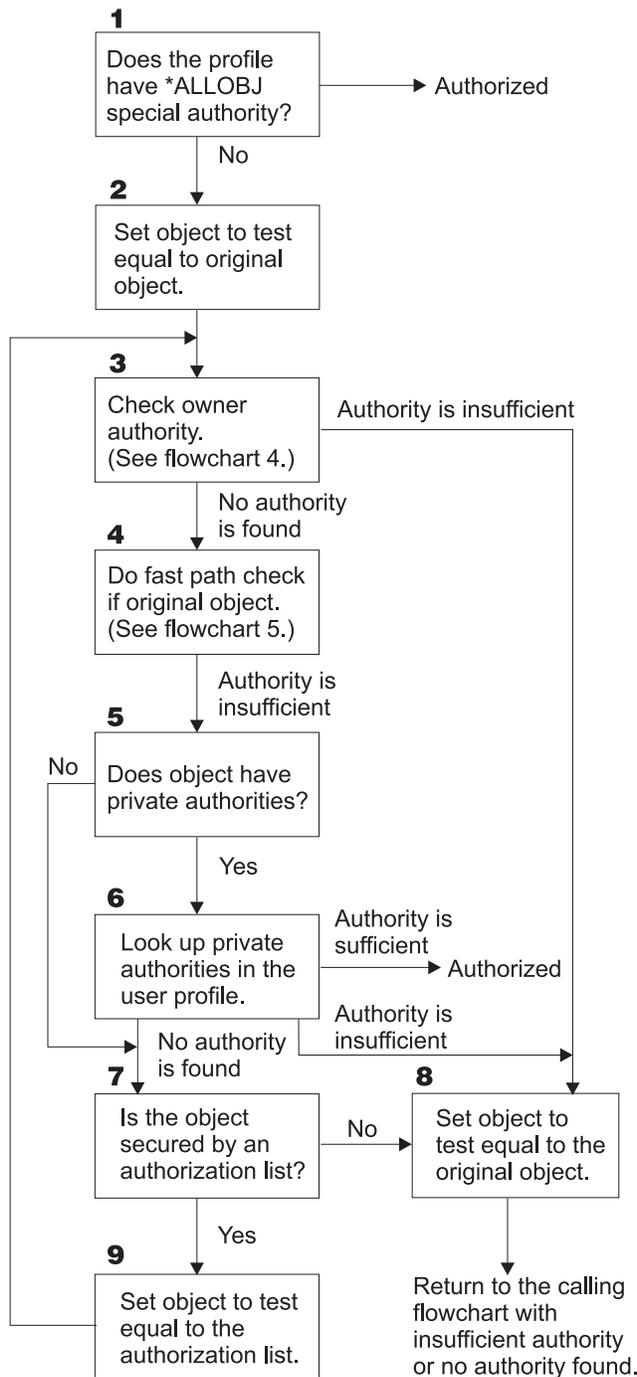
Description of Flowchart 2: Fast path for object authority

1. The system determines whether the object has any private authorities. If it does, the system returns to the calling flowchart with insufficient authority. If it does not, the system proceeds to Step 2.
2. The system determines whether the object is secured by an authorization list. If it is, the system returns to the calling flowchart with insufficient authority. If it does not, the system proceeds to Step 3.
3. The system determines whether the owner of the object has sufficient authority. If it does not, the system returns to the calling flowchart with insufficient authority. If it does, the system proceeds to Step 4.
4. The system determines whether the object has a primary group. If it does, the system proceeds to Step 5. If it does not, the system proceeds to Step 6.
5. The system determines whether the object's primary group has sufficient authority. If it does, the system proceeds to Step 6. If it does not, the system returns to the calling flowchart with insufficient authority.

6. The system determines whether public authority is sufficient. If it is, the object is authorized. If it is not, the system returns to the calling flowchart with insufficient authority.

Flowchart 3: How user authority to an object is checked

The steps in Flowchart 3 are performed for the individual user profile.



RBAFW523-1

Figure 13. Flowchart 3: Check user authority

Description of Flowchart 3: Check user authority

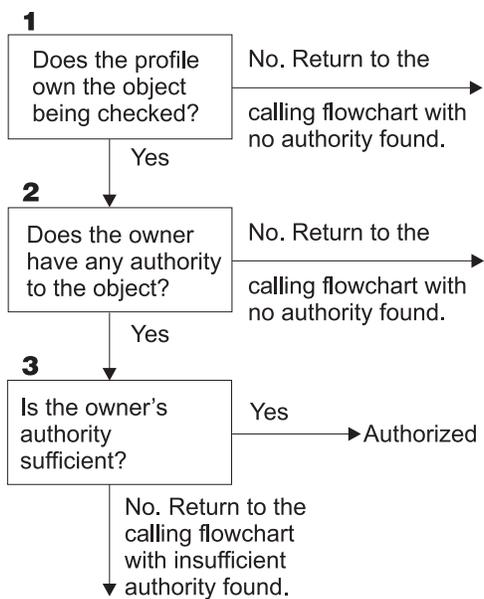
1. The system determines if the user profile has *ALLOBJ authority. If the profile does have *ALLOBJ authority, then the profile is authorized. If it does not have *ALLOBJ authority, then the authority checking proceeds to Step 2.
2. The system sets the authority of the object to be equal to the original object. The authority checking proceeds to Step 3.
3. The system checks the owner authority. If the authority is insufficient, then it proceeds to Step 8. If no authority is found, then it proceeds to Step 4.
4. The system completes a fast path authority check of the original object. (Refer to Flowchart 5). If authority is insufficient, then authority checking proceeds to Step 5.
5. The system determines if the object has private authorities. If it does, then the authority check proceeds to Step 6. If there are no private authorities, then the authority checking goes to Step 7.
6. The system checks for private authorities with the user profile. If the authority is sufficient, then the user is authorized. If authority is not sufficient, then the authority checking proceeds to Step 8. If no authority is found, then the authority checking proceeds to Step 7.
7. The system determines if the object is secured by an authorization list. If it is not, then the authority checking proceeds to Step 8. If it is secured by an authorization list, then the authority checking proceeds to Step 9.
8. The system sets the object to test equal to the original object and returns to the calling flowchart with insufficient authority or no authority found.
9. The system sets the object to test equal to the authorization list and returns to Step 3.

Flowchart 4: How owner authority is checked

Flowchart 4 shows the process for checking owner authority. The name of the owner profile and the owner's authority to an object are stored with the object.

Several possibilities exist for using the owner's authority to access an object:

- The user profile owns the object.
- The user profile owns the authorization list.
- The user's group profile owns the object.
- The user's group profile owns the authorization list.
- Adopted authority is used, and the program owner owns the object.
- Adopted authority is used, and the program owner owns the authorization list.



RBAFW524-0

Figure 14. Flowchart 4: Owner authority checking

Description of Flowchart 4: Owner authority checking

1. The system determines if the user profile owns the object being checked. If the user profile does own the object, then it moves to Step 2. If the user profile does not own the object, then the system returns to the calling flowchart with no authority found.
2. If the user profile does own the object, the system then determines if the owner has authority to the object. If the owner has authority to the object, then the authority check proceeds to Step 3. If the system determines that the owner does not have authority to the object, then the system returns to the calling flowchart with no authority found.
3. If the owner does have authority to the object, then the system determines whether this authority is sufficient to access to object. If the authority is sufficient, then the owner is authorized to the object. If it is not sufficient, then the system returns to the calling flowchart with insufficient authority found.

Flowchart 5: Fast path for user authority checking

Flowchart 5 shows the fast path for testing user authority without searching private authorities.

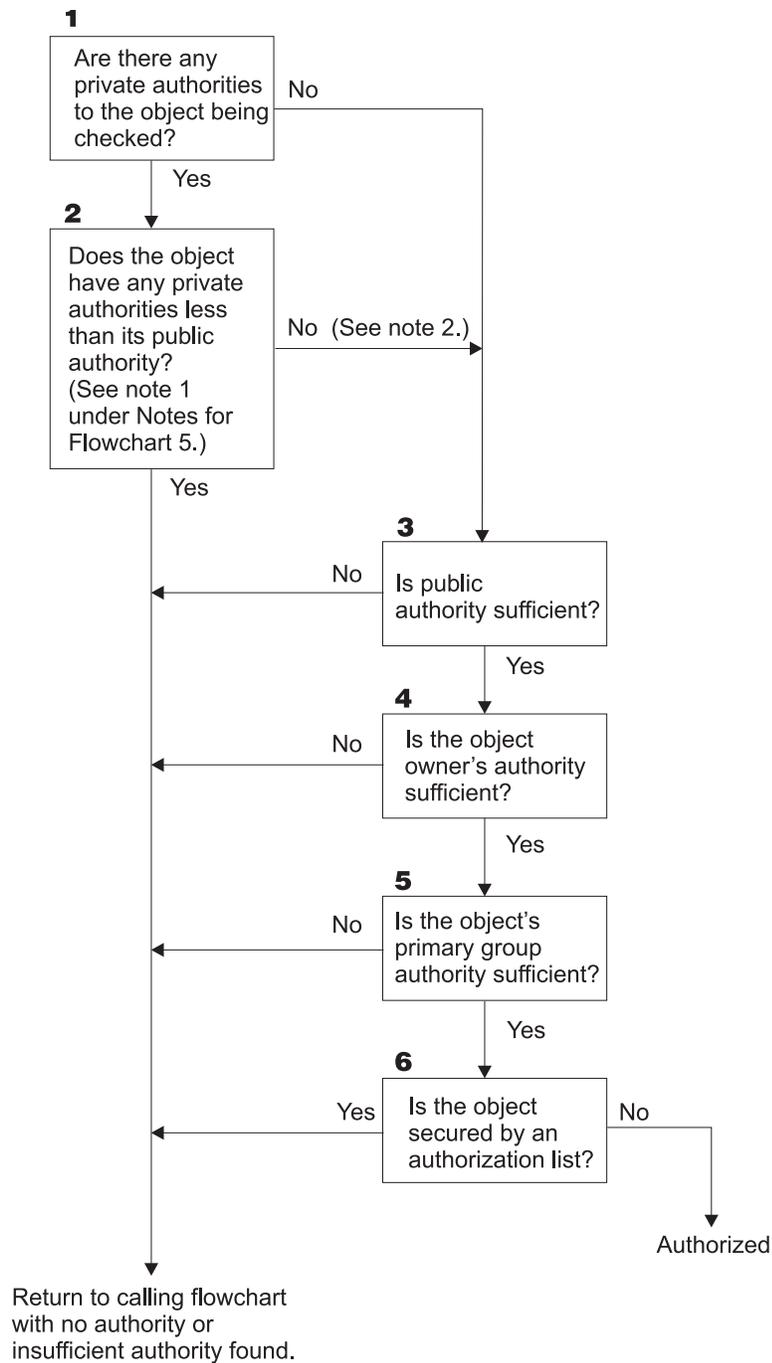


Figure 15. Flowchart 5: Fast path for user authority

Flowchart 5 notes:

1. Authority is considered less than public if any authority that is present for *PUBLIC is not present for another user. In the example shown in Table 123 on page 178, the public has *OBJOPR, *READ, and *EXECUTE authority to the object. WILSONJ has *EXCLUDE authority and does not have any of the authorities the public has. Therefore, this object does have private authority less than its public authority. (OWNAR also has less authority than the public, but owner authority is not considered private authority.)

Table 123. Public versus private authority

Authority	Users			
	OWNAR	DPTMG	WILSONJ	*PUBLIC
<i>Object Authorities:</i>				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
<i>Data Authorities</i>				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. This path provides a method for using public authority, if possible, even though private authority exists for an object. The system tests to make sure that nothing later in the authority checking process might deny access to the object. If the result of these tests is *Sufficient*, searching private authorities can be avoided.

Description of Flowchart 5: Fast path for user authority

This flowchart shows the fast path for testing user authority without searching private authorities.

1. The system determines if there are any private authorities to the object being checked. If there are private authorities to the object, then the authority check proceeds to Step 2. If there is no private authority, the authority check proceeds to Step 3.
2. If private authorities exist, then the system determines if the object has private authorities that are less than its public authority. (See note 1.) If the object does have private authorities that are less than its public authority, then the system returns to the calling flowchart with no authority or insufficient authority found. If the object does not have private authorities that are less than its public authority, (See note 2), then the authority check proceeds to Step 3.
3. If the object does not have any private authorities or the object does not have private authorities that are less than its public authority, then the system determine if the public authority is sufficient. If the public authority is sufficient, then the authority check proceeds to Step 4. If the public authority is insufficient, then system returns to the calling flowchart with no authority or insufficient authority found.
4. If the public authority is sufficient, then the system determines if the object owner's authority is sufficient. If the object owner's authority is sufficient, then the authority check proceeds to Step 5. If the object owner's authority is insufficient, then system returns to the calling flowchart with no authority or insufficient authority found.
5. If the object owner's authority is sufficient, then the system determines if the object's primary group authority is sufficient. If the object's primary group authority is sufficient, then the authority check proceeds to Step 6. If object's primary group authority is insufficient, then the system returns to the calling flowchart with no authority or insufficient authority found.
6. If the object's primary group authority is sufficient, then the system determines if the object is secured by an authorization list. If the object is secured by an authorization list, then the system returns to the

calling flowchart with no authority or insufficient authority found. If the object is not secured by an authorization list, then the user is authorized to the object.

Flowchart 6: How group authority is checked

A user might be a member of up to 16 groups. A group might have private authority to an object, or it might be the primary group for an object.

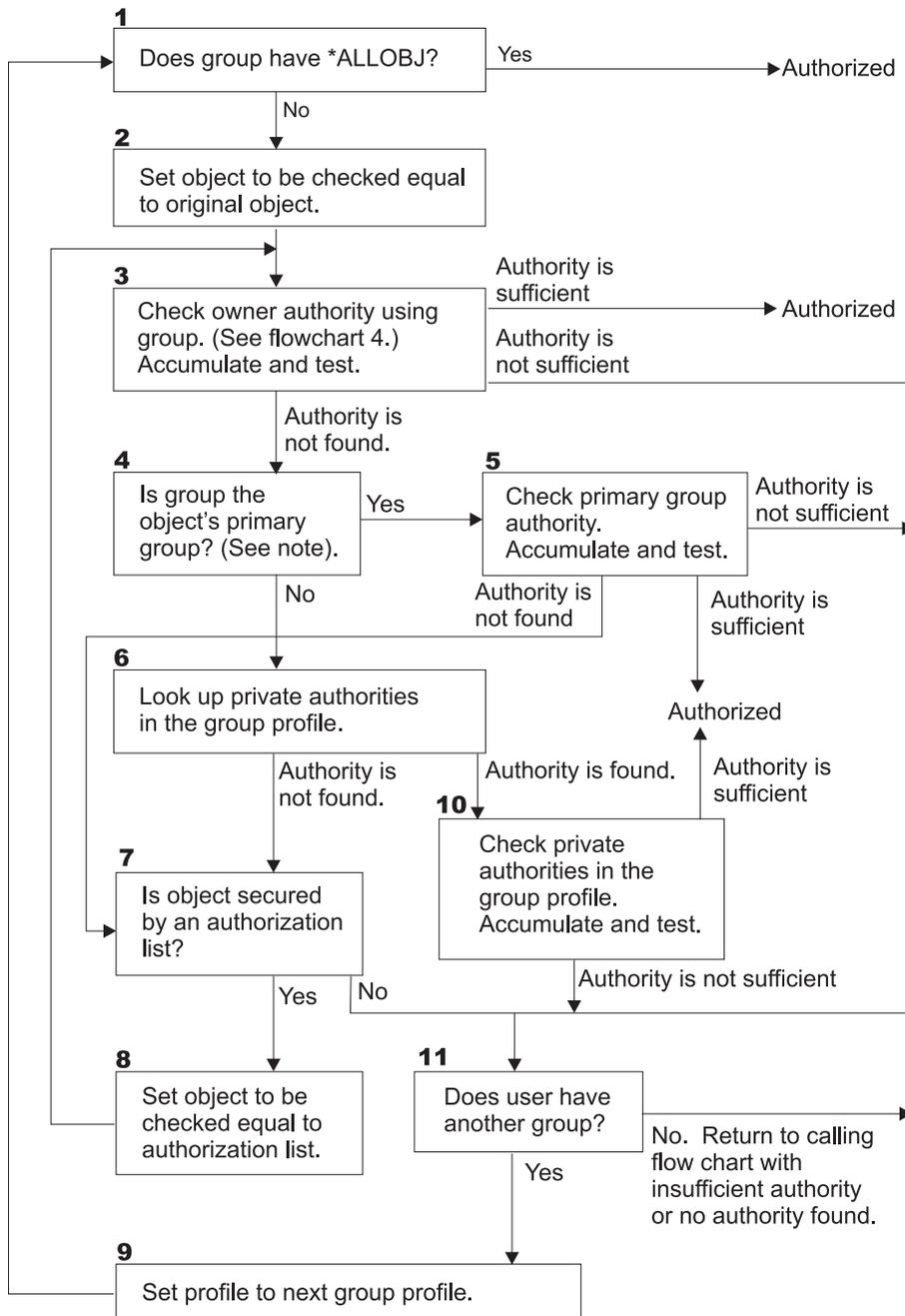
Authority from one or more of the user's groups might be accumulated to find sufficient authority for the object being accessed. For example, WAGNERB needs *CHANGE authority to the CRLIM file. *CHANGE authority includes *OBJOPR, *READ, *ADD, *UPD, *DLT, and *EXECUTE. Table 124 shows the authorities for the CRLIM file:

Table 124. Accumulated group authority

Authority	Users			
	OWNAR	DPT506	DPT702	*PUBLIC
<i>Object Authorities:</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Data Authorities</i>				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	X	
*DLT	X		X	
*EXECUTE	X	X	X	
*EXCLUDE				X

WAGNERB needs both DPT506 and DPT702 to get sufficient authority to the CRLIM file. DPT506 is missing *DLT authority, and DPT702 is missing *ADD authority.

Flowchart 6 on page Figure 16 on page 180 shows the steps in checking group authority.



RBAFW509-1

Figure 16. Flowchart 6: Group authority checking

Note: If the user is signed on as the profile that is the primary group for an object, the user cannot receive authority to the object through the primary group.

Description of Flowchart 6: Group authority checking

1. The system determines if the group has *ALLOBJ authority. If it does, then the group is authorized. If it does not, authority checking proceeds to Step 2.
2. The group does not have *ALLOBJ authority so the system sets the object that is being checked to be equal to the original object.

3. After the system sets the object to the original, it checks owner authority. (See Flowchart 4) If authority is sufficient, then the group is authorized. If the authority is not sufficient, then the authority check goes to Step 11. If the authority is not found, then the authority check proceeds to Step 4.
4. The owner authority is not found so the system checks if the group is the object's primary group.

Note: If the user is signed on as the profile that is the primary group for an object, the user cannot receive authority to the object through the primary group.
If the group is the object's primary group, then the authority check proceeds to Step 5. If the group is not the object's primary group, then authority check proceeds to Step 6.
5. The group is the object's primary group so the system checks and tests the primary group authority. If primary group authority is sufficient, then the group is authorized. If primary group authority is not found, then the authority check goes to Step 7. If the primary group authority is insufficient, then the authority check goes to Step 11
6. The group is not the object's primary group so the system looks up the private authorities in the group profile. If authority is found, then authority checking goes to Step 10. If authority is not found, then authority checking proceeds to Step 7.
7. No authority is found for the private authorities for the group profile so the system checks to see if the object is secured by an authorization list. If the object is secured by an authorization list, then the authority check proceeds to Step 8. If the object is not secured by an authorization list, then the authority check goes to Step 11.
8. The object is secured by an authorization list so the system set the object to be checked equal to the authorization list and authority check returns to Step 3.
9. The user belongs to another group profile so the system sets the profile to the next group profile and returns to Step 1 to start the authority checking process over again.
10. Authority is found for private authorities within the group profile so the private authorities are checked and tested in the group profile. If authorities are sufficient, then the group profile is authorized. If it is not sufficient, then the authority check goes to Step 11.
11. Authority is not found or is insufficient so the system checks to see if the users is associated with another group profile. If the user does belong to another group profile, then the system goes to Step 9. If the user does not belong to another group profile, then the system returns to the calling flowchart with insufficient authority or no authority found.

Flowchart 7: How public authority is checked

When checking public authority, the system must determine whether to use the public authority for the object or the authorization list.

Flowchart 7 shows the process:

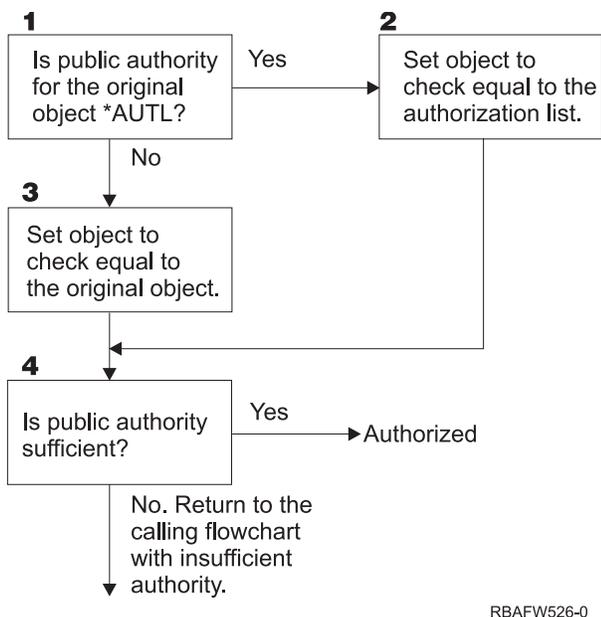


Figure 17. Flowchart 7: Check public authority

Description of Flowchart 7: Check public authority

Flowchart 7 shows how the system must determine whether to use the public authority for the object or the authorization list.

1. The system determine if the public authority for the original object is *AUTL. If the public authority for the original object is *AUTL, then the system proceeds to Step 2. If the public authority for the original object is not *AUTL, then the system proceeds to Step 3.
2. If the public authority for the original object is *AUTL, then the system sets the object being checked equal to the authorization list and proceeds to Step 4.
3. If the public authority for the original object is not *AUTL, then the system sets the object being checked to the original object and proceeds to Step 4.
4. If the object being checked has been set equal to the authorization list or the original object, the system determines if the public authority is sufficient. If the public authority is sufficient, then user is authorized to the object. If the public authority is not sufficient, then the system returns to the calling flowchart with insufficient authority.

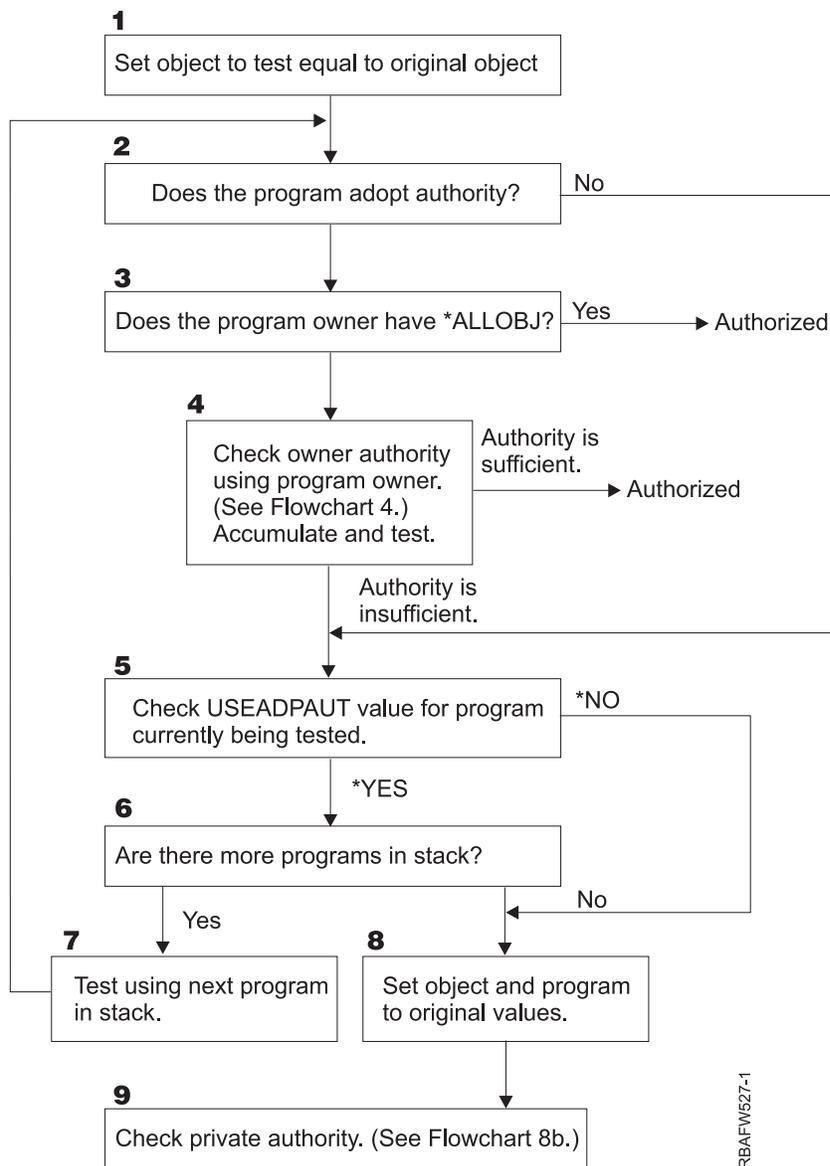
Flowchart 8: How adopted authority is checked

If insufficient authority is found by checking user authority, the system checks adopted authority.

The system might use adopted authority from the original program the user called or from earlier programs in the call stack. To provide the best performance and minimize the number of times private authorities are searched, the process for checking adopted authority checks to see if the program owner has *ALLOBJ special authority or owns the object being tested. This is repeated for every program in the stack that uses adopted authority.

If sufficient authority is not found, the system checks to see if the program owner has private authority for the object being checked. This is repeated for every program in the stack that uses adopted authority.

Figure 18 on page 183 and Figure 19 on page 185 show the process for checking adopted authority.



RBBAFW527-1

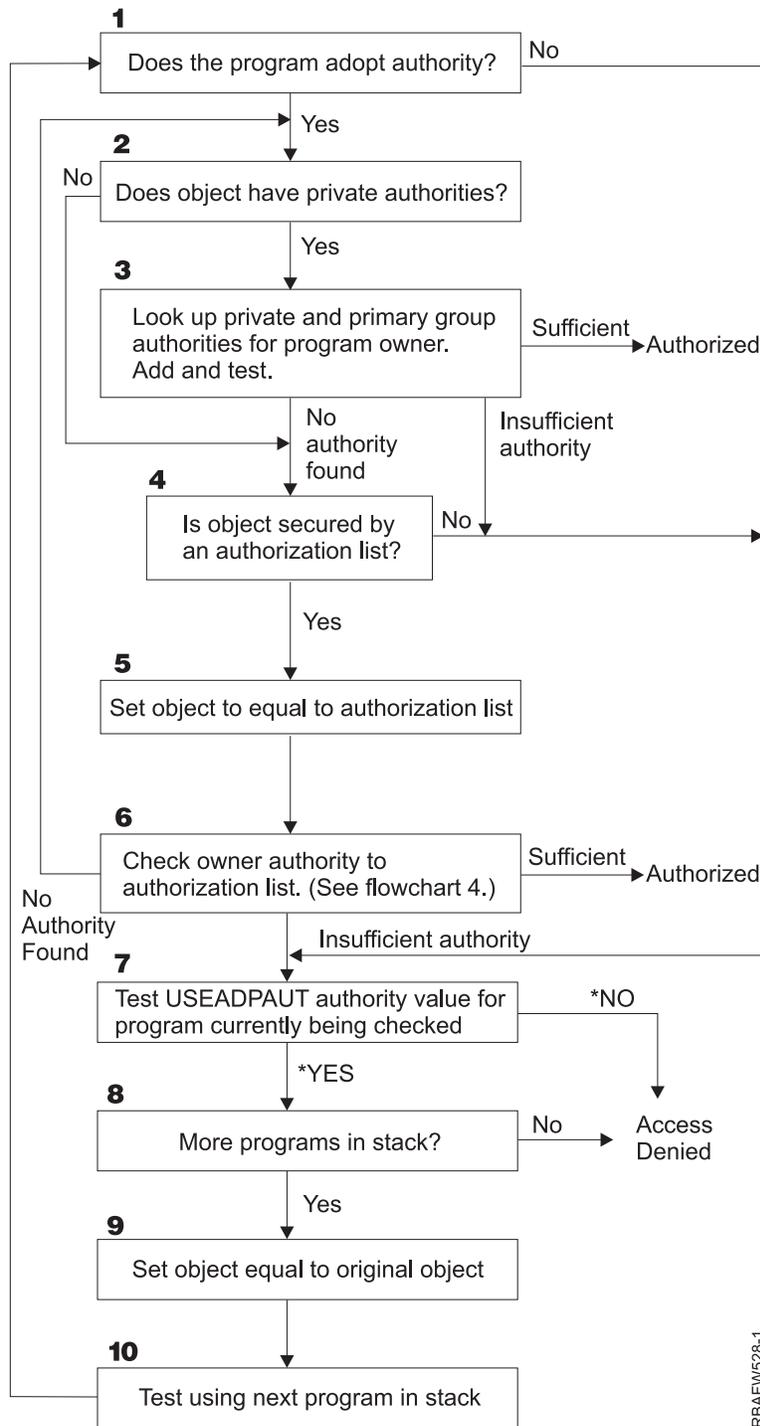
Figure 18. Flowchart 8A: Checking adopted authority user *ALLOBJ and owner

Description of Flowchart 8A: Checking adopted authority user *ALLOBJ and owner

Flowchart 8A describes how the system checks adopted authority when insufficient authority has been found by checking user authority.

1. The system sets the object being checked to the original object and proceeds to Step 2.
2. The system determines if the program adopts authority. If the program does adopt authority, then the authority checking proceeds to Step 3. If the program does not adopt authority and the authority is insufficient, then authority checking goes to Step 5.
3. If the program does adopt authority, then the system determines if the program owner has *ALLOBJ authority. If the program owner does have *ALLOBJ authority, then the user is authorized. If the program owner does not have *ALLOBJ authority, then the authority checking proceeds to Step 4.
4. If the program owner does not have *ALLOBJ authority, then the system checks and tests the owner authority. If the authority is sufficient, then the user is authorized. If the authority is insufficient, then authority checking proceeds to Step 5.

5. The system checks USEADPAUT value for the program currently being test. If the value equals *NO then authority checking proceeds to Step 8. If the value is equal to *YES, then the authority checking proceeds to Step 6.
6. If the USEADPAUT value is equal to *YES, then the system determine if there are more programs waiting in the stack. If there are more programs in the stack, then authority checking proceeds to Step 7. If there are not any more programs waiting in the stack, then authority checking goes to Step 8.
7. Test using the next program in the stack and start back at Step 2.
8. If there are no more programs in the stack or the USEADPAUT value is equal to *NO, then system sets the object and program to the original values and proceeds to Step 9.
9. The system checks private authority. This is described in Flowchart 8B: Checking adopted authority using private authorities.



RBAFW628-1

Figure 19. Flowchart 8B: Checking adopted authority using private authorities

Description of Flowchart 8B: Checking adopted authority using private authorities

1. The system determines whether the program can adopt authority. If yes, proceed to Step 2. If no, proceed to Step 7.
2. The system determines whether the object has private authorities. If yes, proceed to Step 3. If no, proceed to Step 4.

3. The system checks the private and primary group authorities for the program owner. If authority is sufficient, the program is authorized. If insufficient authority is found, proceed to Step 7. If no authority is found, proceed to Step 4.
4. The system determines whether the object is secured by an authorization list. If yes, proceed to Step 5. If no, proceed to Step 7.
5. The system sets object equal to authorization list and then proceeds to Step 6.
6. The system checks the owner's authority to the authorization list. (Refer to Flowchart 4.) If not authority is found, go back to Step 2. If sufficient authority is found, the program is authorized.
7. The system tests the USEADPAUT authority value for the program currently being checked. If *YES, proceed to Step 8. If *NO, access denied.
8. The system checks whether there are more programs in the stack. If yes, proceed to Step 9. If no, access denied.
9. The system sets object equal to original object and proceeds to Step 10.
10. Test using next program in stack and start back at Step 1.

Related concepts:

“Ignoring adopted authority” on page 232

The technique of using adopted authority in menu design requires the user to return to the initial menu before running queries. If you want to provide the convenience of starting query from application menus as well as from the initial menu, you can set up the QRYSTART program to ignore adopted authority.

Authority checking examples

This section includes several examples of authority checking.

These examples demonstrate the steps the system uses to determine whether a user is allowed a requested access to an object. These examples are intended to show how authority checking works and where potential performance problems might occur.

Figure 20 shows the authorities for the PRICES file. Following the figure are several examples of requested access to this file and the authority checking process. In the examples, searching private authorities (Flowchart 4, step 6) is highlighted because this is the part of the authority checking process that can cause performance problems if it is repeated several times.

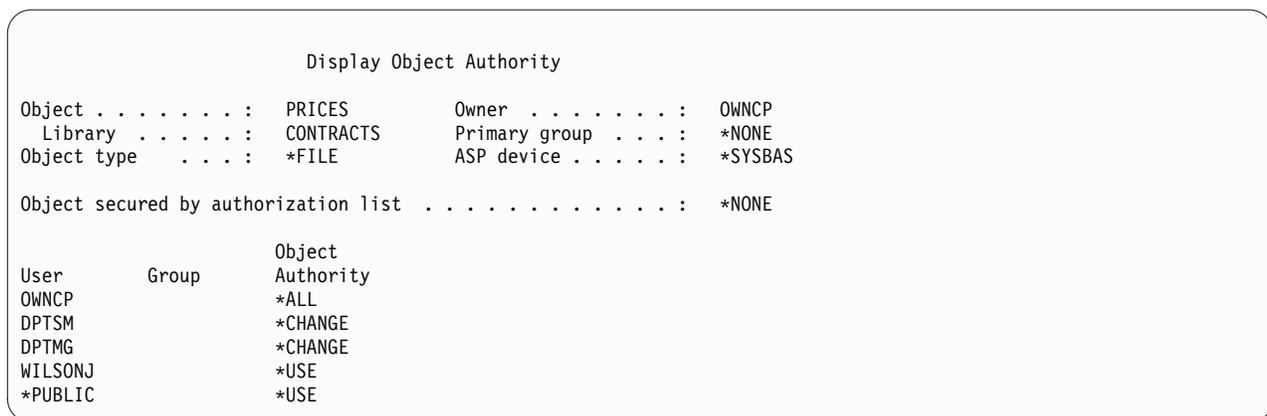


Figure 20. Authority for the PRICES file

Case 1: Using private group authority

This case demonstrates how to use private group authority.

User ROSSM wants to access the PRICES file using the program CPPGM01. CPPGM01 requires *CHANGE authority to the file. ROSSM is a member of group profile DPTSM. Neither ROSSM nor DPTSM has *ALLOBJ special authority. The system performs these steps in determining whether to allow ROSSM access to the PRICES file:

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. Return to Flowchart 3 with no authority found. ROSSM does not own the PRICES file.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1, 2, and 3. Public is not sufficient.
 - d. Flowchart 3, step 5.
 - e. Flowchart 3, step 6. ROSSM does not have private authority to the PRICES file.
 - f. Flowchart 3, steps 7 and 8. The PRICES file is not secured by an authorization list. Return to Flowchart 1 with no authority found.
3. Flowchart 1, steps 3 and 4. DPTSM is the group profile for ROSSM.
 - a. Flowchart 6, steps 1, 2, and 3.
 - 1) Flowchart 4, step 1. DPTSM does not own the PRICES file.
 - b. Flowchart 6, step 4. DPTSM is not the primary group for the PRICES file.
 - c. Flowchart 6, step 6. Authorized. (DPTSM has *CHANGE authority.)

Result:

ROSSM is authorized because the group profile DPTSM has *CHANGE authority.

Analysis:

Using group authority in this example is a good method for managing authorities. It reduces the number of private authorities on the system and is easy to understand and audit. However, using private group authority typically causes two searches of private authorities (for the user and the group), when public authority is not adequate. One search of the private authority can be avoided by making DPTSM the primary group for the PRICES file.

Case 2: Using primary group authority

This case demonstrates how to use primary group authority.

ANDERSJ needs *CHANGE authority to the CREDIT file. ANDERSJ is a member of the DPTAR group. Neither ANDERSJ nor DPTAR has *ALLOBJ special authority. Figure 21 on page 188 shows the authorities for the CREDIT file.

```

Display Object Authority
Object . . . . . : CREDIT      Owner . . . . . : OWNAR
Library . . . . . : ACCTSRCV   Primary group . . . : DPTAR
Object type . . . : *FILE      ASP device . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
OWNAR     DPTAR     Authority
          *ALL
          *CHANGE
          *USE

```

Figure 21. Authority for the CREDIT file

The system performs these steps to determine whether to allow ANDERSJ to have *CHANGE access to the CREDIT file:

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1. DPTAR’s authority is primary group authority, not private authority.
 - b. Flowchart 2, steps 2, 3, 4, 5, and 6. Public authority is not sufficient.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = ACCTSRCV/CREDIT *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. ANDERSJ does not own the CREDIT file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, step 1. The CREDIT file has no private authorities.
 - 2) Flowchart 5, step 3. Public authority is not sufficient. Return to Flowchart 3 with no authority found.
 - d. Flowchart 3, steps 5, 7, and 8. The CREDIT file is not secured by an authorization list. Return to Flowchart 1 with no authority found.
3. Flowchart 1, steps 3 and 4. ANDERSJ is a member of the DPTAR group profile.
 - a. Flowchart 6, steps 1 and 2. Object to check = ACCTSRCV/CREDIT *FILE.
 - b. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPTAR does not own the CREDIT file. Return to Flowchart 6 with no authority found.
 - c. Flowchart 6, steps 4 and 5. Authorized. DPTAR is the primary group for the CREDIT file and has *CHANGE authority.

Result:

ANDERSJ is authorized because DPTAR is the primary group for the CREDIT file and has *CHANGE authority.

Analysis:

If you use primary group authority, the authority checking performance is better than if you specify private authority for the group. This example does not require any search of private authorities.

Related concepts:

“Considerations for primary groups for objects” on page 240
 Any object on the system can have a primary group. Primary group authority can provide a performance advantage if the primary group is the first group for most users of an object.

Case 3: Using public authority

This case describes the steps of using public authority.

User JONESP wants to access the CREDIT file using the program CPPGM06. CPPGM06 requires *USE authority to the file. JONESP is a member of group profile DPTSM and does not have *ALLOBJ special authority. The system performs these steps in determining whether to allow JONESP access to the CREDIT file:

Flowchart 1, step 1.

1. Flowchart 2, step 1. The CREDIT file has no private authorities. DPTAR's authority is primary group authority, not private authority.
2. Flowchart 2, steps 2 and 3. Owner's authority (OWNAR) is sufficient.
3. Flowchart 2, steps 4 and 5. Primary group authority (DPTAR) is sufficient.
4. Flowchart 2, step 6. Authorized. Public authority is sufficient.

Analysis:

This example shows the performance benefit gained when you avoid defining any private authorities for an object.

Case 4: Using public authority without searching private authority

This case describes how to use public authority without searching private authority.

User JONESP wants to access the PRICES file using the program CPPGM06. CPPGM06 requires *USE authority to the file. JONESP is a member of group profile DPTSM and does not have *ALLOBJ special authority. The system performs these steps in determining whether to allow JONESP access to the PRICES file:

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1. The PRICES file has private authorities.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. JONESP does not own the PRICES file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1, 2, and 3. Public authority is sufficient.
 - 2) Flowchart 5, step 4. Owner authority is sufficient. (OWNCP has *ALL.)
 - 3) Flowchart 5, step 5. The PRICES file does not have a primary group.
 - 4) Flowchart 5, step 6. Authorized. (The PRICES file is not secured by an authorization list.)

Analysis:

This example shows the performance benefit gained when you avoid defining any private authorities, which are less than public authority, for an object. Although private authority exists for the PRICES file, the public authority is sufficient for this request and can be used without searching private authorities.

Case 5: Using adopted authority

This case demonstrates the performance advantage in using adopted authority.

User SMITHG wants to access the PRICES file using program CPPGM08. SMITHG is not a member of a group and does not have *ALLOBJ special authority. Program CPPGM08 requires *CHANGE authority to the file. CPPGM08 is owned by the profile OWNCP and adopts owner authority (USRPRF is *OWNER).

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. SMITHG does not own the PRICES file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1, 2, and 3. Public is not sufficient.
 - d. Flowchart 3, step 5.
 - e. **Flowchart 3, step 6.** SMITHG does not have private authority.
 - f. Flowchart 3, steps 7 and 8. The PRICES file is not secured by an authorization list. Return to Flowchart 1 with no authority found.
3. Flowchart 1, step 3. SMITHG does not have a group.
4. Flowchart 1, step 5.
 - a. Flowchart 7, step 1. Public authority is not *AUTL.
 - b. Flowchart 7, step 3. Object to check = CONTRACTS/PRICES *FILE.
 - c. Flowchart 7, step 4. Public authority is not sufficient.
5. Flowchart 1, step 6.
 - a. Flowchart 8A, step 1. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 8A, steps 2 and 3. OWNCP does not have *ALLOBJ authority.
 - c. Flowchart 8A, step 4.
 - 1) Flowchart 4, steps 1, 2, and 3. Authorized. OWNCP owns the PRICES files and has sufficient authority.

Analysis:

This example demonstrates the performance advantage in using adopted authority when the program owner also owns the application objects.

The number of steps required to perform authority checking has almost no effect on performance, because most of the steps do not require retrieving new information. In this example, although many steps are performed, private authorities are searched only once (for user SMITHG).

Compare this with Case 1 on page “Case 1: Using private group authority” on page 186.

- If you were to change Case 1 so that the group profile DPTSM owns the PRICES file and has *ALL authority to it, the performance characteristics of the two examples is the same. However, having a group profile own application objects might represent a security exposure. The members of the group always have the group's (owner) authority, unless you specifically give group members less authority. When you use adopted authority, you can control the situations in which owner authority is used.
- You can also change Case 1 so that DPTSM is the primary group for the PRICES file and has *CHANGE authority to it. If DPTSM is the first group for SMITHG (specified in the GRPPRF parameter of SMITHG's user profile), the performance characteristics is the same as Case 5.

Case 6: User and group authority

This case demonstrates that a user can be denied access to an object even though the user's group has sufficient authority.

User WILSONJ wants to access file PRICES using program CPPGM01, which requires *CHANGE authority. WILSONJ is a member of group profile DPTSM and does not have *ALLOBJ special authority. Program CPPGM01 does not use adopted authority, and it ignores any previous adopted authority (USEADPAUT is *NO).

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1. PRICES has private authorities.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. WILSONJ does not own the PRICES file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1, 2, and 3. Public is not sufficient.
 - d. Flowchart 3, step 5.
 - e. **Flowchart 3, step 6.** WILSONJ has *USE authority, which is not sufficient.
 - f. Flowchart 3, step 8. Object to test = CONTRACTS/PRICES *FILE. Return to Flowchart 1 with insufficient authority.
3. Flowchart 1, step 6.
 - a. Flowchart 8A, step 1. Object to check = CONTRACTS/PRICES *FILE.
 - b. Flowchart 8A, step 2. Program CPPGM01 does not adopt authority.
 - c. Flowchart 8A, step 5. The *USEADPAUT parameter for the CPPGM01 program is *NO.
 - d. Flowchart 8A, steps 8 and 9.
 - 1) Flowchart 8B, step 1. Program CPPGM01 does not adopt authority.
 - 2) Flowchart 8B, step 7. The *USEADPAUT parameter for the CPPGM01 program is *NO. Access is denied.

Analysis:

Giving a user the same authority as the public but less than the user's group does not affect the performance of authority checking for other users. However, if WILSONJ had *EXCLUDE authority (less than public), you might lose the performance benefits shown in Case 4.

Although this example has many steps, private authorities are searched only once. This should provide acceptable performance.

Case 7: Public authority without private authority

This case demonstrates the performance advantage of using public authority without private authority.

The authority information for the ITEM file looks like this:

```

                                Display Object Authority
Object . . . . . : ITEM          Owner . . . . . : OWNIC
Library . . . . . : ITEMLIB      Primary group . . . : *NONE
Object type . . . . : *FILE      ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
OWNIC     Group      Authority
*PUBLIC   Group      *ALL
           Group      *USE

```

Figure 22. Display Object Authority

ROSSM needs *USE authority to the ITEM file. ROSSM is a member of the DPTSM group profile. These are the authority-checking steps:

- Flowchart 1, step 1.
- 1. Flowchart 2, steps 1, 2, and 3. OWNIC’s authority is sufficient.
- 2. Flowchart 2, step 4. The ITEM file does not have a primary group.
- 3. Flowchart 2, step 6. Authorized. Public authority is sufficient.

Analysis:

Public authority provides the best performance when it is used without any private authorities. In this example, private authorities are never searched.

Case 8: Adopted authority without private authority

This case shows the advantage of using adopted authority without private authority.

For this example, all programs in the application are owned by the OWNIC profile. Any program in the application requiring more than *USE authority adopts owner authority. These are the steps for user WILSONJ to obtain *CHANGE authority to the ITEM file using program ICPGM10, which adopts authority:

- 1. Flowchart 1, step 1.
 - a. Flowchart 2, steps 1, 2, 3, 4, and 6. Public authority is not sufficient.
- 2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = ITEMLIB/ITEM *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. WILSONJ does not own the ITEM file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1 and 3. Public authority is not sufficient. Return to Flowchart 3 with no authority found.
 - d. Flowchart 3, steps 5, 7, and 8. The ITEM file is not secured by an authorization list. Return to Flowchart 1 with no authority found.
- 3. Flowchart 1, steps 3 and 5. (WILSONJ does not have a group profile.)
 - a. Flowchart 7, steps 1, 3, and 4. The public has *USE authority, which is not sufficient.
- 4. Flowchart 1, step 6.
 - a. Flowchart 8A, step 1. Object to check = ITEMLIB/ITEM *FILE.
 - b. Flowchart 8A, steps 2, 3, and 4. The OWNIC profile does not have *ALLOBJ authority.
 - 1) Flowchart 4, steps 1, 2, and 3. Authorized. OWNIC has sufficient authority to the ITEM file.

Analysis:

This example shows the benefits of using adopted authority without private authority, particularly if the owner of the programs also owns application objects. This example did not require searching private authorities.

Case 9: Using an authorization list

This case demonstrates the advantage of using authorization lists.

The ARWRK01 file in library CUSTLIB is secured by the ARLST1 authorization list. Figure 23 and Figure 24 show the authorities:

Display Object Authority			
Object	: ARWRK01	Owner	: OWNAR
Library	: CUSTLIB	Primary group	: *NONE
Object type	: *FILE	ASP device	: *SYSBAS
Object secured by authorization list. : ARLST1			
User	Group	Object	Authority
OWNCP		*ALL	
*PUBLIC		*USE	

Figure 23. Authority for the ARWRK01 file

Display Authorization List			
Object	: ARLST1	Owner	: OWNAR
Library	: QSYS	Primary group	: *NONE
User	Group	Object	List
		Authority	Mgt
OWNCP		*ALL	
AMESJ		*CHANGE	
*PUBLIC		*USE	

Figure 24. Authority for the ARLST1 authorization list

User AMESJ, who is not a member of a group profile, needs *CHANGE authority to the ARWRK01 file. These are the authority-checking steps:

1. Flowchart 1, step 1.
 - a. Flowchart 2, steps 1 and 2. The ARWRK01 file is secured by an authorization list.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CUSTLIB/ARWRK01 *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. AMESJ does not own the ARWRK01 file. Return to Flowchart 2 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1 and 3. Public authority is not sufficient. Return to Flowchart 3 with no authority found.
 - d. Flowchart 3, steps 5, 7, and 9. Object to check = ARLST1 *AUTL.
 - e. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. AMESJ does not own the ARLST1 authorization list. Return to Flowchart 3 with no authority found.

- f. Flowchart 3, steps 4 and 5.
- g. Flowchart 3, step 6. Authorized. AMESJ has *CHANGE authority to the ARLST1 authorization list.

Analysis:

This example demonstrates that authorization lists can make authorities easy to manage and provide good performance. This is particularly true if objects secured by the authorization list do not have any private authorities.

If AMESJ were a member of a group profile, it will add additional steps to this example, but it will not add an additional search of private authorities, as long as no private authorities are defined for the ARWRK01 file. Performance problems are most likely to occur when private authorities, authorization lists, and group profiles are combined, as in “Case 11: Combining authorization methods” on page 195.

Case 10: Using multiple groups

This is an example of using multiple groups.

WOODBC needs *CHANGE authority to the CRLIM file. WOODBC is a member of three groups: DPTAR, DPTSM, and DPTMG. DPTAR is the first group profile (GRPPRF). DPTSM and DPTMG are supplemental group profiles (SUPGRPPRF). Figure 25 shows the authorities for the CRLIM file:

Display Object Authority		
Object	: CRLIM	Owner : OWNAR
Library	: CUSTLIB	Primary group : DPTAR
Object type	: *FILE	ASP device : *SYSBAS
Object secured by authorization list : *NONE		
User	Group	Object Authority
OWNAR		*ALL
DPTAR		*CHANGE
DPTSM		*USE
*PUBLIC		*EXCLUDE

Figure 25. Authority for the CRLIM file

These are the authority checking steps:

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1. Return to calling flowchart with insufficient authority.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CUSTLIB/CRLIM *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. WOODBC does not own the CRLIM file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.
 - 1) Flowchart 5, steps 1, 2 and 3. Public authority is not sufficient.
 - d. Flowchart 3, step 5.
 - e. Flowchart 3, step 6. WOODBC does not have any authority to the CRLIM file.
 - f. Flowchart 3, steps 7 and 8. The CRLIM file is not secured by an authorization list. Return to Flowchart 1 with no authority found.
3. Flowchart 1, steps 3 and 4. The first group for WOODBC is DPTAR.
 - a. Flowchart 6, steps 1 and 2. Object to check = CUSTLIB/CRLIM *FILE.

- b. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPTAR does not own the CRLIM file. Return to Flowchart 6 with no authority found.
- c. Flowchart 6, steps 4 and 5. Authorized. DPTAR is the primary group and has sufficient authority.

Case 11: Combining authorization methods

This case shows a poor authority design.

WAGNERB needs *ALL authority to the CRLIMWRK file. WAGNERB is a member of these groups: DPTSM, DPT702, and DPTAR. WAGNERB's first group (GRPPRF) is DPTSM. Figure 26 shows the authority for the CRLIMWRK file.

Display Object Authority			
Object	:	CRLIMWRK	Owner : OWNAR
Library	:	CUSTLIB	Primary group : *NONE
Object type	:	*FILE	ASP device : *SYSBAS
Object secured by authorization list : CRLST1			
User	Group	Object Authority	
OWNAR		*ALL	
DPTSM		*USE	
WILSONJ		*EXCLUDE	
*PUBLIC		*USE	

Figure 26. Authority for CRLIMWRK file

The CRLIMWRK file is secured by the CRLST1 authorization list. Figure 27 shows the authority for the CRLST1 authorization list.

Display Authorization List			
Object	:	CRLST1	Owner : OWNAR
Library	:	QSYS	Primary Group : DPTAR
User	Group	Object Authority	List Mgt
OWNAR		*ALL	X
DPTAR		*ALL	
*PUBLIC		*EXCLUDE	

Figure 27. Authority for the CRLST1 authorization list

This example shows many of the possibilities for authority checking. It also demonstrates how using too many authority options for an object can result in poor performance.

Following are the steps required to check WAGNERB's authority to the CRLIMWRK file:

1. Flowchart 1, step 1.
 - a. Flowchart 2, step 1.
2. Flowchart 1, step 2.
 - a. Flowchart 3, steps 1 and 2. Object to check = CUSTLIB/CRLIMWRK *FILE.
 - b. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. WAGNERB does not own the CRLIMWRK file. Return to Flowchart 3 with no authority found.
 - c. Flowchart 3, step 4.

- 1) Flowchart 5, steps 1 and 2. WILSONJ has *EXCLUDE authority, which is less than the public authority of *USE.
- d. Flowchart 3, steps 5 and 6 (**first search of private authorities**). WAGNERB does not have private authority.
- e. Flowchart 3, steps 7 and 9. Object to check = CRLST1 *AUTL.
- f. Flowchart 3, step 3.
 - 1) Flowchart 4, step 1. WILSONJ does not own CRLST1. Return to Flowchart 3 with no authority found.
- g. Flowchart 3, steps 4 and 5.
- h. Flowchart 3, step 6 (**second search of private authorities**). WAGNERB does not have private authority to CRLST1.
- i. Flowchart 3, steps 7 and 8. Object to check = CUSTLIB/CRLIMWRK *FILE.
- 3. Flowchart 1, steps 3 and 4. WAGNERB's first group profile is DPTSM.
 - a. Flowchart 6, steps 1 and 2. Object to check = CUSTLIB/CRLIMWRK *FILE.
 - b. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPTSM does not own the CRLIMWRK file. Return to Flowchart 6 with no authority found.
 - c. Flowchart 6, step 4. DPTSM is not the primary group for the CRLIMWRK file.
 - d. Flowchart 6, step 6 (**third search of private authorities**). DPTSM has *USE authority to the CRLIMWRK file, which is not sufficient.
 - e. Flowchart 6, step 6 continued. *USE authority is added to any authorities already found for WAGNERB's groups (none). Sufficient authority has not yet been found.
 - f. Flowchart 6, steps 9 and 10. WAGNERB's next group is DPT702.
 - g. Flowchart 6, steps 1 and 2. Object to check = CUSTLIB/CRLIMWRK *FILE.
 - h. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPT702 does not own the CRLIMWRK file. Return to Flowchart 6 with no authority found.
 - i. Flowchart 6, step 4. DPT702 is not the primary group for the CRLIMWRK file.
 - j. Flowchart 6, step 6 (**fourth search of private authorities**). DPT702 has no authority to the CRLIMWRK file.
 - k. Flowchart 6, steps 7 and 8. Object to check = CRLST1 *AUTL
 - l. Flowchart 6, step 3.
 - 1) Flowchart 5, step 1. DPT702 does not own the CRLST1 authorization list. Return to Flowchart 6 with no authority found.
 - m. Flowchart 6, steps 4 and 6. (**fifth search of private authorities**). DPT702 has no authority to the CRLST1 authorization list.
 - n. Flowchart 6, steps 7, 9, and 10. DPTAR is WAGNERB's next group profile.
 - o. Flowchart 6, steps 1 and 2. Object to check = CUSTLIB/CRLIMWRK *FILE.
 - p. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPTAR does not own the CRLIMWRK file. Return to Flowchart 6 with no authority found.
 - q. Flowchart 6, steps 4 and 6. (**sixth search of private authorities**). DPTAR has no authority to the CRLIMWRK file.
 - r. Flowchart 6, steps 7 and 8. Object to check = CRLST1 *AUTL
 - s. Flowchart 6, step 3.
 - 1) Flowchart 4, step 1. DPTAR does not own the CRLST1 authorization list. Return to Flowchart 6 with no authority found.

- t. Flowchart 6, steps 4 and 5. Authorized. DPTAR is the primary group for the CRLST1 authorization list and has *ALL authority.

Result:

WAGNERB is authorized to perform the requested operation using DPTAR's primary group authority to the CRLST1 authorization list.

Analysis:

This example demonstrates poor authority design, both from a management and performance standpoint. Too many options are used, making it difficult to understand, change, and audit. Private authorities are searched 6 separate times, which might cause noticeable performance problems:

Profile	Object	Type	Result
WAGNERB	CRLIMWRK	*FILE	No authority found
WAGNERB	CRLST1	*AUTL	No authority found
DPTSM	CRLIMWRK	*FILE	*USE authority (insufficient)
DPT702	CRLIMWRK	*FILE	No authority found
DPT702	CRLST1	*AUTL	No authority found
DPTAR	CRLIMWRK	*FILE	No authority found

Changing the sequence of WAGNERB's group profiles changes the performance characteristics of this example. Assume that DPTAR is WAGNERB's first group profile (GRPPRF). The system searches private authorities 3 times before finding DPTAR's primary group authority to the CRLST1 authorization list.

- WAGNERB authority for CRLIMWRK file
- WAGNERB authority for CRLST1 authorization list
- DPTAR authority for CRLIMWRK file

Careful planning of group profiles and authorization lists is essential to good system performance.

Authority cache

The system creates authority caches for users to provide flexibility and performance enhancement.

Since Version 3, Release 7, the system creates an authority cache for a user the first time the user accesses an object. Each time the object is accessed, the system looks for authority in the user's cache before looking at the user's profile. This results in a faster check for private authority.

The authority cache contains up to 32 private authorities to objects and up to 32 private authorities to authorization lists. The cache is updated when a user authority is granted or revoked. All user caches are cleared when the system IPL is performed.

While limited use of private authorities is recommended, the cache offers flexibility. For example, you can choose how to secure objects with less concern about the effect on system performance. This is especially true if users access the same objects repeatedly.

Chapter 6. Work management security

This section discusses security issues associated with work management on the system.

The following issues are described in this section.

Related information:

Work management

Job initiation

The system checks the authority to some objects when a job is started.

When you start a job on the system, objects are associated with the job, such as an output queue, a job description, and the libraries on the library list. Authority to some of these objects is checked before the job is allowed to start, while authority to other objects is checked after the job starts. Inadequate authority might cause errors or may cause the job to end.

Objects that are part of the job structure for a job can be specified in the job description, the user profile, and on the Submit Job (SBMJOB) command for a batch job.

Starting an interactive job

This topic is a description of the security activity performed when an interactive job is started.

Because many possibilities exist for specifying the objects used by a job, this is only an example.

When an authority failure occurs during the sign-on process, a message appears at the bottom of the Sign On display describing the error. Some authority failures also cause a job log to be written. If a user is unable to sign on because of an authority failure, either change the users profile to specify a different object or grant the user authority to the object.

After the user enters a user ID and password, these steps are performed before a job is actually started on the system:

1. The user profile and password are verified. The status of the user profile must be *ENABLED. The user profile that is specified on the sign-on display must have *OBJOPR, and *CHANGE authority to itself.
2. The user's authority to use the workstation is checked. See "Workstations" on page 201 for details.
3. The system verifies authority for the values in the user profile and in the user's job description that are used to build the job structure, such as:
 - Job description
 - Output queue
 - Current library
 - Libraries in library list

If any of these objects does not exist or the user does not have adequate authority, a message is displayed at the bottom of the Sign On display, and the user is unable to sign on. If authority is successfully verified for these objects, the job is started on the system.

Note: Authority to the print device and job queue is not verified until the user attempts to use them.

After the job is started, these steps are performed before the user sees the first display or menu:

1. If the routing entry for the job specifies a user program, normal authority checking is done for the program, the program library, and any objects used by the program. If authority is not adequate, a message is sent to the user on the Sign On display and the job ends.
2. If the routing entry specifies the command processor (QCMD):
 - a. Authority checking is done for the QCMD processor program, the program library, and any objects used, as described in step 1.
 - b. The user's authority to the Attention-key-handling program and library is checked. If authority is not adequate, a message is sent to the user and written to the job log. Processing continues. If authority is adequate, the Attention-key-handling program is activated. The program is not started until the first time the user presses the Attention key. At that time, normal authority checking is done for the objects used by the program.
 - c. Normal authority checking is done for the initial program (and its associated objects) specified in the user profile. If authority is adequate, the program is started. If authority is not adequate, a message is sent to the user and written to the job log. The job ends.
 - d. Normal authority checking is done for the initial menu (and its associated objects) specified in the user profile. If authority is adequate, the menu is displayed. If authority is not adequate, a message is sent to the user and written to the job log. The job ends.

Starting a batch job

This topic includes a description of the security activity performed when a batch job is started.

Because several methods exist for submitting batch jobs and for specifying the objects used by the job, this is only a guideline. This example uses a job submitted from an interactive job using the submit job (SBMJOB) command.

When you enter the SBJJOB command, this checking is performed before the job is added to the job queue:

1. If you specify a user profile on the SBJJOB command, you must have *USE authority to the user profile.
2. Authority is checked for objects specified as parameters on the SBJJOB command and in the job description. Authority is checked for the user profile the job will run under.
3. If the security level is 40 or 50 and the SBJJOB command specifies USER(*JOB), the user submitting the job must have *USE authority to the user profile in the job description.
4. If an object does not exist or if authority is not adequate, a message is sent to the user and the job is not submitted.

When the system selects the job from the job queue and attempts to start the job, the authority checking sequence is similar to the sequence for starting an interactive job.

Adopted authority and batch jobs

You can change the parameters for a batch job when it is running under adopted authority.

When a new job is started, a new call stack is created for the job. Adopted authority cannot take effect until the first program is added to the call stack. Adopted authority cannot be used to gain access to any objects, such as an output queue or a job description, which are added to the job structure before the job is routed. Therefore, even if your interactive job is running under adopted authority when you submit a job, that adopted authority is not used when authority is checked for the objects on your SBJJOB request.

You can change characteristics of a batch job when it is waiting to run, using the Change Job (CHGJOB) command. See Job commands for the authority that is required to change parameters for a job.

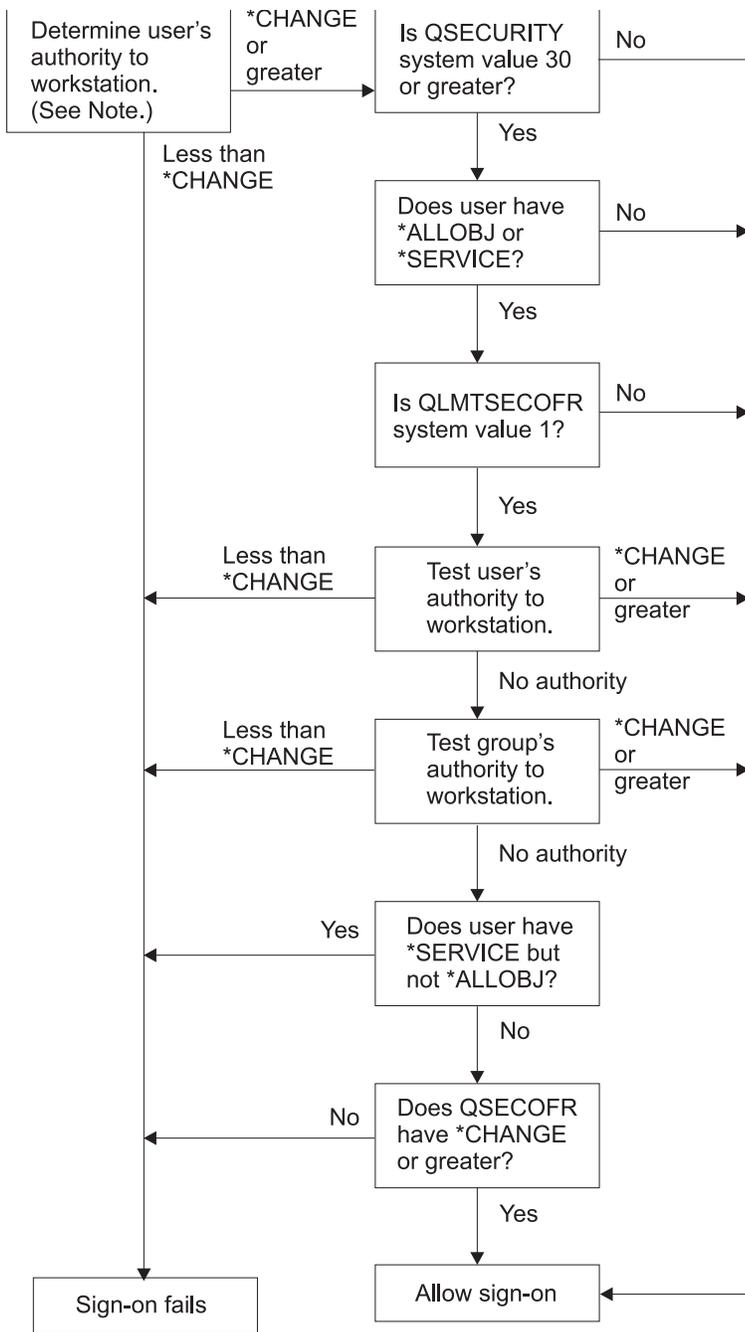
Workstations

The system performs authority checking for a workstation when you sign on.

A *device description* contains information about a particular device or logical unit that is attached to the system. When you sign on the system, your workstation is attached to either a physical or virtual device description. To successfully sign on, you must have *CHANGE authority to the device description.

The QLMTSECOFR (limit security officer) system value controls whether users with *ALLOBJ or *SERVICE special authority must be specifically authorized to device descriptions.

Figure 28 on page 202 shows the logic for determining whether a user is allowed to sign on at a device:



RBAFW529-0

Figure 28. Authority checking for workstations

Note: Normal authority checking is performed to determine whether the user has at least *CHANGE authority to the device description. *CHANGE authority can be found by using the following authorities:

- *ALLOBJ special authority from the user profile, group profile, or supplemental group profiles.
- Private authority to the device description in the user profile, the group profile, or supplemental group profiles.
- Authority to an authorization list used to secure the device description.
- Authority to an authorization list used to secure the public authority.

Authority checking for the device description is done before any programs are in the call stack for the job; therefore, adopted authority does not apply.

Description of authority checking for workstations

The system determines the user's authority to the workstation. (See note 1) If the authority is less than *CHANGE, the sign-on fails. If the authority is *CHANGE or greater, the system checks if the security level on the system is 30 or higher. If it is not, then the user is allowed to sign-on.

If the security level is 30 or higher, the system checks if the user has *ALLOBJ or *SERVICE special authority. If the user does not have either of these special authorities, then sign-on is allowed.

If the user has either *ALLOBJ or *SERVICE special authorities, then the system checks if the QLMTSECOFR system value is set to 1. If it is not set to 1, then sign-on is allowed.

If the QLMTSECOFR system value is set to 1, then the system will test the user's authority to the workstation. If the user's authority is *CHANGE or higher, then sign-on is allowed. If the user's authority is less than *CHANGE, sign-on fails. If the user has no authority to the workstation, the system checks the user's group authority to the workstation.

If the user's group authority is *CHANGE or higher, then sign-on is allowed. If the user's group authority is less than *CHANGE, sign-on fails. If the user's group has no authority to the workstation, the system checks whether the user has *SERVICE but not *ALLOBJ special authority.

If the user has *SERVICE but not *ALLOBJ special authority, then sign-on fails. If the user has *ALLOBJ special authority, then the system checks if QSECOFR has *CHANGE or higher.

If QSECOFR does not have *CHANGE or higher, then sign-on fails. If QSECOFR has *CHANGE or higher, then sign-on is allowed.

The security officer (QSECOFR), service (QSRV), and basic service (QSRVBAS) user profiles are always allowed to sign on at the console. The QCONSOLE (console) system value is used to determine which device is the console. If the QSRV or QSRVBAS profile attempts to sign on at the console and does not have *CHANGE authority, the system grants *CHANGE authority to the profile and allows sign-on.

Ownership of device descriptions

You can specify the ownership of device descriptions to control the authority to the devices.

The default public authority on the CRTDEVxxx commands is *CHANGE. Devices are created in the library QSYS, which is shipped with a CRTAUT value of *SYSVAL. The shipped value for the QCRTAUT system value is *CHANGE.

To limit the users who can sign on at a workstation, set the public authority for the workstation to *EXCLUDE and give *CHANGE authority to specific users or groups.

The security officer (QSECOFR) is not specifically given authority to any devices. If the QLMTSECOFR system value is set to 1 (YES), you must give the security officer *CHANGE authority to devices. Anyone with *OBJMGT and *CHANGE authority to a device can give *CHANGE authority to another user.

If a device description is created by the security officer, the security officer owns that device and is specifically given *ALL authority to it. When the system automatically configures devices, most devices are owned by the QPGMR profile. Devices created by the QLUS program (*APPC type devices) are owned by the QSYS profile.

If you plan to use the QLMTSECOFR system value to limit where the security officer can sign on, any devices you create should be owned by a profile other than QSECOFR.

To change ownership of a display device description, the device must be powered on and varied on. Sign on at the device and change the ownership using the CHGOBJOWN command. If you are not signed on at the device, you must allocate the device before changing ownership, using the Allocate Object (ALCOBJ) command. You can allocate the device only if no one is using it. After you have changed ownership, deallocate the device using the Deallocate Object (DLCOBJ) command.

Signon screen display file

The system administrator can change the system signon display to add text or company logo to the display.

When changing the signon screen display file, the system administrator must make sure not to change the field names or buffer lengths of the display file when adding text to the display file. Changing the field names or buffer lengths can cause signon to fail.

Changing the signon screen display

You can change the source code for the signon display file to change the screen display.

The source code for the signon display file is shipped with the operating system. The source is shipped in file QSYS/QAWTSSRC. This source code can be changed to add text to the signon screen display. Field names and buffer lengths should not be changed.

Display file source for the signon screen

You need to copy the appropriate source file to create your own signon screen display.

The source for the signon display file is shipped as a member (QDSIGNON or QDSIGNON2) in the QSYS/QAWTSSRC physical file. QDSIGNON contains the source for the signon screen source used when system value QPWDLVL is set to 0 or 1. Member QDSIGNON2 contains the signon screen source used when the system value QPWDLVL is set to 2 or 3.

The file QSYS/QAWTSSRC is **deleted and restored** each time the i5/OS operating system is installed. If you plan to create your own version of the signon screen, then you should first copy the appropriate source file member, either QDSIGNON or QDSIGNON2, to your own source file and make changes to the copy in your source file.

Changing the signon display file

This topic includes the steps for changing the signon display file.

To change the format of the Signon display, perform the following steps:

1. Create a changed signon display file.

A hidden field in the display file named UBUFFER can be changed to manage smaller fields.

UBUFFER is 128 bytes long and is stated as the last field in the display file. This field can be changed to function as an input/output buffer so the data specified in this field of the display will be available to application programs when the interactive job is started. You can change the UBUFFER field to contain as many smaller fields as you need if the following requirements are met:

- The new fields must follow all other fields in the display file. The location of the fields on the display does not matter as long as the order in which they are put in the data description specifications (DDS) meets this requirement.
- The length must total 128. If the length of the fields is more than 128, some of the data will not be passed to the application.

- All fields must be input/output fields (type B in DDS source) or hidden fields (type H in DDS source).
2. The order in which the fields in the signon display file are declared must not be changed. The position in which they are shown on the display can be changed. Do not change the existing field names in the source for the signon screen display file.
 3. Do not change the total size of the input or output buffers. Serious problems can occur if the order or size of the buffers is changed.
 4. Do not use the data descriptions specifications (DDS) help function in the signon display file.
 5. Change a subsystem description to use the changed display file instead of the system default of QSYS/QDSIGNON. You can change the subsystem descriptions for subsystems that you want to use the new display. To change the subsystem description, perform the following steps:
 - a. Use the Change Subsystem Description (CHGSBSD) command.
 - b. Specify the new display file on the SGNDSPF parameter.
 - c. Use a test version of a subsystem to verify that the display is valid before attempting to change the controlling subsystem.
 6. Test the change.
 7. Change the other subsystem descriptions.

Notes:

1. The buffer length for the display file must be 318. If it is less than 318, the subsystem uses the default sign-on display, QDSIGNON in library QSYS when system value QPWDLVL is 0 or 1 and QDSIGNON2 in library QSYS when QPWDLVL is 2 or 3.
2. The copyright line cannot be deleted.

Subsystem descriptions

The subsystem descriptions perform several functions on the system.

Subsystem descriptions control:

- How jobs enter your system
- How jobs are started
- Performance characteristics of jobs

Only a few users should be authorized to change subsystem descriptions, and changes should be carefully monitored.

Related concepts:

“Signing on without a user ID and password” on page 16

Your security level determines how the system controls signing on without a user ID and password.

Controlling how jobs enter the system

You can use the subsystem descriptions to control how jobs enter the system.

Several subsystem descriptions are shipped with your system. After you have changed your security level (QSECURITY system value) to level 20 or higher, signing on without entering a user ID and password is not allowed with the subsystems shipped by IBM.

However, defining a subsystem description and job description combination that allows default sign-on (no user ID and password) is possible and represents a security exposure. When the system routes an interactive job, it looks at the workstation entry in the subsystem description for a job description. If the

job description specifies USER(*RQD), the user must enter a valid user ID (and password) on the Sign On display. If the job description specifies a user profile in the *User* field, anyone can press the Enter key to sign on as that user.

At security levels 30 and higher, the system logs an entry (type AF, sub-type S) in the audit journal, if default signon is attempted and the auditing function is active. At security level 40 and higher, the system does not permit default signon, even if a combination of workstation entry and job description exists that allows it. See "Signing on without a user ID and password" on page 16 for more information.

Make sure all workstation entries for interactive subsystems refer to job descriptions with USER(*RQD). Control the authority to change job descriptions and monitor any changes that are made to job descriptions. If the auditing function is active, the system writes a JD type journal entry every time the USER parameter in a job description is changed.

Communications entries in a subsystem description control how communications jobs enter your system. A communications entry points to a default user profile, which allows a job to be started without a user ID and password. This represents a potential security exposure. Evaluate the communications entries on your system and use network attributes to control how communications jobs enter your system. "Network attributes" on page 214 discusses the network attributes that are important for security.

Job descriptions

A job description is a valuable tool for security and work management.

You can also set up a job description for a group of users who need the same initial library list, output queue, and job queue. You can set up a job description for a group of batch jobs that have similar requirements.

A job description also represents a potential security exposure. In some cases, a job description that specifies a profile name for the USER parameter can allow a job to enter the system without appropriate security checking. "Controlling how jobs enter the system" on page 205 discusses how this can be prevented for interactive and communications jobs.

When a batch job is submitted, the job might run using a different profile other than the user who submitted the job. The profile can be specified on the SBMJOB command, or it can come from the USER parameter of the job description. If your system is at security level (QSECURITY system value) 30 or lower, the user submitting a job needs authority to the job description but not to the user profile specified on the job description. This represents a security exposure. At security level 40 and higher, the submitter needs authority to both the job description and the user profile.

For example:

- USERA is not authorized to file PAYROLL.
- USERB has *USE authority to the PAYROLL file and to program PRLIST, which lists the PAYROLL file.
- Job description PRJOB D specifies USER(USERB). Public authority for PRJOB D is *USE.

At security level 30 or lower, USERA can list the payroll file by submitting a batch job:

```
SBMJOB RQSDTA("Call PRLIST") JOBD(PRJOB D) +  
      USER(*JOB D)
```

You can prevent this by using security level 40 and higher or by controlling the authority to job descriptions that specify a user profile.

Sometimes, a specific user profile name in a job description is required for certain types of batch work to function properly. For example, the QBATCH job description is shipped with USER(QPGMR). This job description is shipped with the public authority of *EXCLUDE.

If your system is at security level 30 or lower, any user on the system who has authority to the Submit Job (SBMJOB) command or the start reader commands, and has *USE authority to the QBATCH job description, can submit work under the programmer (QPGMR) user profile, whether the user has authority to the QPGMR profile. At security level 40 and higher, *USE authority to the QPGMR profile is also required.

System operator message queue

You can specify the authorities to control access to the system operator message queue

The IBM i Operational Assistant (ASSIST) menu provides an option to manage your system, users, and devices. The Manage Your System, Users, and Devices menu provides an option to work with system operator messages. You might want to prevent users from responding to messages in the QSYSOPR (system operator) message queue. Incorrect responses to system operator messages can cause problems on your system.

Responding to messages requires *USE and *ADD authorities to the message queue. Removing messages requires *USE and *DLT authorities (See Message commands.) Give the authority to respond to and remove messages in QSYSOPR only to users with system operator responsibility. Public authority to QSYSOPR should be *OBJOPR and *ADD, which allows adding new messages to QSYSOPR.

Attention: All jobs need the ability to add new messages to the QSYSOPR message queue. Do not make the public authority to QSYSOPR *EXCLUDE.

Library lists

The **library list** for a job indicates which libraries are to be searched and the order in which they are to be searched.

When a program specifies an object, the object can be specified with a qualified name, which includes both the object name and the library name. Or, the library for the object can be specified as *LIBL (library list). The libraries on the library list are searched, in order, until the object is found.

Table 125 summarizes the parts of the library list and how they are built during a job. The sections that follow discuss the risks and protection measures for library lists.

Table 125. Parts of the library list. The library list is searched in this sequence:

Part	How it is built
System Portion 15 entries	Initially built using the QSYSLIBL system value. Can be changed during a job with the CHGSYSLIBL command.
Product Library Portion 2 entries	Initially blank. A library is added to the product library portion of the library list when a command or menu runs that was created with a library in the PRDLIB parameter. The library remains in the product library portion of the library list until the command or menu ends.
Current Library 1 entry	Specified in the user profile or on the Sign On display. Can be changed when a command or menu runs that specifies a library for the CURLIB parameter. Can be changed during the job with the CHGCURLIB command.
User Portion 250 entries	Initially built using the initial library list from the user's job description. If the job description specifies *SYSVAL, the QUSRLIBL system value is used. During a job, the user portion of the library list can be changed with the ADDLIBL, RMVLIBL, CHGLIBL, and EDTLIBL commands.

Related concepts:

"Library security and library lists" on page 135

When a library is added to a user's library list, the authority the user has to the library is stored with the

library list information.

“Planning libraries” on page 225

A library is like a directory used to locate the objects in the library. Many factors affect how you choose to group your application information into libraries and manage libraries.

Security risks of library lists

This topic gives specific examples of the possible security exposures of library lists and how to avoid them.

Library lists represent a potential security exposure. If a user is able to change the sequence of libraries on the library list, or add additional libraries to the list, the user might be able to perform functions that break your security requirements.

“Library security and library lists” on page 135 provides some general information about the issues associated with library lists.

This section provides two examples of how changes to a library list might break security requirements.

Change in function

This example shows the possible risk of a change in function when calling a program in the library.

Figure 29 shows an application library. Program A calls Program B, which is expected to be in LIBA. Program B performs updates to File A. Program B is called without a qualified name, so the library list is searched until Program B is found.

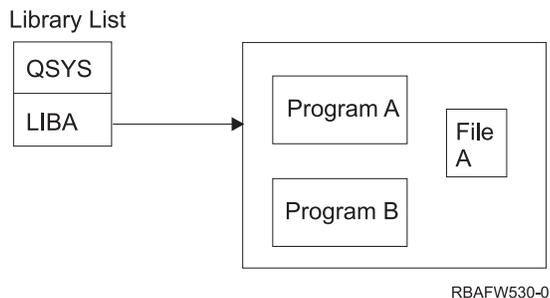


Figure 29. Library list—expected environment

A programmer or another knowledgeable user might place another Program B in the library LIBB. The substitute program might perform different functions, such as making a copy of confidential information or updating files incorrectly. If LIBB is placed ahead of LIBA in the library list, the substitute Program B is run instead of the original Program B, because the program is called without a qualified name:

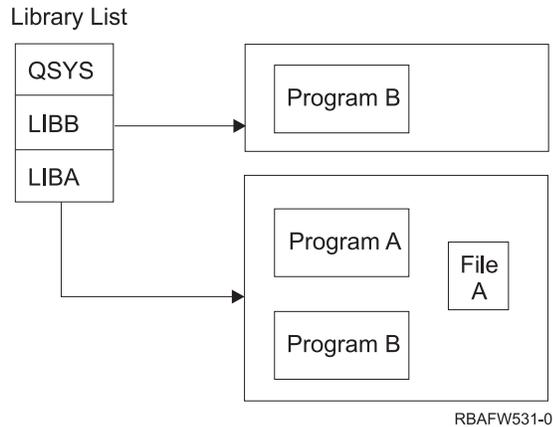


Figure 30. Library list–actual environment

Unauthorized access to information

The example demonstrates the potential risk of unauthorized access to information in the library.

Assume Program A in Figure 29 on page 208 adopts the authority of USER1, who has *ALL authority to File A. Assume that Program B is called by Program A (adopted authority remains in effect). A knowledgeable user can create a substitute Program B that just calls the command processor. The user will have a command line and complete access to File A.

Recommendations for system portion of library list

This topic provides the recommendations for the system portion of the library list.

The system portion of the library list is intended for IBM-supplied libraries. Application libraries that are carefully controlled can also be placed in the system portion of the library list. The system portion of the library list represents the greatest security exposure, because the libraries in this part of the list are searched first.

Only a user with *ALLOBJ and *SECADM special authority can change the QSYSLIBL system value. Control and monitor any changes to the system portion of the library list. Follow these guidelines when adding libraries:

- Only libraries that are specifically controlled should be placed on this list.
- The public should not have *ADD authority to these libraries.
- A few IBM-supplied libraries, such as QGPL are shipped with public authority *ADD for production reasons. Regularly monitor what objects (particularly programs, source files, and commands) are added to these libraries.

The CHGSYSLIBL command is shipped with public authority *EXCLUDE. Only users with *ALLOBJ authority are authorized to the command, unless you grant authority to other users. If the system library list needs to be changed temporarily during a job, you can use the technique described in the topic “Changing the system library list” on page 227.

Recommendations for product library

In this topic you will find the recommendations for protecting the product library.

The product library portion of the library list is searched before the user portion. A knowledgeable user can create a command or menu that inserts a product library into the library list. For example, this statement creates CMDX, which runs program PGMA:

As long as CMDX is running, LIBB is in the product portion of the library list.

Use these measures to protect the product portion of the library list:

- Control authority to the Create Command (CRTCMD), Change Command (CHGCMD), Create Menu (CRTMNU), and Change Menu (CHGMNU) commands.
- When you create commands and menus, specify PRDLIB(*NONE), which removes any entries currently in the product portion of the library list. This protects you from having unknown libraries searched ahead of the library you expect when your command or menu runs.

Note: The default when you create a command or menu is PRDLIB(*NOCHG). *NOCHG means that when the command or menu is run, the product library portion of the library list is not changed.

Recommendations for the current library

This topic provides the recommendations to ensure the security of your system when using the current library.

The current library can be used by decision-support tools, such as Query/400. Any query programs created by a user are, by default, placed in the user's current library. When you create a menu or command, you can specify a current library to be used while the menu is active.

The current library provides an easy method for the user and the programmer to create new objects, such as query programs, without worrying about where they should be located. However, the current library poses a security risk, because it is searched before the user portion of the library list. You can take several precautions to protect the security of your system while still making use of the current library capability:

- Specify *YES for the *Limit capabilities* field in the user profile. This prevents a user from changing the current library on the Sign On display or using the CHGPRF command.
- Restrict authority to the Change Current Library (CHGCURLIB), Create Menu (CRTMNU), Change Menu (CHGMNU), Create Command (CRTCMD), and Change Command (CHGCMD) commands.
- Use the technique described in "Controlling the user library list" on page 226 to set the current library during application processing.

Recommendations for the user portion of the library list

In this topic you will find the recommendations for controlling the user portion of the library list.

The user portion of the library list often changes more than the other portions and is more difficult to control. Many application programs change the library list. Job descriptions also affect the library list for a job.

Here are some suggested alternatives for controlling the user portion of the library list to make sure that unauthorized libraries with substitute programs and files are not used during processing:

- Restrict users of production applications to a menu environment. Set the *Limit capabilities* field in user profiles to *YES to restrict their ability to enter commands. "Planning menus" on page 228 provides an example of this environment.
- Use qualified names (object and library) in your applications. This prevents the system from searching the library list to find an object.
- Control the ability to change job descriptions, because the job description sets the initial library list for a job.
- Use the Add Library List Entry (ADDLIBLE) command at the beginning of the program to ensure the required objects are at the beginning of the user portion of the library list. At the end of the program, the library can be removed.

If the library is already on the library list, but you are not sure if it is at the beginning of the list, you must remove the library and add it. If the sequence of the library list is important to other applications on the system, use the next method instead.

- Use a program that retrieves and saves the library list for a job. Replace the library list with the list required for the application. When the application ends, return the library list to its original setting. See “Controlling the user library list” on page 226 for an example of this technique.

Printing

You can control the security of the output queues on your system.

Most information that is printed on your system is stored as a spooled file on an output queue while it is waiting to print. Unless you control the security of output queues on your system, unauthorized users can display, print, and even copy confidential information that is waiting to print.

One method for protecting confidential output is to create a special output queue. Send confidential output to the output queue and control who can view and manipulate the spooled files on the output queue.

To determine where output goes, the system looks at the printer file, job attributes, user profile, workstation device description, and the print device (QPRTDEV) system value in sequence. If defaults are used, the output queue associated with the QPRTDEV printer is used. The Advanced Function Presentation topic provides examples of how to direct output to a particular output queue.

Securing spooled files

You can specify several parameters to control the security of a spooled file.

A spooled file is a special type of object on the system. You cannot directly grant and revoke authority to view and manipulate a spooled file. The authority to a spooled file is controlled by several parameters on the output queue that holds the spooled file.

When you create a spooled file, you are the owner of that file. You can always view and manipulate any spooled files you own, regardless of how the authority to the output queue is defined. You must have *READ authority to add new entries to an output queue. If your authority to an output queue is removed, you can still access any entries you own on that queue using the Work with Spooled Files (WRKSPLF) command.

The security parameters for an output queue are specified using the Create Output Queue (CRTOUTQ) command or the Change Output Queue (CHGOUTQ) command. You can display the security parameters for an output queue using the Work with Output Queue Description (WRKOUTQD) command.

Attention: A user with *SPLCTL special authority can perform all functions on all entries, regardless of how the output queue is defined. Some parameters on the output queue allow a user with *JOBCTL special authority to view the contents of entries on the output queue.

Display Data (DSPDTA) parameter of output queue

You can specify the Display Data (DSPDTA) parameter to protect the contents of a spooled file.

The DSPDTA parameter determines what authority is required to perform the following functions on spooled files owned by other users:

- View the contents of a spooled file (DSPSPLF command)
- Copy a spooled file (CPYSPLF command)
- Send a spooled file (SNDNETSPLF command)
- Move a spooled file to another output queue (CHGSPLFA command)

<i>Possible values for DSPDTA</i>	
*NO	A user cannot display, send, or copy spooled files owned by other users, unless the user has one of the following authorities: <ul style="list-style-type: none"> • *JOBCTL special authority if the OPRCTL parameter is *YES. • *READ, *ADD, and *DLT authority to the output queue if the *AUTCHK parameter is *DTAAUT. • Ownership of the output queue if the *AUTCHK parameter is *OWNER.
*YES	Any user with *READ authority to the output queue can display, copy, or send the data of spooled files owned by others.
*OWNER	Only the owner of a spooled file or a user with *SPLCTL (spool control) can display, copy, send, or move the file. If the OPRCTL value is *YES, users with *JOBCTL special authority can hold, change, delete, and release spooled files on the output queue, but they cannot display, copy, send, or move the spooled files. This is intended to allow operators to manage entries on an output queue without being able to view the contents.

Authority to Check (AUTCHK) parameter of output queue

You can use the Authority to Check (AUTCHK) parameter to control a user's authority to change or delete a spooled file on your system.

The AUTCHK parameter determines whether *READ, *ADD, and *DLT authority to the output queue allows a user to change and delete spooled files owned by other users.

<i>Possible values for AUTCHK</i>	
*OWNER	Only the user who owns the output queue can change or delete spooled files owned by others.
*DTAAUT	Specifies that any user with *READ, *ADD, and *DLT authority to the output queue can change or delete spooled files owned by others.

Operator Control (OPRCTL) parameter of output queue

The Operator Control (OPRCTL) parameter determines whether a user with *JOBCTL special authority can control the output queue.

<i>Possible values for OPRCTL</i>	
*YES	A user with *JOBCTL special authority can perform all functions on the spooled files, unless the DSPDTA value is *OWNER. If the DSPDTA value is *OWNER, *JOBCTL special authority does not allow the user to display, copy, send, or move spooled files.
*NO	*JOBCTL special authority does not give the user any authority to perform operations on the output queue. Normal authority rules apply to the user.

Output queue and parameter authorities required for printing

This topic includes the reference information about the output queue parameters and authorities required for performing printing management functions.

Table 126 on page 213 shows what combination of output queue parameters and authority to the output queue is required to perform print management functions on the system. For some functions, more than one combination is listed. The owner of a spooled file can always perform all functions on that file. For more information see "Writer commands" on page 496.

The authority and output queue parameters for all commands associated with spooled files are listed on “Spooled file commands” on page 481. Output queue commands are listed on “Output queue commands” on page 454.

Attention: A user with *SPLCTL (spool control) special authority is not subject to any authority restrictions associated with output queues. *SPLCTL special authority allows the user to perform all operations on all output queues. Make careful consideration when giving *SPLCTL special authority to any user.

Table 126. Authority required to perform printing functions

Printing function	Output queue parameters			Output queue authority	Special authority
	DSPDTA	AUTCHK	OPRCTL		
Add spooled files to queue ¹				*READ	None
			*YES		*JOBCTL
View list of spooled files (WRKOUTQ command ²)				*READ	None
			*YES		*JOBCTL
Display, copy, or send spooled files (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSPLF ²)	*YES			*READ	None
	*NO	*DTAAUT		*READ, *ADD, *DLT	None
	*NO	*OWNER		Owner ³	None
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
Change, delete, hold, and release spooled file (CHGSPLFA, DLTSPLF, HLDSPFL, RLSSPLF ²)		*DTAAUT		*READ, *ADD, *DLT	None
		*OWNER		Owner ³	None
			*YES		*JOBCTL
Change, clear, hold, and release output queue (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ ²)		*DTAAUT		*READ, *ADD, *DLT	None
		*OWNER		Owner ³	None
			*YES		*JOBCTL
Start a writer for the queue (STRPRTWTR, STRRMTWTR ²)		*DTAAUT		*CHANGE	None
			*YES		*JOBCTL
¹	This is the authority required to direct your output to an output queue.				
²	Use these commands or equivalent options from a display.				
³	You must be the owner of the output queue.				
⁴	Also requires *USE authority to the printer device description.				
⁵	*CHGOUTQ requires *OBJMGT authority to the output queue, in addition to *READ, *ADD, and *DLT authorities.				

Examples: Output queue

These examples demonstrate how to set security parameters for output queues to meet different requirements.

- Create a general-purpose output queue. All users are allowed to display all spooled files. The system operators are allowed to manage the queue and change spooled files:

```
CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
      OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
```

- Create an output queue for an application. Only members of the group profile GRPA are allowed to use the output queue. All authorized users of the output queue are allowed to display all spooled files. System operators are not allowed to work with the output queue:

```
CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
      OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
      USER(GRPA) AUT(*CHANGE)
```

- Create a confidential output queue for the security officers to use when printing information about user profiles and authorities. The output queue is created and owned by the QSECOFR profile.

```
CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) +
      AUTCHK(*DTAAUT) OPRCTL(*NO) +
      AUT(*EXCLUDE)
```

Even if the security officers on a system have *ALLOBJ special authority, they are not able to access spooled files owned by others on the SECOUTQ output queue.

- Create an output queue that is shared by users printing confidential files and documents. Users can work with only their own spooled files. System operators can work with the spooled files, but they cannot display the contents of the files.

```
CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +
      AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
```

Network attributes

Network attributes control how your system communicates with other systems.

Some network attributes control how remote requests to process jobs and access information are handled. These network attributes directly affect security on your system and are discussed in the topics that follow:

- Job action (JOBACN)
- Client request access (PCSACC)
- DDM request access (DDMACC)

Possible values for each network attribute are shown. The default value is underlined. To set the value of a network attribute, use the Change Network Attribute (CHGNETA) command.

Job Action (JOBACN) network attribute

The JOBACN network attribute determines how the system processes incoming requests to run jobs.

<i>Possible values for JOBACN:</i>	
*REJECT	The input stream is rejected. A message stating the input stream was rejected is sent to both the sender and the intended receiver.
<u>*FILE</u>	The input stream is filed on the queue of network files for the receiving user. This user can display, cancel, or receive the input stream into a database file or submit it to a job queue. A message stating that the input stream was filed is sent to both the sender and the receiver.
*SEARCH	The network job table controls the actions by using the values in the table.

Recommendations:

If you do not expect to receive remote job requests on your system, set the JOBACN network attribute to *REJECT.

Related information:



Client Request Access (PCSACC) network attribute

The PCSACC network attribute determines how the System i Access for Windows licensed program processes requests from attached personal computers to access objects.

The PCSACC network attribute controls whether personal computer jobs can access objects on the System i platform, but it doesn't control whether the personal computer can use workstation emulation.

Note: PCSACC network attribute controls only the DOS and OS/2 clients. This attribute has no effect on any other System i Access clients.

<i>Possible values for PCSACC:</i>	
*REJECT	System i Access rejects every request from the personal computer to access objects on the System i platform. An error message is sent to the PC application.
*OBJAUT	The System i Access programs on the system verify normal object authorities for any object requested by a PC program. For example, if file transfer is requested, authority to copy data from the database file is checked.
*REGFAC	The system uses the system's registration facility to determine which exit program (if any) to run. If no exit program is defined for an exit point and this value is specified, *OBJAUT is used.
<i>qualified- program- name</i>	The System i Access program calls this user-written exit program to determine if the PC request should be rejected. The exit program is called only if normal authority checking for the object is successful. The System i Access program passes information about the user and the requested function to the exit program. The program returns a code indicating whether the request should be allowed or rejected. If the return code indicates the request should be rejected or if an error occurs, an error message is sent to the personal computer.

Risks and recommendations

Use the instructions in this topic to protect the files on your system.

Normal security measures on your system might not be sufficient protections if the System i Access program is installed on your system. For example, if a user has *USE authority to a file and the PCSACC network attribute is *OBJAUT, the user can use the System i Access program and a program on the personal computer to transfer that entire file to the personal computer. The user can then copy the data to a PC diskette or tape and remove it from the premises.

Several methods are available to prevent a System i user with *USE authority to a file from copying the file:

- Setting LMTCPB(*YES) in the user profile.
- Restricting authority to commands that copy files.
- Restricting authority to commands used by System i Access.
- Not giving the user *ADD authority to any library. *ADD authority is required to create a new file in a library.
- Not giving the user access to any *SAVRST device.

None of these methods work for the PC user of the System i Access licensed program. Using an exit program to verify all requests is the only adequate protection measure.

The System i Access program passes information for the following types of access to the user exit program called by the PCSACC network attribute:

- File transfer
- Virtual print
- Message
- Shared folder

Related information:

Programming: iSeries Access

DDM Request Access (DDMACC) network attribute

The DDM Request Access (DDMACC) network attribute determines how the system processes requests from other systems to access data using the distributed data management (DDM) or the distributed relational database function.

<i>Possible values for DDMACC:</i>	
*REJECT	The system does not allow any DDM or DRDA requests from remote systems. *REJECT does not prevent this system from functioning as the requester system and sending requests to other server systems.
*OBJAUT	Remote requests are controlled by the object authority on the system.
<i>qualified- program- name</i>	This user-written exit program is called after normal object authority has been verified. The exit program is called only for DDM files, not for distributed relational database functions. The exit program is passed a parameter list, built by the remote system, that identifies the local system user and the request. The program evaluates the request and sends a return code, granting or denying the requested access.

Related information:

DDMACC parameter considerations

Save and restore operations

The ability to save objects from your system or restore objects to your system represents an exposure to your organization.

For example, programmers often have *OBJEXIST authority to programs because this authority is required to recompile a program (and delete the old copy). *OBJEXIST authority is also required to save an object. Therefore, the typical programmer can make a tape copy of your programs, which might represent a substantial financial investment.

A user with *OBJEXIST authority to an object can also restore a new copy of an object over an existing object. In the case of a program, the restored program might have been created on a different system. It might perform different functions. For example, assume the original program worked with confidential data. The new version might perform the same functions, but it might also write a copy of confidential information to a secret file in the programmer’s own library. The programmer does not need authority to the confidential data because the regular users of the program will be accessing the data.

Restricting save and restore operations

You can restrict the save and restore operations to protect your system.

You can control the ability to save and restore objects in several ways:

- Restrict physical access to save and restore devices, such as tape units and optical units.

- Restrict authority to the device descriptions objects for the save and restore devices. To save an object to a tape unit, you must have *USE authority to the device description for the tape unit.
- Restrict the save and restore commands. This allows you to control what is saved from your system and restored to your system through all interfaces - including save files. See “Example: Restricting save and restore commands” for an example of how to do this. The system sets the restore commands to PUBLIC(*EXCLUDE) when you install your system.
- Only give *SAVSYS special authority to trusted users.

Example: Restricting save and restore commands

This topic shows an example of restricting the save and restore commands.

You can follow these steps to restrict the save and restore commands on your system:

1. To create an authorization list that you can use to give authority to the commands to system operators, type the following example:

```
CRTAUTL AUTL(SRLIST) TEXT('Save and Restore List')
AUT(*EXCLUDE)
```

2. To use the authorization list to secure the save commands, type the following example:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
```

3. To ensure *PUBLIC authority comes from the authorization list, type the following example:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)
```

4. To use the authorization list to secure the restore commands, type the following example:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
```

5. To ensure *PUBLIC authority comes from the authorization list, type the following example:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
AUT(*AUTL)
```

6. Although system operators who are responsible for saving the system have *SAVSYS special authority, they must now be given explicit authority to the SAVxxx commands. You do this by adding the system operators to the authorization list:

```
ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)
```

Note: You might want your system operators to have authority only to the save commands. In that case, secure the save commands and the restore commands with two separate authorization lists.

7. To restrict the save and restore APIs and secure them with an authorization list, type the following commands:

```
GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) USER(*PUBLIC)
AUT(*AUTL)
GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) USER(*PUBLIC)
AUT(*AUTL)
GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) USER(*PUBLIC)
AUT(*AUTL)
```

Performance tuning

Monitoring and tuning performance is not the responsibility of a security officer. However, the security officer should ensure that users are not altering the performance characteristics of the system to speed up their own jobs at the expense of others.

Several work management objects affect the performance of jobs in the system:

- The class sets the run priority and time slice for a job.

- The routing entry in the subsystem description determines the class and the storage pool the job uses.
- The job description can determine the output queue, output priority, job queue, and job priority.

Knowledgeable users with appropriate authority can create their own environment on the system and give themselves better performance than other users. Control this by limiting the authority to create and change work management objects. Set the public authority to work management commands to *EXCLUDE and grant authority to a few trusted users.

Performance characteristics of the system can also be changed interactively. For example, the Work with System Status (WRKSYSSTS) display can be used to change the size of storage pools and the activity levels. Also, a user with *JOBCTL (job control) special authority can change the scheduling priority of any job on the system, subject to the priority limit (PTYLMT) in the user's profile. Assign *JOBCTL special authority and PTYLMT in user profiles carefully.

To allow users to view performance information using the WRKSYSSTS command but not change it, do the following action:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(*PUBLIC)   AUT(*EXCLUDE)
```

Authorize users responsible for system tuning to change performance characteristics:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(USRTUNE)   AUT(*USE)
```

Restricting jobs to batch

You can create or change commands to restrict certain jobs to be run only in a batch environment.

For example, you might want to run certain reports or program compiles in batch. A job running in batch often affects system performance less than the same job running interactively.

For example, to restrict the command that runs program RPTA to batch, do the following action:

- Create a command to run RPTA and specify that the command can be run only in batch:


```
CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)
```

To restrict compiles to batch, do the following for the create command for each program type:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```

Chapter 7. Designing security

This section contains guidelines to help application developers and systems managers include security as part of the overall design. It also contains examples of techniques that you can use to accomplish security objectives on your system.

Protecting information is an important part of most applications. Security should be considered, along with other requirements, at the time the application is designed. For example, when deciding how to organize application information into libraries, try to balance security requirements with other considerations, such as application performance and backup and recovery.

Some of the examples in this section contain sample programs. These programs are included for illustrative purposes only. Many of them will not compile or run successfully as is, nor do they include message handling and error recovery.

The Plan and set up system security in the information center is intended for the security administrator. It contains forms, examples, and guidelines for planning security for applications that have already been developed. If you have responsibility for designing an application, you might find it useful to review the forms and examples in the Plan and set up system security topic for details. They can help you view your application from the perspective of a security administrator and understand what information you need to provide.

The Plan and set up system security topic in the information center also uses a set of example applications for a fictional company called the JKL Toy Company. This section discusses design considerations for the same set of example applications. Figure 31 on page 220 shows the relationships between user groups, applications, and libraries for the JKL Toy Company:

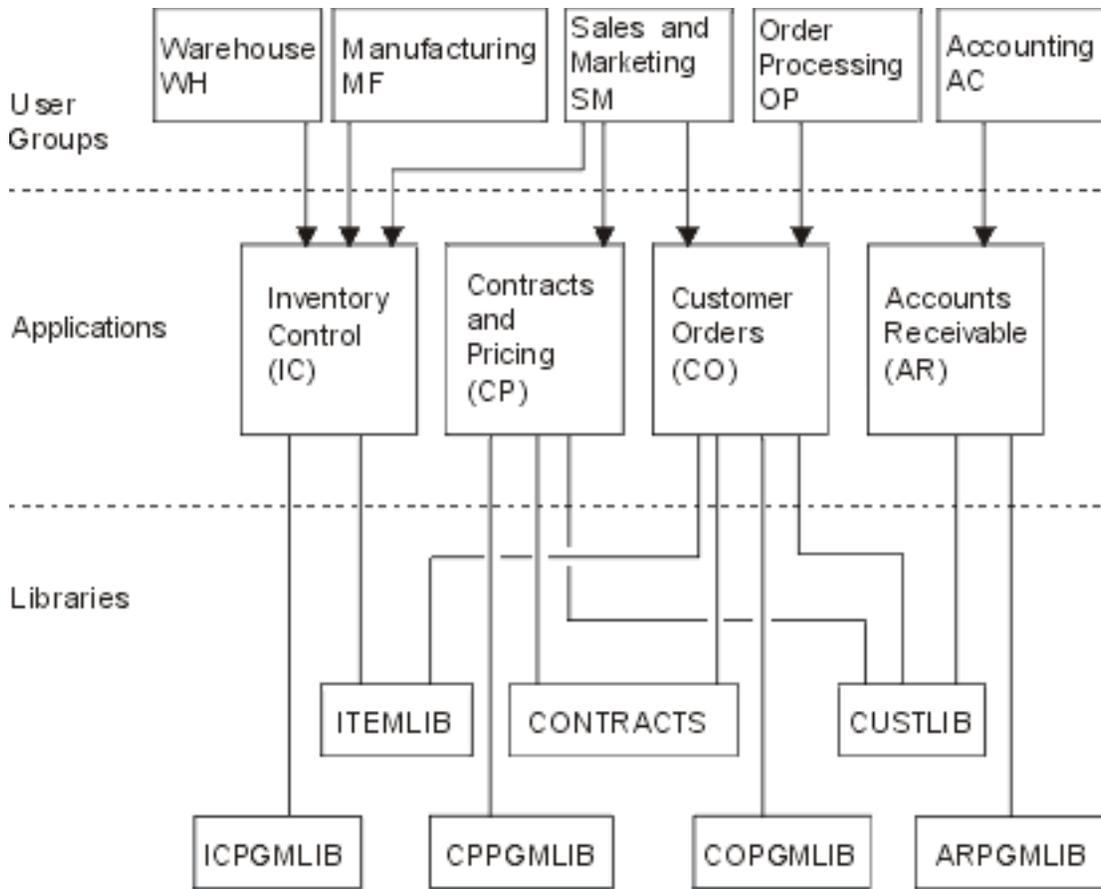


Figure 31. Example applications

Description of graphic

This graphic shows how five sets of user groups access applications and libraries on the system at JKL Toy Company. The user groups include Warehouse, Manufacturing, Sales and Marketing, Order Processing, and Accounting. These user groups have different accesses to different applications, which are stated in the following list.

- The Warehouse, Manufacturing and Sales and Marketing user groups can all access the Inventory Control applications.
- The Sales and Marketing user group also has access to the Contracts and Pricing application and the Customer Order application.
- The Order Processing user group can also access the Customer Order application.
- The Accounting user group only has access to the Accounts Receivable application.

Related information:

Scenarios for HTTP Server

Overall recommendations for security design

Keeping your security design as simple as possible makes it easier to manage and audit security. It also improves application performance and backup performance.

Here is a list of general recommendations for security design:

- Use resource security along with the methods available, such as limited capabilities in the user profile and restricting users to a set of menus, to protect information.

Attention: If you use a product such as System i Access or if you have communication lines attached to your system, do not rely only on limiting capabilities in the user profile and menu access control. You must use resource security to secure any objects that you do not want to be accessible through these interfaces.

- Secure only those objects that really require security. Analyze a library to determine which objects, such as data files, are confidential and secure those objects. Use public authority for other objects, such as data areas and message queues.
- Move from the general to the specific:
 - Plan security for libraries and directories. Deal with individual objects only when necessary.
 - Plan public authority first, followed by group authority and individual authority.
- Make the public authority for new objects in a library (CRTAUT parameter) the same as the public authority for the majority of existing objects in the library.
- To make auditing easier and improve authority-checking performance, avoid defining private authority that is less than the public authority for an object.
- Use authorization lists to group objects with the same security requirements. Authorization lists are simpler to manage than individual authorities and help to recover security information.

Related concepts:

Chapter 5, “Resource security,” on page 131

This section describes each of the components of resource security and how they work together to protect information about your system. It also explains how to use CL commands and displays to set up resource security on your system.

Planning password level changes

Changing password levels should be planned carefully. Operations with other systems might fail or users might not be able to sign on to the system if you haven't planned for the password level change adequately.

Before changing the QPWDLVL system value, make sure that you have saved your security data using the **SAVSECDTA** or **SAVSYS** command. If you have a current backup, you will be able to reset the passwords for all users' profiles, even if you need to return to a lower password level.

Products that you use on the system, and on clients with which the system interfaces, might have problems when the password level (QPWDLVL) system value is set to 2 or 3. Any product or client that sends passwords to the system in an encrypted form, rather than in the clear text that a user enters on a sign-on screen, must be upgraded to work with the password encryption rules for QPWDLVL 2 or 3. Sending the encrypted password is known as password substitution. Password substitution is used to prevent a password from being captured during transmission over a network. Password substitutes generated by older clients that do not support the algorithm for QPWDLVL 2 or 3, even if the specific characters typed in are correct, will not be accepted. This also applies to any System i to System i peer access which utilizes the encrypted values to authenticate from one system to another.

The problem is compounded by the fact that some affected products (such as IBM Toolbox for Java) are provided as middleware. A third party product that incorporates a prior version of one of these products will not work correctly until rebuilt using an updated version of the middleware.

Given this and other scenarios, it is easy to see why careful planning is necessary before you change the QPWDLVL system value.

Considerations for changing QPWDLVL from 0 to 1

Password level 1 allows a system, which doesn't need to communicate with the System i Support for Windows Network Neighborhood (NetServer), to eliminate the NetServer passwords. Eliminating unnecessary encrypted passwords from the system increases the overall security of the system.

At QPWDLVL 1, all current, pre-V5R1 password substitution and password authentication mechanisms will continue to work. There is very little potential for breakage except for functions/services that require the NetServer password.

Considerations for changing QPWDLVL from 0 or 1 to 2

Password level 2 introduces the use of case-sensitive passwords up to 128 characters in length (also called passphrases) and provides the maximum ability to revert back to QPWDLVL 0 or 1.

Regardless of the password level of the system, password level 2 and 3 passwords are created whenever a password is changed or a user signs on to the system. Having a level 2 and 3 password created while the system is still at password level 0 or 1 helps prepare for the change to password level 2 or 3.

Before changing QPWDLVL to 2, the system administrator should use the **PRTUSRPRF TYPE(*PWDLVL)** command to locate all of the user profiles that do not have a password that is usable at password level 2. Depending on the profiles located, the administrator can use one of the following mechanisms to have a password level 2 and 3 password added to the profiles.

- Change the password for the user profile using the CHGUSRPRF or CHGPWD CL command or the QSYCHGPW API. This will cause the system to change the password that is usable at password levels 0 and 1; and the system also creates two equivalent case-sensitive passwords that are usable at password levels 2 and 3. An all-uppercase and all-lowercase version of the password is created for use at password level 2 or 3.

For example, changing the password to C4D2RB4Y results in the system generating C4D2RB4Y and c4d2rb4y password level 2 passwords.

- Sign on to the system through a mechanism that presents the password in clear text (does not use password substitution). If the password is valid and the user profile does not have a password that is usable at password levels 2 and 3, the system creates two equivalent case-sensitive passwords that are usable at password levels 2 and 3. An all-uppercase and all-lowercase version of the password is created for use at password level 2 or 3.

The absence of a password that is usable at password level 2 or 3 can be a problem whenever the user profile also does not have a password that is usable at password levels 0 and 1 or when the user tries to sign on through a product that uses password substitution. In these cases, the user will not be able to sign on when the password level is changed to 2.

If a user profile meets the following description, the system validates the user against the password level 0 password and creates two password level 2 passwords (as described above) for the user profile.

- The user profile does not have a password that is usable at password levels 2 and 3.
- The user profile does have a password that is usable at password levels 0 and 1.
- The user signs on through a product that sends clear text passwords.

Subsequent signons will be validated against the password level 2 passwords.

Any client that uses password substitution will not work correctly at QPWDLVL 2 if the client hasn't been updated to use the new password (passphrase) substitution scheme. The administrator should check whether a client which hasn't been updated to the new password substitution scheme is required.

The clients that use password substitution include:

- TELNET

- System i Access
- System i Host Servers
- QFileSrv.400
- System i NetServer Print support
- DDM
- DRDA
- SNA LU6.2

It is highly recommended that the security data be saved before changing to QPWDLVL 2. This can help make the transition back to QPWDLVL 0 or 1 easier if that becomes necessary.

Avoid changing password system values, such as QPWDMINLEN, QPWDMAXLEN, and QPWDRULES, until after you have tested QPWDLVL 2. This makes it easier to transition back to QPWDLVL 1 or 0 if necessary. However, the QPWDVLDPGM system value must specify either *REGFAC or *NONE before the system allows QPWDLVL to be changed to 2. Therefore, if you use a password validation program, you might want to write a new one that can be registered for the QIBM_QSY_VLD_PASSWRD exit point by using the ADDEXITPGM command.

NetServer passwords are still supported at QPWDLVL 2, so any function/service that requires a NetServer password should still function correctly.

After you are comfortable with running the system at QPWDLVL 2, you can change the password system values to use longer passwords. However, you need to be aware that longer passwords have these effects:

- If passwords greater than 10 characters are specified, the password level 0 and 1 password is cleared. This user profile will not be able to sign on if the system is returned to password level 0 or 1.
- If passwords contain special characters or do not follow the composition rules for simple object names (excluding case sensitivity), the password level 0 and 1 password is cleared.
- If passwords greater than 14 characters are specified, the NetServer password for the user profile is cleared.
- The password system values only apply to the new password level 2 value and do not apply to the system-generated password level 0 and 1 password or NetServer password values (if generated).

Considerations for changing QPWDLVL from 2 to 3

After running the system at QPWDLVL 2 for some period of time, you can consider moving to QPWDLVL 3 to maximize the password security protection.

At QPWDLVL 3, all NetServer passwords are cleared so a system should not be moved to QPWDLVL 3 until there is no need to use NetServer passwords.

At QPWDLVL 3, all password level 0 and 1 passwords are cleared. The administrator can use the **DSPAUTUSR** or **PRTUSRPRF** command to locate user profiles which don't have password level 2 or 3 passwords associated with them.

Changing QPWDLVL to a lower password level

Returning to a lower QPWDLVL value, while possible, is not expected to be a completely painless operation. In general, the mind set should be that this is a one-way trip from lower QPWDLVL values to higher QPWDLVL values. However, there might be cases where a lower QPWDLVL value must be reinstated.

Considerations for changing from QPWDLVL 3 to 2

This change is relatively easy. After the QPWDLVL is set to 2, the administrator needs to determine if any user profile is required to contain NetServer passwords or password level 0 or 1 passwords and, if so, change the password of the user profile to an allowable value.

Additionally, the password system values might need to be changed back to values compatible with NetServer and password level 0 or 1 passwords, if those passwords are needed.

Considerations for changing from QPWDLVL 3 to 1 or 0

Because of the very high potential for causing problems for the system (such as no one can sign on because all of the password level 0 and 1 passwords have been cleared), this change is not supported directly. To change from QPWDLVL 3 to QPWDLVL 1 or 0, the system must first make the intermediary change to QPWDLVL 2.

Considerations for changing from QPWDLVL 2 to 1

Before changing QPWDLVL to 1, you should use the DSPAUTUSR or PRTUSRPRF TYPE(*PWDINFO) command to locate any user profiles that do not have a password level 0 or 1 password. If the user profile requires a password after the QPWDLVL is changed, make sure that a password level 0 and 1 password is created for the profile using one of the following mechanisms:

- Change the password for the user profile using the CHGUSRPRF or CHGPWD CL command or the QSYCHGPW API. This causes the system to change the password that is usable at password levels 2 and 3; and the system also creates an equivalent uppercase password that is usable at password levels 0 and 1. The system is only able to create the password level 0 and 1 password if the following conditions are met:
 - The password is 10 characters or less in length.
 - The password can be converted to uppercase EBCDIC characters A-Z, 0-9, @, #, \$, and underline.
 - The password does not begin with a numeric or underline character.

For example, changing the password to a value of RainyDay can result in the system generating a password level 0 and 1 password of RAINYDAY. But changing the password value to Rainy Days In April can cause the system to clear the password level 0 and 1 password (because the password is too long and it contains blanks).

No message or indication is produced if the password level 0 or 1 password cannot be created.

- Sign on to the system through a mechanism that presents the password in clear text (does not use password substitution). If the password is valid and the user profile does not have a password that is usable at password levels 0 and 1, the system creates an equivalent uppercase password that is usable at password levels 0 and 1. The system is only able to create the password level 0 and 1 password if the conditions listed above are met.

The administrator can then change QPWDLVL to 1. All NetServer passwords are cleared when the change to QPWDLVL 1 takes effect (next IPL).

Considerations for changing from QPWDLVL 2 to 0

The considerations are the same as those for changing from QPWDLVL 2 to 1 except that all NetServer passwords are retained when the change takes effect.

Considerations for changing from QPWLVL 1 to 0

After changing QPWLVL to 0, you should use the DSPAUTUSR or PRTUSRPRF command to locate any user profiles that do not have a NetServer password. If the user profile requires a NetServer password, it can be created by changing the user's password or signing on through a mechanism that presents the password in clear text.

You can then change QPWLVL to 0.

Planning libraries

A library is like a directory used to locate the objects in the library. Many factors affect how you choose to group your application information into libraries and manage libraries.

Library security is effective only if the rules below are followed:

- Libraries contain objects with similar security requirements.
- Users are not allowed to add new objects to restricted libraries. Changes to programs in the libraries are controlled. That is, application libraries should have public authority of *USE or *EXCLUDE unless users need to create objects directly into the library.
- Library lists are controlled.

To access an object, you need authority to the object itself and to the library containing the object. You can restrict access to an object by restricting the object itself, the library containing the object, or both.

*USE authority to a library allows you to find objects in the library. The authority for the object itself determines *how* you can use the object. *USE authority to a library is sufficient to perform most operations on the objects in the library.

Using public authority for objects and restricting access to libraries can be a simple, effective security technique. Putting programs in a separate library from other application objects can also simplify security planning. This is particularly true if files are shared by more than one application. You can use authority to the libraries containing application programs to control who can perform application functions.

Here are two examples of using library security for the JKL Toy Company applications. (See Figure 31 on page 220 for a diagram of the applications.)

- The information in the CONTRACTS library is considered confidential. The public authority for all the objects in the library is sufficient to perform the functions of the Pricing and Contracts application (*CHANGE). The public authority to the CONTRACTS library itself is *EXCLUDE. Only users or groups authorized to the Contracts and Pricing application are granted *USE authority to the library.
- The JKL Toy Company is a small company with a nonrestrictive approach to security, except for the contract and pricing information. All system users are allowed to view customer and inventory information, although only authorized users can change this information. The CUSTLIB and the ITEMLIB libraries, and the objects in the libraries, have public authority of *USE. Users can view information in these libraries through their primary application or by using a SQL query. The program libraries have public authority *EXCLUDE. Only users who are allowed to change inventory information have access to the ICPGMLIB. Programs that change inventory information adopt the authority of the application owner (OWNIC) and thus have *ALL authority to the files in the ITEMLIB library.

Related concepts:

“Library security” on page 135

You can use library security to protect information.

Related reference:

“Library lists” on page 207

The **library list** for a job indicates which libraries are to be searched and the order in which they are to

be searched.

Related information:

Scenarios for HTTP Server

Planning applications to prevent large profiles

To reduce impacts on the performance and security of your system, you need to plan your applications carefully to avoid large profiles.

Because of the potential impacts on performance and security, perform the following actions to prevent profiles from becoming too full:

- Do not have one profile own everything on your system.
Create special user profiles to own applications. Owner profiles that are specific to an application make it easier to recover applications and to move applications between systems. Also, information about private authorities is spread among several profiles, which improves performance. By using several owner profiles, you can prevent a profile from becoming too large because of owning too many objects. Owner profiles also allow you to adopt the authority of the owner profile rather than a more powerful profile that provides unnecessary authority.
- Avoid having applications owned by IBM-supplied user profiles, such as QSECOFR or QPGMR.
These profiles own a large number of IBM-supplied objects and can become difficult to manage. Having applications owned by IBM-supplied user profiles can also cause security problems when moving applications from one system to another. Applications owned by IBM-supplied user profiles can also affect performance for commands, such as **CHKOBJITG** and **WRKOBJOWN**.
- Use authorization lists to secure objects.
If you are granting private authorities to many objects for several users, you should consider using an authorization list to secure the objects. Authorization lists will cause one private authority entry for the authorization list in the user's profile rather than one private authority entry for each object. In the object owner's profile, authorization lists create an authorized object entry for each user with authority to the authorization list.

Library lists

The library list for a job represents a security exposure, while it provides flexibility. This exposure is particularly important if you use public authority for objects and rely on library security as your primary means of protecting information. In this case, a user who gains access to a library has uncontrolled access to the information in the library.

To avoid the security risks of library lists, your applications can specify qualified names. When both the object name and the library are specified, the system does not search the library list. This prevents a potential intruder from using the library list to circumvent security.

However, other application design requirements might prevent you from using qualified names. If your applications rely on library lists, the following techniques can reduce the security exposure.

Note: By using the code examples, you agree to the terms of the Chapter 10, "Code license and disclaimer information," on page 307.

Controlling the user library list

As a security precaution, you might want to make sure that the user portion of the library list has the correct entries in the expected sequence before a job runs. One method for doing this is to use a CL program to save the user's library list, replace it with the list that you want, and restore it at the end of the application.

Here is a sample program to do this:

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

```

PGM
DCL      &USRLIBL *CHAR LEN(2750)
DCL      &CURLIB  *CHAR LEN(10)
DCL      &ERROR  *LGL
DCL      &CMD    *CHAR LEN(2800)
MONMSG   MSGID(CPF0000) +
        EXEC(GOTO SETERROR)
RTVJOBA  USRLIBL(&USRLIBL) +
        CURLIB(&CURLIB)
IF COND(&CURLIB=('*NONE')) +
    THEN(CHGVAR &CURLIB '*CRTDFT ')
CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
/*****/
/*          */
/*   Normal processing   */
/*          */
/*****/
GOTO     ENDPGM
SETERROR: CHGVAR  &ERROR '1'
ENDPGM:  CHGVAR  &CMD +
        ('CHGLIBL LIBL+
        (' *CAT &USRLIBL *CAT') +
        CURLIB(' *CAT &CURLIB *TCAT ' )')
        CALL     QCMDEXC PARM(&CMD 2800)
        IF      &ERROR SNDPGMMSG MSGID(CPF9898) +
        MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
        MSGDTA('The xxxx error occurred')
        ENDPGM

```

Figure 32. Program to replace and restore library list

Notes:

1. Regardless of how the program ends (normally or abnormally), the library list is returned to the version it held when the program was called. This is because error handling includes restoring the library list.
2. Because the CHGLIBL command requires a list of library names, it cannot be run directly. The **RTVJOBA** command, therefore, retrieves the libraries used to build the CHGLIBL command as a variable. The variable is passed as a parameter to the QCMDEXC function.
3. If you exit to an uncontrolled function (for example, a user program, a menu that allows commands to be entered, or the Command Entry display) in the middle of a program, your program should replace the library list on return to ensure adequate control.

Changing the system library list

You might also need to change the system portion of the library list to protect your system.

If your application needs to add entries to the system portion of the library list, you can use a CL program similar to the one shown in Figure 32, with the following changes:

- Instead of using the **RTVJOBA** command, use the Retrieve System Values (**RTVSYVAL**) command to get the value of the QSYSLIBL system value.
- Use the Change System Library List (**CHGSYSLIBL**) command to change the system portion of the library list to the value that you want.
- At the end of your program, use the **CHGSYSLIBL** command again to restore the system portion of the library list to its original value.
- The **CHGSYSLIBL** command is shipped with public authority *EXCLUDE. To use this command in your program, do one of the following actions:
 - Grant the program owner *USE authority to the **CHGSYSLIBL** command and use adopted authority.

- Grant users running the program *USE authority to the **CHGSYSLIBL** command.

Describing library security

As an application designer, you need to provide information about a library for the security administrator. The security administrator uses this information to decide how to secure the library and its objects.

Typical information needed is:

- Any application functions that add objects to the library.
- Whether any objects in the library are deleted during application processing.
- What profile owns the library and its objects.
- Whether the library should be included on library lists.

Figure 33 provides a sample format for providing this information:

Library name: ITEMLIB

Public authority to the library: *EXCLUDE

Public authority to objects in the library: *CHANGE

Public authority for new objects (CRTAUT): *CHANGE

Library owner: OWNIC

Include on library lists? No. Library is added to library list by initial application program or initial query program.

List any functions that require *ADD authority to the library:

No objects are added to the library during normal application processing. List any objects requiring *OBJMGT or *OBJEXIST authority and what functions need that authority:

All work files, whose names begin with the characters ICWRK, are cleared at month-end. This requires *OBJMGT authority.

Figure 33. Format for describing library security

Planning menus

Menus are a good method for providing controlled access on your system. You can use menus to restrict a user to a set of strictly controlled functions by specifying limited capabilities and an initial menu in the user profile.

To use menus as an access control tool, follow these guidelines when designing them:

- Do not provide a command line on menus designed for restricted users.
- Avoid having functions with different security requirements on the same menu. For example, if some application users are allowed to only view information, not change it, provide a menu that has only display and print options for those users.
- Make sure that the set of menus provides all the necessary links between menus so the user does not need a command line to request one.

- Provide access to a few system functions, such as viewing printer output. The ASSIST system menu gives this capability and can be defined in the user profile as the Attention-key-handling program. If the user profile has a class of *USER and has limited capabilities, the user cannot view the output or jobs of other users.
- Provide access to decision-support tools from menus. The topic “Using adopted authority in menu design” on page 230 gives an example of how to do this.
- Consider controlling access to the System Request Menu or some of the options on this menu.
- For users who are allowed to run only a single function, avoid menus entirely and specify an initial program in the user profile. Specify *SIGNOFF as the initial menu.

For example, at the JKL Toy Company, all users see an inquiry menu allowing access to most files. For users who are not allowed to change information, this is the initial menu. The return option on the menu signs the user off. For other users, this menu is called by an inquiry option from application menus. By pressing F12 (Return), the user returns to the calling menu. Because library security is used for program libraries, this menu and the programs it calls are kept in the QGPL library:

```

INQMENU      Inquiry Menu

              1. Item Descriptions
              2. Item Balances
              3. Customer Information
              4. Query
              5. Office

Enter option ==>
F1=Help  F12=Return

```

Figure 34. Sample inquiry menu

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

Related concepts:

“System request menu” on page 233

A user can use the system request function to suspend the current job and display the System Request Menu. The System Request Menu allows the user to send and display messages, transfer to a second job, or end the current job. This might represent a security exposure because the public authority to the System Request Menu is *USE when a system is shipped.

Related reference:

“Limit capabilities” on page 83

You can use the Limit capabilities field to limit the user’s ability to enter commands and to override the initial program, initial menu, current library, and attention-key-handling program specified in the user profile. This field is a tool for preventing users from experimenting on the system.

Related information:

Scenarios for HTTP Server

Describing menu security

As an application designer, you need to provide information about a menu for the security administrator. The security administrator uses this information to decide who should have access to the menu and what authorities are required.

Examples of the type of information that a security administrator needs are:

- Whether any menu options require special authorities, such as *SAVSYS or *JOBCTL.
- Whether menu options call programs that adopt authority.
- What authority to objects is required for each menu option. You should only need to identify those authorities that are greater than normal public authority.

Figure 35 shows a sample format for providing this information.

```
Menu name: MENU1           Library:  QGPLOption number:  3           Description:  Query
Program called: QRYSTART   Library:  QGPL
Authority adopted:  QRYUSR
Special authority required:  None

Object authorities required:  User must have *USE authority to QRYSTART
program. QRYUSR must have *USE authority to libraries containing
files to be queried.  User, QRYUSR, or public must have *USE
authority to files being queried.
```

Figure 35. Format for menu security requirements

Using adopted authority in menu design

The availability of decision-support tools, such as Query/400, poses challenges for security design. No method exists in the resource security definitions for a user to have different authority to a file in different circumstances. However, using adopted authority allows you to define authority to meet different requirements.

For example, you might want users to be able to view information in files using a query tool, but you probably want to make sure that the files are changed only by tested application programs.

Note: “Objects that adopt the owner's authority” on page 149 describes how adopted authority works. “Flowchart 8: How adopted authority is checked” on page 182 describes how the system checks for adopted authority.

Figure 36 shows a sample initial menu that uses adopted authority to provide controlled access to files using query tools:

```
MENU1           Initial Menu
                1. Inventory Control (ICSTART)
                2. Customer Orders  (COSTART)
                3. Query             (QRYSTART)
                4. Office            (OFCSTART)

(no command line)
```

Figure 36. Sample initial menu

The programs that start applications (ICSTART and COSTART) adopt the authority of a profile that owns the application objects. The programs add application libraries to the library list and display the initial application menu. Here is an example of the Inventory Control program (ICSTART).

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

```

PGM
ADDLIBL ITEMLIB
ADDLIBL ICPGMLIB
GO ICMENU
RMLIBL ITEMLIB
RMLIBL ICPGMLIB
ENDPGM

```

Figure 37. Sample initial application program

The program that starts Query (QRYSTART) adopts the authority of a profile (QRYUSR) provided to allow access to files for queries. Figure 38 shows the QRYSTART program:

```

PGM
ADDLIBL ITEMLIB
ADDLIBL CUSTLIB
STRQRY
RMLIBL ITEMLIB
RMLIBL CUSTLIB
ENDPGM

```

Figure 38. Sample program for query with adopted authority

The menu system uses three types of user profiles, shown in Table 127. Table 128 describes the objects used by the menu system.

Table 127. User profiles for menu system

Profile type	Description	Password	Limit capabilities	Special authorities	Initial menu
Application owner	Owns all application objects and has *ALL authority. OWNIC owns Inventory Control application.	*NONE	Not applicable	As needed by application	Not applicable
Application user ¹	Example profile for anyone who uses the menu system	Yes	*YES	None	MENU1
Query Profile	Used to provide access to libraries for query	*NONE	Not applicable	None	Not applicable

¹ The current library specified in the application user profile is used to store any queries created. The Attention-key-handling program is *ASSIST, giving the user access to basic system functions.

Table 128. Objects used by menu system

Object name	Owner	Public authority	Private authorities	Additional information
MENU1 in QGPL library	See Note	*EXCLUDE	*USE authority for any users who are allowed to use the menu	In QGPL library because users do not have authority to application libraries
ICSTART program in QGPL	OWNIC	*EXCLUDE	*USE authority for users authorized to Inventory Control application	Created with USRPRF(*OWNER) to adopt OWNIC authority
QRYSTART program in QGPL	QRYUSR	*EXCLUDE	*USE authority for users authorized to create or run queries	Created with USRPRF(*OWNER) to adopt QRYUSR authority
ITEMLIB	OWNIC	*EXCLUDE	QRYUSR has *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
Files available for Query in ITEMLIB	OWNIC	*USE		

Table 128. Objects used by menu system (continued)

Object name	Owner	Public authority	Private authorities	Additional information
Files not available for Query in ITEMLIB	OWNIC	*EXCLUDE		
Programs in ICPGMLIB	OWNIC	*USE		
Note: A special owner profile can be created for objects used by multiple applications.				

When USERA selects option 1 (Inventory Control) from MENU1, program ICSTART runs. The program adopts the authority of OWNIC, giving *ALL authority to the inventory control objects in ITEMLIB and the programs in ICPGMLIB. USERA is thus authorized to make changes to the inventory control files while using options from the ICMENU.

When USERA exits ICMENU and returns to MENU1, the ITEMLIB and ICPGMLIB libraries are removed from the USERA library list, and program ICSTART is removed from the call stack. USERA is no longer running under adopted authority.

When USERA selects option 3 (Query) from MENU1, program QRYSTART runs. The program adopts the authority of QRYUSR, giving *USE authority to the ITEMLIB library. The public authority to the files in ITEMLIB determines which files USERA is allowed to query.

This technique has the advantage of minimizing the number of private authorities and providing good performance when checking authority:

- The objects in the application libraries do not have private authorities. For some application functions, public authority is adequate. If public authority is not adequate, owner authority is used. “Case 8: Adopted authority without private authority” on page 192 shows the authority checking steps.
- Access to the files for query uses public authority to the files. The QRYUSR profile is only specifically authorized to the ITEMLIB library.
- By default, any query programs created are placed in the user’s current library. The current library should be owned by the user, and the user should have *ALL authority.
- Individual users only need to be authorized to MENU1, ICSTART, and QRYSTART.

Consider these risks and precautions when using this technique:

- USERA has *ALL authority to all entire inventory control objects from ICMENU. Make sure that the menu does not allow access to a command line or allow unwanted delete and update functions.
- Many decision-support tools allow access to a command line. The QRYUSR profile should be a limited capability user without special authorities to prevent unauthorized functions.

Related concepts:

“Planning file security” on page 236

The information contained in database files is often the most important asset on your system. Resource security allows you to control who can view, change, and delete information in a file.

Ignoring adopted authority

The technique of using adopted authority in menu design requires the user to return to the initial menu before running queries. If you want to provide the convenience of starting query from application menus as well as from the initial menu, you can set up the QRYSTART program to ignore adopted authority.

Figure 39 on page 233 shows an application menu that includes the QRYSTART program:

```
ICMENU      Inventory Control Menu

            1. Issues (ICPGM1)
            2. Receipts (ICPGM2)
            3. Purchases (ICPGM3)
            4. Query (QRYSTART)

(no command line)
```

Figure 39. Sample application menu with query

The authority information for the QRYSTART program is the same as shown in Table 128 on page 231. The program is created with the use adopted authority (USEADPAUT) parameter set to *NO, to ignore the adopted authority of previous programs in the stack.

Here are comparisons of the call stacks when USERA selects query from MENU1 (see Figure 36 on page 230) and from ICMENU:

Call stack when query selected from MENU1

- MENU1 (no adopted authority)
- QRYSTART (adopted authority QRYUSR)

Call stack when query selected from ICMENU

- MENU1 (no adopted authority)
- ICMENU (adopted authority OWNIC)
- QRYSTART (adopted authority QRYUSR)

By specifying the QRYSTART program with USEADPAUT(*NO), the authority of any previous programs in the stack is not used. This allows USERA to run a query from ICMENU without having the ability to change and delete files. This is because the authority of OWNIC is not used by the QRYSTART program.

When USERA ends the query and returns to ICMENU, adopted authority is once again active. Adopted authority is ignored only as long as the QRYSTART program is active.

If public authority to the QRYSTART program is *USE, specify USEADPAUT(*NO) as a security precaution. This prevents anyone running under adopted authority from calling the QRYSTART program and performing unauthorized functions.

The inquiry menu (Figure 34 on page 229) at the JKL Toy Company also uses this technique, because it can be called from menus in different application libraries. It adopts the authority of QRYUSR and ignores any other adopted authority in the call stack.

Related concepts:

“Programs that ignore adopted authority” on page 152

You can specify the use adopted authority (USEADPAUT) parameter to control whether a program uses the adopted authority.

Related reference:

“Flowchart 8: How adopted authority is checked” on page 182

If insufficient authority is found by checking user authority, the system checks adopted authority.

Related information:

Scenarios for HTTP Server

System request menu

A user can use the system request function to suspend the current job and display the System Request Menu. The System Request Menu allows the user to send and display messages, transfer to a second job,

or end the current job. This might represent a security exposure because the public authority to the System Request Menu is *USE when a system is shipped.

The simplest way to prevent users from accessing this menu is to restrict authority to the panel group QGMNSYSR:

- To prevent specific users from seeing the System Request Menu, specify *EXCLUDE authority for those users:

```
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP) +
          USER(USERA) AUT(*EXCLUDE)
```

- To prevent most users from seeing the System Request Menu, revoke public authority and grant *USE authority to specific users:

```
RVKOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP) +
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP) +
          USER(USERA) AUT(*USE)
```

Some of the actual commands used for the System Request menu come from the CPX2313 message in the QCPFMSG message file. Commands are qualified with a library name from the CPX2373 message. The values in the CPX2373 message for each command are *NLVLIBL or *SYSTEM. Someone might potentially use the Override Message File (OVRMSGF) command to change the commands that the System Request menu options use.

Each time the System Request key is pressed, the system automatically changes the current user profile of the job to the initial user profile of the job. This is done so that the user does not have any additional authority on the System Request menu or in the Presystem Request Program exit program. After the System Request function is completed, the current user profile of the job is returned to the value that it was before the System Request key was pressed.

You can prevent users from selecting specific options from the System Request Menu by restricting the authority to the associated commands. Table 129 shows the commands associated with the menu options:

Table 129. Options and commands for the system request menu

Option	Command
1	Transfer Secondary Job (TFRSECJOB)
2	End Request (ENDRQS)
3	Display Job (DSPJOB)
4	Display Message (DSPMSG)
5	Send Message (SNDMSG)
6	Display Message (DSPMSG)
7	Display Workstation User (DSPWSUSR)
10	Start System Request at Previous System (TFRPASTHR). (See note below.)
11	Transfer to previous system (TFRPASTHR). (See note below.)
12	Display 3270 emulation options (See note below.)
13	Start System Request at Home System (TFRPASTHR). (See note below.)
14	Transfer to Home System (TFRPASTHR). (See note below.)
15	Transfer to End System (TFRPASTHR). (See note below.)
80	Disconnect Job (DSCJOB)
90	Sign-Off (SIGNOFF)

Table 129. Options and commands for the system request menu (continued)

Option	Command
<p>Notes:</p> <ol style="list-style-type: none"> Options 10, 11, 13, 14, and 15 are displayed only if display station pass-through has been started with the Start Pass-Through (STRPASTHR) command. Option 10, 13, and 14 are only displayed on the target system. Option 12 is only displayed when 3270 emulation is active. Some of the options have restrictions for the System/36 environment. 	

For example, to prevent users from transferring to an alternative interactive job, revoke public authority to the Transfer to Secondary Job (TFRSECJOB) command and grant authority only to specific users:

```
RVKOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(USERA) AUT(*USE)
```

If a user selects an option for which the user does not have authority, a message is displayed.

If you want to prevent users from general use of the commands from the System Request menu but still want them to be able to run a command at a specific time (such as sign-off), you can create a CL program that adopts the authority of an authorized user and runs the command.

Related concepts:

“Planning menus” on page 228

Menus are a good method for providing controlled access on your system. You can use menus to restrict a user to a set of strictly controlled functions by specifying limited capabilities and an initial menu in the user profile.

Planning command security

When your system arrives, the ability to use commands is set up to meet the security needs of most installations. Some commands can be run only by a security officer. Others require a special authority, such as *SAVSYS. Most commands can be used by anyone on the system. You can change the authority to commands to meet your security requirements.

For example, you might want to prevent most users on your system from working with communications. You can set the public authority to *EXCLUDE for all commands that work with communications objects, such the CHGCTLxxx, CHGLINxxx, and CHGDEVxxx commands.

If you need to control which commands can be run by users, you can use object authority to the commands themselves. Every command on the system has object type *CMD and can be authorized to the public or only to specific users. To run a command, the user needs *USE authority to that command. Appendix C, “Commands shipped with public authority *EXCLUDE,” on page 327 lists all the commands that are shipped with the public authority set to *EXCLUDE.

If you use the System/38 library, you need to restrict security-relevant commands in that library also. Or, you might restrict access to the entire library. If you use one or more national language versions of the IBM i licensed program on your system, you need to restrict commands in the additional QSYSxxx libraries on your system as well.

Another useful security measure is to change the default values for some commands. The Change Command Default (CHGCMDDFT) command allows you to do this.

Planning file security

The information contained in database files is often the most important asset on your system. Resource security allows you to control who can view, change, and delete information in a file.

If users require different authority to files depending on the situation, you can use adopted authority.

For critical files on your system, keep a record of what users have authority to the file. If you use group authority and authorization lists, you need to keep track of users who have authority through those methods, as well as users who are directly authorized. If you use adopted authority, you can list programs that adopt the authority of a particular user using the Display Program Adopt (**DSPPGMADP**) command.

You can also use the journaling function on the system to monitor activity against a critical file. Although the primary intent of a journal is to recover information, it can be used as a security tool. It contains a record of who has accessed a file and in what way. You can use the Display Journal (**DSPJRN**) command to view a sampling of journal entries periodically.

Related reference:

“Using adopted authority in menu design” on page 230

The availability of decision-support tools, such as Query/400, poses challenges for security design. No method exists in the resource security definitions for a user to have different authority to a file in different circumstances. However, using adopted authority allows you to define authority to meet different requirements.

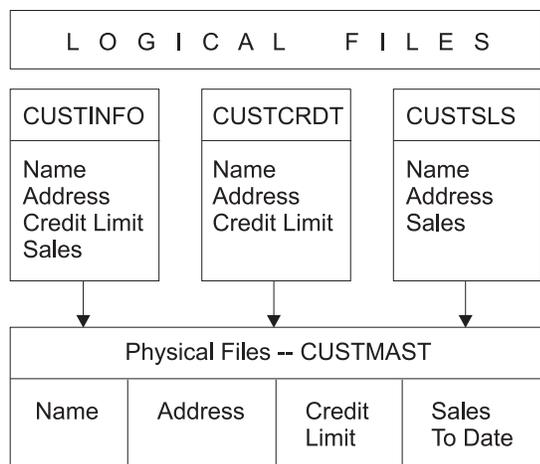
Securing logical files

Resource security on the system supports field-level security of a file. You can also use logical files to protect specific fields or records in a file.

A logical file can be used to specify a subset of *records* that a user can access (by using select and omit logic). Therefore, specific users can be prevented from accessing certain record types. A logical file can be used to specify a subset of *fields* in a record that a user can access. Therefore, specific users can be prevented from accessing certain fields in a record.

A logical file does not contain any data. It is a particular view of one or more physical files that contain the data. Providing access to the information defined by a logical file requires data authority to both the logical file and the associated physical files.

Figure 40 on page 237 shows an example of a physical file and three different logical files associated with it.



RBAFW532-0

Figure 40. Using a logical file for security

Members of the sales department (group profile DPTSM) are allowed to view all fields, but they cannot change the credit limit. Members of the accounts receivable department (group profile DPTAR) are allowed to view all fields, but they cannot change the sales field. The authority to the physical file looks like this:

Table 130. Physical file example: CUSTMAST file

Authority	Users: *PUBLIC
<i>Object Authorities</i>	
*OBJOPR	
*OBJMGT	
*OBJEXIST	
*OBJALTER	
*OBJREF	
<i>Data Authorities</i>	
*READ	X
*ADD	X
*UPD	X
*DLT	X
*EXECUTE	X
*EXCLUDE	

The public should have all data authority but no object operational authority to the CUSTMAST physical file. The public cannot access the CUSTMAST file directly because *OBJOPR authority is required to open a file. The public's authority makes all the data authority potentially available to users of the logical file.

Authority to the logical files looks like this:

```

                Display Object Authority
Object . . . . . : CUSTINFO      Owner . . . . . : OWNAR
  Library . . . . . : CUSTLIB      Primary group . . . : *NONE
Object type . . . . . : *FILE      ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
*PUBLIC   .          Authority
           .          *USE

```

```

                Display Object Authority
Object . . . . . : CUSTCRDT      Owner . . . . . : OWNAR
  Library . . . . . : CUSTLIB      Primary group . . . : DPTAR
Object type . . . . . : *FILE      ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
DPTAR    .          Authority
*PUBLIC  .          *CHANGE
           .          *USE

```

```

                Display Object Authority
Object . . . . . : CUSTSLS      Owner . . . . . : OWNSM
  Library . . . . . : CUSTLIB      Primary group . . . : DPTSM
Object type . . . . . : *FILE      ASP device . . . . . : *SYSBAS

Object secured by authorization list . . . . . : *NONE

User      Group      Object
DPTSM    .          Authority
*PUBLIC  .          *CHANGE
           .          *USE

```

Making the group profile, such as DPTSM, the primary group for the logical file is not necessary for this authority scheme to work. However, using primary group authority eliminates searching private authorities for both the user attempting to access the file and the user's group. "Case 2: Using primary group authority" on page 187 shows how using primary group authority affects the authority checking process.

You can specify data authorities for logical files beginning with V3R1 of the IBM i licensed program. When a pre-V3R1 logical file is restored on a V3R1 system or later, the system converts your logical files the first time a logical file is accessed. The system gives it all data authorities.

To use logical files as a security tool, do this:

- Grant all data authorities to the underlying physical files.
- Revoke *OBJOPR from the physical files. This prevents users from accessing the physical files directly.
- Grant the appropriate data authorities to logical files. Revoke any authorities you do not want.
- Grant *OBJOPR to the logical files.

Related information:

Overriding files

You can use override commands to have a program use a different file with the same format.

For example, assume that a program in the contracts and pricing application at the JKL Toy Company writes pricing information to a work file before making price changes. A user with access to a command line who wanted to capture confidential information can use an override command to cause the program to write data to a different file in a library controlled by the user.

You can make sure that a program processes the correct files by using override commands with `SECURE(*YES)` before the program runs, thus those files are protected from the effects of any file override commands that were previously called. If you use `SECURE(*NO)`, those files are not protected from other file overrides. Their values can be overridden by the effects of any file override commands that were previously called.

File security and SQL

You should pay much attention to file security when using a CL program that adopts authority to start SQL or Query Manager. Both of these query programs allow users to specify a file name. The user can, therefore, access any file that the adopted profile has authority to.

Structured Query Language (SQL) uses cross-reference files to keep track of database files and their relationships. These files are collectively referred to as the SQL catalog. Public authority to the SQL catalog is `*READ`. This means that any user who has access to the SQL interface can display the names and text descriptions for all files on your system. The SQL catalog does not affect the normal authority required to access the contents of database files.

Planning group profiles

A group profile is a useful tool when several users have similar security requirements. You can directly create group files or you can make an existing profile into a group profile. When you use group profiles, you can manage authority more efficiently and reduce the number of individual private authorities for objects.

Group files are particularly useful when job requirements and group membership change. For example, if members of a department have responsibility for an application, a group profile can be set up for the department. As users join or leave the department, the group profile field in their user profiles can be changed. This is easier to manage than removing individual authorities from user profiles.

A group profile is just a special type of user profile. It becomes a group profile when one of the following conditions are met:

- Another profile designates it as a group profile
- You assign a group identification number (gid) to it.

For example:

1. Create a profile called GRPIC:
`CRTUSRPRF GRPIC`
2. When the profile is created, it is an ordinary profile, not a group profile.
3. Designate GRPIC as the group profile for another group profile:
`CHGUSRPRF USERA GRPPRF(GRPIC)`
4. The system now treats GRPIC as a group profile and assigns a gid to it.

Related concepts:

“Group profiles” on page 4

A *group profile* is a special type of user profile. Rather than giving authority to each user individually, you can use a group profile to define authority for a group of users.

Considerations for primary groups for objects

Any object on the system can have a primary group. Primary group authority can provide a performance advantage if the primary group is the first group for most users of an object.

Often, one group of users is responsible for some information about the system, such as customer information. That group needs more authority to the information than other system users. By using primary group authority, you can set up this type of authority scheme without affecting the performance of authority checking.

Related tasks:

“Case 2: Using primary group authority” on page 187

This case demonstrates how to use primary group authority.

Considerations for multiple group profiles

By using group profiles, you can manage authority more efficiently and reduce the number of individual private authorities for objects. However, the misuse of group profiles can have a negative effect on the performance of authority checking. This topic provides some suggestions on using multiple group profiles.

A user can be a member of up to 16 groups: the first group (GRPPRF parameter in the user profile) and 15 supplemental groups (SUPGRPPRF parameter in the user profile).

Here are suggestions when using multiple group profiles:

- Try to use multiple groups in combination with primary group authority and eliminate private authority to objects.
- Carefully plan the sequence in which group profiles are assigned to a user. The user’s first group should relate to the user’s primary assignment and the objects used most often. For example, assume a user called WAGNERB does inventory work regularly and does order entry work occasionally. The profile needed for inventory authority (DPTIC) should be WAGNERB’s first group. The profile needed for order entry work (DPTOE) should be WAGNERB’s first supplemental group.

Note: The sequence in which private authorities are specified for an object has no effect on authority checking performance.

- If you plan to use multiple groups, study the authority checking process described in “How the system checks authority” on page 169. Make sure that you understand how using multiple groups in combination with other authority techniques, such as authorization lists, might affect your system performance.

Accumulating special authorities for group profile members

Special authorities are cumulative for users who are members of multiple groups.

Special authorities of group profiles are available to the members of that group. User profiles that are members of one or more groups have their own special authorities, plus the special authorities of any group profiles for which the user is a member. Special authorities are cumulative for users who are members of multiple groups. For example, assume that profile GROUP1 has *JOBCTL, profile GROUP3 has *AUDIT, and profile GROUP16 has *IOSYSCFG special authorities. A user profile that has all three profiles as its group profiles has *JOBCTL, *AUDIT, and *IOSYSCFG special authorities.

Note: If a group member owns a program, the program adopts only the authority of the owner. The authorities of the owner’s group are not adopted.

Using an individual profile as a group profile

Creating profiles specifically to be group profiles is preferable to making existing profiles into group profiles.

You might find that a specific user has all of the authorities needed by a group of users and be tempted to make that user profile into a group profile. However, using an individual's profile as a group profile might cause problems in the future:

- If the user whose profile is used as the group profile changes responsibilities, a new profile needs to be designated as the group profile, authorities need to be changed, and object ownership needs to be transferred.
- All members of the group automatically have authority to any objects created by the group profile. The user whose profile is the group profile loses the ability to have private objects, unless that user specifically excludes other users.

Try to plan group profiles in advance. Create specific group profiles with password *NONE. If you discover after an application has been running that a user has authorities that should belong to a group of users, do the following actions:

1. Create a group profile.
2. Use the **GRTUSRAUT** command to give the user's authorities to the group profile.
3. Remove the private authorities from the user, because they are no longer needed. Use the **RVKOBJAUT** or **EDTOBJAUT** command.

Comparison of group profiles and authorization lists

Group profiles are used to simplify managing user profiles that have similar security requirements. Authorization lists are used to secure objects with similar security requirements.

Table 131 shows the characteristics of the two methods.

Table 131. Authorization list and group profile comparison

Item being compared	Authorization list	Group profile
Used to secure multiple objects	Yes	Yes
User can belong to more than one	Yes	Yes
Private authority overrides other authority	Yes	Yes
User must be assigned authority independently	Yes	No
Authorities specified are the same for all objects	Yes	No
Object can be secured by more than one	No	Yes
Authority can be specified when the object is created	Yes	Yes ¹
Can secure all object types	No	Yes
Association with object is deleted when the object is deleted	Yes	Yes
Association with object is saved when the object is saved	Yes	Yes ²
¹ The group profile can be given authority when an object is created by using the GRPAUT parameter in the profile of the user creating an object.		
² Primary group authority is saved with the object. Private group authorities are saved if PVTAUT(*YES) is specified on the save command.		

For the authorization list of the item "Authority can be specified when the object is created":

- To assign an authorization list to a library-based object, specify AUT (*LIBCRTAUT) on the CRTxxx command and the CRTAUT (authorization-list-name) for the library. Some objects, such as validation lists, cannot use a value of *LIBCRTAUT in the CRT command.
- To assign an authorization list to a directory-based object, specify the *INDIR value for the DTAAUT and OBJAUT parameters on the MKDIR command. In this way, the authorization list secures both the parent directory and the new one. The system does not allow an arbitrary authorization list to be specified when an object is created.

Planning security for programmers

Programmers pose a problem for the security officer. Their knowledge makes it possible for them to bypass security procedures that are not carefully designed.

Programmers can bypass security to access data they need for testing. They can also circumvent the normal procedures that allocate system resources in order to achieve better performance for their own jobs. Security is often seen by them as a hindrance to doing the tasks required by their job, such as testing applications. However, giving programmers too much authority on the system breaks the security principle of separating duties. It also allows a programmer to install unauthorized programs.

Follow these guidelines when setting up an environment for application programmers:

- Do not grant all special authorities to programmers. If you must give programmers special authorities, give them only the special authority that is required to perform the jobs or tasks that are assigned to the programmer.
- Do not use the QPGMR user profile as a group profile for programmers.
- Use test libraries and prevent access to production libraries.
- Create programmer libraries and use a program that adopts authority to copy selected production data to programmer libraries for testing.
- If interactive performance is an issue, consider changing the commands for creating programs to run only in batch:


```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```
- Perform security auditing of application function before moving applications or program changes from test to production libraries.
- Use the group profile technique when an application is being developed. Have all application programs owned by a group profile. Make programmers who work on the application members of the group and define the programmer user profiles to have the group own any new objects that are created (OWNER(*GRPPRF)). When a programmer moves from one project to another, you can change the group information in the programmer's profile. See "Group ownership of objects" on page 143 for more information.
- Develop a plan for assigning ownership of applications when they are moved into production. To control changes to a production application, all application objects, including programs, should be owned by the user profile that is designated for the application.

Application objects should not be owned by a programmer because the programmer can have uncontrolled access to them in a production environment. The profile that owns the application might be the profile of the individual responsible for the application, or it might be a profile specifically created as the application owner.

Managing source files

To protect the information on your system, you need carefully plan the security of source files.

Source files are important to the integrity of your system. They might also be a valuable company asset, if you have developed or acquired custom applications. Source files should be protected like any other important file on the system. Consider placing source files in separate libraries and controlling who can update them and who can move them to production.

When a source file is created on the system, the default public authority is *CHANGE. This allows any user to update any source member. By default, only the owner of the source file or a user with *ALLOBJ special authority can add or remove members. In most cases, this default authority for source physical files should be changed. Programmers working on an application need *OBJMGT authority to the source files in order to add new members. The public authority should be reduced to *USE or *EXCLUDE, unless the source files are in a controlled library.

Protecting Java class files and jar files in the integrated file system

To run a Java program, you will need read (*R) authority to each Java class and jar file plus execute (*X) authority to each directory in the path to the Java class and jar files. If you use Java class and jar files in the integrated file system, you need to protect them using normal object authorities.

To protect Java files, use the **CHGAUT** command to secure the directories in the path and the files with object authority attributes. A user might need read (*R) authority to the Java class and jar files to run a Java program. They can get that authority from the public authority of the file or from private authority. An authorization list is helpful in setting up private authority for a group of users. Do not give anyone write (*W) authority to the file unless they are allowed to change the file.

You can use the Classpath Security Check Level (CHKPATH) parameter on the **RUNJVA** command to make sure that a running Java application is using the correct files from the CLASSPATH. You can use a value of CHKPATH(*SECURE) to prevent a Java program from running if one or more warning messages are sent for each directory in the CLASSPATH that has public write authority.

Planning security for system programmers or managers

You can limit the authority given to system programmers or managers to protect the files on your system.

Most systems have someone responsible for housekeeping functions. This person monitors the use of system resources, particularly disk storage, to make sure that users regularly remove unused objects to free space. System programmers need broad authority to observe all the objects on the system. However, they do not need to view the contents of those objects.

You can use adopted authority to provide a set of display commands for system programmers, rather than giving special authorities in their user profiles.

For example, you might want Sue and Fred to be the two people who can create and change user profiles without giving them special authorities. You can achieve this by doing the following steps.

1. Write a command or program that is a front end to the **CRT/CHGUSRPRF** command.
2. Have the command or program adopt a profile that can do the creates and changes.
3. Authorize Sue and Fred to the program.

Then Sue and Fred can only do the task through the application.

Using validation lists

Validation list objects provide a method for applications to securely store user-authentication information.

For example, the Internet Connection Server (ICS) uses validation lists to carry out the concept of an Internet user. The ICS can perform basic authentication before a Web page is served. Basic authentication requires users to provide some type of authentication information, such as a password, PIN, or account number. The name of the user and the authentication information can be stored securely in a validation list. The ICS can use the information from the validation list rather than require all users of the ICS to have a System i user id and password.

An internet user can be permitted or denied access to the system from the Web server. The user, however, has no authority to any System i resources or authority to sign-on or run jobs. A System i user profile is never created for the internet users.

To create and delete validation lists, you can use the CL commands Create Validation List (**CRTVLDL**) and the Delete Validation List (**DLTVLDL**). Application Programming Interfaces (APIs) are also provided to allow applications to add, change, remove, verify (authenticate), and find entries in a validation list.

Validation list objects are available for all applications to use. For example, if an application requires a password, the application passwords can be stored in a validation list object rather than a database file. The application can use the validation list APIs to verify a user's password. Since the validation list is encrypted, this method is more secure than using the application alone to verify the user's password.

You can store the authentication information in a decryptable form. If a user has the appropriate security, the authentication information can be decrypted and returned to the user.

Related reference:

“Retain Server Security (QRETSVRSEC)” on page 31

The Retain Server Security (QRETSVRSEC) system value determines whether decryptable authentication information associated with user profiles or validation list (*VLDL) entries can be retained on the host system. This does not include the System i user profile password.

Related information:

Application programming interfaces

Limit access to program function

The limit access to program function allows you to define who can use an application, the parts of an application, or the functions within a program.

This support is not a replacement for resource security. Limit access to program function does not prevent a user from accessing a resource (such as a file or program) from another interface. The function goes through the following processes to do the verification.

- Register a function
- Retrieve information about the function
- Define who can or cannot use the function
- Check to see if the user is allowed to use the function

The limit access to program function lets APIs perform the following tasks: To use this function within an application, the application provider must register the functions when the application is installed. The registered function corresponds to a code block for specific functions in the application. When the user runs the application, before the application invokes the code block, it calls the check usage API to verify that the user has the authority to use the function that is associated with the code block. If the user is allowed to use the registered function, the code block runs. If the user is not allowed to use the function, the user is prevented from running the code block.

The system administrator specifies who is allowed or denied access to a function. The administrator can either use the Work with Function Usage Information (**WRKFCNUSG**) command to manage the access to program function or use Application Administration in the System i Navigator.

Related information:

Application administration

Chapter 8. Backup and recovery of security information

Saving your security information is just as important as saving your data. In some situations, you might need to recover user profiles, object authorities, and the data on your system. If you do not have your security information saved, you might need to manually rebuild user profiles and object authorities. This can be time-consuming and can lead to errors and security exposures.

This topic includes information on the following topics:

- How security information is saved and restored
- How security affects saving and restoring objects
- Security issues associated with *SAVSYS special authority

Planning adequate backup and recovery procedures for security information requires understanding how the information is stored, saved, and restored.

Table 132 shows the commands that are used to save and restore security information. The sections that follow discuss saving and restoring security information in more detail.

Table 132. How security information is saved and restored

Security information saved or restored	Save and restore commands used					
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT	RSTDFROBJ
User profiles	X		X			
Object ownership ¹		X		X		X
Primary group ¹		X		X		X
Public authorities ¹		X		X		X
Private authorities ³	X	X	X	X	X	X
Authorization lists	X		X			
Authority holders	X		X			
Link with the authorization list and authority holders		X		X		
Object auditing value		X		X		
Function registration information ²		X		X		
Function usage information	X		X		X	
Validation lists		X		X		
Server Authentication Entries	X		X			

Table 132. How security information is saved and restored (continued)

Security information saved or restored	Save and restore commands used					
	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT	RSTDFROBJ
¹	The SAVSECDTA , SAVSYS , and RSTUSRPRF commands save and restore ownership, primary group, primary group authority, and public authority for these object types : User profile (*USRPRF), Authorization list (*AUTL), and Authority holder (*AUTHLR).					
²	The object to save/restore is QUSEXRGOBJ, type *EXITRG in QUSRSYS library.					
³	Private authorities for all objects are saved with SAVSECDTA . RSTUSRPRF will restore the authority information needed to restore the private authorities. The private authorities are restored with RSTAUT . Private authorities for individual objects can be saved with the SAV , SAVLIB , SAVOBJ , and SAVCHGOBJ commands. Private authorities for individual objects can be restored with the RST , RSTLIB , and RSTOBJ commands if they were saved with the save command.					

Related information:

Backup and recovery



Backup and recovery PDF

How security information is stored

Planning adequate backup and recovery procedures for security information requires understanding how the information is stored and saved.

Security information is stored with objects, user profiles, and authorization lists:

Authority information stored with object:

- Public authority
- Owner name
- Owner’s authority to object
- Primary group name
- Primary group’s authority to object
- Authorization list name
- Object auditing value
- Whether any private authority exists
- Whether any private authority is less than public

Authority information stored with user profile:

- *Heading Information:*
 - The user profile attributes shown on the Create User Profile display.
 - The uid and gid.
- *Private Authority Information:*
 - Private authority to objects. This includes private authority to authorization lists.
- *Ownership Information:*
 - List of owned objects
 - For each owned object, a list of users with private authority to the object.
- *Primary Group Information:*

- List of objects for which the profile is the primary group.
- *Auditing Information:*
 - Action auditing value
 - Object auditing value
- *Function Usage Information:*
 - Usage settings for registered functions.
- *Server Authentication Information:*
 - Server authentication entries.

Authority Information Stored with Authorization Lists:

- Normal authority information stored with any object, such as the public authority and owner.
- List of all objects secured by the authorization list.

Related concepts:

“Additional information associated with a user profile” on page 115

This topic discusses the private authorities, owned object information, and primary group object information that are associated with a user profile.

Saving security information

Security information is stored differently on the save media than it is on your system. When you save user profiles, the private authority information stored with the user profile is formatted into an authority table.

An authority table is built and saved for each user profile that has private authorities. This reformatting and saving of security information can be lengthy if you have many private authorities on your system.

This is how security information is stored on the save media:

Authority information saved with object:

- Public authority
- Owner name
- Owner’s authority to object
- Primary group name
- Primary group’s authority to object
- Authorization list name
- Field level authorities
- Object auditing value
- Whether any private authority exists
- Whether any private authority is less than public
- Private authorities for the object, if PVTAUT(*YES) is specified on the SAVxxx command

Authority information saved with authorization list:

- Normal authority information stored with any object, such as the public authority, owner, and primary group.

Authority information saved with user profile:

- The user profile attributes shown on the Create User Profile display.
- Other application information associated with the user profile. For example:
 - Server authentication entries

- User Application Information entries that are added using the Update User Application Information (QsyUpdateUserApplicationInfo) API

Authority table saved associated with user profile:

- One record for each private authority of the user profile, including usage settings for registered functions.

Function registration information saved with QUSEXRGOBJ object:

- The function registration information can be saved by saving the QUSEXRGOBJ *EXITRG object in QUSRSYS.

Recovering security information

Recovering your system often requires restoring data and associated security information.

The typical sequence for recovery is:

1. Restore user profiles and authorization lists (RSTUSRPRF USRPRF(*ALL)).
2. Restore objects (RSTCFG, RSTLIB, RSTOBJ, RSTDLO or RST).
3. Restore the private authorities to objects (RSTAUT).

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

Related information:



Backup and Recovery

Restoring user profiles

There might be some changes that are made to a user profile when it is restored.

The following rules apply:

- If profiles are being restored individually (RSTUSRPRF USRPRF(*ALL) is not specified), SECDTA(*PWDGRP) is not requested, and the profile that is being restored does not exist on the system, these fields are changed to *NONE:
 - Group profile name (GRPPRF)
 - Password (PASSWORD)
 - Document password (DOCPWD)
 - Supplemental group profiles (SUPGRPPRF)

Product passwords are changed to *NONE, so they will be incorrect after restoring an individual user profile that did not exist on the system.

- If profiles are being restored individually (RSTUSRPRF USRPRF(*ALL) is not specified) SECDTA(*PWDGRP) is not requested, and the profile exists on the system, the password, document password, and group profile are not changed.

User profiles can be restored individually with the password and group information restored from the save media by specifying the SECDTA(*PWDGRP) parameter on the RSTUSRPRF command. *ALLOBJ and *SECADM special authorities are required to restore the password and group information when restoring individual profiles. Product passwords restored with the user profile will be incorrect after restoring an individual user profile that existed on the system, unless the SECDTA(*PWDGRP) parameter is specified on the RSTUSRPRF command.

- If all of the user profiles are being restored to your system, all of the fields in any of the profiles that already exist on the system are restored from the save media, including the password.

Attention:

1. User Profiles saved from a system with a different password level (QPWDLVL system value) than the system that is being restored might result in having a password that is not valid on the restored system. For example, if the saved user profile came from a system that was running password level 2, the user can have a password of "This is my password". This password will not be valid on a system running password level 0 or 1.
2. Keep a record of the security officer (QSECOFR) password associated with each version of your security information that is saved. This ensures that you can sign on to your system if you need to do a complete restore operation.

You can use DST (Dedicated Service Tools) to reset the password for the QSECOFR profile.

- If a profile exists on the system, the restore operation does not change the uid or gid.
- If a profile does not exist on the system, the uid and gid for a profile are restored from the save media. If either the uid or the gid already exists on the system, the system generates a new value and issues a message (CPI3810).
- *ALLOBJ special authority is removed from user profiles that are being restored to a system at security level 30 or higher in either of these situations:
 - The profile was saved from a different system and the user performing the RSTUSRPRF does not have *ALLOBJ and *SECADM special authorities.
 - The profile was saved from a system at security level 10 or 20.

Attention: The system uses the machine serial number on the system and on the save media to determine whether objects are being restored to the same system or to a different system.

*ALLOBJ special authority is not removed from these IBM-supplied profiles:

- QSYS (system) user profile
- QSECOFR (security officer) user profile
- QLPAUTO (licensed program automatic install) user profile
- QLPINSTALL (licensed program install) user profile

- | • If a profile is restored (all profiles or individual profile) that already exists on the system, the restore operation will not change the existing user expiration fields.
- | • If a profile is restored (all profiles or individual profile) that does not yet exist on the system, all fields in the user profile are restored from the save media, including the user expiration interval and user expiration date fields:
 - | – If the profile is enabled and user expiration date is past, the user profile will be set to disabled and CPF2271 diagnostic message will be sent.
 - | – If the profile is enabled and the user expiration date has not past, the job scheduler entry will be added.

Related information:

Resetting the QSECOFR i5/OS user profile password

Restoring objects

When you restore an object to the system, the system uses the authority information stored with the object. This topic describes the rules applicable to the authority information when restoring objects.

The following applies to the security of the restored object:

Object ownership:

- If the profile that owns the object exists on the system, ownership is restored to that profile.
- If the owner profile does not exist on the system, ownership of the object is given to the QDFTOWN (default owner) user profile.

- If the object exists on the system and the owner on the system is different from the owner on the save media, the object is not restored unless ALWOBJDIF(*ALL), ALWOBJDIF(*OWNER), or ALWOBJDIF(*COMPATIBLE) is specified. In that case, the object is restored and the owner on the system is used.
- See “Restoring programs” on page 252 for additional considerations when restoring programs.

Primary group:

For an object that does not exist on the system:

- If the profile that is the primary group for the object is on the system, the primary group value and authority are restored for the object.
- If the profile that is the primary group does not exist on the system:
 - The primary group for the object is set to none.
 - The primary group authority is set to no authority.

When an existing object is restored, the primary group for the object is not changed by the restore operation.

Public authority:

- If the object that is being restored does not exist on the system, public authority is set to the public authority of the saved object.
- If the object that is being restored does exist and is being replaced, public authority is not changed. The public authority from the saved version of the object is not used.
- The CRTAUT for the library is not used when restoring objects to the library.

Authorization list:

- If an object, other than a document or folder, already exists on the system and is linked to an authorization list, the ALWOBJDIF parameter determines the result:
 - If ALWOBJDIF(*NONE) is specified, the existing object must have the same authorization list as the saved object. If not, the object is not restored.
 - If ALWOBJDIF(*ALL), ALWOBJDIF(*AUTL), or ALWOBJDIF(*COMPATIBLE) is specified, the object is restored. The object is linked to the authorization list that is associated with the existing object.
- If a document or folder that already exists on the system is restored, the authorization list that is associated with the object on the system is used. The authorization list from the saved document or folder is not used.
- If the authorization list does not exist on the system, the object is restored without being linked to an authorization list and the public authority is changed to *EXCLUDE.
- If the object is being restored on the same system from which it was saved, the object is linked to the authorization list again.
- If the object is being restored on a different system, the ALWOBJDIF parameter on the restore command is used to determine whether the object is linked to the authorization list:
 - If ALWOBJDIF(*ALL), ALWOBJDIF(*AUTL), or ALWOBJDIF(*COMPATIBLE) is specified, the object is linked to the authorization list.
 - If ALWOBJDIF(*NONE) is specified, then the object is not linked to the authorization list and the public authority of the object is changed to *EXCLUDE.

Private authorities:

- Private authority is saved with user profiles, and with objects if PVTAUT(*YES) is specified on the SAVxxx command.

- If user profiles have private authority to an object that is being restored, those private authorities are typically not affected. Restoring certain types of programs might result in private authorities being revoked.
- If an object is deleted from the system, the private authority for the object no longer exists on the system. When an object is deleted, all private authority to the object is removed from user profiles. If the object is then restored from a save version, the private authorities can be restored if PVTAUT(*YES) was specified when the object was saved.
- If private authorities need to be recovered and the private authorities were not saved with the object, then the Restore Authority (RSTAUT) command must be used. The normal sequence is:
 1. Restore user profiles
 2. Restore objects
 3. Restore authority

Object auditing:

- If the object that is being restored does not exist on the system, the object auditing (OBJAUD) value of the saved object is restored.
- If the object that is being restored does exist and is being replaced, the object auditing value is not changed. The OBJAUD value of the saved version of the object is not restored.
- If a library or directory that is being restored does not exist on the system, the create object or directory auditing (CRTOBJAUD) value for the library or directory is restored.
- If a library or directory that is being restored exists and is being replaced, the CRTOBJAUD value for the library or directory is not restored. The CRTOBJAUD value for the existing library or directory is used.

Authority holder:

- If a file is restored and an authority holder exists for that file name as well as the library to which it is being restored, the file is linked to the authority holder.
- The authority information associated with the authority holder replaces the public authority and owner information saved with the file.

User domain objects:

The system restricts user domain objects (*USRSPC, *USRIDX, and *USRQ) to the libraries specified in the QALWUSRDMN system value. If a library is removed from the QALWUSRDMN system value after a user domain object of type *USRSPC, *USRIDX, or *USRQ is saved, the system changes the object to system domain when it is restored.

Function registration information:

The function registration information can be restored by restoring the QUSEXRGOBJ *EXITRG object into QUSRSYS. This restores all of the registered functions. The usage information associated with the functions is restored when user profiles and authorities are restored.

Applications that use certificates registration:

The applications that use certificates registration information can be restored by restoring the QUSEXRGOBJ *EXITRG object into QUSRSYS. This restores all of the registered applications. The association of the application to its certificate information can be restored by restoring the QYCDCERTI *USRIDX object into QUSRSYS.

Related concepts:

“Restoring programs” on page 252

Restoring programs to your system that are obtained from an unknown source poses a security exposure. This topic provides information about the factors that should be taken into consideration when restoring

programs.

“Restoring authorization lists” on page 254

No method exists for restoring an individual authorization list. When you restore an authorization list, authority and ownership are established just as they are for any other object that is restored.

Restoring authority

When security information is restored, private authorities must be rebuilt. When you restore a user profile that has an authority table, the authority table for the profile is also restored.

The Restore Authority (**RSTAUT**) command rebuilds the private authority in the user profile by using the information from the authority table. The grant authority operation runs for each private authority in the authority table. This can be a lengthy process if authority is being restored for many profiles and if many private authorities exist in the authority tables.

The **RSTUSRPRF** and **RSTAUT** commands can be run for a single profile, a list of profiles, a generic profile name, or all profiles. The system searches the save media or save file that was created by the **SAVSECDDTA** command, the **SAVSYS** command, or the **QSRSAVO** API to find the profiles you want to restore.

If the private authorities are saved with objects, you can optionally restore them with the objects. It is suggested if you are saving and restoring a relatively small number of objects, rather than an entire system.

Restoring field authority:

The following steps are required to restore private field authorities for database files that do not already exist on the system:

- Restore or create the necessary user profiles.
- Restore the files.
- Run the Restore Authority (**RSTAUT**) command.

The private field authorities are not fully restored until the private object authorities that they restrict are also established again.

Restoring programs

Restoring programs to your system that are obtained from an unknown source poses a security exposure. This topic provides information about the factors that should be taken into consideration when restoring programs.

Programs might perform operations that break your security requirements. Of particular concern are programs that contain restricted instructions, programs that adopt their owner authority, and programs that have been tampered with. This includes object types ***PGM**, ***SRVPGM**, ***MODULE**, and ***CRQD**. You can use the **QVfyOBRST**, **QFRCCVNRST**, and **QALWOBJRST** system values to prevent these object types from being restored to your system.

The system uses a validation value to help protect programs. This value is stored with a program and recalculated when the program is restored. The system's actions are determined by the **ALWObjDIF** parameter on the restore command and the Force conversion on restore (**QFRCCVNRST**) system value.

Note: Programs contain information that allows the program to be re-created at restore time if necessary. The information needed to re-create the program remains with the program even when the observability of the program is removed. If a program validation error is determined to exist at the time the program is restored, the program will be re-created in order to correct the program validation error.

Restoring programs that adopt the owner's authority:

When a program that adopts owner authority is restored, the ownership and authority to the program might be changed. The following applies:

- The user profile doing the restore operation must either own the program or have *ALLOBJ and *SECADM special authorities.
- The user profile doing the restore operation can receive the authority to restore the program by
 - Being the program owner.
 - Being a member of the group profile that owns the program (unless you have private authority to the program).
 - Having *ALLOBJ and *SECADM special authority.
 - Being a member of a group profile that has *ALLOBJ and *SECADM special authority.
 - Running under adopted authority that meets one of the tests just listed.
- If the restoring profile does not have adequate authority, all public and private authorities to the program are revoked, and the public authority is changed to *EXCLUDE.
- If the owner of the program does not exist on the system, ownership is given to the QDFTOWN user profile. Public authority is changed to *EXCLUDE and the authorization list is removed.

Related concepts:

“Restoring objects” on page 249

When you restore an object to the system, the system uses the authority information stored with the object. This topic describes the rules applicable to the authority information when restoring objects.

Related reference:

“Security-related restore system values” on page 41

This topic introduces the security-related restore system values on your IBM i operating system.

Restoring licensed programs

This topic introduces the instructions on restoring the licensed programs on your system.

The Restore Licensed Programs (**RSTLICPGM**) command is used to install IBM-supplied programs on your system. It can also be used to install non-IBM programs that were created by using the IBM System Manager for IBM i licensed program.

When your system is shipped, only users with *ALLOBJ special authority can use the **RSTLICPGM** command. The RSTLICPGM procedure calls an exit program to install programs that are not supplied by IBM.

To protect security on your system, the exit program should not run using a profile with *ALLOBJ special authority. Instead of having a user with *ALLOBJ authority run the command directly, use a program that adopts *ALLOBJ special authority to run the **RSTLICPGM** command.

Here is an example of this technique. The program to be installed using the **RSTLICPGM** command is called CPAPP (Contracts and Pricing).

1. Create a user profile with sufficient authority to successfully install the application. Do not give this profile *ALLOBJ special authority. In this example, the user profile is called OWNCP.
2. Write a program to install the application. In this example, the program is called CPINST:

Note: By using the code examples, you agree to the terms of the Chapter 10, “Code license and disclaimer information,” on page 307.

```
PGM
RSTLICPGM CPAPP
ENDPGM
```

3. Create the CPINST program to adopt the authority of a user with *ALLOBJ special authority, such as QSECOFR, and authorize OWNCP to the program:

```
CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +  
      AUT(*EXCLUDE)  
GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +  
      USER(OWNCP) AUT(*USE)
```

4. Sign on as OWNCP and call the CPINST program. When the CPINST program runs the RSTLICPGM command, you are running under QSECOFR authority. When the exit program runs to install the CPAPP programs, it drops adopted authority. The programs called by the exit program run under the authority of OWNCP.

Restoring authorization lists

No method exists for restoring an individual authorization list. When you restore an authorization list, authority and ownership are established just as they are for any other object that is restored.

The link between authorization lists and objects is established if the objects are restored after the authorization list. Users' private authorities to the list are restored using the **RSTAUT** command.

Authorization lists are saved by either the **SAVECDTA** command or the **SAVSYS** command. Authorization lists are restored by the command:

```
RSTUSRPRF USRPRF(*ALL)
```

Recovering from a damaged authorization list

When an authorization list that secures an object becomes damaged, access to the object is limited to users that have all object (*ALLOBJ) special authority.

To recover from a damaged authorization list, two steps are required:

1. Recover users and their authorities on the authorization list.
2. Recover the association of the authorization list with the objects.

These steps must be done by a user with *ALLOBJ special authority.

Related concepts:

"Restoring objects" on page 249

When you restore an object to the system, the system uses the authority information stored with the object. This topic describes the rules applicable to the authority information when restoring objects.

Recovering the authorization list

Use the instructions in this topic to recover the authorization list.

If users' authorities to the authorization list are known, you can restore the authorization list by following the steps below.

1. Delete the authorization list.
2. Create the authorization list again.
3. Add all known users to it.

If you do not know all of the user authorities, you can restore the authorization list by using the last saved SAVSYS or SAVECDTA tapes. To restore the authorization list, do the following actions:

1. Delete the damaged authorization list using the Delete Authorization List (DLTAUTL) command.
2. Restore the authorization list by restoring user profiles:
RSTUSRPRF USRPRF(*ALL)
3. Restore users' private authorities to the list by using the RSTAUT command.

This procedure restores user profile values from the save media. Refer to “Restoring user profiles” on page 248 for more information about restoring user profiles values from save media.

Recovering the association of objects to the authorization list

Follow the steps in this topic to recover the association of objects to the authorization list.

When the damaged authorization list is deleted, the objects that were secured by the authorization list need to be added to the new authorization list. Do the following actions:

1. Find the objects that were associated with the damaged authorization list by using the Reclaim Storage (**RCLSTG**) command. Reclaim storage assigns the objects that were associated with the authorization list to the QRCLAUTL authorization list.
2. Use the Display Authorization List Objects (**DSPAUTOBJ**) command to list the objects that are associated with the QRCLAUTL authorization list.
3. Use the Grant Object Authority (**GRTOBJAUT**) command to secure each object with the correct authorization list:

```
GRTOBJAUT OBJ(library-name/object-name) +  
           OBJTYPE(object-type) +  
           AUTL(authorization-list-name)
```

If a large number of objects are associated with the QRCLAUTL authorization list, create a database file by specifying OUTPUT(*OUTFILE) on the **DSPAUTOBJ** command. You can write a CL program to run the **GRTOBJAUT** command for each object in the file.

Restoring the operating system

When you perform a manual IPL on your system, the IPL or Install the System menu provides an option to install the operating system. The dedicated service tools (DST) function provides the ability to require anyone using this menu option to enter the DST security password. You can use this to prevent someone from restoring an unauthorized copy of the operating system.

To secure the installation of your operating system, do the following actions:

1. Perform a manual IPL.
2. From the IPL or Install the System menu, select DST.
3. From the Use DST menu, select the option to work with the DST environment.
4. Select the option to change DST passwords.
5. Select the option to change the operating system install security.
6. Specify 1 (secure).
7. Press F3 (exit) until you return to the IPL or Install the System menu.
8. Complete the manual IPL and return the keylock to its normal position.

Notes:

1. If you no longer want to secure the installation of the operating system, follow the same steps and specify 2 (not secure).
2. You can also prevent installation of the operating system by keeping your keylock switch in the normal position and removing the key.

*SAVSYS special authority

To save or restore an object, you must have *OBJEXIST authority to the object or *SAVSYS special authority. A user with *SAVSYS special authority does not need any additional authority to an object to save or restore it.

*SAVSYS special authority gives a user the capability to save an object and take it to a different system to be restored or to display (dump) the media to view the data. It also gives a user the capability to save an object and free storage thus deleting the data in the object. When saving documents, a user with *SAVSYS special authority has the option to delete those documents. *SAVSYS special authority should be given carefully.

Auditing save and restore operations

A security audit record is written for each restore operation if the action auditing value (QAUDLVL system value or AUDLVL in the user profile) includes *SAVRST. When you use a command that restores a large number of objects, such as RSTLIB, an audit record is written for each object restored. This might cause problems with the size of the audit journal receiver, particularly if you are restoring more than one library.

The **RSTCFG** command does not create an audit record for each object restored. If you want to have an audit record of this command, set object auditing for the command itself. One audit record will be written whenever the command is run.

Commands that save a very large number of objects, such as SAVSYS, SAVSECDTA, and SAVCFG, do not create individual audit records for the objects saved, even if the saved objects have object auditing active. To monitor these commands, set up object auditing for the commands themselves.

Chapter 9. Auditing security on System i

This section describes techniques for auditing the effectiveness of security on your system.

People audit their system security for several reasons:

- To evaluate whether the security plan is complete.
- To make sure that the planned security controls are in place and working. This type of auditing is performed by the security officer as part of daily security administration. It is also performed, sometimes in greater detail, as part of a periodic security review by internal or external auditors.
- To make sure that system security is keeping pace with changes to the system environment. Some examples of changes that affect security are:
 - New objects created by system users
 - New users admitted to the system
 - Change of object ownership (authorization not adjusted)
 - Change of responsibilities (user group changed)
 - Temporary authority (not timely revoked)
 - New products installed
- To prepare for a future event, such as installing a new application, moving to a higher security level, or setting up a communications network.

The techniques described in this section are appropriate for all of these situations. Which things you audit and how often depends on the size and security needs of your organization. The purpose of this section is to discuss what information is available, how to obtain it, and why it is needed, rather than to give guidelines for the frequency of audits.

This section has three parts:

- A checklist of security items that can be planned and audited.
- Information about setting up and using the audit journal provided by the system.
- Other techniques that are available to gather security information about the system.

Security auditing involves using commands in the System i environment and accessing log and journal information about the system. You might want to create a special profile to be used by someone doing a security audit of your system. The auditor profile will need *AUDIT special authority to be able to change the audit characteristics of your system. Some of the auditing tasks suggested in this section require a user profile with *ALLOBJ and *SECADM special authority. Make sure that you set the password for the auditor profile to *NONE when the audit period has ended.

Related concepts:

“Security audit journal” on page 6

You can use security audit journals to audit the effectiveness of security on your system.

Checklist for security officers and auditors

You can use the checklist to plan and audit your system's security.

As you plan security, choose the subjects from this collection that best meet your security requirements. When you audit the security of your system, use the list to evaluate the controls that you have in place and to determine if additional controls are needed.

Each list serves as a review of the information in this topic collection. They contain brief descriptions of how to do each item and how to verify that the item has been done, including what entries in the QAUDJRN journal to look for. Details about the items are found throughout this topic collection.

Physical security

You can use the physical security checklist to plan or audit physical security of your system.

Note: See Planning and setting up system security for a complete discussion of physical security on the System i product.

Here is a checklist for planning physical security of your system:

- ___ • The system unit and console are in a secure location.
- ___ • Backup media is protected from damage and theft.
- ___ • The keylock switch setting on the processor unit is in the Secure or Auto position. The keys are removed and kept separately under tight physical security. See Planning physical security for the system unit for more information about the keylock switch.
- ___ • Access to publicly located workstations and the console is restricted. Use the DSPOBJAUT command to see who has *CHANGE authority to the workstations. Look for AF entries in the audit journal with the object type field equal to *DEVD to find attempts to sign on at restricted workstations.
- ___ • Sign-on for users with *ALLOBJ or *SERVICE special authority is limited to a few workstations. Check to see that the QLMTSECOFR system value is 1. Use the DSPOBJAUT command for devices to see if the QSECOFR profile has *CHANGE authority.

System values

Setting up the auditing function for system values helps you to track the changed values on the system.

- Security system values follow recommended guidelines. To print the security system values, type: WRKSYSVAL *SEC OUTPUT(*PRINT). Two important system values to audit are:
 - QSECURITY, which should be set to 40 or higher.
 - QMAXSIGN, which should not be greater than 5.

Note: If the auditing function is active, an SV entry is written to the QAUDJRN journal whenever a system value is changed.

- Use the Display Security Attributes (DSPSECA) command to verify the current and pending values of QSECURITY (security level) and QPWDLVL (password level), and the current setting of the security related system (whether the values can be changed).
- Review decisions about system values periodically. This is particularly important when the system environment changes, such as the installation of new applications or a communications network.

IBM-supplied user profiles

You can perform auditing tasks on IBM-supplied user profiles by verifying their passwords.

- The password has been changed for the QSECOFR user profile.

This profile is shipped with the password set to QSECOFR so you can sign on to install your system. The password must be changed the first time you sign on to your system and changed periodically after the installation.

Verify that it has been changed by checking a DSPAUTUSR list for the date the QSECOFR password was changed and by attempting to sign on with the default password.

- The IBM passwords for dedicated service tools (DST) are changed.

User IDs for service tools do not appear on a DSPAUTUSR list. To verify that the user IDs and passwords are changed, start DST and attempt to use the default values.

- With the exception of QSECOFR, do not sign on with the IBM-supplied user profiles.

These IBM-supplied profiles are designed to own objects or to run system functions. Use a DSPAUTUSR list to verify that the IBM-supplied user profiles listed in Appendix B, "IBM-supplied user profiles," on page 319, except QSECOFR, have a password of *NONE.

Related concepts:

"IBM-supplied user profiles" on page 128

A number of user profiles are shipped with your system software. These IBM-supplied user profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

"Working with service tools user IDs" on page 129

There are several enhancements and additions to service tools that make them easier to use and understand.

Related reference:

Appendix B, "IBM-supplied user profiles," on page 319

This section contains information about the user profiles that are shipped with the system. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

Password control

You can use the password control mechanism to audit your system security.

- Users can change their own passwords.

Allowing users to define their own passwords reduces the need for users to write down their passwords. Users should have access to the CHGPWD command or to the Change Password function from the Security (GO SECURITY) menu.

- A password change is required according to the organization's security guidelines, such as every 30 to 90 days.

The QPWDEXPITV system value is set to meet the security guidelines.

- If a user profile has a password expiration interval that is different from the system value, it meets the security guidelines.

Review user profiles for a PWDEXPITV value other than *SYSVAL.

- Trivial passwords are prevented by using the system values to set the password rules and by using a password approval program.

Use the WRKSYSVAL *SEC command and look at the settings for the values beginning with QPWD.

- Group profiles have a password of *NONE.

Use the DSPAUTUSR command to check for any group profiles that have passwords.

Whenever the system is not operating at password level 3 and users change their password, the system attempts to create an equivalent password that is usable at the other password levels. You can use the PRTUSRPRF TYPE(*PWDLVL) command to see which user profiles have passwords that are usable at the various password levels.

Note: The equivalent password is a best effort attempt to create a usable password for the other password levels but it may not have passed all of the password rules if the other password level was in effect. For example, if password BbAaA3x is specified at password level 2, the system will

create an equivalent password of BBAAA3X for use at password levels 0 and 1. This can be true even if the QPWDLMTCHR system value includes 'A' as one of the limited characters (QPWDLMTCHR is not enforced at password level 2) or QPWDLMTREP system value specified that consecutive characters cannot be the same (because the check is case-sensitive at password level 2 but not case sensitive at password levels 0 and 1).

User and group profiles

You can validate the user and group profiles and their authorities to audit the security effectiveness on your system.

- Each user is assigned a unique user profile.

Set the QLMTDEVSSN system value to 1. Although limiting each user to one device session at a time does not prevent sharing user profiles, it discourages it.

- User profiles with *ALLOBJ special authority are limited, and are not used as group profiles.

Use the DSPUSRPRF command to check the special authorities for user profiles and to determine which profiles are group profiles. The topic “Printing selected user profiles” on page 302 shows how to use an output file and query to determine this.

- The *Limit capabilities* field is *YES in the profiles of users who should be restricted to a set of menus.

The topic “Printing selected user profiles” on page 302 gives an example of how to determine this.

- Programmers are restricted from production libraries.

Use the DSPOBJAUT command to determine the public and private authorities for production libraries and critical objects in the libraries. “Planning security for programmers” on page 242 has more information about security and the programming environment.

- Membership in a group profile is changed when job responsibilities change.

To verify group membership, use one of these commands:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF profile-name *GRPMBR
```

- You should use a naming convention for group profiles.

When authorities are displayed, you can then easily recognize the group profile.

- The administration of user profiles is adequately organized.

No user profiles have large numbers of private authorities. The topic “Examining large user profiles” on page 302 discusses how to find and examine large user profiles on your system.

- Employees are removed from the system immediately when they are transferred or released.

Regularly review the DSPAUTUSR list to make sure only active employees have access to the system. To make sure user profiles are deleted immediately after employees leave, review the DO (Delete Object) entries in the audit journal.

- Management regularly verifies the users authorized to the system.

Use the DSPAUTUSR command to view users authorization information.

- The password for an inactive employee is set to *NONE.

Use the DSPAUTUSR command to verify that the inactive user profiles do not have passwords.

- Management regularly verifies the users with special authorities, particularly *ALLOBJ *SAVSYS, and *AUDIT special authorities.

The topic “Printing selected user profiles” on page 302 gives an example of how to determine this.

Authorization control

Authorization control enables you to audit the security of the information stored on your system.

You can use the following checklist to help you audit authorization control security.

- Owners of data understand their obligation to authorize users on a need-to-know basis.
- Owners of objects regularly verify the authority to use the objects, including public authority.

The WRKOBJOWN command provides a display for working with the authorities to all objects owned by a user profile.

- Sensitive data is not public. Check the authority for user *PUBLIC for critical objects using the DSPOBJAUT command.
- Authority to user profiles is controlled.

The public authority to user profiles should be *EXCLUDE. This prevents users from submitting jobs that run under another user’s profile.

- Job descriptions are controlled:
 - Job descriptions with public authority of *USE or greater are specified as USER(*RQD). This means jobs submitted using the job description must run using the submitter’s profile.
 - Job descriptions that specify a user have public authority *EXCLUDE. Authorization to use these job descriptions is controlled. This prevents unauthorized users from submitting jobs that run using another profile’s authority.

To find out what job descriptions are on the system, type:

```
DSPOBJD OBJ(*ALL/*ALL) OBJTYPE(*JOB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```

To check the *User* parameter of a job description, use the Display Job Description (DSPJOB) command. To check the authority to a job description, use the Display Object Authority (DSPOBJAUT) command.

Note: At security level 40 or 50, a user submitting a job using a job description that specifies a user profile name must have *USE authority to both the job description and the user profile. At all security levels, an attempt to submit or schedule a job without *USE authority to the user specified in the job description causes an AF entry with violation type J in the audit journal.

- Users are not allowed to sign on by pressing the Enter key on the Sign On display.

Make sure no workstation entries in the subsystem descriptions specify a job description that has a user profile name specified for the USER parameter.

Default sign-on is prevented at security level 40 or 50, even if a subsystem description allows it. At all security levels, an AF entry with violation type S is written to the audit journal if default sign-on is attempted and a subsystem description is defined to allow it.

- The library list in application programs is controlled to prevent a library that contains a similar program from being added before the production libraries.

The topic “Library lists” on page 207 discusses methods for controlling the library list.

- Programs that adopt authority are used only when required and are carefully controlled.

See the topic “Analyzing programs that adopt authority” on page 303 for an explanation of how to evaluate the use of the program adopt function.

- Application program interfaces (APIs) are secured.
- Good object security techniques are used to avoid performance problems.

Unauthorized access

Use this checklist along with auditing journal to audit unauthorized attempts to access information.

- Security-related events are logged to the security auditing journal (QAUDJRN) when the auditing function is active.

To audit authority failures, use the following system values and settings:

- QAUDCTL must be set to *AUDLVL.
- QAUDLVL must include the values of *PGMFAIL and *AUTFAIL.

The best method to detect unauthorized attempts to access information is to review entries in the audit journal on a regular basis.

- The QMAXSIGN system value limits the number of consecutive incorrect access attempts to five or less. The QMAXSGNACN system value is set at 2 or 3.
- The QSYSMSG message queue is created and monitored.
- The audit journal is audited for repeated attempts by a user. (Authorization failures cause AF type entries in the audit journal.)
- Programs fail to access objects using interfaces that are not supported. (QSECURITY system value is set to 40 or 50.)
- User ID and password are required to sign on.

Security levels 40 and 50 enforce this. At level 20 or 30, you must make sure that no subsystem descriptions have a workstation entry that uses a job description that has a user profile name.

Unauthorized programs

The Check Object Integrity (CHKOBJITG) command allows you to audit unauthorized changes to program changes on the system.

- The QALWOBJRST system value is set to *NONE to prevent anyone from restoring security-sensitive programs to the system.
- The Check Object Integrity (CHKOBJITG) command is run periodically to detect unauthorized changes to program objects.

This command is described in “Checking for objects that have been altered” on page 304.

Communications

This checklist can be used to plan and audit the controls needed over various types of communications on the system.

- Use call-back procedures to protect telephone communications.
- Use encryption on sensitive data.
- Control remote sign-on. The QRMTSIGN system value is set to *FRCSIGNON or a pass-through validation program is used.
- Use the JOBACN, PCSACC, and DDMACC network attributes to control access to data from other systems, including personal computers. The JOBACN network attribute should be *FILE.

Using the security audit journal

The security audit journal is the primary source of auditing information about the system. This section describes how to plan, set up, and manage security auditing, what information is recorded, and how to view that information.

A security auditor inside or outside your organization can use the auditing function that is provided by the system to gather information about security-related events that occur on the system.

You can define auditing on your system at three different levels:

- System-wide auditing that occurs for all users.
- Auditing that occurs for specific objects.
- Auditing that occurs for specific users.

You use system values, user profile parameters, and object parameters to define auditing. “Planning security auditing” describes how to do this.

When a security-related event that might be audited occurs, the system checks whether you have selected that event for audit. If you have, the system writes a journal entry in the current receiver for the security auditing journal (QAUDJRN in library QSYS).

When you want to analyze the audit information you have collected in the QAUDJRN journal, you can use the Display Journal (DSPJRN) command. With this command, information from the QAUDJRN journal can be written to a database file. You can use an application program or a query tool to analyze the data.

Related reference:

Appendix F, “Layout of audit journal entries,” on page 563

This section contains layout information for all entry types with journal code T in the audit (QAUDJRN) journal. These entries are controlled by the action and object auditing you define.

Appendix E, “Object operations and auditing,” on page 499

This topic collection lists operations that can be performed against objects on the system, and whether those operations are audited.

Planning security auditing

The security auditing function is optional. You must take specific steps to set up security auditing.

To plan the use of security auditing on your system, follow these steps:

- Determine which security-relevant events you want to record for all system users. The auditing of security-relevant events is called *action auditing*.
- Check whether you need additional auditing for specific users.
- Decide whether you want to audit the use of specific objects on the system.
- Determine whether object auditing should be used for all users or specific users.

Planning the auditing of actions

The QAUDCTL (audit control) system value, the QAUDLVL (audit level) system value, the QAUDLVL2 (audit level extension) system value, and the AUDLVL (action auditing) parameter in user profiles work together to control action auditing.

The functions of each system value are as follows:

- The QAUDLVL system value specifies which actions are audited for all users of the system.
- The QAUDLVL2 system value also specifies which actions are audited for all users of the system, and is used when more than 16 auditing values are needed.
- The AUDLVL parameter in the user profile determines which actions are audited for a specific user. The values for the AUDLVL parameter apply *in addition to* the values for the QAUDLVL and QAUDLVL2 system values.
- The QAUDCTL system value starts and stops action auditing.

The events that you choose to log depends on both your security objectives and your potential exposures. “Action auditing” on page 113 describes the possible audit level values and how you can use them. It shows whether they are available as a system value, a user profile parameter, or both.

Related reference:

“Auditing Level (QAUDLVL)” on page 67

The Auditing Level (QAUDLVL) system value along with the QAUDLVL2 system value determines which security-related events are logged to the security audit journal (QAUDJRN) for all system users.

“Auditing Level Extension (QAUDLVL2)” on page 69

The Auditing Level Extension (QAUDLVL2) system value is required when more than sixteen auditing values are needed.

“Action auditing” on page 113

For an individual user, you can specify which security-relevant actions should be recorded in the audit journal. The actions specified for an individual user apply in addition to the actions specified for all users by the QAUDLVL and QAUDLVL2 system values.

Action auditing values:

This table lists the possible values available on the QAUDLVL and QAUDLVL2 system values and the CHGUSRAUD command when auditing actions of the system.

Table 133. Action auditing values

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*NONE	Yes	Yes	If the QAUDLVL system value is *NONE, no actions are logged on a system-wide basis. Actions are logged for individual users based on the AUDLVL value in their user profiles. If the AUDLVL value in a user profile is *NONE, no additional action auditing is done for this user. Any actions specified for the QAUDLVL system value are logged for this user.
*ATNEVT	Yes	No	Attention events: The system writes a journal entry for events that require further examination. With this information, you can determine the potential significance of the attention event to the system.
*AUTFAIL	Yes	Yes	Authorization failures: Unsuccessful attempts to sign on the system and to access objects are logged. *AUTFAIL can be used regularly to monitor users trying to perform unauthorized functions on the system. *AUTFAIL can also be used to assist with migration to a higher security level and to test resource security for a new application.
*CMD	No	Yes	Commands: The system logs command strings run by a user. If a command is run from a CL program that is created with LOG(*NO) and ALWRTVSRC(*NO), then only the command name and library name are logged. *CMD can be used to record the actions of a particular user, such as the security officer.
*CREATE	Yes	Yes	Creating objects: The system writes a journal entry when a new or replacement object is created. *CREATE can be used to monitor when programs are created or recompiled.
*DELETE	Yes	Yes	Deleting objects: The system writes a journal entry when an object is deleted.

Table 133. Action auditing values (continued)

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*JOBBAS	Yes	Yes	Job base functions: Actions that affect a job are logged, such as starting or stopping a job, holding, releasing, canceling, or changing the job.
*JOBCHGUSR	Yes	Yes	Job change user: Changes to a thread's active user profile or its group profiles are logged.
*JOBDTA	Yes	Yes	Job tasks: Actions that affect a job are logged, such as starting or stopping a job, holding, releasing, canceling, or changing the job, changing the thread's active user profile or group profile. *JOBDTA can be used to monitor who is running batch jobs. *JOBDTA is composed of two values, which are *JOBBAS and *JOBCHGUSR, to enable you to better customize your auditing.
*NETBAS	Yes	Yes	Network base functions: IP rules actions, sockets connections, APPN directory search filter, APPN end point filter.
*NETCLU	Yes	Yes	Cluster or cluster resource group operations: An audit journal entry is written when any of these events occur: <ul style="list-style-type: none"> • A cluster node or cluster resource group is added, created, or deleted. • A cluster node or cluster resource group is started, ended, updated, or removed. • Automatic failure of a system that switches access to another system. • Access is manually switched from one system to another system in a cluster.
*NETCMN	Yes	Yes	Network communications auditing: The violations detected by the APPN Filter support are logged to the security auditing journal when the Directory search filter and the End point filter are audited. *NETCMN is composed of several values to allow you to better customize your auditing. The following values make up *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Yes	Yes	Network failures: An audit journal entry is written when trying to connect to a TCP/IP port that does not exist, or trying to send information to a TCP/IP port that is not open or available.

Table 133. Action auditing values (continued)

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*NETSCK	Yes	Yes	<p>Socket tasks: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • An inbound TCP/IP socket connection is accepted. • An outbound TCP/IP socket connection is established. • An IP address is assigned through DHCP (Dynamic Host Configuration Protocol). • An IP address is unable to be assigned through DHCP because all of the IP addresses are being used. • Mail is filtered or rejected.
*OBJMGT	Yes	Yes	<p>Object management tasks: Moving an object to a different library or renaming it is logged. *OBJMGT can be used to detect copying confidential information by moving the object to a different library.</p>
*OPTICAL	Yes	Yes	<p>Optical functions: All optical functions are audited, including functions related to optical files, optical directories, optical volumes, and optical cartridges. *OPTICAL can be used to detect attempts to create or delete an optical directory.</p>
*PGMADP	Yes	Yes	<p>Adopting authority: The system writes a journal entry when adopted authority is used to gain access to an object. *PGMADP can be used to test where and how a new application uses adopted authority.</p>
*PGMFAIL	Yes	Yes	<p>Program failures: The system writes a journal entry when a program causes an integrity error. *PGMFAIL can be used to assist with migration to a higher security level or to test a new application.</p>
*PRTDTA	Yes	Yes	<p>Printing functions: Printing a spooled file, printing directly from a program, or sending a spooled file to a remote printer is logged. *PRTDTA can be used to detect printing confidential information.</p>
*SAVRST	Yes	Yes	<p>Restore operations: *SAVRST can be used to detect attempts to restore unauthorized objects.</p>

Table 133. Action auditing values (continued)

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*SECCFG	Yes	Yes	<p>Security configuration: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • User profiles are created, changed, deleted, or restored. • Changes are made to programs, system values, subsystem routing, or to the auditing attributes of an object. • The QSECOFR password is reset to the shipped value. • The service tools security officer password is defaulted.
*SECDIRSRV	Yes	Yes	<p>Directory service functions: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • Changes or updates are made to auditing, authority, passwords, and ownership. • Successful binds and unbinds. • Changes are made to directory security policies (for example, password policy)
*SECIPC	Yes	Yes	<p>Interprocess communications: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • Changes are made to the ownership or authority of an IPC object. • A create, delete, or retrieve of an IPC object. • Shared memory attach.

Table 133. Action auditing values (continued)

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*SECNAS	Yes	Yes	<p>Network authentication service actions: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • Service ticket invalid. • Service principals do not match. • Client principals do not match. • Ticket IP address mismatch. • Decryption of the ticket failed. • Decryption of the authentication failed. • Realm is not within client and local realms. • Ticket is a replay attempt. • Ticket not yet valid. • Remote or local IP address mismatch. • Decryption of KRB_AP_PRIV or KRB_AP_SAFE checksum error. • For KRB_AP_PRIV or KRB_AP_SAFE: Timestamp error, replay error, or sequence order error. • For graphics symbol set accept: Expired credentials, checksum error, or channel bindings. • For graphics symbol set unwrap or graphics symbol set verify: Expired context, decrypt/decode, checksum error, or sequence error.
*SECRUN	Yes	Yes	<p>Security runtime functions: Changes to object ownership, authority, and primary group are written to the audit journal.</p>
*SECCKD	Yes	Yes	<p>Socket descriptors: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • A socket descriptor is given to another job. • A socket descriptor is received. • A socket descriptor is unusable.
*SECVFY	Yes	Yes	<p>Verification functions: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • A profile handle or token is generated. • All profile tokens were invalidated. • The maximum number of profile tokens has been generated. • All profile tokens for a user have been removed. • A user profile has been authenticated. • A target profile was changed during a pass-through session.

Table 133. Action auditing values (continued)

Possible value	Available on QAUDLVL and QAUDLVL2 system values	Available on CHGUSRAUD command	Description
*SECVLDL	Yes	Yes	<p>Validation list operations: An audit journal entry is written when any of these events occur:</p> <ul style="list-style-type: none"> • An add, change, remove, or find of a validation list entry. • Successful or unsuccessful verification of a validation list entry.
*SECURITY	Yes	Yes	<p>Security tasks: Security-relevant events, such as changing a user profile or system value, are logged. *SECURITY can be used to keep a record of all security activity.</p> <p>*SECURITY is composed of several values to allow you to better customize your auditing. The following values make up *SECURITY:</p> <ul style="list-style-type: none"> *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
*SERVICE	Yes	Yes	<p>Service tasks: The use of service tools, such as DMPOBJ (Dump Object) and STRCPYSCN (Start Copy Screen), is logged. *SERVICE can be used to detect attempts to circumvent security by using service tools.</p>
*SPLFDTA	Yes	Yes	<p>Operations on spooled files: Actions performed on spooled files are logged, including creating, copying, and sending. *SPLFDTA can be used to detect attempts to print or send confidential data.</p>
*SYSMGT	Yes	Yes	<p>Systems management tasks: The system writes a journal entry for systems management activities, such as changing a reply list or the power on/off schedule. *SYSMGT can be used to detect attempts to use systems management functions to circumvent security controls.</p>

Security auditing journal entries:

This topic provides information about the journal entries that are written for the action auditing values specified on the QAUDLVL and QAUDLVL2 system values and in the user profile.

It shows:

- The type of entry written to the QAUDJRN journal.
- The model database output file that can be used to define the record when you create an output file with the DSPJRN command. Complete layouts for the model database outfiles are found in Appendix F, "Layout of audit journal entries," on page 563.

- The detailed entry type. Some journal entry types are used to log more than one type of event. The detailed entry type field in the journal entry identifies the type of event.
- The ID of the message that can be used to define the entry-specific information in the journal entry.

Table 134. Security auditing journal entries

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
Action Auditing:				
*ATNEVT	IM	QASYIMJ5	P	A potential intrusion has been detected. Further evaluation is required to determine if this is an actual intrusion or an expected and permitted action.
*AUTFAIL	AF	QASYAFJE/J4/J5	A	An attempt was made to access an object or perform an operation to which the user was not authorized.
			B	Restricted instruction
			C	Validation failure
			D	Use of unsupported interface, object domain failure
			E	Hardware storage protection error, program constant space violation
			F	ICAPI authorization error.
			G	ICAPI authentication error.
			H	Scan exit program action.
			I	System Java inheritance not allowed
			J	An attempt was made to submit or schedule a job under a job description which has a user profile specified. The submitter did not have *USE authority to the user profile.
			K	An attempt was made to perform an operation for which the user did not have the required special authority.
			N	The profile token was not a regenerable profile token.
			O	Optical Object Authority failure
			P	An attempt was made to use a profile handle that is not valid on the QWTSETP API.
			R	Hardware protection error
			S	Default signon attempt.
			T	Not authorized to TCP/IP port.
			U	A user permission request was not valid.
			V	The profile token was not valid for generating new profile token.
			W	The profile token was not valid for exchange.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			X	System violation, see description of AF (Authority Failure) journal entries for details
			Y	Not authorized to the current JUID field during a clear JUID operation.
			Z	Not authorized to the current JUID field during a set JUID operation.
	CV	QASYCVJ4/J5	E	Connection ended abnormally.
			R	Connection rejected.
	DI	QASYDIJ4/J5	AF	Authority failures.
			PW	Password failures.
	GR	QASYGRJ4/J5	F	Function registration operations.
	KF	QASYKFJ4/J5	P	An incorrect password was entered.
	IP	QASYIPJE/J4/J5	F	Authority failure for an IPC request.
	PW	QASYPWJE/J4/J5	A	APPC bind failure.
			C	CHKPWD failure.
			D	An incorrect service tool user ID was entered.
			E	An incorrect service tool user ID password was entered.
			P	An incorrect password was entered.
			Q	Attempted signon (user authentication) failed because user profile was disabled.
			R	Attempted signon (user authentication) failed because password was expired.
			S	SQL decrypt a password that was not valid.
			U	User name not valid.
			X	Service tools user is disabled.
			Y	Service tools user not valid.
			Z	Service tools password not valid.
	VC	QASYVCJE/J4/J5	R	A connection was rejected because of incorrect password.
	VO	QASYVOJ4/J5	U	Unsuccessful verification of a validation list entry.
	VN	QASYVNJE/J4/J5	R	A network logon was rejected because of expired account, incorrect hours, incorrect user ID, or incorrect password.
	VP	QASYVPJE/J4/J5	P	An incorrect network password was used.
	X1	QASYX1J5	F	Delegate of identity token failed.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			U	Get user from identity token failed.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*CMD ¹	CD	QASYCDJE/J4/J5	C	A command was run.
			L	An S/36E control language statement was run.
			O	An S/36E operator control command was run.
			P	An S/36E procedure was run.
			S	Command run after command substitution took place.
			U	An S/36E utility control statement was run.
*CREATE ²	CO	QASYCOJE/J4/J5	N	Creation of a new object, except creation of objects in QTEMP library.
			R	Replacement of existing object.
	DI	QASYDIJ4/J5	CO	Object created.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*DELETE ²	DO	QASYDOJE/J4/J5	A	Object deleted.
			C	Pending delete committed.
			D	Pending create rolled back.
			P	Delete pending.
			R	Pending delete rolled back.
	DI	QASYDIJ4/J5	DO	Object deleted.
	XD	QASYXDJ5	G	Group names (associated with DI entry)
*JOBBAS	JS	QASYJSJ5	A	The ENDJOBABN command was used.
			B	A job was submitted.
			C	A job was changed.
			E	A job was ended.
			H	A job was held.
			I	A job was disconnected.
			N	The ENDJOB command was used.
			P	A program start request was attached to a prestart job.
			Q	Query attributes changed.
			R	A held job was released.
			S	A job was started.
			U	CHGUSRTRC command.
*JOBCHGUSR	JS	QASYJSJ5	M	Change profile or group profile.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			T	Change profile or group profile using a profile token.
*JOBDA	JS	QASYJSJE/J4/J5	A	The ENDJOBABN command was used.
			B	A job was submitted.
			C	A job was changed.
			E	A job was ended.
			H	A job was held.
			I	A job was disconnected.
			M	Change profile or group profile.
			N	The ENDJOB command was used.
			P	A program start request was attached to a prestart job.
			Q	Query attributes changed.
			R	A held job was released.
			S	A job was started.
			T	Change profile or group profile using a profile token.
			U	CHGUSRTRC command.
	SG	QASYSGJE/J4/J5	A	Asynchronous i5/OS signal process.
			P	Asynchronous Private Address Space Environment (PASE) signal processed.
	VC	QASYVCJE/J4/J5	S	A connection was started.
			E	A connection was ended.
	VN	QASYVNJE/J4/J5	F	Logoff requested.
			O	Logon requested.
	VS	QASYVSJE/J4/J5	S	A server session was started.
			E	A server session was ended.
*NETBAS	CV	QASYCVJE/J4/J5	C	Connection established.
			E	Connection ended normally.
			R	Rejected connection.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file.
			N	IP rules have been unloaded for an IP Security connection.
			P	IP rules have been loaded for an IP Security connection.
			R	IP rules have been read and copied to a file.
			U	IP rules have been unloaded (removed).
	IS	QASYISJ4/J5	1	Phase 1 negotiation.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A violation was detected by the APPN Filter support when the Directory search filter was audited.
	NE	QASYNEJE/J4/J5	A	A violation is detected by the APPN Filter support when the End point filter is audited.
*NETCLU	CU	QASYCUJE/J4/J5	M	Creation of an object by the cluster control operation.
			R	Creation of an object by the Cluster Resource Group (*GRP) management operation.
*NETCMN	CU	QASYCUJE/J4/J5	M	Creation of an object by the cluster control operation.
			R	Creation of an object by the Cluster Resource Group (*GRP) management operation.
	CV	QASYCVJ4/J5	C	Connection established.
			E	Connection ended normally.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file.
			N	IP rule have been unloaded for an IP Security connection.
			P	IP rules have been loaded for an IP Security connection.
			R	IP rules have been read and copied to a file.
			U	IP rules have been unloaded (removed).
	IS	QASYISJ4/J5	1	Phase 1 negotiation.
			2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A violation was detected by the APPN Filter support when the Directory search filter was audited.
	NE	QASYNEJE/J4/J5	A	A violation is detected by the APPN Filter support when the End point filter is audited.
	SK	QASYSKJ4/J5	A	Accept
			C	Connect
			D	DHCP address assigned
			F	Filtered mail
			P	Port unavailable
			R	Reject mail
			U	DHCP address denied
*NETFAIL	SK	QASYSKJ4/J5	P	Port unavailable
*NETSCK	SK	QASYSKJ4/J5	A	Accept

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			C	Connect
			D	DHCP address assigned
			F	Filtered mail
			R	Reject mail
			U	DHCP address denied
*OBJMGT ²	DI	QASYDIJ4/J5	OM	Object rename
	OM	QASYOMJE/J4/J5	M	An object was moved to a different library.
			R	An object was renamed.
*OFCSRV	ML	QASYMLJE/J4/J5	O	A mail log was opened.
	SD	QASYSDJE/J4/J5	S	A change was made to the system distribution directory.
*OPTICAL	O1	QASY01JE/J4/J5	R	Open file or directory
			U	Change or retrieve attributes
			D	Delete file directory
			C	Create directory
			X	Release held optical file
	O2	QASY02JE/J4/J5	C	Copy file or directory
			R	Rename file
			B	Back up file or directory
			S	Save held optical file
			M	Move file
	O3	QASY03JE/J4/J5	I	Initialize volume
			B	Backup volume
			N	Rename volume
			C	Convert backup volume to primary
			M	Import
			E	Export
			L	Change authorization list
			A	Change volume attributes
			R	Absolute read
*PGMADP	AP	QASYAPJE/J4/J5	S	A program started that adopts owner authority. The start entry is written the first time adopted authority is used to gain access to an object, not when the program enters the call stack.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			E	A program ended that adopts owner authority. The end entry is written when the program leaves the call stack. If the same program occurs more than once in the call stack, the end entry is written when the highest (last) occurrence of the program leaves the stack.
			A	Adopted authority was used during program activation.
*PGMFAIL	AF	QASYAFJE/J4/J5	B	A program ran a restricted machine interface instruction.
			C	A program which failed the restore-time program validation checks was restored. Information about the failure is in the <i>Validation Value Violation Type</i> field of the record.
			D	A program accessed an object through an unsupported interface or callable program not listed as a callable API.
			E	Hardware storage protection violation.
			R	Attempt made to update an object that is defined as read-only. (Enhanced hardware storage protection is logged only at security level 40 and higher)
*PRDTA	PO	QASYPOJE/J4/J5	D	Printer output was printed directly to a printer.
			R	Output sent to remote system to print.
			S	Printer output was spooled and printed.
*SAVRST ²	OR	QASYORJE/J4/J5	N	A new object was restored to the system.
			E	An object was restored that replaces an existing object.
	RA	QASYRAJE/J4/J5	A	The system changed the authority to an object being restored. ³
	RJ	QASYRJJE/J4/J5	A	A job description that contains a user profile name was restored.
	RO	QASYROJE/J4/J5	A	The object owner was changed to QDFTOWN during restore operation. ³
	RP	QASYRPJE/J4/J5	A	A program that adopts owner authority was restored.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
	RQ	QASYRQJE/J4/J5	A	A *CRQD object with PROFILE(*OWNER) was restored.
	RU	QASYRUJE/J4/J5	A	Authority was restored for a user profile using the RSTAUT command.
	RZ	QASYRZJE/J4/J5	A	The primary group for an object was changed during a restore operation.
			O	Auditing of an object was changed with CHGOBJAUD command.
			U	Auditing for a user was changed with CHGUSRAUD command.
*SECCFG	AD	QASYADJE/J4/J5	D	Auditing of a DLO was changed with CHGDLOAUD command.
			O	Auditing of an object was changed with CHGOBJAUD or CHGAUD commands.
			S	The scan attribute was changed using CHGATR command or the Qp0lSetAttr API, or when the object was created.
			U	Auditing for a user was changed with CHGUSRAUD command.
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CP	QASYCPJE/J4/J5	A	Create, change, or restore operation of user profile when QSYSRESPA API is used.
	CQ	QASYCQJE/J4/J5	A	A *CRQD object was changed.
	CY	QASYCYJ4/J5	A	Access Control function
			F	Facility Control function
			M	Master Key function
	DO	QASYDOJE/J4/J5	A	Object was deleted not under commitment control
			C	A pending object delete was committed
			D	A pending object create was rolled back
			P	The object delete is pending (the delete was performed under commitment control)
			R	A pending object delete was rolled back
	DS	QASYDSJE/J4/J5	A	Request to reset DST QSECOFR password to system-supplied default.
			C	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
			C	Change.
			D	Delete.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			I	Initialize environment variable space.
	GR	QASYGRJ4/J5	A	Exit program added
			D	Exit program removed
			F	Function registration operation
			R	Exit program replaced
	JD	QASYJDE/J4/J5	A	The USER parameter of a job description was changed.
	KF	QASYKFJ4/J5	C	Certificate operation.
			K	Key ring file operation.
			T	Trusted root operation.
	NA	QASYNaje/J4/J5	A	A network attribute was changed.
	PA	QASYPaje/J4/J5	A	A program was changed to adopt owner authority.
	SE	QASYSEJE/J4/J5	A	A subsystem routing entry was changed.
	SO	QASYSOJ4/J5	A	Add entry.
			C	Change entry.
			R	Remove entry.
	SV	QASYSVJE/J4/J5	A	A system value was changed.
			B	Service attributes were changed.
			C	Change to system clock.
			E	Change to option
			F	Change to system-wide journal attribute
	VA	QASYVAJE/J4/J5	S	The access control list was changed successfully.
			F	The change of the access control list failed.
			V	Successful verification of a validation list entry.
	VU	QASYVUJE/J4/J5	G	A group record was changed.
			M	User profile global information changed.
			U	A user record was changed.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Audit change.
			BN	Successful bind
			CA	Authority change
			CP	Password change
			OW	Ownership change
			PO	Policy change
			UB	Successful unbind

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
*SECIPC	IP	QASYIPJE/J4/J5	A	The ownership or authority of an IPC object was changed.
			C	Create an IPC object.
			D	Delete an IPC object.
			G	Get an IPC object.
*SECNAS	X0	QASYX0J4/J5	1	Service ticket valid.
			2	Service principals do not match.
			3	Client principals do not match.
			4	Ticket IP address mismatch.
			5	Decryption of the ticket failed
			6	Decryption of the authenticator failed
			7	Realm is not within client and local realms
			8	Ticket is a replay attempt
			9	Ticket not yet valid
			A	Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error
			B	Remote IP address mismatch
			C	Local IP address mismatch
			D	KRB_AP_PRIV or KRB_AP_SAFE timestamp error
			E	KRB_AP_PRIV or KRB_AP_SAFE replay error
			F	KRB_AP_PRIV KRB_AP_SAFE sequence order error
			K	GSS accept - expired credential
			L	GSS accept - checksum error
			M	GSS accept - channel bindings
			N	GSS unwrap or GSS verify expired context
			O	GSS unwrap or GSS verify decrypt/decode
			P	GSS unwrap or GSS verify checksum error
			Q	GSS unwrap or GSS verify sequence error
*SECRUN	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
*SECCKD	GS	QASYGSJE/J4/J5	G	A socket descriptor was given to another job. (The GS audit record is created if it is not created for the current job.)
			R	Receive descriptor.
			U	Unable to use descriptor.
*SECURITY	AD	QASYADJE/J4/J5	D	Auditing of a DLO was changed with CHGDLOAUD command.
			O	Auditing of an object was changed with CHGOBJAUD or CHGAUD commands.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
			U	Auditing for a user was changed with CHGUSRAUD command.
	X1	QASYADJE/J4/J5	D	Delegate of identity token successful
			G	Get user from identity token successful
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	CP	QASYCPJE/J4/J5	A	Create, change, or restore operation of user profile when QSYRESPA API is used
	CQ	QASYCQJE/J4/J5	A	A *CRQD object was changed.
	CV	QASYCVJ4/J5	C	Connection established.
			E	Connection ended normally.
			R	Connection rejected.
	CY	QASYCYJ4/J5	A	Access Control function
			F	Facility Control function
			M	Master Key function
	DI	QASYDIJ4/J5	AD	Audit change
			BN	Successful bind
			CA	Authority change
			CP	Password change
			OW	Ownership change
			PO	Policy change
			UB	Successful unbind
	DO	QASYDOJE/J4/J5	A	Object was deleted not under commitment control
			C	A pending object delete was committed
			D	A pending object create was rolled back

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			P	The object delete is pending (the delete was performed under commitment control)
			R	A pending object delete was rolled back
	DS	QASYDSJE/J4/J5	A	Request to reset DST QSECOFR password to system-supplied default.
			C	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
			C	Change.
			D	Delete.
			I	Initialize environment variable space.
	GR	QASYGRJ4/J5	A	Exit program added
			D	Exit program removed
			F	Function registration operation
			R	Exit program replaced
	GS	QASYGSJE/J4/J5	G	A socket descriptor was given to another job. (The GS audit record is created if it is not created for the current job.)
			R	Receive descriptor.
			U	Unable to use descriptor.
	IP	QASYIPJE/J4/J5	A	The ownership or authority of an IPC object was changed.
			C	Create an IPC object.
			D	Delete an IPC object.
			G	Get an IPC object.
	JD	QASYJDJE/J4/J5	A	The USER parameter of a job description was changed.
	KF	QASYKFJ4/J5	C	Certificate operation.
			K	Key ring file operation.
			T	Trusted root operation.
	NA	QASYNAJE/J4/J5	A	A network attribute was changed.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PA	QASYPAJE/J4/J5	A	A program was changed to adopt owner authority.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.
	PS	QASYPSJE/J4/J5	A	A target user profile was changed during a pass-through session.
			E	An office user ended work on behalf of another user.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			H	A profile handle was generated through the QSYGETPH API.
			I	All profile tokens were invalidated.
			M	The maximum number of profile tokens have been generated.
			P	Profile token generated for user.
			R	All profile tokens for a user have been removed.
			S	An office user started work on behalf of another user.
			V	User profile authenticated.
	SE	QASYSEJE/J4/J5	A	A subsystem routing entry was changed.
	SO	QASYSOJ4/J5	A	Add entry.
			C	Change entry.
			R	Remove entry.
	SV	QASYSVJE/J4/J5	A	A system value was changed.
			B	Service attributes were changed.
			C	Change to system clock.
			E	Change to option
			F	Change to system-wide journal attribute
	VA	QASYVAJE/J4/J5	S	The access control list was changed successfully.
			F	The change of the access control list failed.
	VO		V	Successful verify of a validation list entry.
	VU	QASYVUJE/J4/J5	G	A group record was changed.
			M	User profile global information changed.
			U	A user record was changed.
	X0	QASYX0J4/J5	1	Service ticket valid.
			2	Service principals do not match
			3	Client principals do not match
			4	Ticket IP address mismatch
			5	Decryption of the ticket failed
			6	Decryption of the authenticator failed
			7	Realm is not within client and local realms
			8	Ticket is a replay attempt
			9	Ticket not yet valid

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			A	Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error
			B	Remote IP address mismatch
			C	Local IP address mismatch
			D	KRB_AP_PRIV or KRB_AP_SAFE timestamp error
			E	KRB_AP_PRIV or KRB_AP_SAFE replay error
			F	KRB_AP_PRIV KRB_AP_SAFE sequence order error
			K	GSS accept - expired credential
			L	GSS accept - checksum error
			M	GSS accept - channel bindings
			N	GSS unwrap or GSS verify expired context
			O	GSS unwrap or GSS verify decrypt/decode
			P	GSS unwrap or GSS verify checksum error
			Q	GSS unwrap or GSS verify sequence error
*SECVFY	PS	QASYPSJE/J4/J5	A	A target user profile was changed during a pass-through session.
			E	An office user ended work on behalf of another user.
			H	A profile handle was generated through the QSYGETPH API.
			I	All profile tokens were invalidated.
			M	The maximum number of profile tokens have been generated.
			P	Profile token generated for user.
			R	All profile tokens for a user have been removed.
			S	An office user started work on behalf of another user.
			V	User profile authenticated.
	X1	QASYX1J5	D	Delegate of identity token successful
			G	Get user from identity token successful
*SECVLDL	VO		V	Successful verification of a validation list entry.
*SERVICE	ST	QASYSTJE/J4/J5	A	A service tool was used.
	VV	QASYVVJE/J4/J5	C	The service status was changed.
			E	The server was stopped.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			P	The server paused.
			R	The server was restarted.
			S	The server was started.
*SPLFDTA	SF	QASYSFJE/J4/J5	A	A spooled file was read by someone other than the owner.
			C	A spooled file was created.
			D	A spooled file was deleted.
			H	A spooled file was held.
			I	An inline file was created.
			R	A spooled file was released.
			S	A spooled file was saved.
			T	A spooled file was restored.
			U	A spooled file was changed.
			V	Only non-security relevant spooled files attributes changed.
*SYSMGT	DI	QASYDIJ4/J5	CF	Configuration changes
			CI	Create instance
			DI	Delete instance
			RM	Replication management
	SM	QASYSMJE/J4/J5	B	Backup options were changed using xxxxxxxxxx.
			C	Automatic cleanup options were changed using xxxxxxxxxx.
			D	A DRDA* change was made.
			F	An HFS file system was changed.
			N	A network file operation was performed.
			O	A backup list was changed using xxxxxxxxxx.
			P	The power on/off schedule was changed using xxxxxxxxxx.
			S	The system reply list was changed.
			T	The access path recovery times were changed.
	VL	QASYVLJE/J4/J5	A	The account is expired.
			D	The account is disabled.
			L	Logon hours were exceeded.
			U	Unknown or unavailable.
			W	Workstation not valid.
Object Auditing:				
*CHANGE	DI	QASYDIJ4/J5	IM	LDAP directory import
			ZC	Object change

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
	ZC	QASYZCJ4/J5	C	Object changes
			U	Upgrade of open access to an object
	AD	QASYADJEJ4/J5	D	Auditing of an object was changed with CHGOBJAUD command.
			O	Auditing of an object was changed with CHGOBJAUD command.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
			U	Auditing for a user was changed with CHGUSRAUD command.
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	CA	QASYCAJE/J4/J5	A	Changes to authorization list or object authority.
	OM	QASYOMJE/J4/J5	M	An object was moved to a different library.
			R	An object was renamed.
	OR	QASYORJE/J4/J5	N	A new object was restored to the system.
			E	An object was restored that replaces an existing object.
	OW	QASYOWJE/J4/J5	A	Object ownership was changed.
	PG	QASYPGJE/J4/J5	A	The primary group for an object was changed.
	RA	QASYRAJE/J4/J5	A	The system changed the authority to an object being restored.
	RO	QASYROJE/J4/J5	A	The object owner was changed to QDFTOWN during restore operation.
	RZ	QASYRZJE/J4/J5	A	The primary group for an object was changed during a restore operation.
	GR	QASYGRJ4/J5	F	Function registration operations ⁵
	LD	QASYLDJE/J4/J5	L	Link a directory.
			U	Unlink a directory.
	VF	QASYVFJE/J4/J5	A	The file was closed because of administrative disconnection.
			N	The file was closed because of normal client disconnection.
			S	The file was closed because of session disconnection.
	VO	QASYVOJ4/J5	A	Add validation list entry.
			C	Change validation list entry.
			F	Find validation list entry.
			R	Remove validation list entry.
	VR	QASYVRJE/J4/J5	F	Resource access failed.

Table 134. Security auditing journal entries (continued)

Action or object auditing value	Journal entry type	Model database outfile	Detailed entry	Description
			S	Resource access was successful.
	YC	QASYCJE/J4/J5	C	A document library object was changed.
	ZC	QASYZCJE/J4/J5	C	An object was changed.
			U	Upgrade of open access to an object.
*ALL ⁴	CD	QASYCDJ4/J5	C	Command run
	DI	QASYDIJ4/J5	EX	LDAP directory export
			ZR	Object read
	GR	QASYGRJ4/J5	F	Function registration operations ⁵
	LD	QASYLDJE/J4/J5	K	Search a directory.
	YR	QASYRJE/J4/J5	R	A document library object was read.
	ZR	QASYZRJE/J4/J5	R	An object was read.
<p>¹ This value can only be specified for the AUDLVL parameter of a user profile. It is not a value for the QAUDLVL system value.</p> <p>² If object auditing is active for an object, an audit record is written for a create, delete, object management, or restore operation even if these actions are not included in the audit level.</p> <p>³ See the topic "Restoring objects" on page 249 for information about authority changes which might occur when an object is restored.</p> <p>⁴ When *ALL is specified, the entries for both *CHANGE and *ALL are written.</p> <p>⁵ When the QUSRSYS/QUSEXRGOBJ *EXITRG object is being audited.</p>				

Planning the auditing of object access

The i5/OS operating system provides the ability to log accesses to an object in the security audit journal by using system values and the object auditing values for users and objects. This is called *object auditing*.

The QAUDCTL system value, the OBJAUD value for an object, and the OBJAUD value for a user profile work together to control object auditing. The OBJAUD value for the object and the OBJAUD value for the user who is using the object determine whether a specific access should be logged. The QAUDCTL system value starts and stops the object auditing function.

Table 135 shows how the OBJAUD values for the object and the user profile work together.

Table 135. How object and user auditing work together

OBJAUD value for object	OBJAUD value for user		
	*NONE	*CHANGE	*ALL
*NONE	None	None	None
*USRPRF	None	Change	Change and Use
*CHANGE	Change	Change	Change
*ALL	Change and Use	Change and Use	Change and Use

You can use object auditing to keep track of all users that are accessing a critical object on the system. You can also use object auditing to keep track of all the object that are accessed by a particular user. Object auditing is a flexible tool that enables you to monitor those object accesses that are important to your organization.

Taking advantage of the capabilities of object auditing requires careful planning. Poorly designed auditing might generate many more audit records than you can analyze. This can have a severe effect on system performance. For example, setting the OBJAUD value to *ALL for a library results in an audit entry being written every time the system searches for an object in that library. For a heavily used library on a busy system, this would generate a very large number of audit journal entries.

Here are some examples of how to use object auditing.

- If certain critical files are used throughout your organization, you can periodically review who is accessing them using a sampling technique:
 1. Set the OBJAUD value for each critical file to *USRPRF using the Change Object Auditing command:

```

                Change Object Auditing (CHGOBJAUD)

Type choices, press Enter.

Object . . . . . file-name
Library . . . . . library-name
Object type . . . . . *FILE
ASP device . . . . . *
Object auditing value . . . . . *USRPRF
```

2. Set the OBJAUD value for each user in your sample to *CHANGE or *ALL using the CHGUSRAUD command.
 3. Make sure the QAUDCTL system value includes *OBJAUD.
 4. When sufficient time has elapsed to collect a representative sample, set the OBJAUD value in the user profiles to *NONE or remove *OBJAUD from the QAUDCTL system value.
 5. Analyze the audit journal entries by using the techniques described in “Analyzing audit journal entries with query or a program” on page 296.
- If you are concerned about who is using a particular file, you can collect information about all accesses to the file for a period of time:
 1. Set object auditing for the file independent of user profile values:


```
CHGOBJAUD OBJECT(library-name/file-name)
                OBJTYPE(*FILE) OBJAUD(*CHANGE or *ALL)
```
 2. Make sure that the QAUDCTL system value includes *OBJAUD.
 3. When sufficient time has elapsed to collect a representative sample, set the OBJAUD value in the object to *NONE.
 4. Analyze the audit journal entries using the techniques described in “Analyzing audit journal entries with query or a program” on page 296.
 - To audit all object accesses for a specific user, do the following actions:
 1. Set the OBJAUD value for all objects to *USRPRF using the CHGOBJAUD and CHGAUD commands:

Change Object Auditing (CHGOBJAUD)

Type choices, press Enter.

```
Object . . . . . *ALL
Library . . . . . *ALLAVL
Object type . . . . . *ALL
ASP device . . . . . *
Object auditing value . . . . . *USRPRF
```

Attention: Depending on how many objects are on your system, this command might take many hours to run. Setting up object auditing for all objects on the system often is not necessary and will severely degrade performance. Selecting a subset of object types and libraries for auditing is recommended.

2. Set the OBJAUD value for the specific user profile to *CHANGE or *ALL using the CHGUSRAUD command.
3. Make sure the QAUDCTL system value includes *OBJAUD.
4. When you have collected a specific sample, set the OBJAUD value for the user profile to *NONE.

Related reference:

“Object auditing” on page 112

The object auditing value for a user profile works with the object auditing value for an object to determine whether the user’s access of an object is audited.

Displaying object auditing:

Use the DSPOBJD command to display the current object auditing level for an object. Use the DSPDLOAUD command to display the current object auditing level for a document library object.

Setting default auditing for objects:

You can use the QCRTOBJAUD system value and the CRTOBJAUD value for libraries and directories to set object auditing for newly created objects.

For example, if you want all new objects in the INVLIB library to have an audit value of *USRPRF, use the following command:

```
CHGLIB LIB(INVLIB) CRTOBJAUD(*USRPRF)
```

This command affects the auditing value of new objects only. It does not change the auditing value of objects that already exist in the library.

Use the default auditing values carefully. Improper use might result in many unwanted entries in the security audit journal. Effective use of the object auditing capabilities of the system requires careful planning.

Preventing loss of auditing information

Two system values control what the system does when error conditions might cause the loss of audit journal entries.

Audit force level

The QAUDFRCLVL system value determines how often the system writes audit journal entries from memory to auxiliary storage.

The QAUDFRCLVL system value works like the force level for database files. You should follow similar guidelines in determining the correct force level for your installation.

If you allow the system to determine when to write entries to auxiliary storage, the system balances the performance effect against the potential loss of information in a power outage. *SYS is the default choice.

If you set the force level to a low number, you minimize the possibility of losing audit records, but you might notice a negative performance effect. If your installation requires that no audit records be lost in a power failure, you must set the QAUDFRCLVL to 1.

Audit end action

The Auditing End Action (QAUDENDACN) system value determines what the system does if it is unable to write an entry to the audit journal.

The default value is *NOTIFY. The system performs the following tasks if it is unable to write audit journal entries and QAUDENDACN is *NOTIFY:

1. The QAUDCTL system value is set to *NONE to prevent additional attempts to write entries.
2. Message CPI2283 is sent to the QSYSOPR message queue and the QSYSMSG message queue (if it exists) every hour until auditing is successfully restarted.
3. Normal processing continues.
4. If an IPL is performed on the system, message CPI2284 is sent to the QSYSOPR and QSYSMSG message queues during the IPL.

Note: In most cases, performing an IPL resolves the problem that caused auditing to fail. After you have restarted your system, set the QAUDCTL system value to the correct value. The system attempts to write an audit journal record whenever this system value is changed.

You can set the QAUDENDACN to turn off your system if auditing fails (*PWRDWNSYS). Use this value only if your installation requires that auditing be active for the system to run. If the system is unable to write an audit journal entry and the QAUDENDACN system value is *PWRDWNSYS, the following events take place:

1. The system shuts down immediately (the equivalent of issuing the PWRDWNSYS *IMMED command).
2. SRC code B900 3D10 is displayed.

Next, you must do the following actions:

1. Start an IPL from the system unit. Make sure that the device specified in the console (QCONSOLE) system value is powered on.
2. To complete the IPL, sign on at the console using a user with *ALLOBJ and *AUDIT special authority. The system starts in a restricted state with a message indicating that an auditing error caused the system to stop.
3. The QAUDCTL system value is set to *NONE.
4. To restore the system to normal, set the QAUDCTL system value to a value other than *NONE. When you change the QAUDCTL system value, the system attempts to write an audit journal entry. If it is successful, the system returns to a normal state.

If the system does not successfully return to a normal state, use the job log to determine why auditing has failed. Correct the problem and reset the QAUDCTL value.

Choosing not to audit QTEMP objects

You can choose to not audit QTEMP objects by specifying the *NOQTEMP value.

The value, *NOQTEMP, can be specified as a value for the system value QAUDCTL. If you use the *NOQTEMP value, you must also specify either *OBJAUD or *AUDLVL for the QAUDCTL. When auditing is active and *NOQTEMP is specified, the following actions on objects in the QTEMP library will NOT be audited.

- Changing or reading objects in QTEMP (journal entry types ZC, ZR).
- Changing the authority, owner, or primary group of objects in QTEMP (journal entry types CA, OW, PG).

Using CHGSECAUD to set up security auditing

Overview:

Using the CHGSECAUD command, you can activate system security auditing for actions by ensuring that the security journal exists, setting the QAUDCTL system value to *AUDLVL, and setting the QAUDLVL system value to the default set of values. The default set includes *AUTFAIL, *CREATE, *DELETE, *SECURITY, and *SAVRST action audits.

```
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*DFTSET)
```

Purpose:

Set up the system to collect security events in the QAUDJRN journal.

How To:

```
CHGSECAUD  
DSPSECAUD
```

Authority:

The user must have *ALLOBJ and *AUDIT special authority.

Journal Entry:

```
CO (create object)  
SV (system value change)  
AD (object and user audit changes)
```

Note: The CHGSECAUD command creates the journal and journal receiver if it does not exist. The CHGSECAUD then sets the QAUDCTL, QAUDLVL, and QAUDLVL2 system values.

Related reference:

“Options on the Security Tools menu” on page 707

You can use the Security Tools (SECTOOLS) menu to simplify the management and control of the security on your system with plenty of options and commands that it provides.

Setting up security auditing

With security auditing, you can collect information about security events in the QAUDJRN journal.

Overview:

Purpose:

Set up the system to collect security events in the QAUDJRN journal.

How To:

```
CRTJRNRCV  
CRTJRN QSYS/QAUDJRN  
WRKSYSVAL *SEC
```

CHGOBJAUD
CHGDLOAUD
CHGUSRAUD

Authority:

*ADD authority to QSYS and to journal
receiver library
*AUDIT special authority

Journal Entry:

CO (create object)
SV (system value change)
AD (object and user audit changes)

Note: QSYS/QAUDJRN must exist before QAUDCTL can be changed, otherwise the system auditing function doesn't know the journal name and won't find it.

To set up security auditing, do the following steps. You need *AUDIT special authority to complete these steps.

1. Create a journal receiver in a library of your choice by using the Create Journal Receiver (**CRTJRNRCV**) command. This example uses a library called JRNLIB for journal receivers.

```
CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +  
           THRESHOLD(100000) AUT(*EXCLUDE)  +  
           TEXT('Auditing Journal Receiver')
```

- a. Place the journal receiver in a library that is saved regularly. Do **not** place the journal receiver in library QSYS, even though that is where the journal will be.
- b. Choose a journal receiver name that can be used to create a naming convention for future journal receivers, such as AUDRCV0001. You can use the *GEN option when you change journal receivers to continue the naming convention.

It's very helpful to using this type of naming convention if you choose to have the system manage changing your journal receivers.

- c. Specify a receiver threshold appropriate to your system size and activity. The size you choose should be based on the number of transactions on your system and the number of actions that you choose to audit. If you use system change-journal management support, the journal receiver thresholds must be at least 100 000 KB. For more information about journal receiver threshold, refer to Journal management.
 - d. Specify *EXCLUDE on the AUT parameter to limit access to the information that is stored in the journal.
2. Create the QSYS/QAUDJRN journal by using the Create Journal (**CRTJRN**) command:

```
CRTJRN  JRN(QSYS/QAUDJRN) +  
        JRNRCV(JRNLIB/AUDRCV0001) +  
        MNGRCV(*SYSTEM) DLTRCV(*NO) +  
        AUT(*EXCLUDE) TEXT('Auditing Journal')
```

- The name QSYS/QAUDJRN must be used.
- Specify the name of the journal receiver that you created in the previous step.
- Specify *EXCLUDE on the AUT parameter to limit access to the information stored in the journal. You must have authority to add objects to QSYS to create the journal.
- Use the *Manage receiver* (MNGRCV) parameter to have the system change the journal receiver and attach a new one when the attached receiver exceeds the threshold specified in the creation of the journal receiver. If you choose this option, you do not need to use the CHGJRN command to detach receivers and create and attach new receivers manually.

- Do not have the system delete detached receivers. Specify DLTRCV(*NO), which is the default. The QAUDJRN receivers are your security audit trail. Make sure that they are adequately saved before deleting them from the system.

The Journal management topic provides more information about working with journals and journal receivers.

3. Set the audit level (QAUDLVL) system value or the audit level extension (QAUDLVL2) system value by using the WRKSYSVAL command. The QAUDLVL and QAUDLVL2 system values determine which actions are logged to the audit journal for all users on the system. See “Planning the auditing of actions” on page 263.
4. If necessary, set action auditing for individual users by using the CHGUSRAUD command. See “Planning the auditing of actions” on page 263.
5. If necessary, set object auditing for specific objects by using the CHGOBJAUD, CHGAUD, and CHGDLOAUD commands. See “Planning the auditing of object access” on page 286.
6. If necessary, set object auditing for specific users by using the CHGUSRAUD command.
7. Set the QAUDENDACN system value to control what happens if the system cannot access the audit journal. See “Audit end action” on page 289.
8. Set the QAUDFRCLVL system value to control how often audit records are written to auxiliary storage. See “Preventing loss of auditing information” on page 288.
9. Start auditing by setting the QAUDCTL system value to a value other than *NONE.

The QSYS/QAUDJRN journal must exist before you can change the QAUDCTL system value to a value other than *NONE. When you start auditing, the system attempts to write a record to the audit journal. If the attempt is not successful, you receive a message and the auditing does not start.

Managing the audit journal and journal receivers

The system provides a mechanism for managing the audit journal and journal receivers. You can use the methods described in this topic to audit the security on your system.

The auditing journal QSYS/QAUDJRN is intended solely for security auditing. Objects should not be journaled to the audit journal. Commitment control should not use the audit journal. User entries should not be sent to this journal using the Send Journal Entry (SNDJRNE) command or the Send Journal Entry (QJOSJRNE) API.

The system uses special locking protection to make sure that it can write audit entries to the audit journal. When auditing is active (the QAUDCTL system value is not *NONE), the system arbitrator job (QSYSARB) holds a lock on the QSYS/QAUDJRN journal. You cannot perform certain operations on the audit journal when auditing is active, such as:

- **DLTJRN** command
- Moving the journal
- Restoring the journal
- **WRKJRN** command

The information recorded in the security journal entries is described in Appendix F, “Layout of audit journal entries,” on page 563. All security entries in the audit journal have a journal code of T. In addition to security entries, system entries also appear in the journal QAUDJRN. These are entries with a journal code of J, which relate to initial program load (IPL) and general operations performed on journal receivers (for example, saving the receiver).

If damage occurs to the journal or to its current receiver so that the auditing entries cannot be journaled, the QAUDENDACN system value determines what action the system takes. Recovery from a damaged journal or journal receiver is the same as for other journals.

You might want to have the system manage the changing of journal receivers. Specify MNGRCV(*SYSTEM) when you create the QAUDJRN journal, or change the journal to that value. If you specify MNGRCV(*SYSTEM), the system automatically detaches the receiver when it reaches its threshold size and creates and attaches a new journal receiver. This is called *system change-journal management*.

If you specify MNGRCV(*USER) for the QAUDJRN, a message is sent to the threshold message queue that was specified for the journal when the journal receiver reaches a storage threshold. The message indicates that the receiver has reached its threshold. Use the **CHGJRN** command to detach the receiver and attach a new journal receiver. This prevents *Entry not journaled* error conditions. If you do receive a message, you must use the **CHGJRN** command in order for security auditing to continue.

The default message queue for a journal is QSYSOPR. If your installation has a large volume of messages in the QSYSOPR message queue, you can associate a different message queue, such as AUDMSG, with the QAUDJRN journal. You can use a message handling program to monitor the AUDMSG message queue. When a journal threshold warning is received (CPF7099), you can automatically attach a new receiver. If you use system change-journal management, then message CPF7020 is sent to the journal message queue when a system change journal completes. You can monitor for this message so that you can know when to do a save of the detached journal receivers.

Attention: The automatic cleanup function that is provided when using Operational Assistant menus does not clean up the QAUDJRN receivers. To avoid problems with disk space, regularly detach, save, and delete QAUDJRN receivers.

See the Journal management topic for complete information about managing journals and journal receivers.

The QAUDJRN journal is created during an IPL if it does not exist and the QAUDCTL system value is set to a value other than *NONE. This occurs only after an unusual situation, such as replacing a disk device or clearing an auxiliary storage pool.

Related information:

Journal management

Saving and deleting audit journal receivers

You should regularly detach the current audit journal receiver and attach a new one.

Overview:

Purpose:

Attach a new audit journal receiver; Save and delete the old receiver

How To:

- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- SAVOBJ (to save old receiver)
- DLTJRNRCV (to delete old receiver)

Authority:

*ALL authority to journal receiver *USE authority to journal

Journal Entry:

J (system entry to QAUDJRN)

Note: Select a time when the system is not busy.

You should regularly detach the current audit journal receiver and attach a new one for two reasons:

- Analyzing journal entries is easier if each journal receiver contains the entries for a specific, manageable time period.
- Large journal receivers can affect system performance and take valuable space on auxiliary storage.

It is suggested to have the system manage receivers automatically. You can specify this by using the *Manage receiver* parameter when you create the journal.

If you have set up action auditing and object auditing to log many different events, you might need to specify a large threshold value for the journal receiver. If you are managing receivers manually, you might need to change journal receivers several times a day. If you log only a few events, you might want to change receivers to correspond with the backup schedule for the library containing the journal receiver.

You use the **CHGJRN** command to detach a receiver and attach a new receiver.

System-managed journal receivers:

You can follow the steps described in this topic to save or delete the journal receivers.

If you have the system manage the receivers, use the following procedure to save all detached QAUDJRN receivers and to delete them:

1. Type **WRKJRNA QAUDJRN**. The display shows you the currently attached receiver. Do not save or delete this receiver.
2. Use F15 to work with the receiver directory. This shows all receivers that have been associated with the journal and their corresponding status.
3. Use the SAVOBJ command to save each receiver. Do not receive the currently attached receiver.
4. Use the DLTJRNRCV command to delete each receiver after it is saved.

An alternative to the preceding procedure can be done by using the journal message queue and monitoring for the CPF7020 message which indicates that the system change journal has completed successfully.

Related information:



Backup and Recovery

User-managed journal receivers:

You can follow the steps described here to detach, save, or delete journal receivers manually.

If you choose to manage journal receivers manually, use the following procedure to detach, save and delete a journal receiver:

1. Type **CHGJRN JRN(QAUDJRN) JRNRCV(*GEN)**. This command:
 - a. Detaches the currently attached receiver.
 - b. Creates a new receiver with the next sequential number.
 - c. Attaches the new receiver to the journal.

For example, if the current receiver is AUDRCV0003, the system creates and attaches a new receiver called AUDRCV0004.

The Work with Journal Attributes (WRKJRNA) command tells you which receiver is currently attached: **WRKJRNA QAUDJRN**.

2. Use the Save Object (SAVOBJ) command to save the detached journal receiver. Specify object type *JRNRCV.
3. Use the Delete Journal Receiver (DLTJRNRCV) command to delete the receiver. If you try to delete the receiver without saving it, you will receive a warning message.

Stopping the audit function

You might want to use the audit function periodically, rather than all the time. For example, you might want to use it when testing a new application. Or you might use it to perform a quarterly security audit.

To stop the auditing function, do the following actions:

1. Use the **WRKSYSVAL** command to change the QAUDCTL system value to *NONE. This stops the system from logging any more security events.
2. Detach the current journal receiver using the **CHGJRN** command.
3. Save and delete the detached receiver, using the **SAVOBJ** and **DLTJRNRCV** commands.
4. You can delete the QAUDJRN journal after you change QAUDCTL to *NONE. If you plan to resume security auditing in the future, you should leave the QAUDJRN journal on the system.

If the QAUDJRN journal is set up with MNGRCV(*SYSTEM), the system detaches the receiver and attaches a new one whenever you perform an IPL, whether security auditing is active. You need to delete these journal receivers. Saving them before deleting them is not necessary, because they do not contain any audit entries.

Analyzing audit journal entries

After you have set up the security auditing function, you can use several different methods to analyze the events that are logged.

- View selected entries at your workstation using the Display Journal (DSPJRN) command.
- Copy selected entries to output files using the Copy Audit Journal Entries (CPYAUDJRNE) or DSPJRN command, and then using a query tool or program to analyze entries.
- Use the Display Audit Journal Entries (DSPAUDJRNE) command.

Note: IBM has stopped providing enhancements for the DSPAUDJRNE command. The command does not support all security audit record types, and the command does not list all the fields for the records it supports.

- Use the Receive Journal Entry (RCVJRNE) command on the QAUDJRN journal to receive the entries as they are written to the QAUDJRN journal.

Viewing audit journal entries

Overview:

Purpose:

View QAUDJRN entries

How To:

DSPJRN (Display Journal command)

Authority:

*USE authority to QSYS/QAUDJRN *USE authority to journal receiver

The Display Journal (DSPJRN) command allows you to view selected journal entries at your workstation. To view journal entries, do the following actions:

1. Type DSPJRN QAUDJRN and press F4. On the prompt display, you can enter information to select the range of entries that is shown. For example, you can select all entries in a specific range of dates, or you can select only a certain type of entry, such as an incorrect sign-on attempt (journal entry type PW).

The default is to display entries from only the attached receiver. You can use RCVRNG(*CURCHAIN) to see entries from all receivers that are in the receiver chain for the QAUDJRN journal, up to and including the receiver that is currently attached.

2. When you press the Enter key, you see the Display Journal Entries display:

```

                                Display Journal Entries

Journal . . . . . : QAUDJRN      Library . . . . . : QSYS
Largest sequence number on this screen . . . . . : 0000000000000000012
Type options, press Enter.
  5=Display entire entry

Opt   Sequence  Code  Type  Object      Library      Job      Time
     1         J   PR           SCPF         10:24:55
     2         T   CA           SCPF         10:24:55
     3         T   CO           SCPF         10:24:55
     4         T   CA           SCPF         10:24:55
     5         T   CO           SCPF         10:24:55
     6         T   CA           SCPF         10:24:55
     7         T   CO           SCPF         10:24:55
     8         T   CA           SCPF         10:24:56
     9         T   CO           SCPF         10:24:56
    10         T   CA           SCPF         10:24:57
    11         T   CO           SCPF         10:24:57
    12         T   CA           SCPF         10:24:57
                                           More...

F3=Exit  F12=Cancel

```

3. Use option 5 (Display entire entry) to see information about a specific entry:

```

                                Display Journal Entry

Object . . . . . :                Library . . . . . :
Member . . . . . :
Incomplete data . . : No          Minimized entry data : *None
Sequence . . . . . : 1198
Code . . . . . : T - Audit trail entry
Type . . . . . : CO - Create object

      Entry specific data
Column *...+....1....+....2....+....3....+....4....+....5
00001  'NISAVLDCK QSYS      *PGM  CLE
00051  '
00101  '
00151  '
00201  '
00251  '
00301  '

                                           More...

Press Enter to continue.

F3=Exit  F6=Display only entry specific data
F10=Display only entry details  F12=Cancel  F24=More keys

```

4. You can use F6 (Display only entry specific data) for entries with a large amount of entry-specific data. You can also select a hexadecimal version of that display. You can use F10 to display details about the journal entry without any entry-specific information.

Appendix F, "Layout of audit journal entries," on page 563 contains the layout for each type of QAUDJRN journal entry.

Analyzing audit journal entries with query or a program

Overview:

Purpose:

Display or print selected information from journal entries.

How To:

DSPJRN OUTPUT(*OUTFILE), Create a query or program, or Run a query or program

Authority:

*USE authority to QSYS/QAUDJRN, *USE authority to journal receiver, and *ADD authority to library for output file

You can use the Display Journal (DSPJRN) command to write selected entries from the audit journal receivers to an output file. You can use a program or a query to view the information in the output file.

For the output parameter of the DSPJRN command, specify *OUTFILE. You see additional parameters prompting you for information about the output file:

```

                                Display Journal (DSPJRN)
Type choices, press Enter.
:
Output . . . . . > *OUTFILE
Outfile format . . . . . *TYPE5
File to receive output . . . . . dspjrnout
Library . . . . . mylib
Output member options:
Member to receive output . . . *FIRST
Replace or add records . . . . *REPLACE
Entry data length:
Field data format . . . . . *OUTFILFMT
Variable length field length
Allocated length . . . . .

```

All security-related entries in the audit journal contain the same heading information, such as the entry type, the date of the entry, and the job that caused the entry. The QADSPJR5 (with record format QJORDJE5) is provided to define these fields when you specify *TYPE5 as the output file format parameter. See “Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” on page 564 for more information.

For more information about other records and their output file formats, see Appendix F, “Layout of audit journal entries,” on page 563.

If you want to perform a detailed analysis of a particular entry type, use one of the model database outfiles provided. Table 134 on page 270 shows the name of the model database output file for each entry type. Appendix F, “Layout of audit journal entries,” on page 563 shows the file layouts for each model database output file.

For example, to create an output file called AUDJRNAF5 in QGPL that includes only authority failure entries:

1. Create an empty output file with the format defined for AF journal entries:

```

CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)

```
2. Use the DSPJRN command to write selected journal entries to the output file:

```

DSPJRN JRN(QAUDJRN) ... +
JRNCD E(T) ENTYP(AF) OUTPUT(*OUTFILE) +
OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)

```
3. Use Query or a program to analyze the information in the AUDJRNAF5 file.

Here are a few examples of how you might use QAUDJRN information:

- If you suspect someone is trying to break into your system:

1. Make sure the QAUDLVL system value includes *AUTFAIL.
 2. Use the CRTDUPOBJ object command to create an empty output file with the QASYPWJ5 format.
 3. A PW type journal entry is logged when someone enters an incorrect user ID or password on the Sign On display. Use the DSPJRN command to write PW type journal entries to the output file.
 4. Create a query program that displays or prints the date, time, and workstation for each journal entry. This information should help you determine where and when the attempts are occurring.
- If you want to test the resource security you have defined for a new application:
 1. Make sure the QAUDLVL system value includes *AUTFAIL.
 2. Run application tests with different user IDs.
 3. Use the CRTDUPOBJ object command to create an empty output file with the QASYAFJ5 format.
 4. Use the DSPJRN command to write AF type journal entries to the output file.
 5. Create a query program that displays or prints information about the object, job and user. This information should help you to determine what users and application functions are causing authority failures.
 - If you are planning a migration to security level 40:
 1. Make sure the QAUDLVL system value includes *PGMFAIL and *AUTFAIL.
 2. Use the CRTDUPOBJ object command to create an empty output file with the QASYAFJ5 format.
 3. Use the DSPJRN command to write AF type journal entries to the output file.
 4. Create a query program that selects the type of violations you are experiencing during your test and prints information about the job and program that causes each entry.

Note: Table 134 on page 270 shows which journal entry is written for each authority violation message.

Relationship of object Change Date/Time to audit records

Reports written to detect changes to programs, or other objects, are sometimes based on the Change Date/Time field of the object instead of information in the security audit journal. The following list describes reasons why there might be a difference between the date on the object and the date on the source for the object.

- The **CHGPGM** command is used to force program re-creation to update the Change Date/Time field of the program. This operation writes a ZC (Change to Object) audit record.
- The Sign Object (QYDOSGNO) API is used to digitally sign a program or command to update the Change Date/Time field for the program or command. This operation writes a ZC audit record.

The operating system can also automatically update the Change Date/Time field of an object in the following situations:

- When a user profile has private authority to an object, and that object is then deleted, the system updates the Change Date/Time field of that user profile as it removes that private authority.
- If security auditing is on when the object is deleted, a DO (Delete Operation) audit record is written for the deleted object.
- Because the system automatically updates every user profile that has private authority to the deleted object, no audit records are written for those user profiles, even though their Change Date/Time fields are updated.

To track when your users have used normal system interfaces to change objects, use the security auditing journal. Reports to detect changes to objects that are based solely on the Change Date/Time field of an object can only produce partial results.

Why you should not use the Date/Time field for general security auditing

The main guideline used to decide what to audit for i5/OS is to audit the security-relevant actions of users. The second guideline is to not write audit records for operations that the operating system automatically performs. In some cases, those automatic operations might be audited if the operating system performs the operation by using a function that is also designed to be used by users.

The objectives for maintaining the Change Date/Time field of an object are different from the audit objectives. The main purpose of the Change Date/Time field is to indicate when an object is changed. An updated Change Date/Time field does not indicate what was changed for the object or who made the change. One of the main uses of this field is to indicate that the object should be saved by the Save Changed Objects (SAVCHGOBJ) command. The SAVCHGOBJ command does not need to know when the last change was made, only that the object was changed since it was last saved. This feature allows performance to be optimized for database files. The Change Date/Time field is updated only the first time the file is changed after it was last saved. Performance can be affected if the Change Date/Time field was updated each time a record in the file was updated, added, or deleted.

Other techniques for monitoring security

The security audit journal (QAUDJRN) is the primary source of information about security-related events on your system. The following sections discuss other ways to observe security-related events and the security values on your system.

You will find additional information in Appendix G, "Commands and menus for security commands," on page 707. This section includes examples to use the commands and information about the menus for the security tools.

Monitoring security messages

Some security-relevant events, such as incorrect sign-on attempts, cause a message in the QSYSOPR message queue. You can also create a separate message queue called QSYSMSG in the QSYS library.

If you create the QSYSMSG message queue in the QSYS library, messages about critical system events are sent to that message queue as well as to QSYSOPR. The QSYSMSG message queue can be monitored separately by a program or a system operator. This provides additional protection of your system resources. Critical system messages in QSYSOPR are sometimes missed because of the volume of messages sent to that message queue.

Using the history log

Not all of the authority failure and integrity violation messages are found in the QHST log. These messages are listed here.

Some security-related events, such as exceeding the incorrect sign-on attempts specified in the QMAXSIGN system value, cause a message to be sent to the QHST (history) log. Security messages are in the range 2200 to 22FF. They have the prefixes CPI, CPF, CPC, CPD, and CPA.

Beginning with Version 2 Release 3 of the i5/OS licensed program, some authority failure and integrity violation messages are no longer sent to the QHST (history) log. All information that was available in the QHST log can be obtained from the security audit journal. Logging information to the audit journal provides better system performance and more complete information about these security-related events than the QHST log. The QHST log should not be considered a complete source of security violations. Use the security audit functions instead.

These messages are no longer written to the QHST log:

- CPF2218. These events can be captured in the audit journal by specifying *AUTFAIL for the QAUDLVL system value.

- CPF2240. These events can be captured in the audit journal by specifying *AUTFAIL for the QAUDLVL system value.
- CPF2220. These events can be captured in the audit journal by specifying *AUTFAIL for the QAUDLVL system value.
- CPF4AAE. These events can be captured in the audit journal by specifying *AUTFAIL for the QAUDLVL system value.
- CPF2246. These events can be captured in the audit journal by specifying *AUTFAIL for the QAUDLVL system value.

Using journals to monitor object activity

If you include the *AUTFAIL value for system action auditing (the QAUDLVL system value), the system writes an audit journal entry for every unsuccessful attempt to access a resource. For critical objects, you can also set up object auditing so the system writes an audit journal entry for each successful access.

The audit journal records only that the object was accessed. It does not log every transaction to the object. For critical objects on your system, you might want more detailed information about the specific data that was accessed and changed. Object journaling can provide you with those details. Object journaling is used primarily for object integrity and recovery. Refer to the Journal management topic for a list of object types which can be journaled, and what is journaled for each object type. A security officer or auditor can also use these journal entries to review object changes. Do not journal any objects to the QAUDJRN journal.

Journal entries can include:

- Identification of the job, user, and the time of access
- Before- and after-images of all object changes
- Records of when the object was opened, closed, changed, saved, created, deleted, and so on.

A journal entry cannot be altered by any user, even the security officer. A complete journal or journal receiver can be deleted, but this is easily detected.

If you are journaling a database file, data area, data queue, library, or integrated file system object, you can use the **DSPJRN** command to print all the changes for that particular object. Here are some examples:

Type the following command for a particular database file.

```
DSPJRN JRN(library/journal) +
      FILE(library/file) OUTPUT(*PRINT)
```

Type the following command for a particular data area.

```
DSPJRN JRN(library/journal) +
      OBJ((library/object name *DTAARA)) OUTPUT(*PRINT)
```

Type the following command for a particular data queue.

```
DSPJRN JRN(library/journal) +
      OBJ((library/object name *DTAQ) OUTPUT(*PRINT)
```

Type the following command for a particular integrated file system object.

```
DSPJRN JRN(library/journal) +
      OBJPATH('path name') OUTPUT(*PRINT)
```

Type the following command for a particular library.

```
DSPJRN JRN(library/journal) +
      OBJ(*LIBL/library-name *LIB) OUTPUT(*PRINT)
```

For example, if journal JRNCUST in library CUSTLIB is used to record information about file CUSTFILE (also in library CUSTLIB), the command can be:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
      FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

You can also create an output file and do a query or use SQL to select all of the records from the output file for a specific output.

Type the following command to create an output file for a particular database file.

```
DSPJRN JRN(library/journal) +  
        FILE(library/file name) +  
        OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Type the following command to create an output file for a particular data area.

```
DSPJRN JRN(library/journal) +  
        OBJ((library/object name *DTAARA)) +  
        OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Type the following command to create an output file for a particular data queue.

```
DSPJRN JRN(library/journal) +  
        OBJ((library/object name *DTAQ)) +  
        OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Type the following command to create an output file for a particular integrated file system object.

```
DSPJRN JRN(library/journal) +  
        OBJPATH('path name') +  
        OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

Type the following command to create an output file for a particular library.

```
DSPJRN JRN(library/journal) +  
        OBJ(*LIBL/library-name *LIB) +  
        OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(library/outfile) ENTDTALEN(*CALC)
```

If you want to find out which journals are on the system, use the Work with Journals (**WRKJRN**) command. If you want to find out which objects are being journaled by a particular journal, use the Work with Journal Attributes (**WRKJRNA**) command.

Related information:

Journal management

Analyzing user profiles

You can display or print a complete list of all the users on your system by using the Display Authorized Users (**DSPAUTUSR**) command.

The list can be sequenced by profile name or group profile name. Here is an example of the group profile sequence.

Display Authorized Users

Group Profile	User Profile	Password Last Changed	No Password	Text
DPTSM	ANDERSOR	08/04/0x		Roger Anders
	VINCENTM	09/15/0x		Mark Vincent
DPTWH	ANDERSOR	08/04/0x		Roger Anders
	WAGNERR	09/06/0x		Rose Wagner
QSECOFR	JONESS	09/20/0x		Sharon Jones
	HARRISOK	08/29/0x		Ken Harrison
*NO GROUP	DPTSM	09/05/0x	X	Sales and Marketing
	DPTWH	08/13/0x	X	Warehouse
	RICHARDS	09/05/0x		Janet Richards
	SMITHJ	09/18/0x		John Smith

Printing selected user profiles

You can use the Display User Profile (DSPUSRPRF) command to create an output file, which you can process using a query tool.

```
DSPUSRPRF USRPRF(*ALL) + TYPE(*BASIC) OUTPUT(*OUTFILE)
```

You can use a query tool to create a variety of analysis reports of your output file, such as:

- A list of all users who have both *ALLOBJ and *SPLCTL special authority.
- A list of all users sequenced by a user profile field, such as initial program or user class.

You can create query programs to produce different reports from your output file. For example:

- List all user profiles that have any special authorities by selecting records where the UPSPAU field is not equal to *NONE.
- List all users who are allowed to enter commands by selecting records where the *Limit capabilities* field (called UPLTCP in the model database output file) is equal to *NO or *PARTIAL.
- List all users who have a particular initial menu or initial program.
- List inactive users by looking at the date last sign-on field.
- List all users who do not have a password for use at password levels 0 and 1 by selecting records where the Password present for level 0 or 1 field (called UPENPW in the model output file) is equal to N.
- List all users who have a password for use at password levels 2 and 3 by selecting records where the Password present for level 2 or 3 field (called UPENPH in the model output file) is equal to Y.

Examining large user profiles

You might want to evaluate the security effectiveness of large user profiles on your system. User profiles with large numbers of authorities, appearing to be randomly spread over most of the system, can reflect a lack of security planning.

Here is one method for locating large user profiles and evaluating them.

1. Use the Display Object Description (DSPOBJD) command to create an output file containing information about all the user profiles on the system:

```
DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +  
        DETAIL(*BASIC) OUTPUT(*OUTFILE)
```

2. Create a query program to list the name and size of each user profile, in descending sequence by size.

3. Print detailed information about the largest user profiles and evaluate the authorities and owned objects to see if they are appropriate:

```
DSPUSRPRF USRPRF(user-profile-name) +  
          TYPE(*OBJAUT) OUTPUT(*PRINT)  
DSPUSRPRF USRPRF(user-profile-name) +  
          TYPE(*OBJOWN) OUTPUT(*PRINT)
```

Note: Directories and directory-based objects are not printed. WRKOBJOWN and WRKOBJPVT commands can be used to display directory-based objects and library-based objects, but there is no print function associated with these commands.

Some IBM-supplied user profiles are very large because of the number of objects they own. Listing and analyzing them is not necessary. However, you should check for programs adopting the authority of the IBM-supplied user profiles that have *ALLOBJ special authority, such as QSECOFR and QSYS. See “Analyzing programs that adopt authority.”

Related reference:

Appendix B, “IBM-supplied user profiles,” on page 319

This section contains information about the user profiles that are shipped with the system. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

Analyzing object and library authorities

You can audit the object and library authorities on your system.

You can use the following method to determine who has authority to libraries on the system:

1. Use the DSPOBJD command to list all the libraries on the system:
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
2. Use the Display Object Authority (DSPOBJAUT) command to list the authorities to a specific library:
DSPOBJAUT OBJ(*library-name*) OBJTYPE(*LIB) +
 ASPDEV(*asp-device-name*) OUTPUT(*PRINT)
3. Use the Display Library (DSPLIB) command to list the objects in the library:
DSPLIB LIB(*library-name*) ASPDEV(*asp-device-name*) OUTPUT(*PRINT)

Using these reports, you can determine what is in a library and who has access to the library. If necessary, you can use the DSPOBJAUT command to view the authority for selected objects in the library also.

Analyzing programs that adopt authority

Programs that adopt the authority of a user with *ALLOBJ special authority represent a security exposure. You can analyze these programs to audit the security of the system.

The following method can be used to find and inspect those programs that adopt authority:

1. For each user with *ALLOBJ special authority, use the Display Programs That Adopt (DSPPGMADP) command to list the programs that adopt that user’s authority:

```
DSPPGMADP USRPRF(user-profile-name) +  
          OUTPUT(*PRINT)
```

Note: The topic “Printing selected user profiles” on page 302 shows how to list users with *ALLOBJ authority.

2. Use the DSPOBJAUT command to determine who is authorized to use each adopting program and what the public authority is to the program:

```
DSPOBJAUT OBJ(library-name/program-name) +  
          OBJTYPE(*PGM) ASPDEV(asp-device-name) OUTPUT(*PRINT)
```

Note: The object type parameter might need to be *PGM, *SQLPKG, or *SRVPGM as indicated by the DSPPGMADP report.

3. Inspect the source code and program description to evaluate:

- Whether the user of the program is prevented from excess function, such as using a command line, while running under the adopted profile.
- Whether the program adopts the minimum authority level needed for the intended function. Applications that use program failure adopted authority can be designed using the same owner profile for objects and programs. When the authority of the program owner is adopted, the user has *ALL authority to application objects. In many cases, the owner profile does not need any special authorities.

4. Verify when the program was last changed, using the DSPOBJD command:

```
DSPOBJD OBJ(library-name/program-name) +  
        OBJTYPE(*PGM) ASPDEV(asp-device-name) DETAIL(*FULL)
```

Note: The object type parameter might need to be *PGM, *SQLPKG, or *SRVPGM as indicated by the DSPPGMADP report.

Checking for objects that have been altered

An altered object is often an indication that someone is attempting to tamper with your system. You can use the Check Object Integrity (**CHKOBJITG**) command to check those objects that have been altered.

You might want to run this command after someone has:

- Restored programs to your system
- Used dedicated service tools (DST)

When you run the command, the system creates a database file containing information about any potential integrity problems. You can check objects owned by one or more profiles, objects that match a path name, or all objects on the system. You can look for objects whose domain have been altered and objects that have been tampered with. You can recalculate program validation values to look for objects of type *PGM, *SRVPGM, *MODULE, and *SQLPKG that have been altered. You can check the signature of objects that can be digitally signed. You can check if libraries and commands have been tampered with. You can also start an integrated file system scan or check if objects failed a previous integrated file system scan.

Running the **CHKOBJITG** command requires *AUDIT special authority. The command might take a long time to run because of the scans and calculations that it performs. You should run it at a time when your system is not busy. Most IBM commands duplicated from a release before V5R2 will be logged as violations. These commands should be deleted and re-created using the Create Duplicate Object (**CRTDUPOBJ**) command each time a new release is loaded.

Related information:

Scanning support

Checking the operating system

You can use the Check System (QYDOCHKS) API to check if any key operating system object has been changed since it was signed.

Any object that is not signed or has been changed since it was signed will be reported as an error. Only signatures from a system trusted source are valid.

Running the QYDOCHKS API requires *AUDIT special authority. The API might take a long time to run because of the calculations it performs. You should run it at a time when your system is not busy.

Related reference:

Auditing the security officer's actions

You can keep a record of all actions performed by users with *ALLOBJ and *SECADM special authority for tracking purpose.

To do this, you can use the action auditing value in the user profile:

1. For each user with *ALLOBJ and *SECADM special authority, use the CHGUSRAUD command to set the AUDLVL to have all values that are not included in the QAUDLVL or QAUDLVL2 system values on your system. For example, if the QAUDLVL system value is set to *AUTFAIL, *PGMFAIL, *PRTDTA, and *SECURITY, use this command to set the AUDLVL for a security officer user profile:

```
CHGUSRAUD USER(SECUSER) +
    AUDLVL(*CMD *CREATE *DELETE +
          *OBJMGT *OFCSRVR *PGMADP +
          *SAVRST *SERVICE, +
          *SPLFDTA *SYSMTGT)
```

“Action auditing” on page 113 shows all the possible values for action auditing.

2. Remove the *AUDIT special authority from user profiles with *ALLOBJ and *SECADM special authority. This prevents these users from changing the auditing characteristics of their own profiles.

You cannot remove special authorities from the QSECOFR profile. Therefore, you cannot prevent a user signed on as QSECOFR from changing the auditing characteristics of that profile. However, if a user signed on as QSECOFR uses the CHGUSRAUD command to change auditing characteristics, an AD entry type is written to the audit journal.

It is recommended that security officers (users with *ALLOBJ or *SECADM special authority) use their own profiles for better auditing. The password for the QSECOFR profile should not be distributed.

3. Make sure the QAUDCTL system value includes *AUDLVL.
4. Use the DSPJRN command to review the entries in the audit journal using the techniques described in “Analyzing audit journal entries with query or a program” on page 296.

Chapter 10. Code license and 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.

Appendix A. Security commands

This section contains the system commands related to security. You can use these commands in place of the system menus by typing these commands on a command line. The commands are divided into task-oriented groups.

The Control language (CL) topic contains more detailed information about these commands. The tables in Appendix D, "Authority required for objects used by commands," on page 339 show what object authorities are required to use these commands.

For more information about tools and suggestions about how to use the security tools, see the Configuring the system to use security tools topic.

Authority holders commands

This table provides a list of the commands that allow you to work with authority holders.

Table 136. Authority holders commands

Command name	Descriptive name	Function
CRTAUTHLR	Create Authority Holder	Secure a file before the file exists. Authority holders are valid only for program-described database files.
DLTAUTHLR	Delete Authority Holder	Delete an authority holder. If the associated file exists, the authority holder information is copied to the file.
DSPAUTHLR	Display Authority Holder	Display all the authority holders on the system.

Authority lists commands

You can use these commands to perform different tasks on authority lists.

Table 137. Authority lists commands

Command name	Descriptive name	Function
ADDAUTLE	Add Authorization List Entry	Add a user to an authorization list. You specify what authority the user has to all the objects on the list.
CHGAUTLE	Change Authorization List Entry	Change users' authorities to the objects on the authorization list.
CRTAUTL	Create Authorization List	Create an authorization list.
DLTAUTL	Delete Authorization List	Delete an entire authorization list.
DSPAUTL	Display Authorization List	Display a list of users and their authorities to an authorization list.
DSPAUTLOBJ	Display Authorization List Objects	Display a list of objects secured by an authorization list.
EDTAUTL	Edit Authorization List	Add, change, and remove users and their authorities on an authorization list.
RMVAUTLE	Remove Authorization List Entry	Remove a user from an authorization list.
RTVAUTLE	Retrieve Authorization List Entry	Used in a control language (CL) program to get one or more values associated with a user on the authorization list. The command can be used with the CHGAUTLE command to give a user new authorities in addition to the existing authorities that the user already has.

Table 137. Authority lists commands (continued)

Command name	Descriptive name	Function
WRKAUTL	Work with Authorization Lists	Work with authorization lists from a list display.

Object authority and auditing commands

You can refer to this table for commands that you can use to work with object authority and auditing.

Table 138. Object authority and auditing commands

Command name	Descriptive name	Function
CHGAUD	Change Auditing	Change the auditing value for an object.
CHGAUT	Change Authority	Change the authority of users to objects.
CHGOBJAUD	Change Object Auditing	Specify whether access to an object is audited.
CHGOBJOWN	Change Object Owner	Change the ownership of an object from one user to another.
CHGOBJPGP	Change Object Primary Group	Change the primary group for an object to another user or to no primary group.
CHGOWN	Change Owner	Change the ownership of an object from one user to another.
CHGPGP	Change Primary Group	Change the primary group for an object to another user or to no primary group.
DSPAUT	Display Authority	Display users' authority to an object.
DSPLNK	Display Links	Show a list of names of specified objects in directories and options to display information about the objects.
DSPOBJAUT	Display Object Authority	Displays the object owner, public authority to the object, any private authorities to the object, and the name of the authorization list used to secure the object.
DSPOBJD	Display Object Description	Displays the object auditing level for the object.
EDTOBJAUT	Edit Object Authority	Add, change, or remove a user's authority for an object.
GRTOBJAUT	Grant Object Authority	Specifically give authority to named users, all users (*PUBLIC), or users of the referenced object for the objects named in this command.
RVKOBJAUT	Revoke Object Authority	Remove one or more (or all) of the authorities given specifically to a user for the named objects.
WRKAUT	Work with Authority	Work with object authority by selecting options on a list display.
WRKLNK	Work with Links	Show a list of names of specified objects in directories and options to work with the objects.
WRKOBJ	Work with Objects	Work with object authority by selecting options on a list display.
WRKOBJOWN	Work with Objects by Owner	Work with the objects owned by a user profile.
WRKOBJPGP	Work with Objects by Primary Group	Work with the objects for which a profile is the primary group using options from a list display.
WRKOBJPVT	Work with Objects by Private Authorities	Work with the objects for which a profile is privately authorized, using options from a list display.

Passwords commands

These commands enable the security administrator to assign, change, verify, or reset password associated with a user profile.

Table 139. Passwords commands

Command name	Descriptive name	Function
CHGDSTPWD	Change Dedicated Service Tools Password	Reset the DST security capabilities profile to the default password shipped with the system.
CHGPWD	Change Password	Change the user's own password.
CHGUSRPRF	Change User Profile	Change the values specified in a user's profile, including the user's password.
CHKPWD	Check Password	Verify a user's password. For example, if you want the user to enter the password again to run a particular application, you can use CHKPWD in your CL program to verify the password.
CRTUSRPRF ¹	Create User Profile	When you add a user to the system, you assign a password to the user.
<p>¹ When a CRTUSRPRF is done, you cannot specify that the *USRPRF is to be created into an independent auxiliary storage pool (ASP). However, when a user is privately authorized to an object on an independent ASP, the user is the owner of an object on an independent ASP, or the user is the primary group of an object on an independent ASP, the profile's name is stored on the independent ASP. If the independent ASP 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.</p>		

User profiles commands

As a security administrator, you will need to use these commands to work with user profiles.

Table 140. User profiles commands

Command name	Descriptive name	Function
CHGPRF	Change Profile	Change some of the attributes of the user's own profile.
CHGUSRAUD	Change User Audit	Specify the action and object auditing for a user profile.
CHGUSRPRF	Change User Profile	Change the values specified in a user's profile such as the user's password, special authorities, initial menu, initial program, current library, and priority limit.
CHKOBJITG	Check Object Integrity	Check the objects owned by one or more user profiles or check the objects that match the path name to ensure the objects have not been tampered with.
CRTUSRPRF	Create User Profile	Add a user to the system and to specify values such as the user's password, special authorities, initial menu, initial program, current library, and priority limit.
DLTUSRPRF	Delete User Profile	Delete a user profile from the system. This command provides an option to delete or change ownership of objects owned by the user profile.
DMPUSRPRF	Dump User Profile	Allows you to dump the user profile and related information.

Table 140. User profiles commands (continued)

Command name	Descriptive name	Function
DSPAUTUSR	Display Authorized Users	Displays or prints the following for all user profiles on the system: associated group profile (if any), whether the user profile has a password usable at any password level, whether the user profile has a password usable at the various password levels, whether the user profile has a password usable with NetServer, the date the password was last changed, and the user profile text.
DSPSSTUSR	Display Service Tools User ID	Displays a list of service tools user identifiers. It can also be used to show detailed information about a specific service tools user ID, including the status and privileges of that user.
DSPUSRPRF	Display User Profile command	Display a user profile in several different formats.
GRTUSRAUT	Grant User Authority	Copy private authorities from one user profile to another user profile.
PRTPRFINT	Print Profile Internals	Print a report of internal information about the number of entries.
PRTUSRPRF	Print User Profile	Analyze user profiles that meet specified criteria.
RTVUSRPRF	Retrieve User Profile	Used in a control language (CL) program to get and use one or more values that are stored and associated with a user profile.
WRKUSRPRF	Work with User Profiles	Work with user profiles by entering options on a list display.

Related user profile commands

This table lists some other commands that are related to user profiles. These commands allow you to restore or save the user profiles and their attributes.

Table 141. Related user profile commands

Command name	Descriptive name	Function
DSPPGMADP	Display Programs That Adopt	Display a list of programs and SQL packages that adopt a specified user profile.
RSTAUT	Restore Authority	Restore authorities for objects held by a user profile when the user profile was saved. These authorities can only be restored after a user profile is restored with the Restore User Profile (RSTUSRPRF) command.
RSTUSRPRF	Restore User Profile	Restore a user profile and its attributes. Restoring specific authority to objects is done with the RSTAUT command after the user profile is restored. The RSTUSRPRF command also restores all authorization lists and authority holders if RSTUSRPRF(*ALL) is specified.
SAVSECDTA	Save Security Data	Saves all user profiles, authorization lists, and authority holders without using a system that is in a restricted state.
SAVSYS	Save System	Saves all user profiles, authorization lists, and authority holders on the system. A dedicated system is required to use this function.

Auditing commands

You can use these commands to manage auditing on an object.

Table 142. Auditing commands

Command name	Descriptive name	Function
CHGAUD	Change Auditing	Specify the auditing for an object.
CHGDLOAUD	Change Document Library Object Auditing	Specify whether access is audited for a document library object.
CHGOBJAUD	Change Object Auditing	Specify the auditing for an object.
CHGUSRAUD	Change User Audit	Specify the action and object auditing for a user profile.

Document library objects commands

This table lists the commands that you can use to work with document library objects.

Table 143. Document library objects commands

Command name	Descriptive name	Function
ADDDLOAUT	Add Document Library Object Authority	Give a user access to a document or folder or to secure a document or folder with an authorization list or an access code.
CHGDLOAUD	Change Document Library Object Auditing	Specify the object auditing level for a document library object.
CHGDLOAUT	Change Document Library Object Authority	Change the authority for a document or folder.
CHGDLOOWN	Change Document Library Object Owner	Transfers document or folder ownership from one user to another user.
CHGDLOPGP	Change Document Library Object Primary Group	Change the primary group for a document library object.
DSPAUTLDLO	Display Authorization List Document Library Objects	Display the documents and folders that are secured by the specified authorization list.
DSPDLOAUD	Display Document Library Object Auditing	Displays the object auditing level for a document library object.
DSPDLOAUT	Display Document Library Object Authority	Display authority information for a document or a folder.
EDTDLOAUT	Edit Document Library Object Authority	Add, change, or remove users' authorities to a document or folder.
GRTUSRPMN	Grant User Permission	Gives permission to a user to handle documents and folders or to do office-related tasks on behalf of another user.
RMVDLOAUT	Remove Document Library Object Authority	Remove a user's authority to documents or folders.
RVKUSRPMN	Revoke User Permission	Takes away document authority from one user (or all users) to access documents on behalf of another user.

Server authentication entries commands

These commands allow you to display, add, remove, or change server authentication entries for a user profile.

Table 144. Server authentication entries commands

Command name	Descriptive name	Function
ADDSVRAUTE	Add Server Authentication Entry	Add server authentication information for a user profile.
CHGSVRAUTE	Change Server Authentication Entry	Change existing server authentication entries for a user profile.
DSPSVRAUTE	Display Server Authentication Entries	Display server authentication entries for a user profile.
RMVSVRAUTE	Remove Server Authentication Entry	Remove server authentication entries from the specified user profile.

These commands allow a user to specify a user name, the associated password, and the name of a remote server machine. Distributed Relational Database Access (DRDA) uses these entries to run database access requests as the specified user on the remote server.

System distribution directory commands

You can use these commands to add, remove, change, rename, or display entries in the system distribution directory.

Table 145. System distribution directory commands

Command name	Descriptive name	Function
ADDDIRE	Add Directory Entry	Adds new entries to the system distribution directory. The directory contains information about a user, such as the user ID and address, system name, user profile name, mailing address, and telephone number.
CHGDIRE	Change Directory Entry	Changes the data for a specific entry in the system distribution directory. The system administrator has authority to update any of the data contained in a directory entry, except the user ID, address, and the user description. Users can update their own directory entries, but they are limited to updating certain fields.
DSPDIRE	Display Directory Entries	Display, print, or create a database file for some or all system distribution directory entries.
RMVDIRE	Remove Directory Entry	Removes a specific entry from the system distribution directory. When a user ID and address is removed from the directory, it is also removed from any distribution lists.
RNMDIRE	Rename Directory Entry	Renames a local or remote user ID and address to a new user ID and address. This will rename all occurrences of the specified user ID and address in all IBM-supplied files.
WRKDIRE	Work with Directory	Provides a set of displays that allow a user to view, add, change, and remove entries in the system distribution directory.

Validation lists commands

These two commands allow you to create and delete validation lists in a library.

Table 146. Validation lists commands

Command name	Descriptive name	Function
CRTVLDL	Create Validation List	Create a validation list object that contains entries consisting of an identifier, data that will be encrypted by the system when it is stored, and free-form data.
DLTVLDL	Delete Validation List	Delete the specified validation list from a library.

Function usage information commands

You can use these commands to change or display function usage information.

Table 147. Function usage information commands

Command name	Descriptive name	Function
CHGFCNUSG	Change function usage	Change the usage information for a registered function.
DSPFCNUSG	Display function usage	Display a list of function identifiers and the detailed usage information for a specific function.
WRKFCNUSG	Work with function usage	Display a list of function identifiers and change or display function usage information.

Auditing security tools commands

These commands enable you to work with security auditing, the entries from the security audit journal and the system values that control security auditing.

For more information about the security tools, see Appendix G, “Commands and menus for security commands,” on page 707.

Table 148. Auditing security tools commands

Command name	Descriptive name	Function
CHGSECAUD	Change Security Auditing	Set up security auditing and to change the system values that control security auditing.
CPYAUDJRNE	Copy Audit Journal Entries	Copy entries from the security audit journal to output files that you can query. You can select specific entry types, specific users, and a time period.
DSPAUDJRNE ¹	Display Audit Journal Entries	Display or print information about entries in the security audit journal. You can select specific entry types, specific users, and a time period.
DSPSECAUD	Display Security Auditing Values	Display information about the security audit journal and the system values that control security auditing.
1	IBM has stopped providing enhancements for the DSPAUDJRNE command. The command does not support all security audit record types, and the command does not list all the fields for the records it does support.	

Authority security tools commands

You can use these commands to perform various printing tasks that are related to security settings.

Table 149. Authority security tools commands

Command name	Descriptive name	Function
PRTJOBDAUT	Print Job Description Authority	Print a list of job descriptions whose public authority is not *EXCLUDE. You can use this command to print information about job descriptions that specify a user profile that every user on the system can access.
PRTPUBAUT	Print Publicly Authorized Objects	Print a list of objects of the specified type whose public authority is not *EXCLUDE.
PRTPVTAUT	Print Private Authorities	Print a list of private authorities for objects of the specified type.
PRTQAUT	Print Queue Authority	Print the security settings for output queues and job queues on your system. These settings control who can view and change entries in the output queue or job queue.
PRTSBSDAUT	Print Subsystem Description Authority	Print a list of subsystem descriptions in a library that contains a default user in a subsystem entry.
PRTRGPGM	Print Trigger Programs	Print a list of trigger programs that are associated with database files on your system.
PRTUSROBJ	Print User Objects	Print a list of the user objects (objects not supplied by IBM) that are in a library.

System security tools commands

You can use these commands to work with system security.

Table 150. System security tools commands

Command name	Descriptive name	Function
CHGSECA ¹	Change Security Attributes	Set new starting values for generating user ID numbers or group ID numbers. Users can specify a starting user ID number and a starting group ID number.
CFGSYSSEC	Configure System Security	Set security-relevant system values to their recommended settings. The command also sets up security auditing on your system.
CLRSVRSEC	Clear Server Security Data	Clear decryptable authentication information that is associated with user profiles and validation list (*VLDL) entries. Note: This is the same information that was cleared in releases previous to V5R2 when the QRETSVRSEC system value was changed from '1' to '0'.
DSPSECA	Display Security Attributes	Display the current and pending values of some system security attributes.
PRTCMNSEC	Print Communications Security	Print the security attributes of the *DEVD, *CTL, and *LIND objects on the system.
PRTSYSSECA	Print System Security Attributes	Print a list of security-relevant system values and network attributes. The report shows the current value and the recommended value.
RVKPUBAUT	Revoke Public Authority	Set the public authority to *EXCLUDE for a set of security-sensitive commands on your system.

Table 150. System security tools commands (continued)

Command name	Descriptive name	Function
¹	To use this command, you must have *SECADM special authority.	

Appendix B. IBM-supplied user profiles

This section contains information about the user profiles that are shipped with the system. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

Default values for user profiles

This table shows the default values that are used for all IBM-supplied user profiles and on the Create User Profile (**CRTUSRPRF**) command. The parameters are sequenced in the order they appear on the Create User Profile display.

Table 151. Default values for user profiles

User profile parameter	Default values	
	IBM-supplied user profiles	Create user profile display
Password (PASSWORD)	*NONE	*USRPRF ⁴
Set password to expired (PWDEXP)	*NO	*NO
Status (STATUS)	*ENABLED	*ENABLED
User class (USRCLS)	*USER	*USER
Assistance level (ASTLVL)	*SYSVAL	*SYSVAL
Current library (CURLIB)	*CRTDFT	*CRTDFT
Initial program (INLPGM)	*NONE	*NONE
Initial menu (INLMNU)	MAIN	MAIN
Initial menu library	*LIBL	*LIBL
Limited capabilities (LMTCPB)	*NO	*NO
Text (TEXT)	*BLANK	*BLANK
Special authority (SPCAUT)	*ALLOBJ ¹ *SAVSYS ¹	*USRCLS ²
Special environment (SPCENV)	*SYSVAL	*SYSVAL
Display sign-on information (DSPSGNINF)	*SYSVAL	*SYSVAL
Block password change (PWDCHGBLK)	*SYSVAL	*SYSVAL
Local password management (LCLPWDMGT)	*YES	*YES
Password expiration interval (PWDEXPITV)	*SYSVAL	*SYSVAL
Limit device sessions (LMTDEVSSN)	*SYSVAL	*SYSVAL
Keyboard buffering (KBDUF)	*SYSVAL	*SYSVAL
Maximum storage (MAXSTG)	*NOMAX	*NOMAX
Priority limit (PTYLMT)	0	3
Job description (JOBDD)	QDFTJOBDD	QDFTJOBDD
Job description library	QGPL	*LIBL
Group profile (GRPPRF)	*NONE	*NONE
Owner (OWNER)	*USRPRF	*USRPRF
Group authority (GRPAUT)	*NONE	*NONE
Group authority type (GRPAUTTYP)	*PRIVATE	*PRIVATE
Supplemental groups (SUPGRPPRF)	*NONE	*NONE

Table 151. Default values for user profiles (continued)

User profile parameter	Default values	
	IBM-supplied user profiles	Create user profile display
Accounting code (ACGCDE)	*SYS	*BLANK
Document password (DOCPWD)	*NONE	*NONE
Message queue (MSGQ)	*USRPRF	*USRPRF
Delivery (DLVRY)	*NOTIFY	*NOTIFY
Severity (SEV)	00	00
Printer device (PRTDEV)	*WRKSTN	*WRKSTN
Output queue (OUTQ)	*WRKSTN	*WRKSTN
Attention program (ATNPGM)	*NONE	*SYSVAL
Sort sequence (SRTSEQ)	*SYSVAL	*SYSVAL
Language identifier (LANGID)	*SYSVAL	*SYSVAL
Country or Region Identifier (CNTRYID)	*SYSVAL	*SYSVAL
Coded Character Set Identifier (CCSID)	*SYSVAL	*SYSVAL
Character identifier control (CHRIDCTL)	*SYSVAL	*SYSVAL
Set Job Attributes (SETJOBATR)	*SYSVAL	*SYSVAL
Locale (LOCALE)	*NONE	*SYSVAL
User Option (USROPT)	*NONE	*NONE
User Identification Number (UID)	*GEN	*GEN
Group Identification Number (GID)	*NONE	*NONE
Home Directory (HOMEDIR)	*USRPRF	*USRPRF
EIM association (EIMASSOC)	*NOCHG	*NOCHG
User expiration date (USREXPDATE)	*NONE	*NONE
Authority (AUT)	*EXCLUDE	*EXCLUDE
Action auditing (AUDLVL) ³	*NONE	*NONE
Object auditing (OBJAUD) ³	*NONE	*NONE
¹	When the system security level is changed from level 10 or 20 to level 30 or above, this value is removed.	
²	When a user profile is automatically created at security level 10, the *USER user class gives *ALLOBJ and *SAVSYS special authority.	
³	Action and object auditing are specified using the CHGUSRAUD command.	
⁴	When you perform a CRTUSRPRF, you cannot 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, the user is the owner of an object in an independent disk pool, or the user 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.	

IBM-supplied user profiles

This table lists each IBM-supplied profile, its purpose, and any values for the profile that are different from the defaults for IBM-supplied user profiles.

Note:

IBM-supplied user profiles now includes additional user profiles that are shipped with the licensed program products. The table includes only some, but not all user profiles for licensed program products; therefore, the list is not inclusive.

Attention:

- Password for the QSECOFR profile

You must change the password for the QSECOFR profile after you install your system. This password is the same for every System i product and poses a security exposure until it is changed. However, Do not change any other values for IBM-supplied user profiles. Changing these profiles can cause system functions to fail.

- Authorities for IBM-supplied profiles

Use caution when removing authorities that IBM-supplied profiles have for objects that are shipped with the operating system. Some IBM-supplied profiles are granted private authorities to objects that are shipped with the operating system. Removing any of these authorities can cause system functions to fail.

Table 152. IBM-supplied user profiles

Profile name	Descriptive name	Parameters different from default values
QADSM	ADSM user profile	<ul style="list-style-type: none"> • USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: ADSM profile used by ADSM server • SPCAUT: *JOBCTL, *SAVSYS • JOBD: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	APD user profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *JOBCTL • JOBD: QADSM/QADSM • TEXT: Internal APD User Profile
QAFUSR	APD user profile	<ul style="list-style-type: none"> • TEXT: Internal APD User Profile
QAFDFTUSR	APD user profile	<ul style="list-style-type: none"> • INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Internal APD User Profile
QAUTPROF	IBM authority user profile	
QBRMS	BRM user profile	
QCLUMGT	Cluster management profile	<ul style="list-style-type: none"> • STATUS: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	High availability cluster profile	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG

Table 152. IBM-supplied user profiles (continued)

Profile name	Descriptive name	Parameters different from default values
QCOLSRV	Management central collection services user profile	
QDBSHR	Database share profile	• AUT: *ADD, *DELETE
QDBSHRDO	Database share profile	• AUT: *ADD, *DELETE
QDFTOWN	Default owner profile	• PTYLMT: 3
QDIRSRV	i5/OS Directory Server server user profile	• LMTCPB: *YES • JOB: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
QDLFM	DataLink File Manager profile	• SRTSEQ: *HEX
QDOC	Document profile	• AUT: *CHANGE
QDSNX	Distributed systems node executive profile	• PTYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX
QEJBSVR	WebSphere® Application Server user profile	
QEJB	Enterprise Java user profile	
QFNC	Finance profile	• PTYLMT: 3
QGATE	VM/MVS bridge profile	• CCSID: *HEX • SRTSEQ: *HEX
QIPP	Internet printing profile	• MSGQ: QUSRSYS/QIPP
QLPAUTO	Licensed program automatic install profile	• USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Licensed program install profile	• USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG
QLWISVR	Default profile for IAS servers	• LMTDEVSSN: *NO • DSPSGNINF: *NO • LOCALE: *SYSVAL • MSGQ: QUSRSYS/QLWISVR

Table 152. IBM-supplied user profiles (continued)

Profile name	Descriptive name	Parameters different from default values
QMGTC	Management central profile	<ul style="list-style-type: none"> • JOBD: QSYS/QYPSJOB
QMSF	Mail server framework profile	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QMQM	MQSeries® user profile	<ul style="list-style-type: none"> • USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: MQM user which owns the QMQM library
QNFSANON	NFS user profile	
QNETSPLF	Network spooling profile	
QNTF	Network time profile	<ul style="list-style-type: none"> • JOBD: QTOTNTP • JOBD LIBRARY: QSYS
QPGMR	Programmer profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Performance Explorer user profile	<ul style="list-style-type: none"> • PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: IBM-supplied User Profile
QPM400	IBM Performance Management for System i (PM System i)	<ul style="list-style-type: none"> • SPCAUT: *IOSYSCFG, *JOBCTL
QRDARSADM	Content Manager OnDemand user profile	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • TEXT: OnDemand Administration Profile
QRDAR	Content Manager OnDemand owning profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: OnDemand owning profile
QRDARS4001	Content Manager OnDemand owning profile 1	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: OnDemand file owning profile 1
QRDARS4002	Content Manager OnDemand owning profile 2	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: OnDemand file owning profile 2
QRDARS4003	Content Manager OnDemand owning profile 3	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: OnDemand file owning profile 3

Table 152. IBM-supplied user profiles (continued)

Profile name	Descriptive name	Parameters different from default values
QRDARS4004	Content Manager OnDemand owning profile 4	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: OnDemand file owning profile 4
QRDARS4005	Content Manager OnDemand owning profile 5	<ul style="list-style-type: none"> • INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: OnDemand file owning profile 5
QRMTCAL	Remote Calendar user profile	<ul style="list-style-type: none"> • TEXT: OfficeVision Remote Calendar User
QRJE	Remote job entry profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS¹ *JOBCTL
QSECOFR	Security officer profile	<ul style="list-style-type: none"> • PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PASSWORD: QSECOFR
QSNADS	SNA distribution services profile	<ul style="list-style-type: none"> • CCSID: *HEX • SRTSEQ: *HEX
QSOC	OptiConnect user profile	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Spool profile	
QSPLJOB	Spool job profile	
QSRV	Service profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹, *SAVSYS¹, *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Service Agent user profile	
QSRVBAS	Service basic profile	<ul style="list-style-type: none"> • USRCLS: *PGMR • SPCAUT: *ALLOBJ¹ *SAVSYS¹ *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	CC Server user profile	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: CC Server User Profile
QSVCM	Client Management Server user profile	<ul style="list-style-type: none"> • TEXT: Client Management Server User Profile

Table 152. IBM-supplied user profiles (continued)

Profile name	Descriptive name	Parameters different from default values
QSVSM	ECS user profile	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • STATUS: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: SystemView System Manager User Profile
QSVSMSS	Managed System Service user profile	<ul style="list-style-type: none"> • STATUS: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Managed System Service User Profile
QSYS	System profile	<ul style="list-style-type: none"> • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG
QSYSOPR	System operator profile	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *ALLOBJ¹, *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Triggered cache manager profile	<ul style="list-style-type: none"> • STATUS: *DISABLED
QTCP	Transmission control protocol (TCP) profile	<ul style="list-style-type: none"> • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Trivial File Transfer Protocol	
QTMPLPD	Transmission control protocol/Internet protocol (TCP/IP) printing support profile	<ul style="list-style-type: none"> • PTYLMT: 3 • AUT: *USE
QTMPLPD	Remote LPR user profile	<ul style="list-style-type: none"> • JOBID: QGPL/QDFTJOBID • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD
QTMTWSG	HTML Workstation Gateway Profile user profile	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMTWSG • TEXT: HTML Workstation Gateway Profile
QTMHHTTP	HTML Workstation Gateway Profile user profile	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTTP • TEXT: HTTP Server Profile
QTMHHTTP1	HTML Workstation Gateway Profile user profile	<ul style="list-style-type: none"> • MSGQ: QUSRSYS/QTMHHTTP • TEXT: HTTP Server CGI Profile

Table 152. IBM-supplied user profiles (continued)

Profile name	Descriptive name	Parameters different from default values
QTSTRQS	Test request profile	
QUSER	Workstation user profile	<ul style="list-style-type: none"> • PTYLMT: 3
QWEBADMIN	Profile for the Web Admin GUI	<ul style="list-style-type: none"> • LMTDEVSSN: *NO • DSPSGNINF: *NO • MSGQ: QUSRSYS/QWEBADMIN
QWSERVICE	Default profile for Integrated Web Services server	<ul style="list-style-type: none"> • LMTDEVSSN: *NO • DSPSGNINF: *NO • LOCALE: *SYSVAL • MSGQ: QUSRSYS/QWSERVICE
QYCMCIMOM	Server user profile	
QYPSJSVR	Management Central Java Server profile	
QYPUOWN	Internal APU user profile	<ul style="list-style-type: none"> • TEXT: Internal APU — User profile
¹ When the system security level is changed from level 10 or 20 to level 30 or above, this value is removed.		

Appendix C. Commands shipped with public authority *EXCLUDE

This section identifies which commands have restricted authorization (public authority is *EXCLUDE) when your system is shipped. It shows which IBM-supplied user profiles are authorized to use these restricted commands.

For more information about IBM-supplied user profiles, see the topic “IBM-supplied user profiles” on page 128.

In Table 153, 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. The special authorities required for a command are listed in Appendix D, “Authority required for objects used by commands,” on page 339.

If you choose to grant other users or the public *USE authority to these commands, update this table to indicate that which commands are no longer restricted on your system. Using some commands might require the authority to certain objects on the system as well as to the commands themselves. See Appendix D, “Authority required for objects used by commands,” on page 339 for the object authorities required for commands.

Table 153. Authorities of IBM-supplied user profiles to restricted commands

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDASPCPYD	R				
ADDCADMRE	R				
ADDCADNODE	R				
ADDCLUMON	R				
ADDCLUNODE	R				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	R				
ADDCRGNODE	R				
ADDCRSDMNK	R				
ADDDEVDMNE	R				
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	R				
ADDDWDFN					
ADDJWDFN					
ADDMFS	R				
ADDMSTPART					
ADDNETJOBE	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				
ADDPDXDFN		S		S	
ADDPDXFTR		S		S	
ADDPDRCRQA		S	S	S	S
ADDPDFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZCMDPFR	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZOBJCVN	R				
ANZPFRDTA	R				
ANZPGM	R				
ANZPRB		S	S	S	S
ANZPRACT	R				
ANZS34OCL	R				
ANZS36OCL	R				
APYJRNCHG		S		S	
APYPTF				S	
APYRMTPTF		S	S	S	S
CFGDSTSRV		S	S		
CFGRPDS		S	S		
CFGSYSSEC	R				
CHGACTSCDE	R				
CHGASPA	R				
CHGASPACT					
CHGASPCPYD	R				
CHGASPSSN	R				
CHGCAD	R				
CHGCLU	R				
CHGCLUCFG	R				
CHGCLUMON	R				
CHGCLUNODE	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDIRSRVA					
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
CHGGPHPKG	R				
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	S	S	
CHGJRNA		S	S		
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	R				
CHGNETA	R				
CHGNETJOBE	R				
CHGNFSEXP	R				
CHGNWSA	R				
CHGNWSCFG	R				
CHGOBJCRQA		S	S	S	S
CHGOPTA	R				
CHGPEXDFN		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	

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGS34LIBM	R				
CHKASPBAL	R				
CHKCMNTRC				S	
CHKMSTKVV					
CHKPRDOPT		S	S	S	S
CLRMSTKEY					
CPHDTA	R				
CPYFCNARA	R				
CPYFRMLDIF					
CPYGPHFMT	R				
CPYGPHPKG	R				
CPYPFRCOL	R				
CPYPRDFTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CPYTOLDIF					
CRTADMMDMN	R				
CRTAUTHLR	R				
CRTCAD	R				
CRTCLS	R				
CRTCLS	R				
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTJOB	R				
CRTNWSCFG	R				
CRTPFRTA	R				
CRTPFRSUM					
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	R				
CRTQSTLOD	R				
CRTSBS		S	S		
CRTUDFS	R				
CRTUDFS	R				
CRTVLDL	R				
CVTBASSTR	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CVTBASUNF	R				
CVTBGUDTA	R				
CVTDIR	R				
CVTPFCOL	R				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS38JOB	R				
CVTTCPL		S	S	S	S
DB2LDIF					
DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCAD	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				
DLTGPHPKG	R				
DLTHSTDTA	R				
DLTINTSVR	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
DLTPFCOL	R				
DLTPFRDTA	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
DLTUDFS	R				
DLTVLDL	R				
DLTWNTSVR	R				
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPYSOBY		S	S	S	S
DMPTRC	R	S		S	
DMPUSRPRF					
DSPASPCPYD	R				
DSPASPSSN	R				
DSPCLUINF	R				
DSPCRGINF	R				
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				
DSPPFRTDA	R				
DSPPFRRPH	R				
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				
ENCTOMSTK	R				
ENDASPBAL	R				
ENDASPSSN	R				
ENDCAD	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDDW					
ENDHOSTSVR		S	S	S	S
ENDIDXMON	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ENDJW					
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDNFSSVR	R		S	S	S
ENDPEX		S		S	
ENDPFTRTC	R			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
ENDWCH	R				
GENCPHK	R				
GENCRSDMNK	R				
GENMAC	R				
GENPIN	R				
GENS36RPT	R				
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSINTSVR	R				
INSPTF ²				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				
LDIF2DB					
LODOPTFMW	R				
LODPTF				S	
LODQSTDB	R				
MGRS36	R				
MGRS36APF	R				
MGRS36CBL	R				
MGRS36DFU	R				
MGRS36DSPF	R				
MGRS36ITM	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
MGRS36LIB	R				
MGRS36MNU	R				
MGRS36MSGF	R				
MGRS36QRY	R				
MGRS36RPG	R				
MGRS36SEC	R				
MGRS38OBJ	R				
MIGRATE	R				
PKGPRDDST		S	S	S	S
PRTACTRPT	R				
PRTCMNTRC				S	
PRTCPTRPT	R				
PRTJOBTRPT	R				
PRTJOBTRC	R				
PRTLCKRPT	R				
PRTPOLRPT	R				
PRTSCRPT	R				
PRTSYSRPT	R				
PRTTNSRPT	R				
PRTTRCRPT	R				
PRTDSKINF	R				
PRTERLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	R				
PWRDWN SYS	R		S		
RCLDBXREF	R				
RCLOBJOWN	R				
RCLOPT	R				
RCLSPLSTG		S	S	S	S
RCLSTG		S	S	S	S
RCLTMPSTG		S	S	S	S
RESMGRNAM	R	S	S	S	S
RLSCMNDEV		S	S	S	S
RLSDSTQ		S	S		
RLSIFSLCK	R				
RLSRMTPHS		S	S		
RMVACC	R				
RMVASPCPYD	R				
RMVCADMRE	R				
RMVCADNODE	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVCLUMON	R				
RMVCLUNODE	R				
RMVCRGDEVE	R				
RMVCRGNODE	R				
RMVCRSDMNK	R				
RMVDEVDMNE	R				
RMVDFRID	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVDWDFN					
RMVEXITPGM	R				
RMVJRNCHG		S		S	
RMVJWDFN					
RMVLANADP	R				
RMVMFS	R				
RMVNETJOBE	R				
RMVOPTCTG	R				
RMVOPTSVR	R				
RMVPEXDFN		S		S	
RMVPEXFTR		S		S	
RMVPTF				S	
RMVRMTPTF		S	S	S	S
RMVRPYLE		S			
RMVTRCFTR	R				
RSTAUT	R				
RST ³					
RSTCFG	R				
RSTDFROBJ	R				
RSTDLO	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ ³					
RSTPFRCOL	R				
RSTPFRDTA					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				
RSTUSRPRF	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
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				
SAVPFRCOL	R				
SAVPFRDTA					
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
SETMSTKEY					
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
STRASPBAL	R				
STRASPSSN	R				
STRBEST	R				
STRCAD	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRDW					
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJW	R				

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
STRJOBTRC					
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF ¹			S	S	S
STRNFSSVR	R				
STRNETINS	R				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	R				
STRSPLRCL	R				
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				
STRWCH	R				
TRCASPBAL	R				
TRCCPIC	R				
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	R				
UPDPTFINF	R				
VFYCMN		S	S	S	S
VFYLNKLPDA		S	S	S	S
VFYMSTK	R				
VFYPIN	R				
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKASPCPYD	R				
WRKCNTINF				S	S

Table 153. Authorities of IBM-supplied user profiles to restricted commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
WRKDEVTBL	R				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFCNARA	R				
WRKJRN		S	S	S	
WRKLICINF	R				
WRKNWSCFG	R				
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKPTFORD	R			S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
WRKTRC	R				
WRKTXIDX	R				
WRKUSRTBL	R				
WRKWCH	R				

¹ The QMSF user profile is also authorized to this command.

² QSRV can only run this command if an IPL is not being done.

³ In addition to QSYS, user profile QRDARS400 has authority.

Appendix D. Authority required for objects used by commands

The tables in this section 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 of the objects to which you need authority, 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 IBM i 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.

The following sections 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.

Authority required for object

The authorities specified in the tables show the object authorities and the data authorities that are required for the object when using the command.

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 requires *READ and *ADD authority.

Object type

The value refers to the type of the object specified in the Referenced object column.

File system

The value refers to the type of file system that the referenced object belongs to.

For the integrated file system in the IBM i operating system, refer to Integrated file system.

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.

Table 154. Description of authority types

Authority	Name	Functions allowed
<i>Object authorities:</i>		
*OBJOPR	Object Operational	Look at the description of an object. Use the object as determined by the user's data authorities.

Table 154. Description of authority types (continued)

Authority	Name	Functions allowed
*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.
*OBJREF	Object Reference	Specify a database file as the parent in a referential constraint. For example, assume that 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.
<i>Data authorities:</i>		
*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.		

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

Table 155. System-defined authority

Authority	*ALL	*CHANGE	*USE	*EXCLUDE
<i>Object Authorities</i>				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
<i>Data Authorities</i>				
*READ	X	X	X	
*ADD	X	X		

Table 155. System-defined authority (continued)

Authority	*ALL	*CHANGE	*USE	*EXCLUDE
*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 156. System-defined authority

Authority	*RWX	*RW	*RX	*R	*WX	*W	*X
<i>Object authorities</i>							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
<i>Data authorities</i>							
*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

Command usage assumptions

There are some default assumptions you need to consider before using any command.

1. *USE authority is required to use any 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 that is used by the command. These files and panel groups are shipped with public authority *USE.

General rules for object authorities on commands

This table shows the 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	*X	
	Directory when pattern is specified (* or ?)	*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))	Object to be displayed	*USE	*EXECUTE
	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 (QAxxxx), 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 (QPxxxx 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 that is 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 additional authority to the output queue. A user with *SPLCTL special authority does not need any additional 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 is 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 most objects

This table lists commands that can work on most objects in alphabetical order.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 shows which IBM-supplied user profiles are authorized to the command. The security officer can grant *USE authority to others.

Table 157. Common commands for most objects

Command	Referenced object	Authority needed	
		For object	For library
ALCOBJ ^{1,2,11}	Object	*OBJOPR	*EXECUTE
ANZOBJCVN (Q) ²⁰			
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

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
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	
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
DLTOBJ ³⁵	Object	*OBJEXIST	*EXECUTE
	ASP Device (if specified)	*USE	
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 the general rules.	Refer to the general rules.
	ASP Device (if specified)	*USE	

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
DSPOBJD ^{2, 28}	Output file	Refer to the general rules.	Refer to the general rules.
	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	
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
MOV OBJ ^{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			
PRIPVTAUT ²⁶			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Object	*OBJMGT	*EXECUTE
RMVDFRID (Q) ¹⁰			
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 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
RSTDFROBJ (Q) ¹⁰	QSYS/QPSRLDSP printer output, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Output file, if specified	Refer to the general rules	Refer to the general rules
	QSYS/QASRRSTO field reference file for output file, if an output file is specified and does not exist	*USE	*EXECUTE
RSTOBJ (Q) ^{3,13, 31, 33}	Object, if it already exists in the library	*OBJEXIST ⁸	*EXECUTE, *ADD
	Object, if it is *CFGL, *CNL, *CTLD, *DEV, *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
RSTOBJ (Q)	Tape unit or optical unit	*USE	*EXECUTE
	Tape (QSYSTAP) file or diskette (QSYSDKT) file	*USE ⁸	*EXECUTE
	Optical File (OPTFILE) ²²	*R	Not applicable
	Parent Directory of optical file (OPTFILE) ²²	*X	Not applicable
	Path prefix of OPTFILE ²²	*X	Not applicable
	Optical volume ²⁴	*USE	Not applicable
	QSYS/QPSRLDSP printer output, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	QSYS/QASRRSTO field reference file for output file, if an output file is specified and does not exist	*USE	*EXECUTE
RSTSYSINF	ASP device description ²⁵	*USE	
	Save file	*USE	*EXECUTE
	Tape unit or optical unit	*USE	*EXECUTE
	Optical File (OPTFILE) ²²	*R	Not applicable
	Parent Directory of optical file (OPTFILE) ²²	*X	Not applicable
	Path prefix of OPTFILE ²²	*X	Not applicable
RVKPUBAUT ²⁰	Optical volume ²⁴	*USE	Not applicable

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
RTVOBJD ^{2, 29}	Object	Some authority other than *EXCLUDE	*EXECUTE
RVKOBJAUT ^{3,5,15, 27}	ASP Device (if specified)	*USE	
SAVCHGOBJ ^{3, 32}	Object (8)	*OBJEXIST	*EXECUTE
	Tape unit or 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
	Command user space, if specified	*USE	*EXECUTE
SAVCHGOBJ	Optical File (OPTFILE) ²²	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) ²²	*WX	Not applicable
	Path prefix of optical file (OPTFILE) ²²	*X	Not applicable
	Root Directory (/) of optical volume ^{22, 23}	*RWX	Not applicable
	Optical volume ²⁴	*CHANGE	
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE ⁸	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE ⁸	*EXECUTE
	ASP device description ²⁵	*USE	
SAVOBJ ^{3, 32}	Object	*OBJEXIST ⁸	*EXECUTE
	Media definition	*USE	*EXECUTE
	Tape unit or 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
	Command user space, if specified	*USE	*EXECUTE
SAVOBJ	Optical File (OPTFILE) ²²	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) ²²	*WX	Not applicable
	Path prefix of OPTFILE ²²	*X	Not applicable
	Root directory (/) of optical volume ^{22, 23}	*RWX	Not applicable
	Optical volume ²⁴	*CHANGE	
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE ⁸	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE ⁸	*EXECUTE
	ASP device description ²⁵	*USE	

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
SAVSTG ¹⁰			
SAVSYS ¹⁰	Tape unit, optical unit	*USE	*EXECUTE
	Root directory (/) of optical volume ²²	*RWX	Not applicable
	Optical volume ²⁴	*CHANGE	Not applicable
SAVSYSINF	Media definition	*USE	*EXECUTE
	Tape unit or optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Optical File (OPTFILE) ²²	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) ²²	*WX	Not applicable
	Path prefix of OPTFILE ²²	*X	Not applicable
	Root directory (/) of optical volume ^{22, 23}	*RWX	Not applicable
	Optical volume ²⁴	*CHANGE	
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	
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
STROBJCVN (Q) ²⁰			
STRSAVSYNC ³⁴			
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.

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
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: <ul style="list-style-type: none"> • 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.		
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 a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter.		
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 do one of the following actions: <ul style="list-style-type: none"> • 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 (GRPAUTYP) field in the user profile that is running the command. If the from-object has a primary group, the new object might 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 namespace switch.		

Table 157. Common commands for most objects (continued)

Command	Referenced object	Authority needed	
		For object	For library
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 an 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 is 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 is returned to indicate that the values are not available for retrieval.		
30	See the CHGPGM, CHGSRVPGM, and CHGMOD commands to determine the authority needed to convert programs, service programs, and modules.		
31	You must have *ALLOBJ special authority to specify *YES for the PVTAUT parameter.		
32	You must have either *ALLOBJ or *SAVSYS special authority to specify *YES for the PVTAUT parameter.		
33	You must have *SAVSYS special authority to specify a name for the DFRID parameter.		
34	You must have *SAVSYS and *JOBCTL special authority.		
35	Some supported object types may require additional object and library authorities. Refer to the Delete Object (QLIDLTO) API documentation for more information.		

Access path recovery commands

This table lists the specific authorities required for the access path recovery commands

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 Presentation (AFP) commands

This table lists the specific authorities required for the Advanced Function Presentation (AFP) commands.

Command	Referenced object	Authority needed	
		For object	For library
ADDFNTTBLE	DBCS font table	*CHANGE	*EXECUTE
CHGCDEFNT	Font resource	*CHANGE	*EXECUTE
CHGFNTTBLE	DBCS font table	*CHANGE	*EXECUTE
CRTFNTRSC	Source file	*USE	*EXECUTE
	Font resource: REPLACE(*NO)		*READ, *ADD
	Font resource: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTFNNTBL	DBCS font table		*READ, *ADD
CRTFORMDF	Source file	*USE	*EXECUTE
	Form definition: REPLACE(*NO)		*READ, *ADD
	Form definition: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTOVL	Source file	*USE	*EXECUTE
	Overlay: REPLACE(*NO)		*READ, *ADD
	Overlay: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTPAGDFN	Source file	*USE	*EXECUTE
	Page definition: REPLACE(*NO)		*READ, *ADD
	Page definition: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTPAGSEG	Source file	*USE	*EXECUTE
	Page segment: REPLACE(*NO)		*READ, *ADD
	Page segment: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
DLTFNTRSC	Font resource	*OBJEXIST	*EXECUTE
DLTFNNTBL	DBCS 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
DSPFNNTBL	DBCS font table	*USE	*EXECUTE
RMVFNTTBLE	DBCS 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

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the AF_INET sockets over SNA commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 ADDIPSRTE ¹ ADDIPSLOC ¹ CFGIPS	CHGIPSIFC ¹ CHGIPSLOC ¹ CHGIPSTOS ¹ CVTIPSIFC	CVTIPSLOC ENDIPSIFC (Q) PRTIPSCFG RMVIPSIFC ¹	RMVIPSLOC ¹ RMVIPSRTE ¹ STRIPSIFC (Q)

¹ You must have *IOSYSCFG special authority to use this command.

Alerts commands

This table lists the specific authorities required for the alerts commands.

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

This table lists the specific authorities required for the application development commands.

Command	Referenced object	Authority needed	
		For object	For library
FNDSTRPDM	Source part	*READ	*EXECUTE
MGRFORMD	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			
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, 4}			
WRKMBRPDM ¹	Source file	*USE	*EXECUTE
WRKOBJPDM ¹	File	*READ or Ownership	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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).		
⁴	This command requires *ALLOBJ special authority.		

Authority holder commands

This table lists the specific authorities required for the authority holder commands.

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 the general rules.	Refer to the general rules.

Authorization list commands

This table lists the specific authorities required for the authorization list commands.

Command	Referenced object	Authority needed	
		For object	For QSYS library
ADDAUTLE ¹	*AUTL	*AUTLMGT or ownership	*EXECUTE
CHGAUTLE ¹	*AUTL	*AUTLMGT or ownership	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Owner or *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
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		

Command	Referenced object	Authority needed	
		For object	For QSYS library
¹	You must be the owner or have authorization list management authority.		
²	If you 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

This table lists the specific authorities required for the binding directory commands.

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

This table lists the specific authorities required for the 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 change request description	*CHANGE	*EXECUTE
CHGRSCCRQA (Q)	Change request description	*CHANGE	*EXECUTE
CRTCRQD	Change request description		*READ, *ADD
DLTCRQD	Change request description	*OBJEXIST	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the class commands.

Command	Referenced object	Authority needed	
		For object	For library
CHGCLS	Class	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Class		*READ, *ADD
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

This table lists the specific authorities required for the 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

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the cluster commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
ADDCADMRE (Q) ¹	QMRAP1 service program	*USE	
ADDCADNODE (Q) ¹	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
ADDCLUMON (Q) ¹	QCSTCTL2 service program	*USE	
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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server 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	
CHGCAD (Q) ¹	QCSTCRG1 service program	*USE	
CHGCLU (Q) ¹	QCSTCTL service program	*USE	
CHGCLUMON (Q) ¹	QCSTCTL2 service program	*USE	

Command	Referenced object	Authority needed	
		For object	For library
CHGCLUNODE (Q) ¹	QCSTCTL service program	*USE	
CHGCLURCY	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
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server 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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
I CRTCAD (Q) ¹	QCSTCRG1 service program	*USE	
	Cluster resource group		*OBJOPR, *ADD, *READ (QUSRSYS)
CRTCLU (Q) ¹	QCSTCTL service program	*USE	

Command	Referenced object	Authority needed	
		For object	For library
CRTCRCG (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
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
DLTCAD (Q) ¹	QCSTCRG1 service program	*USE	
	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCLU (Q) ¹	QCSTCTL service program	*USE	
DLTCRG ¹	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
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)
ENDCAD (Q)	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*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	
PRTCADMRE (Q)	QCSTCRG3 service program	*USE	
	QFPADAP1	*USE	
	Cluster Resource Group	*USE	*EXECUTE (QUSRSYS)

Command	Referenced object	Authority needed	
		For object	For library
1 RMVCADMRE (Q) ¹	QMRAP1 service program	*USE	
1 RMVCADNODE (Q) ¹	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
RMVCLUMON (Q) ¹	QCSTCTL2 service 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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
1 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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
1 RMVDEVDMNE (Q) ¹	QCSTDD service program	*USE	
1 RTVCLU	QHASM/QHA-API service program	*USE	
	QCSTCTL1 service program	*USE	
1 RTVCRG	QCSTCTL1 service program	*USE	
	QCSTCRG3 service program	*USE	
	Cluster resource group	*USE	*EXECUTE (QUSRSYS)
STRCAD (Q) ¹	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
STRCHTSVR	Authorization list	*CHANGE	
STRCLUNOD (Q) ¹	QCSTCTL service program	*USE	

Command	Referenced object	Authority needed	
		For object	For library
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	
	Controller description	*USE, *OBJMGT	
	Line description	*USE, *OBJMGT	
	Network server description	*USE, *OBJMGT	
WRKCLU ⁴	Cluster resource group	*USE	*EXECUTE
¹	You must have *IOSYSCFG special authority to use this command.		
²	The authority applies to calling user profile and user profile to run exit program.		
³	The calling user profile is granted *CHANGE and *OBJEXIST authority to the cluster resource group.		
⁴	You must have *SERVICE special authority or be authorized to the i5/OS Service Trace Function through Application Administration in System i Navigator. 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.		

Command (*CMD) commands

This table lists the specific authorities required for the commands related to the operations on command.

Command	Referenced object	Authority needed	
		For object	For library
CHGCMD	Command	*OBJMGT	*EXECUTE
CHGCMDDFT	Command	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Proxy command	*OBJMGT	*EXECUTE
CRTCMD	Source file	*USE	*EXECUTE
	Command: REPLACE(*NO)		*READ, *ADD
	Command: REPLACE(*YES)	Refer to the general rules.	Refer to the general rules.
CRTPRXCMD	Proxy command: REPLACE(*NO)		*READ, *ADD
	Proxy command: REPLACE(*YES)	See General Rules on page D-2	See General Rules on page D-2
DLTCMD	Command	*OBJEXIST	*EXECUTE
DSPCMD	Command	*USE	*EXECUTE
GENCMDDOC ³	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

Command	Referenced object	Authority needed	
		For object	For library
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.		
³	You must have execute (*X) authority to the directories in the path for the generated file, and write and execute (*WX) authorities to the parent directory of the generated file.		

Commitment control commands

This table lists the specific authorities required for the 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
ROLLBACK			
STRCMTCTL	Message queue, when specified on NFYOBJ keyword	*OBJOPR, *ADD	*EXECUTE
	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 *READ	*EXECUTE
WRKCMTDFN ¹			
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the configuration commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
	Printer output (QPSRLDSP), if output(*print) is specified	*USE	*EXECUTE
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	QSYS/QASRRSTO field reference file, if output file is specified and it does not exist	*USE	*EXECUTE
RTVCFGSTS	Object	*OBJOPR	*EXECUTE
RTVCFGSRC	Object	*USE	*EXECUTE
	Source file	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
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, 5, 6, 7}	Object	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS ⁴	Object	*OBJOPR	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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 a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter, or RESETSYS(*YES).		
⁶	You must have *IOSYSCFG special authority when the object is a media library and the status is *ALLOCATE or *DEALLOCATE.		
⁷	You must have *IOSYSCFG and *SECADM special authorities to specify GENPTHCERT(*YES).		

Configuration list commands

This table lists the specific authorities required for the configuration list commands.

Command	Referenced object	Authority needed	
		For object	For library
ADDCFGL 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
CRTCFL 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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		
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		

Command	Referenced object	Authority needed	
		For object	For library
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.		

Cryptography commands

This table lists the specific authorities required for the cryptography commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
ADDCKMKSFE	User file	*ADD, *OBJOPR, *READ	
	User library		*EXECUTE
	User directory	*X	
	User stream file	*R	
ADDMSTPART (Q) ¹			
CHKMSTKVV (Q) ¹			
CLRMSTKEY (Q) ¹			
CRTCKMKSF	User library		*ADD, *EXECUTE
DSPCKMKSFE	User file	*OBJOPR, *READ	
	User library		*EXECUTE
GENCKMKSFE	User file	*ADD, *OBJOPR, *READ	
	User library		*EXECUTE
RMVCKMKSFE	User file	*DLT, *OBJOPR	
	User library		*EXECUTE
SETMSTKEY (Q) ¹			
TRNCKMKSF	User file	*OBJOPR, *READ, *UPD	
	User library		*EXECUTE
¹ You must have *ALLOBJ and *SECADM special authorities to use this command.			

Data area commands

This table lists the specific authorities required for the 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 even though 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the device description commands.

Command	Referenced object	Authority needed	
		For object	For library
CFGDEVMLB ⁴	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGASPACT (Q) ⁷	Device description	*USE	
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
CHGDEVCRP 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
CHGDEVNWSH 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

Command	Referenced object	Authority needed	
		For object	For library
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
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		
CRTDEVNWSH ⁴	Device description		*EXECUTE
CRTDEVOPT ⁴	Device description		*EXECUTE
CRTDEVPR 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
DSPASPSTS	Device description	*USE	
DSPCNNSTS	Device description	*OBJOPR	*EXECUTE
DSPDEVD	Device description	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
ENDASPBAL (Q)			
ENDDEVRCY	Device description	*USE	*EXECUTE
HLDCMNDDEV ²	Device description	*OBJOPR	*EXECUTE
PRTCMNSEC ^{4,5}			
RLSCMNDDEV	Device description	*OBJOPR	*EXECUTE
RSMDEVRCY	Device description	*USE	*EXECUTE
SETASPGRP ⁶	All device descriptions in ASP group	*USE	
	All the specified libraries in the library list before the library namespace and the library list are changed	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD ³	Device description	*OBJOPR	*EXECUTE
¹	To remove an associated output queue, object existence (*OBJEXIST) authority to the output queue and execute (*EXECUTE) 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.		
⁶	When *CURUSR is specified for the ASP group (ASPGRP) or the Libraries for the current thread (USRLIBL) parameter, you must also have read (*READ) authority to the job description that is listed in your user profile and execute (*EXECUTE) authority to the library where the job description is located.		
⁷	You must have *JOBCTL special authority to run this command.		

Device emulation commands

This table lists the specific authorities required for the 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
EMLPRTKEY	Emulation device description when specified	*OBJOPR	*EXECUTE
	Emulation device description when location specified	*OBJOPR	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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, workstation device, and workstation 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, printer output, 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

This table lists the specific authorities required for the directory and directory shadowing commands.

These commands do not require any object authorities:			
ADDDIRE ² ADDDIRSHD ¹ CHGSYSDIRA ² CHGDIRE ³	CHGDIRSHD ¹ CPYFRMDIR ¹ CPYTODIR ¹ DSPDIRE	ENDDIRSHD ⁴ RMVDIRE ¹ RMVDIRSHD ¹ RNMDIRE ²	STRDIRSHD ⁴ WRKDIRE ^{3,5} WRKDIRLOC ^{1,5} 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.		

Directory server commands

This table lists the specific authorities required for the directory server commands.

Command	Referenced object	Authority needed	
		For object	For library
CHGDIRSRVA ¹			

Command	Referenced object	Authority needed	
		For object	For library
CPYTOLDIF ²	LDIF stream file (if it already exists)	*STMF	*W, *OBJEXIST, *OBJMGT
	Parent directory of LDIF stream file	*DIR	*WX
CPYFRMLDIF ²	LDIF stream file	*STMF	*R
	Parent directory of LDIF stream file	*DIR	*X
DB2LDIF ²	LDIF stream file (if it already exists)	*STMF	*W, *OBJEXIST, *OBJMGT
	Parent directory of LDIF stream file	*DIR	*WX
LDIF2DB ²	LDIF stream file	*STMF	*R
	Parent directory of LDIF stream file	*DIR	*X
¹ You must have *ALLOBJ and *IOSYSCFG special authority. ² To use this command, you must meet one of the following conditions: <ul style="list-style-type: none"> • Have *ALLOBJ and *IOSYSCFG special authorities • Provide the administrator DN and password • Be a Directory Server administrator 			

Disk commands

This table lists the specific authorities required for the disk commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 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

This table lists the specific authorities required for the display station pass-through commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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			

Command	Referenced object	Authority needed	
		For object	For library
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			
<p>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.</p> <p>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.</p>			

Distribution commands

This table lists the specific authorities required for the distribution commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST ¹	Requested file	*CHANGE	*EXECUTE
RCVDST ¹	Requested file	*CHANGE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
RLSDSTQ (Q)			

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the distribution list commands.

These commands do not require any object authorities:			
ADDDSTLE ¹ CHGDSTL ¹	CRTDSTL DLTDSL ¹	DSPDSTL RMVDSTLE ¹	RNMDSTL 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

This table lists the specific authorities required for the 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
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

Command	Referenced object	Authority needed	
		For object	For library
CHKDLO ²	Document library object	As required by the AUT keyword	*EXECUTE
CHKDOC	Document	*CHANGE	*EXECUTE
	Spelling aid dictionary	*CHANGE	*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 the general rules.	Refer to the general rules.
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
MRGDOC ⁵	Document	*USE	*EXECUTE
	From-folder	*USE	*EXECUTE
	To-document if document is replaced	Refer to the general rules.	Refer to the general rules.
	To-folder if to-document is new	Refer to the general rules.	Refer to the general rules.
PAGDOC	Document	*CHANGE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
PRTDOC	Folder	*USE	*EXECUTE
	Document	*USE	*EXECUTE
	DLTPF, DLTF, and DLTOVR commands, if an <i>INDEX</i> instruction is specified	*USE	*EXECUTE
	CRTPE, OVRPRTE, DLTSPLF, and DLTOVR commands, if a <i>RUN</i> instruction is specified	*USE	*EXECUTE
	Save document, if SAVOUTPUT (*YES) is specified	*USE	*EXECUTE
	Save folder, if SAVOUTPUT (*YES) is specified	*USE	*EXECUTE
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 (Q) ^{7, 8, 9}	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 the general rules.	Refer to the general rules.
	Save file	*USE	*EXECUTE
	Optical file (OPTFILE) ¹⁷	*R	Not applicable
	Path prefix of optical file (OPTFILE) ¹⁷	*X	Not applicable
	Optical volume ¹⁹	*USE	Not applicable
	Tape unit 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 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 the general rules.	Refer to the general rules.
	Optical File (OPTFILE) ¹⁷	*RW	Not applicable
	Parent directory of optical file (OPTFILE) ¹⁷	*WX	Not applicable
	Path Prefix of optical file (OPTFILE) ¹⁷	*X	Not applicable
	Root Directory (/) of volume ^{17, 18}	*RWX	Not applicable
Optical Volume ¹⁹	*CHANGE	Not applicable	
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	You 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	You must have authority to the object being used as the merge source. For example, if MRGTYPE(*QRY) is specified, you 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 you have at least *USE authority are returned in the document list or output file.		
⁷	You must have *SAVSYS, *ALLOBJ special authority, or have been enrolled in the system distribution directory.		
⁸	You must have *SAVSYS or *ALLOBJ special authority to use the following parameter combination: RSTDLO DLO(*MAIL).		
⁹	You must have *ALLOBJ special authority to specify a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter.		
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	You must have *SAVSYS or *ALLOBJ special authority to use the following parameter combinations: <ul style="list-style-type: none"> • 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	You must have *ALLOBJ special authority when OWNER (*ALL) or OWNER (name) and Name is a different user profile as the caller.		
21	You must have all object (*ALLOBJ) or audit (*AUDIT) special authority to use this command.		
22	You must have all object (*ALLOBJ) special authority to use this command when specifying *DST for the object class that is to be located.		

Domain Name System commands

This table lists the specific authorities required for the Domain Name System (DNS) commands.

Command	Referenced object	Authority needed	
		For object	For library
CHKDNSCFG ¹	Existing configuration file	*R	
	Path to existing configuration file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
CHKDNSZNE ¹	Existing zone file	*R	
	Path to existing zone file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	

Command	Referenced object	Authority needed	
		For object	For library
CRTRNDCCFG ¹	Existing entropy source file	*R	
	Path to existing entropy source file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
RUNDNSUPD	Existing batch input file	*R	
	Path to existing batch input file	*X	
	Existing key file	*R	
	Path to existing key file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
RUNRNDCMD	Existing RNDC configuration file	*R	
	Path to existing RNDC configuration file	*X	
	Existing key file	*R	
	Path to existing key file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
STRDIGQRY	Existing batch input file	*R	
	Path to existing batch input file	*X	
	Existing trusted key file	*R	
	Path to existing trusted key file	*X	
	Existing key file	*R	
	Path to existing key file	*X	
	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
STRHOSTQRY	Existing output file	*W	
	Path to existing output file	*X	
	Parent of new output file	*RX	
¹ You must have *IOSYSCFG special authority to run this command.			

Double-byte character set commands

This table lists the specific authorities required for the 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
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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
RMVEWCPTCE	Source file	*USE	*EXECUTE

File commands

This table lists the specific authorities required for the file commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

Command	Referenced object	Authority needed	
		For object	For library
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
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	Printer output	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified	*OBJOPR	*EXECUTE
CHGSAVF	Save file	*OBJOPR, and (*OBJMGT or *OBJALTER).	*EXECUTE
CHGSRCPF	Source physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGTAPF	Tape file	*OBJOPR, *OBJMGT	*EXECUTE
	Device if device name specified	*OBJOPR	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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 the general rules.	Refer to the general rules.
	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 the general rules.	Refer to the general rules.
CPYFRMIMPF	From-file	*OBJOPR, *READ	*USE
	To-file (device file)	*OBJOPR, *READ	*USE
	To-file (physical file)	Refer to the general rules.	Refer to the general rules.
	Based-on file if from-file is logical file	*READ	*USE
	command CRTDDMF	*USE	*USE
CPYFRMQRYF ¹	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to the general rules.	Refer to the general rules.
CPYFRMSTMF	Stream file	*R	
	Directories in stream file path name prefix	*X	
	Target database file, if MBROPT(*ADD) specified	*WX	*X
	Target database file, if MBROPT(*REPLACE or *NONE) specified	*WX, *OBJMGT	*X
	Target database file, if new member created	*WX	*X, *ADD
	Conversion table *TBL used to translate data	*R	*X
	Target save file exists	*RWX, *OBJMGT	*X
	Target save file is created		*RWX
CPYFRMTAP	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to the general rules.	Refer to the general rules.
CPYSRCF	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to the general rules.	Refer to the general rules.

Command	Referenced object	Authority needed	
		For object	For library
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 the general rules.	Refer to the general rules.
	Based-on file if from-file is logical file	*READ	*USE
	command CRTDDMF	*USE	*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	
	Database file and stream file, if AUT(*FILE) or AUT(*INDIRFILE) is specified	*OBJMGT	
	Conversion table *TBL used to translate data	*R	*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
CRTDDMF	DDM file: REPLACE(*NO)		*READ, *ADD
	DDM file: REPLACE(*YES)	Refer to the general rules.	*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 the general rules.	*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 the general rules.	*READ, *ADD, *EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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 the general rules.	*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 REFACCPH 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
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
	Printer output: Replace(*NO)		*READ, *ADD, *EXECUTE
	Printer output: Replace(*YES)	Refer to the general rules.	*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 the general rules.	*READ, *ADD
	Create Display File (CRTDSPF) command	*OBJOPR	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
CRTTAPF	Tape file: REPLACE(*NO)		*READ, *ADD
	Tape file: REPLACE(*YES)	Refer to the general rules.	*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 the general rules.	Refer to the general rules.
DSPDDMF	DDM file	*OBJOPR	
DSPDTA	Data file	*USE	*EXECUTE
	Program	*USE	*EXECUTE
	Display file	*USE	*EXECUTE
DSPFD ²	File	*OBJOPR	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
	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 the general rules.	Refer to the general rules.
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
PRTRGPGM ¹¹			

Command	Referenced object	Authority needed	
		For object	For library
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
RMVPCST	File	*OBJMGT or *OBJALTER	*EXECUTE
RMVPFTRG	Physical file	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	File containing member	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F ⁴ (Q)	To-file	*ALL	Refer to the general rules.
	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	Not applicable
	Parent Directory of OPTFILE ⁸	*WX	Not applicable
	Path Prefix of OPTFILE ⁸	*X	Not applicable
	Root Directory (/) of Optical Volume ^{8,9}	*RWX	Not applicable
	Optical Volume ¹⁰	*CHANGE	Not applicable
SAVS36F	From-file	*USE	*EXECUTE
	To-file, when it is a physical file	*ALL	Refer to the general rules.
	Device file or device description	*USE	*EXECUTE
SAVS36LIBM	To-file, when it is a physical file	*ALL	Refer to the general rules.
	From-file	*USE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
STRAPF ³	Source file	*OBJMGT, *CHANGE	*READ, *ADD
	Commands CRTPE, CRTLE, 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

Command	Referenced object	Authority needed	
		For object	For library
WRKDDMF ³	DDM file	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF ^{3,5}	Files	*OBJOPR	*USE
WRKPFCST ³			*EXECUTE
¹	The CPYFRMQRYP command uses a FROMOPNID parameter rather than a FROMFILE parameter. A user must have sufficient authority to perform the OPNQRYP command before running the CPYFRMQRYP command. If CRTFILE(*YES) is specified on the CPYFRMQRYP command, the first file specified on the corresponding OPNQRYP 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

This table lists the specific authorities required for the 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

Command	Referenced object	Authority needed	
		For object	For library
WRKFTR ¹	Filter	Any authority	*EXECUTE
WRKFTRACNE ¹	Filter	*USE	*EXECUTE
WRKFTRSLTE ¹	Filter	*USE	*EXECUTE

¹ To use an individual operation, you must have the authority required by the operation.

Finance commands

This table lists the specific authorities required for the finance commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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.

IBM i graphical operations commands

This table lists the specific authorities required for the IBM i graphical operations commands.

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			

Command	Referenced object	Authority needed	
		For object	For library
¹	The workstation object is an internal object that is created when you install the IBM i 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 authorities: <ul style="list-style-type: none"> • 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the host server commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 catalog commands

This table lists the specific authorities required for the image catalog commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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	Authority needed	
			For object	For library ¹
ADDIMGCLGE	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	*X	
	Device name when FROMDEV specified	*DEV	*USE	
	Image file when FROMFILE specified	*STMF	*R, *OBJMGT	
	Image file path prefix when FROMFILE specified	*DIR	*X	
	Image file parent directory when FROMFILE specified	*DIR	*RX	
CHGIMGCLG	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the general rules	
	New image catalog directory path prefix when DIR parameter specified	*DIR	Refer to the general rules	
CHGIMGCLGE	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the general rules	
CRTIMGCLG	QUSRSYS	*LIB		*READ, *ADD
	Image catalog if DIR(*REFIMGCLG) specified	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Image catalog directory path prefix ²	*DIR	Refer to the general rules	
DLTIMGCLG	Image catalog	*IMGCLG	*OBJEXIST	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the general rules	
LODIMGCLG	Image catalog	*IMGCLG	*USE	*EXECUTE
	Image catalog when WRTPTC(*ALL) or WRTPTC(*NONE) is specified	*IMGCLG	*CHANGE	*EXECUTE
	Virtual device	*DEV	*USE	
	Image catalog directory path prefix	*DIR	Refer to the general rules	
LODIMGCLGE	Image catalog	*IMGCLG	*USE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the general rules	
RMVIMGCLGE	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the general rules	
RTVIMGCLG	Image catalog	*IMGCLG	*USE	*EXECUTE
	Device description if DEV parameter specified	*DEV	*USE	
STRNETINS (Q)	Network optical device	*DEV	*USE	
VFYIMGCLG	Image catalog	*IMGCLG	*USE	*EXECUTE
	Virtual device	*DEV	*USE	
	Image catalog directory path prefix	*DIR	Refer to the general rules	
WRKIMGCLG	Image catalog	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE	Image catalog	*IMGCLG	*USE	*EXECUTE

¹ The library that image catalog objects reside in is QUSRSYS.

² If a directory is created, you also need write (*W) authority to the directory to contain the new directory.

Integrated file system commands

This table lists the specific authorities required for the integrated file system commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 when LNKTYPE(*HARD) is specified	*STMF	QOpenSys, "root" (/),UDFS	*OBJEXIST
	Parent of new link	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Path prefix	Refer to the general rules.		
CHGATR	Object when setting an attribute other than *USECOUNT, *ALWCKPWRT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL, *CRTOBJAUD	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 ²⁶	*DIR and *STMF	QOpenSys, "root" (/), UDFS	
	Object when setting the following attributes: *SETUID, *SETGID, *RSTRDRNMUNL	Any	All except QSYS.LIB and QDLS	Ownership ¹⁵
*CRTOBJAUD ⁹				
Path prefix ⁹	Refer to the general rules.			
CHGAUD ⁴				

Command	Referenced object	Object type	File system	Authority needed for object ¹
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
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory or library	All	*RX
CHGCURDIR	Object	Any directory		*R
	Optical volume	*DDIR	QOPT ⁸	*X
	Path prefix	Refer to the general rules.		
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
CHGOWN ²⁴	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
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory or library	All	*RX
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

Command	Referenced object	Object type	File system	Authority needed for object ¹
CHGPGP	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
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory or library	All	*RX
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
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory	All	*RX
	Path prefix	Refer to the general rules.		
CHKOUT	Object	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory	All	*RX
	Path prefix	Refer to the general rules.		

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
CPY ²⁵	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	
CPY ²⁵	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
CPYFRMSTMF	See "File commands" on page 381			
CPYTOSTMF	See "File commands" on page 381			
CRTDIR ^{21, 22}	Parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Any		*ADD
		*DDIR	QOPT ¹¹	*WX
CRTDIR	Path prefix	Refer to the general rules.		
	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 the general rules.		
DSPCURDIR	Path prefix	*DIR	QOpenSys, "root" (/), UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT ¹¹	*RX
DSPCURDIR	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
DSPF	Database file	*FILE	QSYS.LIB	*USE
	Database file library	*LIB	QSYS.LIB	*EXECUTE
	Stream file	*STMF	QOpenSys, "root" (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
	Path prefix	Refer to the general rules.		

Command	Referenced object	Object type	File system	Authority needed for object ¹
DSPLNK	Any	Any	"root" (/), QOpenSys, UDFS QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	None
	File, Option 12 (Work with Links)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	"root" (/), QOpenSys, UDFS	*R
DSPLNK	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 ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Parent directory of referenced object - Pattern specified ¹³	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB ²⁷	*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 ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Parent directory of referenced object - Option 12 (Work with Links)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Command	Referenced object	Object type	File system	Authority needed for object ¹
DSPLNK	Prefix of parent referenced object - No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Prefix of parent referenced object - Pattern specified ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
DSPLNK	Prefix of parent referenced object - Option 12 (Work with Links)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Command	Referenced object	Object type	File system	Authority needed for object ¹
DSPLNK	Relative Path Name ¹⁴ : Current working directory containing object -No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*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 ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
DSPLNK	Relative Path Name ¹⁴ : Prefix of current working directory containing object -No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
DSPLNK	Relative Path Name ¹⁴ : Prefix of current working directory containing object -Pattern specified ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
DSPMFSINF	Object	Any	Any	None
	Path Prefix	Refer to the general rules.		
EDTF	Database file, existing member	*FILE	QSYS.LIB	*CHANGE
	Database file library	*LIB	QSYS.LIB	*EXECUTE
	Database file, new member	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Database file library, new member	*LIB	QSYS.LIB	*EXECUTE, *ADD
	Stream file, existing file	*STMF	QOpenSys, "root" (/), UDFS	*R
	User space	*USRSPC	QSYS.LIB	*CHANGE
	Parent directory when creating a new stream file	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Path prefix	Refer to the general rules.		

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
	Journal	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Path Prefix	Refer to the general rules.		
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
MOV	Path (source), parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, "root" (/)	*RX, *OBJEXIST
		others	QOpenSys, "root" (/)	*RWX
	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

Command	Referenced object	Object type	File system	Authority needed for object ¹
MOV	Path prefix (target)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	others	*X
		*DDIR	QOPT ¹¹	*X
	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	Not applicable
	*DSTMF	QOPT ¹¹	*RW	
MOV	Moved into QSYS *MBR	*STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT ¹¹	*RW
MOV	Optical volume (Source and Target)	*DDIR	QOPT ⁸	*CHANGE
	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 the general rules.		
RCLLNK ¹⁶				
RLSIFSLCK ¹⁸	object	*STMF	"root" (/), QOpenSys, UDFS	*R
	Path prefix	Refer to the general rules.		
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

Command	Referenced object	Object type	File system	Authority needed for object ¹
RMVDIR	Parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT ¹¹	*WX
	Directory that contains objects when SUBTREE(*ALL) is specified	Any directory	All	*RX
	Optical volume	*DDIR	QOPT ⁸	*CHANGE
	Path Prefix	Refer to the general rules.		
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
RMVLNK	Parent Directory	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, "root" (/), UDFS	*WX
		*DDIR	QOPT ¹¹	*WX
	Optical volume	*DDIR	QOPT ⁸	*CHANGE
		Path prefix	Refer to the general rules.	
RNM ¹⁹	Object	*DIR	QOpenSys, "root" (/), UDFS	*OBJMGT, *W
		Not *DIR	QOpenSys, "root" (/), UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Not applicable
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		others	QSYS.LIB	*OBJMGT
	*DSTMF	QOPT ¹¹	*W	
	Optical Volume (Source and Target)	*DDIR	QOPT ⁸	*CHANGE

Command	Referenced object	Object type	File system	Authority needed for object ¹
RNM	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	
RST (Q) ^{23, 28, 30}	Object, if it exists ²	Any	QOpenSys, "root" (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Varies ¹⁰
			QDLS	*ALL
	Path prefix	Refer to the general rules.		
	Parent directory created by the restore operation due to CRTPRNDIR(*YES) ²	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Parent directory owner specified on parameter PRNDIROWN ^{2, 6}	*USRPRF	QSYS.LIB	*ADD
RST (Q)	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, optical unit, or save file	*DEV, *FILE	QSYS.LIB	*RX
	Media definition	*MEDDFN	QSYS.LIB	*USE
RST (Q)	Library for device description, media definition, 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

Command	Referenced object	Object type	File system	Authority needed for object ¹
RST (Q)	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
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
RTVCURDIR	Current directory	*DIR	QOpenSys, "root" (/), UDFS, QOPT ¹¹	*X
		*DDIR	QOPT ¹¹	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Any		*R
SAV ²⁹	Object ²	Any	QOpenSys, "root" (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Varies ¹⁰
			QDLS	*ALL
	Path prefix	Refer to the general rules.		
	Tape unit, optical unit	*DEVVD	QSYS.LIB	*RX
	Media definition	*MEDDFN	QSYS.LIB	*USE
SAV	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, media definition, save file, or save-while-active message queue	*LIB	QSYS.LIB	*EXECUTE
SAV	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

Command	Referenced object	Object type	File system	Authority needed for object ¹
SAV	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
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 the general rules.		
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
	Journal	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Path Prefix	Refer to the general rules.		
WRKAUT ^{6,7}	Object	*DOC or *FLR	QDLS	*ALL
		All	not QDLS	*OBJMGT or ownership
		*DDIR and *DSTMF	QOPT ¹¹	*NONE
	Optical volume	*DDIR	QOPT ⁸	*USE
	Path prefix	Refer to the general rules.		

Command	Referenced object	Object type	File system	Authority needed for object ¹
WRKLNK	Any	Any	"root" (/), QOpenSys, UDFS, QSYS.LIB ²⁷ , QDLS, QOPT ¹¹	None
	File, Option 12 (Work with Links)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	"root" (/), QOpenSys, UDFS	*R
	Symbolic link object	*SYMLNK	"root" (/), QOpenSys, UDFS	None
	Optical volume	*DDIR	QOPT ⁸	*USE
WRKLNK	Parent directory of referenced object - No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Parent directory of referenced object - Pattern Specified	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB ²⁷	*R
		*FLR	QDLS	*R
		*DDIR	QOPT ¹¹	*R
		*DDIR		*R
WRKLNK	Parent directory of referenced object- Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Parent directory of referenced object - Option 12 (Work with Links)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Command	Referenced object	Object type	File system	Authority needed for object ¹
WRKLNK	Prefix of parent referenced object - No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Prefix of parent referenced object - Pattern specified ¹³	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R
WRKLNK	Prefix of parent referenced object - Option 12 (Work with Links)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*SYMLNK	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB ²⁷	*X
		*FLR	QDLS	*X
		*DDIR	QOPT ¹¹	*X
		*DDIR		*R

Command	Referenced object	Object type	File system	Authority needed for object ¹
WRKLNK	Relative Path Name ¹⁴ : Current working directory containing object -No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB ²⁷	*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 ²⁷	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT ¹¹	*RX
		*DDIR		*R
WRKLNK	Relative Path Name ¹⁴ : Prefix of current working directory containing object -No Pattern ¹³	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB ²⁷	*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 ²⁷	*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 . 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.

Command	Referenced object	Object type	File system	Authority needed for object ¹
6 7 8 9 10	<p>If the profile that is specified using the PRNDIROWN parameter is not the user doing the restore operation, *SAVSYS or *ALLOBJ special authority is required.</p> <p>These commands require the authority shown plus the authorities required for the DSPCURDIR command.</p> <p>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.</p> <p>The user must have *AUDIT special authority to change the *CRTOBJAUD attribute, and the user does not need any of the normal path name prefix authorities (*X and *R).</p> <p>Authority required varies by the command used. See the respective SAVOBJ or RSTOBJ command for the required authority.</p>			
11 12 13 14 15	<p>Authority required by QOPT against media formatted in "Universal Disk Format" (UDF).</p> <p>*ADD is needed only when object being moved to is a *MRB.</p> <p>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.</p> <p>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'.</p> <p>If you have *ALLOBJ special authority, you do not need the listed authority.</p>			
16 17 18 19 20	<p>You must have *ALLOBJ special authority to use this command.</p> <p>In the above table, QSYS.LIB refers to independent ASP QSYS.LIB file systems as well as QSYS.LIB file system.</p> <p>To use this command, you must have *IOSYSCFG special authority.</p> <p>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:</p> <ul style="list-style-type: none"> • The user has all object (*ALLOBJ) special authority. • The user is the owner of the object being unlinked. • The user is the owner of the directory. <p>If RMVLNK (*YES) is specified, the user must also have *OBJEXIST authority to all objects in the specified directory.</p>			
21 22 23 24 25	<p>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.</p> <p>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.</p> <p>You must have *ALLOBJ special authority to specify a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter. Also, you must have *SAVSYS or *ALLOBJ special authority to specify *UDFS as the value for the RBDMFS parameter.</p> <p>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.</p> <p>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.</p>			

Command	Referenced object	Object type	File system	Authority needed for object ¹
²⁶	The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority to specify the *CRTOBJSCAN and *SCAN attributes.			
²⁷	When you display the contents of the /QSYS.LIB directory, user profile (*USRPRF) objects to which the caller does not have any authority (such as *EXCLUDE) are not returned.			
²⁸	The user must have *ALLOBJ special authority to specify *YES for the PVTAUT parameter.			
²⁹	The user must have *ALLOBJ or *SAVSYS special authority to specify *YES for the PVTAUT parameter.			
³⁰	You must have *SAVSYS or *ALLOBJ special authority to specify *UDFS as the value for the RBDMFS parameter.			

Interactive data definition commands

This table lists the specific authorities required for the 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
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

This table lists the specific authorities required for the Internetwork Packet Exchange (IPX) commands.

Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the information search index commands.

Command	Referenced object	Authority needed	
		For object	For library
ADDSCHIDX	Search index	*CHANGE	*USE
	Panel group	*USE	*EXECUTE
CHGSCHIDX	Search index	*CHANGE	*USE
CRTSCHIDX	Search Index		*READ, *ADD
DLTSCHIDX	Search index	*OBJEXIST	*EXECUTE
RMVSCHIDX	Search index	*CHANGE	*USE
STRSCHIDX	Search index	*USE	*EXECUTE
WRKSCHIDX ¹	Search index	*ANY	*USE
WRKSCHIDX	Search index	*USE	*USE

IPL attribute commands

This table lists the specific authorities required for the IPL attribute commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the Java commands.

Command	Referenced object	Authority needed	
		For object	For library
ANZJVM	QSYS/STRSRVJOB command	*USE	
	QSYS/STRDBG command	*USE	
DSPJVMJOB ¹	Java Virtual Machine jobs		
GENJVMMDMP ¹			

Command	Referenced object	Authority needed	
		For object	For library
PRTJVMJOB ¹			
WRKJVMJOB ¹			
¹ You must have *JOBCTL special authority to use this command.			

Job commands

This table lists the specific authorities required for the Job commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
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	*READ	*EXECUTE
	Sort sequence table ⁷	*USE	*EXECUTE
CHGPI	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			

Command	Referenced object	Authority needed	
		For object	For library
DSPACTPJ	Auxiliary storage pool (ASP) device description	*USE	
	Program library		*EXECUTE
DSPJOB ¹			
DSPJOBTL			
DSPJOBLOG ^{1,5}	Output file and member exist	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Member does not exist	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Output file does not exist	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB ¹			
ENDJOBABN ¹			
ENDLOGSVR ⁶			
ENDPJ ⁶	Auxiliary storage pool (ASP) device description	*USE	
	Program library		*EXECUTE
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
SBMJOB ^{2, 12, 17, 18}	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
STRLOGSVR ⁶			
STRPJ ⁶	Subsystem description	*USE	
	Program	*USE	*EXECUTE
	Auxiliary storage pool (ASP) device description	*USE	

Command	Referenced object	Authority needed	
		For object	For library
TFRBCHJOB	Job queue	*READ	*EXECUTE
TFRGRPJOB	First group program	*USE	*EXECUTE
TFRJOB ⁸	Job queue	*USE	*EXECUTE
	Subsystem description to which the job queue is allocated	*USE	
TFRSECJOB			
WRKACTJOB			
WRKARMJOB ¹⁶			
WRKASPJOB	Device description	*USE	
WRKJOB ¹			
WRKJOBLOG			
WRKSBJJOB			
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 i5/OS through Application Administration in System i Navigator. 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.		
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: <ul style="list-style-type: none"> • The job queue where the job is placed must be associated with an active subsystem. • The workstation associated with the job must have a corresponding workstation entry in the subsystem description associated with the new subsystem. • The workstation 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.		

Command	Referenced object	Authority needed	
		For object	For library
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.		
16	To work with a specific job or to display details of a specific job, one of the following conditions must apply: <ul style="list-style-type: none"> • The command must be issued from within that job. • The issuer of the command must be running under a user profile that is the same as the job user identity of the job. • The issuer of the command must be running under a user profile that has job control (*JOBCTL) special authority. 		
17	You must have the use (*USE) authority to the Changing Accounting Code (CHGACGCDE) command to specify a character-value accounting code on the Accounting code (ACGCDE) parameter.		
18	You must have the job control (*JOBCTL) special authority to use the Submitted for (SBMFOR) parameter.		

Job description commands

This table lists the specific authorities required for the job description commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
CHGJOB	Job description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	User profile (USER)	*USE	
CPYAUDJRNE ⁸	Output file already exists	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Output file does not exist		*EXECUTE *ADD
CRTJOB (Q)	Job description		*READ, *ADD
	User profile (USER)	*USE	
DLTJOB	Job description	*OBJEXIST	*EXECUTE
DSPJOB	Job description	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT ¹			
WRKJOB	Job description	Any	*USE
¹	You must have *ALLOBJ or *AUDIT special authority to use this command.		

Job queue commands

This table lists the specific authorities required for the job queue commands.

Command	Referenced object	Job queue parameters ⁴		Special authority	Authority needed	
		AUTCHK	OPRCTL		For object	For library
CHGJOBQ	Job queue	*DTAAUT			*READ, *ADD, *DLT, *OBJMGMT	*EXECUTE
		*OWNER			Owner ²	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
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
WRKJOBQD	Job queue				*READ	*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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the journal commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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		*EXEC, *ADD
APYJRNCHG (Q)	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Nonintegrated 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 (Q)	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
CHGJRNA (Q) ¹⁰			
CHGJRNOBJ ⁹	Journal	*OBJOPR, *OBJMGT	
	Nonintegrated file system objects	*READ, *OBJMGT	
	Integrated file system objects	*R, *OBJMGT	*X
	Object path SUBTREE(*ALL)	*RX, *OBJMGT	
	Object path SUBTREE(*NONE)	*R, *OBJMGT	
CHGRMTJRN	Source journal	*CHANGE, *OBJMGT	*EXECUTE
	Source journal	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File	*USE	*EXECUTE
CPYAUDJRNE ⁸	Output file already exists	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Output file does not exist		*EXECUTE, *ADD
CRTJRN	Journal		*READ, *ADD
	Journal receiver	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Journal	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE ⁸			

Command	Referenced object	Authority needed	
		For object	For library or directory
DSPJRN ⁶	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, no object selection is specified, the specified object has been deleted from the system, the specified object has never been journaled, *IGNFILSLT or *IGNOBSLT is specified for any selected journal codes, or when OBJJID is specified, or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Nonintegrated file system object if specified	*USE	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
	Integrated file system object if specified	*R (It can be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
DSPJRNMMNU ¹			
ENDJRN	See "Integrated file system commands" on page 392.		
ENDJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNLIB	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Library	*OBJOPR, *OBJMGT, *READ	
ENDJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP ²			
JRNPF ³			

Command	Referenced object	Authority needed	
		For object	For library or directory
RCVJRNE	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, no object selection is specified, the specified object has been deleted from the system, the specified object has never been journaled, *IGNFILSLT or *IGNOBSLT is specified for any selected journal codes, or when OBJJID is specified, or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Nonintegrated file system object if specified	*USE	*EXECUTE
	Integrated file system object if specified	*R (It can be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
	Exit program	*EXECUTE	*EXECUTE
RMVJRCHG (Q)	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Nonintegrated file system objects whose journaled changes are being removed	*OBJMGT, *CHANGE	*EXECUTE
RTVJRNE	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, no object selection is specified, the specified object has been deleted from the system, the specified object has never been journaled, *IGNFILSLT or *IGNOBSLT is specified for any selected journal codes, or when OBJJID is specified, or the journal is a remote journal.	*OBJEXIST, *USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	Nonintegrated file system object if specified	*USE	*EXECUTE
	Integrated file system object if specified	*R (It can be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
	Source journal	*CHG, *OBJMGT	
SNDJRNE	Journal	*OBJOPR, *ADD	*EXECUTE
	Nonintegrated file system object if specified	*OBJOPR	*EXECUTE
	Integrated file system object if specified	*R	*X
STRJRN	See "Integrated file system commands" on page 392.		
STRJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library or directory
STRJRNLIB	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Library	*OBJOPR, *OBJMGT, *READ	
STRJRNPf	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE
WRKJRN ⁴ (Q)	Journal	*USE	*READ ⁷
	Journal receiver	*USE	*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 STRJRNPf 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 or RST 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.		
¹⁰	You must have *JOBCTL special authority to use this command.		

Journal receiver commands

This table lists the specific authorities required for the journal receiver commands.

Command	Referenced object	Authority needed	
		For object	For library
CRTJRNRVC	Journal receiver		*READ, *ADD
DLTJRNRVC	Journal receiver	*OBJOPR, *OBJEXIST, and a data authority other than *EXECUTE	*EXECUTE
	Journal	*OBJOPR	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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
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.		

Kerberos commands

This table lists the specific authorities required for the Kerberos commands.

Command	Referenced object	Object type	Authority needed for object
ADDKRBKTE	Each directory in the path name preceding the target key table file to be open.	*DIR	*X
	Parent directory of the target keytab file when add is specified, if the file does not already exist.	*DIR	*WX
	Keytab file when list is specified.	*STMF	*R
	Target keytab file when add or delete is specified.	*STMF	*RW
	Each directory in the path to the configuration files.	*DIR	*X
	Configuration files	*STMF	*R
ADDKRBTKT	Each directory in the path name preceding the key table file	*DIR	*X
	Key table file	*STMF	*R
	Each directory in the path name preceding the credentials cache file	*DIR	*X
	Credential cache file	*STMF	*RW
	Parent directory of the cache file to be used, if specified by the KRB5CCNAME environment variable, and the file is being created	*DIR	*WX
	Each directory in the path name to the configuration files	*DIR	*X
	Configuration files	*STMF	*R
CHGKRBPWD			

Command	Referenced object	Object type	Authority needed for object
DLTKRBCCF	Each directory in the path name preceding the credentials cache file, if the credentials cache file does not reside in the default directory.	*DIR	*X
	Parent directory of the credentials cache file, if the credentials cache file does not reside in the default directory.	*DIR	*WX
	Credentials cache file, if the credentials cache file does not reside in the default directory.	*STMF	*RW, *OBJEXIST
	Each directory in the path name to the configuration files, if the credentials cache file does not reside in the default directory.	*DIR	*X
	Configuration files, if the credentials cache file does not reside in the default directory.	*STMF	*R
DLTKRBCCF	All directories in the path name, if the credentials cache file resides in the default directory.	*DIR	*X
	Credentials cache file, if the credentials cache file resides in the default directory.	*STMF	*RW
	Each directory in the path to the configuration files, if the credentials cache file resides in the default directory.	*DIR	*X
	Configuration files, if the credentials cache file resides in the default directory.	*STMF	*R
DSPKRBCCF	Each directory in the path name preceding the key table file	*DIR	*X
	Key table file	*STMF	*R
	Each directory in the path name preceding the credentials cache file	*DIR	*X
	Credential cache file	*STMF	*RW
DSPKRBKTE	Each directory in the path name preceding the target key table file to be open.	*DIR	*X
	Parent directory of the target keytab file when add is specified, if the file does not already exist.	*DIR	*WX
	Keytab file when list is specified.	*STMF	*R
	Target keytab file when add or delete is specified.	*STMF	*RW
	Each directory in the path to the configuration files.	*DIR	*X
	Configuration files	*STMF	*R

Command	Referenced object	Object type	Authority needed for object
RMVCRBKTE	Each directory in the path name preceding the target key table file to be open.	*DIR	*X
	Parent directory of the target keytab file when add is specified, if the file does not already exist.	*DIR	*WX
	Keytab file when list is specified.	*STMF	*R
	Target keytab file when add or delete is specified.	*STMF	*RW
	Each directory in the path to the configuration files.	*DIR	*X
	Configuration files	*STMF	*R

Language commands

This table lists the specific authorities required for the language commands.

Command	Referenced object	Authority needed	
		For object	For library
CLOSE	Close command	*USE	*EXECUTE
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 the general rules.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	Refer to the general rules.	*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 the general rules.	*READ, *ADD
	Binding directory	*USE	*EXECUTE
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTBNDCBL	Source file	*USE	*EXECUTE
	Include 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 the general rules.	Refer to the general rules.
	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 the general rules.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	Refer to the general rules.	*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 the general rules.	*READ, *ADD
	Binding directory	*USE	*EXECUTE
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCLMOD	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 the general rules.	*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 the general rules.	*READ, *ADD
CRTCLMOD	Source file	*USE	*EXECUTE
	Include 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 the general rules.	Refer to the general rules.
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
CRTCLPGM	Source file	*USE	*EXECUTE
	Include 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 the general rules.	Refer to the general rules.
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTCLPGM (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 the general rules.	*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 the general rules.	*READ, *ADD
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF or MAKEDEP parameter	Refer to the general rules.	*READ, *ADD
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 the general rules.	*READ, *ADD
	Directory specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	*USE	*EXECUTE
	File specified in OUTPUT, PPSRCSTMF, TEMPLATE or MAKEDEP parameter	Refer to the general rules.	*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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTRPTPGM (RPG/400 licensed program and S/38 environment)	Source file	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
	Source file for generated RPG program	Refer to the general rules.	Refer to the general rules.
	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 the general rules.	*READ, *ADD
CRTS36RPG	Source file	*USE	*READ, *ADD
	Program: REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTS36RPGR	Source file	*USE	*READ, *ADD
	Display file: REPLACE(*NO)		*READ, *ADD
	Display file: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTS36RPT	Source file	*USE	*EXECUTE
	Source file for generated RPG program	Refer to the general rules.	Refer to the general rules.
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
CRTSQLCI (DB2® Query Manager and SQL Development for i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
CRTSQLCBL (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLCBLI (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLCPPI (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLFTN (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*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 i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLRPG (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
CRTSQLRPGI (DB2 Query Manager and SQL Development for i5/OS 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 the general rules.	*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
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 the general rules.	*READ, *ADD
	Table specified in SRTSEQ parameter	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
DLTCLD	Locale object	*OBJEXIST, *OBJMGT	*EXECUTE
ENDCBLDBG (COBOL/400 licensed program or S/38 environment)	Program	*CHANGE	*EXECUTE
ENTCBLDBG (S/38 environment)	Program	*CHANGE	*EXECUTE
INCLUDE	Source file	*USE	*EXECUTE
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Service program	*OBJMGT, *USE	*EXECUTE
	Module	*OBJMGT, *USE	*EXECUTE
	Database source file	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
RTVCLDSRC	Locale object	*USE	*EXECUTE
	To-file	Refer to the general rules.	Refer to the general rules.
RUNSQLSTM 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 i5/OS 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 for more information about security requirements for structured query language (SQL) statements.			

Library commands

This table lists the specific authorities required for the library commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

Command	Referenced object	Authority needed	
		For object	For library being acted on
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 (Q) ^{7, 17, 19}	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	See General Rules	See General Rules
	QSYS/QASAVOBJ field reference file for output file, if an output file is specified and does not exist	*USE	*EXECUTE
RSTLIB (Q)	Tape (QSYSTAP) or diskette (QSYSDKT) file	*USE ⁶	*EXECUTE
	QSYS/QPSRLDSP printer output, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Save file	*USE	*EXECUTE
	Optical File (OPTFILE) ¹²	*R	Not applicable
	Path prefix of optical file (OPTFILE) ¹²	*X	Not applicable
	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 ¹⁸	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 the general rules.	Refer to the general rules.
	QSYS/QASAVOBJ field reference file, if output file is specified and does not exist	*USE ⁶	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE ⁶	*EXECUTE
	Command user space, if specified	*USE	*EXECUTE
SAVLIB	Optical File ¹²	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) ¹²	*WX	Not applicable
	Path Prefix of optical file (OPTFILE) ¹²	*X	Not applicable
	Root Directory (/) of Optical Volume ^{12, 13}	*RWX	Not applicable
	Optical volume ¹¹	*CHANGE	
	ASP device description ¹⁵	*USE	
SAVRSTLIB	On the source system, same authority as required by SAVLIB command.		
	On the target system, same authority as required by RSTLIB command.		
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, 16}	Library		*USE

Command	Referenced object	Authority needed	
		For object	For library being acted on
1	The authority needed for the library being acted on is indicated in this column. For example, to add the library CUSTLIB to a library list using the ADDLIB 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 a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter.		
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 namespace switch.		
16	This command requires *ALLOBJ special authority.		
17	You must have *ALLOBJ special authority to specify *YES for the PVTAUT parameter.		
18	You must have *ALLOBJ or *SAVSYS special authority to specify *YES for the PVTAUT parameter.		
19	You must have *SAVSYS special authority to specify a name for the DFRID parameter.		

License key commands

This table lists the specific authorities required for the license key commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
ADDLICENSE (Q)	Output file	*USE	*EXECUTE
DSPLICENSE (Q)	Output file	Refer to the general rules.	Refer to the general rules.
RMVLICENSE (Q)	Output file	*CHANGE	*EXECUTE

Licensed program commands

This table lists the specific authorities required for the licensed program commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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)	WRKLCINF command	*USE	*EXECUTE
DLTLICPGM ^{1,2} (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM ^{1,2} (Q)			
SAVLICPGM ^{1,2} (Q)			
WRKLCINF (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 DLTDL0 command also apply to this command.		
³	To use individual operations, you must have the authority required by the individual operation.		

Line description commands

This table lists the specific authorities required for the 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

Command	Referenced object	Authority needed	
		For object	For library
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
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
CRTLINS DLC 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

Command	Referenced object	Authority needed	
		For object	For library
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
DTLIND	Line description	*OBJEXIST	*EXECUTE
DSPLIND	Line description	*USE	*EXECUTE
ENDLINRCY	Line description	*OBJOPR	*EXECUTE
PRTCMNSEC ^{2, 3}			
RSMLINRCY	Line description	*OBJOPR	*EXECUTE
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

This table lists the specific authorities required for the Local Area Network (LAN) commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT

Locale commands

This table lists the specific authorities required for the locale commands.

Command	Referenced object	Authority needed	
		For object	For library
CRTLOCALE	Source file	*USE	*USE, *ADD
DTLOCALE	Locale	*OBJEXIST	*EXECUTE

Mail server framework commands

This table lists the specific authorities required for the mail server framework commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the 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	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA ⁴	Tape Library description	*CHANGE	*EXECUTE
CHGTAPCTG	Tape Library description	*USE	*EXECUTE
CHKTAP	Tape device description	*USE	*EXECUTE
CRTTAPCGY	Tape Library description		
DLTMEDDFN	Media definition	*OBJEXIST	*EXECUTE
DLTTAPCGY	Tape Library description		
DMPTAP (Q) ⁵	Tape 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
DUPTAP	Tape device description	*USE	*EXECUTE
INZTAP	Tape device description	*USE	*EXECUTE
RMVTAPCTG	Tape Library 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

Command	Referenced object	Authority needed	
		For object	For library
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.		
5	To use this command, you must have *ALLOBJ special authority when TYPE(*HEX) is specified or the tape has the secure volume flag or secured file flag set.		

Menu and panel group commands

This table lists the specific authorities required for the 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 the general rules.	*READ, *ADD
CRTPNLGRP	Panel group: Replace(*NO)		*READ, *ADD
	Panel group: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
	Source file	*USE	*EXECUTE
	Include file	*USE	*EXECUTE
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Refer to the general rules.	*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

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the 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
SNDPGMMMSG	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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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
<p>The following commands do not require any object authorities.</p> <p>They are shipped with public authority *EXCLUDE. You must have *ALLOBJ special authority to use these commands.</p>			
ANZS34OCL ANZS36OCL CHGS34LIBM CHKS36SRCA CVTBASSTR CVTBASUNF CVTBGUDTA CVTS36FCT	CVTS36JOB CVTS38JOB GENS36RPT GENS38RPT MGRS36 MGRS36APF ¹ MGRS36CBL MGRS36DFU ¹	MGRS36DSPF MGRS36ITM MGRS36LIB MGRS36MNU MGRS36MSGF MGRS36QRY ¹ MGRS36RPG MGRS36SEC MGRS38OBJ	MIGRATE QMUS36 RESMGRNAM RSTS38AUT STRS36MGR STRS38MGR
<p>¹ You must have *ALLOBJ special authority and have IBM i option 4 installed.</p>			

Mode description commands

This table lists the specific authorities required for the 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
<p>¹ To use individual operations, you must have the authority required by the individual operation.</p> <p>² To use this command, you must have *IOSYSCFG special authority.</p>			

Module commands

This table lists the specific authorities required for the 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
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	<p>You need *USE authority to the:</p> <ul style="list-style-type: none"> • 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	<p>To use individual operations, you must have the authority required by the individual operation.</p>		

NetBIOS description commands

This table lists the specific authorities required for the NetBIOS description commands.

Command	Referenced object	Authority needed	
		For object	For library
CHGNTBD ²	NetBIOS description	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD ²	NetBIOS description		*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the network commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 the general rules.	Refer to the general rules.
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
VFYAPCCNN	Device description	*CHANGE	
WRKNETF ^{2,3}			
WRKNETJOBE ³	QUSRSYS/QANFNJE	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the 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 the general rules.		
DSPMFSINF	some_dirs	*DIR	"root" (/)	*RX
	Path prefix	Refer to the general rules.		
ENDNFSSVR ^{1,4}	none			
EXPORTFS ^{1,2}	Path prefix	Refer to the general rules.		
MOUNT ^{1,3}	dir_to_be_mounted_over	*DIR	"root" (/)	*W
RLSIFSLCK ¹	object	*STMF	"root" (/), QOpenSys, UDFS	*R
	Path prefix	Refer to the general rules.		
RMVMFS ¹				
STATFS	some_dirs	*DIR	"root" (/)	*RX
	Path prefix	Refer to the general rules.		
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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	*STMF	"root" (/)	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG ²	Path (root and /QFPNWSSTG)	*DIR	"root" (/)	*WX
CHGNWSUSRA ⁴	User Profile	*USRPRF		*OBJMGT, *USE
CRTNWSSTG ²	Path (root and /QFPNWSSTG)	*DIR	"root" (/)	*WX
DLTINTSVR ⁵	Network server description	*NWSD	QSYS.LIB	*OBJEXIST
	Line description	*LIND	QSYS.LIB	*OBJEXIST
	Network server storage space - Path (/QFPNWSSTG)	*DIR	"root" (/)	*WX
	Parent directory (name of the storage space)	*DIR	"root" (/)	*RWX, *OBJEXIST
	Files that make up the storage space	*STMF	"root" (/)	*OBJEXIST
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	*STMF	"root" (/)	*OBJEXIST

Command	Referenced object	Object type	File system	Authority needed for object
DLTWNTSVR ⁵	Network server description	*NWSD	QSYS.LIB	*OBJEXIST
	Line description	*LIND	QSYS.LIB	*OBJEXIST
	Network server storage space - Path (/QFPNWSSTG)	*DIR	"root" (/)	*WX
	Parent directory (name of the storage space)	*DIR	"root" (/)	*RWX, *OBJEXIST
	Files that make up the storage space	*STMF	"root" (/)	*OBJEXIST
DSPNWSSTG	Path prefix	Refer to the general rules		
	Files that make up the storage space	*STMF	"root" (/)	*R
INSINTSVR ⁶	Network server description	*NWSD	Not applicable	*USE
	Line description	*LIND	Not applicable	*USE
	Network server storage space - Path (/QFPNWSSTG)	*DIR	"root" (/)	*WX
INSWNTSVR ^{6,7}	Network server description	*NWSD	Not applicable	*USE
	Line description	*LIND	Not applicable	*USE
	Network server configuration	*NWSCFG	Not applicable	*USE
	Network server storage space - Path (/QFPNWSSTG)	*DIR	"root" (/)	*WX
RMVNWSSTGL ²	Path (/QFPNWSSTG)	*DIR	"root" (/)	*X
	Parent directory (name of the storage space)	*DIR	"root" (/)	*WX
	Files that make up the storage space	*STMF	"root" (/)	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Path prefix	Refer to the general rules		
	Files that make up the storage space	*STMF	"root" (/)	*R
These commands do not require any object authorities:				
ADDRMTSVR CHGNWSA ^{4(Q)} CHGNWSALS CRTNWSALS DLTNWSALS DSPNWSA	DSPNWSALS DSPNWSASN DSPNWSSTC DSPNWSUSRA SBMNWSCMD (Q) ³		SNDNWSMSG WRKNWSALS WRKNWSEN WRKNWSSN WRKNWSSTS	
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.			

Command	Referenced object	Object type	File system	Authority needed for object
⁵	To use this command, you must have *IOSYSCFG and *ALLOBJ special authorities.			
⁶	To use this command, you must have *IOSYSCFG, *ALLOBJ, and *JOBCTL special authorities.			
⁷	You must have *SECADM special authority to specify a nondefault value for the IPSECRULE, CHAPAUT, or SPCERTID parameter.			

Network server configuration commands

This table lists the specific authorities required for the network server configuration commands.

Command	Referenced object	Authority needed	
		For object	For QUSRSYS library
CHGNWSCFG ^{1,3}	Network server configuration	*CHANGE	*EXECUTE
CRTNWSCFG ^{1,3}	Network server configuration	*USE	*READ, *ADD
DLTNWSCFG ^{1,3}	Network server configuration	*OBJEXIST	*EXECUTE
DSPNWSCFG ^{1,3}	Network server configuration	*USE	*EXECUTE
INZNWSCFG ^{1,2}	Network server configuration	*CHANGE	*EXECUTE
WRKNWSCFG ¹	Network server configuration	*USE	*EXECUTE
¹	To use this command, you must have *IOSYSCFG special authority.		
²	To use this command, you must have *SECADM special authority.		
³	To specify or view a nondefault value for the IPSECRULE, CHAPAUT, or SPCERTID parameter, you must have security administrator (*SECADM) special authority.		

Network server description commands

This table lists the specific authorities required for the 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

Command	Referenced object	Authority needed	
		For object	For QSYS library
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the office services commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT ^{2,3,6} (Q) GRTUSRPMN ^{1,2} RMVACC ¹ (Q) RVKACCAUT ¹	RVKUSRPMN ^{1,2} WRKDOCLIB ⁴ WRKDOCPTQ ⁵	
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 mails 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

This table lists the specific authorities required for the online education commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the operational assistant commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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			
CHGPWRSCDE ³			
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	
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

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the optical commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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		
		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	Not applicable	Not applicable
	Optical Device	*USE	*EXECUTE	*CHANGE ³
	Server CSI	*USE	*EXECUTE	Not applicable
CHKOPTVOL	Optical device	*USE	*EXECUTE	*USE
	Root directory (/) of volume	*RWX	Not applicable	Not applicable
CPYOPT	Optical Device	*USE	*EXECUTE	*USE - Source Volume
				*ALL - Target Volume
	Each preceding dir in path of source file	*X	Not applicable	Not applicable
	Each preceding dir in path of destination file	*X	Not applicable	Not applicable
	Source file (*DSTMF) ⁵	*R	Not applicable	Not applicable
	Parent dir of destination file	*WX	Not applicable	Not applicable
	Parent of parent dir if creating dir	*WX	Not applicable	Not applicable

Command	Referenced object	Authority needed		
		Object	Library	Optical volume ¹
CPYOPT	Destination file if replaced due to SLTFILE(*ALL)	*W	Not applicable	Not applicable
	Destination file if replaced due to SLTFILE(*CHANGED)	*RW	Not applicable	Not applicable
	Each dir in path that precedes source dir	*X	Not applicable	Not applicable
	Each dir in path that precedes target dir	*X	Not applicable	Not applicable
CPYOPT	Dir being copied ⁵	*R	Not applicable	Not applicable
	Dir being copied if it contains entries	*RX	Not applicable	Not applicable
	Parent of target dir	*WX	Not applicable	Not applicable
	Target dir if replaced due to SLTFILE(*ALL)	*W	Not applicable	Not applicable
	Target dir if replaced due to SLTFILE(*CHANGED)	*RW	Not applicable	Not applicable
	Target dir if entries are to be created	*WX	Not applicable	Not applicable
CPYOPT	Source files	*R	Not applicable	Not applicable
	Destination file if replaced due to SLTFILE(*ALL)	*W	Not applicable	Not applicable
	Destination file if replaced due to SLTFILE(*CHANGED)	*RW	Not applicable	Not applicable
CRTDEVOPT ⁴	Optical Device		*EXECUTE	
CVTOPTBKU	Optical Device	*USE	*EXECUTE	*ALL
DSPOPT	Path Prefix when DATA (*SAVRST) ⁵	*X	Not applicable	Not applicable
	File Prefix when (*SAVRST) ²	*R	Not applicable	Not applicable
	Optical Device	*EXECUTE	*USE	
	Server CSI	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	Server CSI	*USE	*EXECUTE	
DUPOPT	Optical Device	*USE	*EXECUTE	*USE - Source Volume
				*ALL - Target Volume
INZOPT	Root directory (/) of volume	*RWX	Not applicable	Not applicable
	Optical Device	*USE	*EXECUTE	*ALL
LODOPTFMW	Stream file	*R	Not applicable	Not applicable
	Path prefix	Refer to the general rules.		

Command	Referenced object	Authority needed		
		Object	Library	Optical volume ¹
RCLOPT (Q)	Optical Device	*USE	*EXECUTE	
RMVOPTCTG (Q)	Optical Device	*USE	*EXECUTE	
RMVOPTSVR (Q)	Server CSI	*USE	*EXECUTE	
STRNETINS (Q) ⁶	Network optical device	*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	<p>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.</p> <ul style="list-style-type: none"> • 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).			
⁶	You must have *JOBCTL special authority to use this command.			

Output queue commands

This table lists the specific authorities required for the 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
	Message queue				*OBJOPR *ADD	*EXECUTE
	Workstation customization object				*USE	*EXECUTE
	User-data transform program				*OBJOPR *EXECUTE	*EXECUTE
User-driver program				*OBJOPR *EXECUTE	*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
	Message queue				*OBJOPR *ADD	*EXECUTE
	Workstation customization object				*USE	*EXECUTE
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

Command	Referenced object	Output queue parameters		Special authority	Authority needed	
		AUTCHK	OPRCTL		For object	For library
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 outqueue.					
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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the performance commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
ADDDWDFN (Q) ⁷			
ADDJWDFN (Q) ⁷			
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	

Command	Referenced object	Authority needed	
		For object	For library
ANZBESTMDL (Q) ⁴	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Application libraries that contain the database files to be analyzed		*EXECUTE
	Job description	*USE	*EXECUTE
ANZCMDPFR (Q)	Command file	*USE	*EXECUTE
	Output file	*USE	*EXECUTE, *ADD
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
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
CHGJOBTP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGMGTCOL	MGTCOL	*OBJMGT	
	User library		*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

Command	Referenced object	Authority needed	
		For object	For library
CPYGPHEMT (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
CPYPFCOL (Q)	From library		*EXECUTE
	To library		*EXECUTE, *ADD
CPYPRDTA (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

Command	Referenced object	Authority needed	
		For object	For library
CRTPEXDTA (Q) ⁵	*MGTCOL Library		*EXECUTE
	Data library ¹		*READ, *ADD ²
CRTPFRDTA (Q)	From Library		*EXECUTE
	To Library		*ADD, *READ
	From Library		*USE
CRTPFRSUM (Q)	User library		*ADD, *READ
CVTPFRCOL (Q)	From library		*USE
	To library		*USE, *ADD
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
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
DLTPFRCOL (Q)	Library		*EXECUTE
DLTPFRDTA (Q) ⁴	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	Output file	Refer to the general rules	Refer to the general rules
DMPTRC (Q) ⁵	Library where the trace data will be stored		*EXECUTE, *ADD
	Output file (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q) ⁴	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Historical data library		*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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
ENDDW (Q) ⁷			
ENDJOBTRC (Q) ⁴	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDJW (Q) ⁷			
ENDPEX (Q) ⁵	Data Library ¹		*READ, *ADD ²
ENDPFCOL (Q)			
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
PRTJOBTRPT (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
	Output file	*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

Command	Referenced object	Authority needed	
		For object	For library
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 (QTRJOB) library		*EXECUTE
	Job description	*USE	*EXECUTE
PRTRCRPT (Q) ⁴	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVDWDFN (Q) ⁷			
RMVJWDFN (Q) ⁷			
RMVPEXDFN (Q) ⁵			
RMVPEXFTR (Q) ⁵			
RSTPFCOL (Q)	Library associated with the restore collection	*EXECUTE,, *ADD ⁶	
	Save file	*USE	*EXECUTE
SAVPFCOL (Q)	Library containing collection to be saved	*EXECUTE ⁶	
	Save file, if empty	*USE, *ADD	*EXECUTE, *ADD
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
STRBEST (Q) ⁴	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON ³	Output file	*OBJOPR, *ADD	*EXECUTE
STRDW (Q) ⁷	User library		*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRJW (Q) ⁷	User library		*EXECUTE
STRPEX (Q) ⁵			
STRPFCOL (Q)			
STRPFRG (Q) ⁴	QPFR/QPGSTART *PGM	*USE	*EXECUTE
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

Command	Referenced object	Authority needed	
		For object	For library
These commands do not require any object authorities:			
<ul style="list-style-type: none"> • ENDDBMON³ • 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 the STRDBMON or ENDDBMON commands, where the JOB command parameter uses a generic name or a specific name which belongs to a user which is different from the current user, requires that you have *JOBCTL special authority or be authorized to the SQL Administrator function of IBM i through Application Administration in System i Navigator. The Change Function Usage Information (CHGFCNUSG) command, with a function ID of QIBM_DB_SQLADM, can also be used to change the list of authorized users.		
⁵	To use this command, you must have *SERVICE special authority or you must be authorized to the Service Trace function of IBM i through Application Administration in System i Navigator. 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.		
⁶	If you have *SAVSYS special authority, you do not need the authority specified.		
⁷	To use this command, you must have service (*SERVICE) special authority, or be authorized to the Disk Watcher function of the operating system through System i Navigator Application Administration support. The Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_DISK_WATCHER, can also be used to change the list of users that are allowed to use the disk watcher tool.		

Print descriptor group commands

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

Command	Referenced object	Authority needed	
		For object	For library
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

This table lists the specific authorities required for the problem commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
ADDPBACNE (Q)	Filter	*USE, *ADD	*EXECUTE
ADDPBLSL (Q)	Filter	*USE, *ADD	*EXECUTE
ANZPRB (Q)	SNDSRVRQS command	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPBACNE (Q)	Filter	*USE, *UPD	*EXECUTE
CHGPBLSL (Q)	Filter	*USE, *UPD	*EXECUTE
DLTPRB (Q) ³	Command: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	Output file	Refer to the general rules.	Refer to the general rules.
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
VFYPRB (Q)	Device description	*USE	*EXECUTE
WRKPRB (Q) ²	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE	*EXECUTE
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

This table lists the specific authorities required for the program commands.

Command	Referenced object	Authority needed	
		For object	For library
The object authorities required for the CRTxxx PGM commands are listed in the Languages table in "Language commands" on page 424.			
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 re-create 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 re-create 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			
CRTPGM	Program, Replace(*NO)	Refer to the general rules.	*READ, *ADD
	Program, Replace(*YES)	Refer to the general rules.	*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 the general rules.	*READ, *ADD
	Service program, Replace(*YES)	Refer to the general rules.	*READ, *ADD
	Module	*USE	*EXECUTE
	Service program specified in BNDSRVPGM parameter	*USE	*EXECUTE
	Export source file	*OBJOPR *READ	*EXECUTE
	Binding directory	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
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
DSPPGMREF	Program	*OBJOPR	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
DSPPGMVAR ¹			
DPSRVPGM	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			

Command	Referenced object	Authority needed	
		For object	For library
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Service program	*OBJMGT, *USE	*EXECUTE
	Module	*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
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

Command	Referenced object	Authority needed	
		For object	For library
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 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.		

QSH shell interpreter commands

This table lists the specific authorities required for the QSH shell interpreter commands.

The commands listed in this table do not require any authorities to objects.

Command	Referenced object	Authority needed	
		For object	For library
STRQSH ^{1, 2}			
QSH ^{1, 2}			
¹	QSH is an alias for the STRQSH CL command.		
²	You need *RX authority to all scripts and *X authority to all directories in the path to the script.		

Query commands

This table lists the specific authorities required for the 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
CRTQMORY	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

Command	Referenced object	Authority needed	
		For object	For library
DLTQMFORM	Query management form	OBJEXIST	*EXECUTE
DLTQMQR	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, CPYSRCE, CRTPRTE, CRTSRCPF, DLTE, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RTVQMQR	Query manager query	*USE	*EXECUTE
	Target source file	*ALL	*READ, *ADD
	ADDPFM, CHGPFM, CLRPFM, CPYSRCE, CRTPRTE, CRTSRCPF, DLTE, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RUNQR	Query definition	*USE	*USE
	Input files	*USE	*EXECUTE
	Output files	Refer to the general rules.	Refer to the general rules.
STRQMQR ¹	Query management query	*USE	*EXECUTE
	Query management form, if specified	*USE	*EXECUTE
	Query definition, if specified	*USE	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
	ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCE, CRTPRTE, CRTSRCPF, DLTE, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTE RMVM commands (if OUTPUT(*OUTFILE) is specified)	*USE	*EXECUTE
STRQMPC ¹	Source file containing query manager procedure	*USE	*EXECUTE
	Source file containing command source file, if specified	*USE	*EXECUTE
	OVRPRTE command, if statements result in printed report or query object.	*USE	*EXECUTE
STRQR			*EXECUTE
WRQMFORM ³	Query management form	Any authority	*USE
WRQMQR ³	Query management query	Any authority	*USE
WRQR 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 the CHGQRYA command, you must have *JOBCTL special authority or be authorized to the SQL Administrator function of IBM i through Application Administration in System i Navigator. The Change Function Usage Information (CHGFCNUSG) command, with a function ID of QIBM_DB_SQLADM, can also be used to change the list of authorized users.		

Question and answer commands

This table lists the specific authorities required for the question and answer commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 or QAQAxxBQPY ¹	*READ	*USE
WRKCNTINF			*EXECUTE
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

This table lists the specific authorities required for the 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 do 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

This table lists the specific authorities required for the registration facility commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the relational database commands.

Command	Referenced object	Authority needed	
		For object	For library
ADDRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE
CHGRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE
	Remote location device description ⁷	*CHANGE	
DSPRDBDIRE	Output file, if specified	Refer to the general rules.	Refer to the general rules.
These commands do not require any authority to objects:			

Command	Referenced object	Authority needed	
		For object	For library
RMVRDBDIRE WRKRDBDIRE			
¹ Authority verified when the RDB directory entry is used.			

Resource commands

This table lists the specific authorities required for the resource commands.

Command	Referenced object	Authority needed	
		For object	For library
DSPHDWRSC			
DSPSFWRSC	Output file, if specified	Refer to the general rules.	Refer to the general rules.
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

This table lists the specific authorities required for the 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
ADDRJEWTR	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
CHGRJEWTR	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
RMVRJEWTR	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
STRRJESL	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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the service commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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, CRTTAPE, 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

Command	Referenced object	Authority needed	
		For object	For library
DLTPTF (Q)	Cover letter file ⁴		*EXECUTE
	PTF save file ⁴		*EXECUTE
DLTRC (Q)	RMVM command	*USE	
	QSYS Library	*EXECUTE	
	Database Files	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Output file	Refer to the general rules.	Refer to the general rules.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
DSPSSTUSR ¹⁹			
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, DLTRC	*USE	
ENDWCH ¹⁶ (Q)	Watch sessions watching for a message within a job log ¹⁷		
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 the general rules.	Refer to the general rules.
PRTERLOG (Q)	Output file	Refer to the general rules.	Refer to the general rules.
PRTINTDTA ^{12,13} (Q)			
PRTRC ¹¹ (Q)	QSYS Library	*EXECUTE	
	Database Files	*USE	
	DLTRC command	*USE	
RMVPTF (Q)	Product library	*OBJMGT	
RMVTRCFTR ¹¹			
RUNLPDA (Q)	Line description	*READ	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
SAVAPARDTA ⁶ (Q)	Commands: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVE, DLTF, DMPOBJ, DMPYSOBY, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB, and WRKSYSVAL	*USE	*EXECUTE
	Existing problem ⁷	*CHANGE	*EXECUTE
SNDPTFORD ¹⁰ (Q)	CRTIMGCLG	*USE	
	QUSRSYS		*ADD, *READ
SNDSRVRQS (Q)			
STRCMNTRC ¹¹ (Q)	NWID (network ID) or line description	*USE	*EXECUTE
	Watched job ¹⁷		
	Trace exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
STRCPYSCN	Job queue	*USE	*EXECUTE
	Device description	*USE	*EXECUTE
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
STRSRVJOB (Q)	User profile of job	*USE	*EXECUTE
STRSST ³ (Q)			
STRTRC (Q) ^{11, 15}	Watched job ¹⁷		
	Trace exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
STRWCH ¹⁶ (Q)	Watched job ¹⁷		
	Watch exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
TRCCNN ¹¹ (Q)	Watched job ¹⁷		
	Trace exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT ¹¹ (Q)	Watched job ¹⁷		
	Trace exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
TRCJOB (Q)	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	Exit program, if specified	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
TRCTCPAPP ¹¹ (Q)	Line description	*USE	
	Network interface	*USE	
	Network interface	*USE	
	Watched job ¹⁷		
	Trace exit program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*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/QVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB ^{1, 10} (Q)	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKPTFORD (Q)	QESCPTFO and SNDPTFORD	*USE	
WRKSRVPVD (Q)			
WRKTRC ¹¹ (Q)			
WRKWCH ¹⁸ (Q)			

¹ You need authority to the PRERRLOG command for some analysis procedures or if the error log records are being saved.

² All restrictions for the RSTOBJ command also apply.

³ You must have Service (*SERVICE) special authority to use 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. The following restrictions apply for the IMGDIR parameter: <ul style="list-style-type: none"> • You must have *X authority to each directory in the path. • You must have *WX authority to the directory that contains optical image. 		
11	To use this command, you must have *SERVICE special authority, or be authorized to the Service Trace function of IBM i through Application Administration in System i Navigator. 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 IBM i through Application Administration in System i Navigator. 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 IBM i through Application Administration in System i Navigator. You can also use the Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_ALLOBJ_TRACE_ANY_USER, to change the list of users that are allowed to perform trace operations.		

Command	Referenced object	Authority needed	
		For object	For library
16	To use this command, you must have service (*SERVICE) special authority, or be authorized to the service watch function of i5/OS through Application Administration in System i Navigator. You can also use the Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_WATCH, to change the list of users that are allowed to start and end watch operations.		
17	Job control (*JOBCTL) special authority is needed if the job is running under a different user from the job user identity of the job being watched. All object (*ALLOBJ) special authority is needed if *ALL is specified for the watched job name, or if a generic user name is specified. A user that does not have *ALLOBJ special authority can perform the function if they are authorized to the Watch Any Job function of i5/OS through Application Administration in System i Navigator. You can also use the Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_WATCH_ANY_JOB, to change the list of users that are allowed to start and end watch operations.		
18	To use this command, you must have service (*SERVICE) special authority, or be authorized to the service trace function and service watch function of i5/OS through Application Administration in System i Navigator. You can also use the Change Function Usage (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_TRACE and QIBM_SERVICE_WATCH, to change the list of users that are allowed to perform trace operations.		
19	You must have Audit (*AUDIT) and Security Administrator (*SECADM) special authorities to use this command.		

Spelling aid dictionary commands

This table lists the specific authorities required for the 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 the general rules.	*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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the spooled file commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 the general rules for Display (DSP) or other operation using output file (OUTPUT (*OUTFILE))	Refer to the general rules for Display (DSP) or other operation using output file (OUTPUT (*OUTFILE))	
	Spooled file	*OWNER				Owner ⁶		
	Output queue ³	*YES					*READ	
		*NO	*DTAAUT				*READ, *ADD, *DLT	
		*NO	*OWNER				Owner ⁴	
	*YES or *NO		*YES	*JOBCTL				
DLTEXPSPLF (Q) ¹⁰	Independent disk pool ⁹					*USE		
DLTSPLF ¹	Output queue ³		*DTAAUT			*READ, *ADD, *DLT		
			*OWNER			Owner ⁴		
				*YES	*JOBCTL			

Command	Referenced object	Output queue parameters			Special authority	Authority needed	
		DSPDTA	AUTCHK	OPRCTL		For object	For library
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) ¹⁰	Independent disk pool ⁹					*USE	
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	
SNDTCPSPLF _{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	
STRSPLRCL (Q) ^{9, 10}	Independent disk pool ⁹					*USE	
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.						
9	You must have *USE authority to all independent disk pools in an independent disk pool group.						
10	You must have *SPLCTL special authority to run this command.						

Subsystem description commands

This table lists the specific authorities required for the subsystem description commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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 ⁹	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description ⁹	*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 ⁹	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description ⁹	*OBJOPR, *READ	*EXECUTE
CHGAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description ⁹	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description ⁹	*OBJOPR, *READ	*EXECUTE
	User profile	*USE	

Command	Referenced object	Authority needed	
		For object	For library
CHGJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	User profile	*USE	
	Job description ⁹	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD ^{5,7}	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	signon display file ⁴	*USE	*EXECUTE
CHGWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description ⁹	*OBJOPR, *READ	*EXECUTE
CRTSBSD ⁵ (Q)	Subsystem description		*READ, *ADD
	signon display file ⁴	*USE	*EXECUTE
	Auxiliary storage pool (ASP) device description ⁸	*USE	
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
	Auxiliary storage pool (ASP) device description	*USE	
WRKSBS ^{2,3}	Subsystem description	Any authority	*USE
WRKSBSD ³	Subsystem description	Any authority	*USE

Command	Referenced object	Authority needed	
		For object	For library
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.		
7	You must have *ALLOBJ and *SECADM special authorities to change the auxiliary storage pool (ASP) group name.		
8	To specify an ASP device description that does not exist, you must have all object (*ALLOBJ) special authority.		
9	To specify a job description that does not exist, you must have all object (*ALLOBJ) special authority.		

System commands

This table lists the specific authorities required for the system commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. The Commands shipped with public authority *EXCLUDE topic 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
PWRDWN SYS ¹	Image catalog (if specified)	*USE	
RTV SYSINF (Q) ²	Library	*READ, *ADD, *EXECUTE	
These commands do not require any object authorities:			
CHGSHRPOOL DPSYSSTS ENDSYS ¹ PRTSYSINF (Q)	RCLACTGRP ¹ RCLRSC RETURN RTVGRPA	SIGNOFF UPDSYSINF (Q) ³ WRKSHRPOOL	WRKSYSSTS
1	You must have job control (*JOBCTL) special authority to use this command.		
2	You must have *SAVSYS special authority to use this command.		
3	You must have *SECADM, *ALLOBJ, *AUDIT, *JOBCTL, and *SAVSYS special authorities to use this command.		

System reply list commands

This table lists the specific authorities required for the system reply list commands.

These commands do not require object authorities:

ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE
--------------	--------------	--------------	----------

System value commands

This table lists the specific authorities required for the system value commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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

This table lists the specific authorities required for the System/36 environment commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
CRTMSGFMNU	Menu: REPLACE(*NO)		*READ, *ADD
	Menu: REPLACE(*YES)	Refer to the general rules.	*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 the general rules.	*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

Command	Referenced object	Authority needed	
		For object	For library
CRTS36MNU	Menu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Menu: REPLACE(*YES)	Refer to the general rules.	*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	
CRTS36MSGF	Message file: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Message file: REPLACE(*YES)	Refer to the general rules.	*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	
DS36	S/36 configuration object QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Program, to change attributes	*OBJMGT, *USE	*EXECUTE
	Program, to view attributes	*USE	*EXECUTE
EDTS36PRCA	File QS36PRC, to change attributes	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, to view attributes	*USE	*EXECUTE
EDTS36SRCA	Source file QS36SRC, to change attributes	*OBJMGT, *USE	*EXECUTE
	Source file QS36SRC, to view attributes	*USE	*EXECUTE

Command	Referenced object	Authority needed	
		For object	For library
RSTS36F (Q)	From-file	*USE	*EXECUTE
	To-file	*ALL	Refer to the general rules.
	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
RSTS36LIBM (Q)	From-file	*USE	*EXECUTE
	To-file	*ALL	Refer to the general rules.
	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 the general rules.
	Device file or device description	*USE	*EXECUTE
SAVS36LIBM	From-file	*USE	*EXECUTE
	To-file, when it is a physical file	*ALL	Refer to the general rules.
	Device file or device description	*USE	*EXECUTE
WRKS36	S/36 configuration object QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Program, to change attributes	*OBJMGT, *USE	*EXECUTE
	Program, to view attributes	*USE	*EXECUTE
WRKS36PRCA	File QS36PRC, to change attributes	*OBJMGT, *USE	*EXECUTE
	File QS36PRC, to view attributes	*USE	*EXECUTE
WRKS36SRCA	Source file QS36SRC, to change 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

This table lists the specific authorities required for the table commands.

Command	Referenced object	Authority needed	
		For object	For library
CRITBL	Table		*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE
DLTTBL	Table	*OBJEXIST	*EXECUTE
WRKTBL ¹	Table	Any authority	*USE

¹ To use an individual operation, you must have the authority required by the operation.

TCP/IP commands

This table lists the specific authorities required for the TCP/IP commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
CPYTCPHT ⁶	File objects		
CVTTCPCL (Q)	File objects	*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
SETVTBL	Table objects	*USE	*EXECUTE
SNDTCPSPLF ²	Workstation customizing object	*USE	*EXECUTE
STRTCPFTP	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE
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

Command	Referenced object	Authority needed	
		For object	For library
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:

ADDCOMSMP ¹	CFGRTG	CHGVTMAP	RMVTCPRSI ¹
ADDNETTBLE ¹	CFGTCPSMTP	DSPVTMAP	RMVTCPRTE ¹
ADDOSPFARA ¹	CFGTCPSNMP	ENDTCP (Q)	RMVTCPSVR ¹
ADDOSPFLNK ¹	CFGTCPTELN	ENDTCPENN	RMVUSRSNMP ¹
ADDOSPFIFC ¹	CHGCOMSNMP ¹	ENDTCPIFC (Q)	RNMTCPHTE ¹
ADDOSPFRRNG ¹	CHGDHCPSVR ¹	MGRTCPHT ¹	SETVTMAP
ADDPCLTBLE ¹	CHGFTPA ¹	NETSTAT	STRTCP (Q)
ADDRIPACP ¹	CHGLPDA ¹	PING	STRTCPIFC (Q)
ADDRIPFLT ¹	CHGOSPFA ¹	RMVCOMSNMP ¹	VFYTCPCNN
ADDRIPIFC ¹	CHGOSPFARA ¹	RMVNETTBLE ¹	WRKNAMSMTP ³
ADDRIPIGN ¹	CHGOSPFIFC ¹	RMVOSPFARA ¹	WRKNETTBLE ¹
ADDSRVTBLE ¹	CHGOSPFLNK ¹	RMVOSPFIFC ¹	WRKPCLTBLE ¹
ADDTCPHTE ¹	CHGOSPFRRNG ¹	RMVOSPFLNK ¹	WRKSRVTBLE ¹
ADDTCPIFC ¹	CHGRIPA ¹	RMVOSPFRRNG ¹	WRKTCPSTS
ADDTCPPORT ¹	CHGRIPFLT ¹	RMVPCLTBLE ¹	
ADDTCPRSI ¹	CHGRIPIFC ¹	RMVRIPACP ¹	
ADDTCPRTE ¹	CHGSMTPA ¹	RMVRIPFLT ¹	
	CHGSNMPA ¹	RMVRIPIFC ¹	
ADDUSRSNMP ¹	CHGTCPA ¹	RMVRIPIGN ¹	
CFGTCP	CHGTCPHTE ¹	RMVSRVTBLE ¹	
CFGTCPAPP	CHGTCPIFC ¹	RMVTCPHTE ¹	
CFGTCPFTP ¹	CHGTCPRTE ¹	RMVTCPIFC ¹	
CFGTCPLPD ¹	CHGTELNA ¹	RMVTCPPORT ¹	
	CHGUSRSNMP ¹		

- ¹ You must have *IOSYSCFG special authority to use this command.
- ² The **SNDCPSPLF** command and the LPR command use the same combinations of referenced object authorities as the **SDNETSPLF** 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.
- ⁶ For the required authorities, refer to the description of the Display (DSP) or other operation using output file (OUTPUT(*OUTFILE)) section in the General rules for object authorities on commands topic.

Time zone description commands

This table lists the specific authorities required for the time zone description commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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
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.			

User index, user queue, and user space commands

This table lists the specific authorities required for the user index, user queue, and user space commands.

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-defined file system commands

This table lists the specific authorities required for the 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 the general rules.		
CRTUDFS ^{1,2,6,7} (Q)	/dev/QASPxx or /dev/IASPname	*DIR	"root" (/)	*RWX
DLTUDFS ^{1,2,4,5,8,9,10} (Q)	/dev/QASPxx or /dev/IASPname	*DIR	"root" (/)	*RWX
	any integrated file system object in the UDFS		"root" (/)	*OBJEXIST
	Any non-empty directory object	*DIR	"root" (/)	*WX
DSPUDFS	some_dirsxx	*DIR	"root" (/)	*RX
MOUNT ^{1,2,3}	dir_to_be_ mounted_over	*DIR	"root" (/)	*W
	Path Prefix	Refer to the general rules.		
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	There are two directory naming conventions depending on the location of the user-defined file system (UDFS). Use one of the following conventions: <ul style="list-style-type: none"> • - /dev/QASPxx where xx is 01 for the system asp or 02-32 for the basic user asps. • - /dev/IASPname where IASPname is the name of the independent ASP. 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	You 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.			
8	You must have write (*W) and execute (*X) authority to all of the non-empty directory objects in the UDFS.			
9	If any non-empty directory object in the UDFS has the "restricted rename and unlink" attribute set to Yes (this attribute is equivalent to the S_ISVTX mode bit), then one or more of the following conditions must be true: <ul style="list-style-type: none"> • You must be the owner of all the objects contained in the directory. • You must be the owner of the directory. • You must have all object (*ALLOBJ) special authority. 			
10	The UDFS cannot be deleted if it contains an object with the <i>read only</i> attribute set to <i>yes</i> or if it contains an object that is checked out.			

User profile commands

This table lists the specific authorities required for the user profile commands.

Commands identified by (Q) are shipped with public authority *EXCLUDE. Appendix C, "Commands shipped with public authority *EXCLUDE," on page 327 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)			
ANZPFACT ^{3, 14, 15(Q)}			
CHGACTPRFL ^{14(Q)}			
CHGACTSCDE ^{3, 14,} 15(Q)			
CHGDSTPWD ¹			

Command	Referenced object	Authority needed	
		For object	For library
CHGEXPCDE ^{3, 14, 15(Q)}			
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
CHGUSRPTI	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
DMPUSRPRF ^{22(Q)}	User profile		
DSPACTPRFL ^{14(Q)}			

Command	Referenced object	Authority needed	
		For object	For library
DSPACTSCD ¹⁴ (Q)			
DSPAUTUSR ⁶	User profile	*READ	
DSPEXPSCD ¹⁴ (Q)			
DSPPGMADP	User profile	*OBJMGT	
	Output file	Refer to the general rules.	Refer to the general rules.
DSPSSTUSR ²³			
DSPUSRPRF ¹⁹	User profile	*READ	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
DSPUSRPTI	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	
RTVUSRPTI	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 a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter.		

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 cannot 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 display the current object auditing value and action auditing value displayed. Otherwise, the value *NOTAVL is displayed to indicate that the values are unavailable for display.		
20	You must have either *ALLOBJ or *AUDIT special authority to retrieve the current OBJAUD and AUDLVL values. Otherwise, the value *NOTAVL is returned to indicate that the values are unavailable for retrieval.		
21	To use this command, you must have service (*SERVICE) special authority, or be authorized to the Service Dump function of i5/OS through the support of the System i Navigator Application Administration. The Change Function Usage (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.		
22	To use this command, you must have *SERVICE special authority or have the authorization to the QIBM_SERVICE_DUMP function usage list.		
23	You must have either security administrator (*SECADM) or audit (*AUDIT) special authority to use this command.		

Validation list commands

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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

This table lists the specific authorities required for the 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	
		*OWNER			Owner ³	
			*YES	*JOBCTL		
	New output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR ¹	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner ³	
			*YES	*JOBCTL		
HLDWTR ¹	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner ³	
			*YES	*JOBCTL		
RLSWTR ¹	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner ³	
			*YES	*JOBCTL		

Command	Referenced object	Output queue parameters		Special authority	Authority needed	
		AUTCHK	OPRCTL		For object	For library
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
	Workstation customization object				*USE	*EXECUTE
	User-driver program				*OBJOPR *EXECUTE	*EXECUTE
	User-data transform program				*OBJOPR *EXECUTE	*EXECUTE
	User separator program				*OBJOPR *EXECUTE	*EXECUTE
Device Description				*OBJOPR, *READ		
STRRMTWTR ¹	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner ³	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Message queue				*OBJOPR, *ADD	*EXECUTE
	Workstation customization object				*USE	*EXECUTE
	User-driver program				*OBJOPR *EXECUTE	*EXECUTE
	User-data transform program				*OBJOPR *EXECUTE	*EXECUTE
WRKWTR						

Appendix E. Object operations and auditing

This topic collection lists operations that can be performed against objects on the system, and whether those operations are audited.

The lists are organized by object type. The operations are grouped by whether they are audited when *ALL or *CHANGE is specified for the OBJAUD value of the CHGOBJAUD or CHGDLOAUD command.

Whether an audit record is written for an action depends on a combination of system values, including a value in the user profile of the user performing the action, and a value defined for the object. "Planning the auditing of object access" on page 286 describes how to set up auditing for objects.

- | Please also refer to section "Relationship of object Change Date/Time to audit records" on page 298.

Operations shown in the tables in uppercase, such as CPYF, refer to CL commands, unless they are labeled as an application programming interface (API).

Operations common to all object types

This list describes the operations that you can perform against all object types, and whether those operations are audited.

- Read operation

CRTDUPOBJ

Create Duplicate Object (if *ALL is specified for *"from-object"*).

DMPOBJ

Dump Object

DMPSYSOBJ

Dump System Object

QSRSAVO

Save Object API

QsrSave

Save Object in Directory API

SAV Save Object in Directory

SAVCHGOBJ

Save Changed Object

SAVLIB

Save Library

SAVOBJ

Save Object

SAVSAVFDTA

Save Save File Data

SAVDLO

Save DLO Object

SAVLICPGM

Save Licensed Program

SAVSHF

Save Bookshelf

Note: The audit record for the save operation will identify if the save was done with the STG(*FREE).

- Change operation

APYJRNCHG

Apply Journalized Changes

CHGJRNOBJ

Change Journalized Object

CHGOBJD

Change Object Description

CHGOBJOWN

Change Object Owner

CRTxxxxxx

Create object

Notes:

1. If *ALL or *CHANGE is specified for the target library, a ZC entry is written when an object is created.
2. If *CREATE is active for action auditing, a CO entry is written when an object is created.

DLTxxxxxx or DLTOBJ

Delete object

Notes:

1. If *ALL or *CHANGE is specified for the library containing the object, a ZC entry is written when an object is deleted.
2. If *ALL or *CHANGE is specified for the object, a ZC entry is written when it is deleted.
3. If *DELETE is active for action auditing, a DO entry is written when an object is deleted.

ENDJRNxxx

End Journaling

GRTOBJAUT

Grant Object Authority

Note: If authority is granted based on a referenced object, an audit record is not written for the referenced object.

MOV OBJ

Move Object

QLICOBJD

Change Object Description API

QLIRNMO

Rename Object API

QjoEndJournal

End Journaling

QjoStartJournal

Start Journaling

QSRRSTO

Restore Object API

QsrRestore

Restore Object in Directory API

RCLSTG

Reclaim Storage:

- If an object is secured by a damaged *AUTL, an audit record is written when the object is secured by the QRCLAUTL authorization list.
- An audit record is written if an object is moved into the QRCL library.

RMVJRNCHG

Remove Journalled Changes

RNM OBJ

Rename Object

RST Restore Object in Directory**RSTCFG**

Restore Configuration Objects

RSTLIB

Restore Library

RSTLICPGM

Restore Licensed Program

RSTOBJ

Restore Object

RVKOBJAUT

Revoke Object Authority

STRJRNxxx

Start Journaling

- Operations that are not audited

Prompt¹

Prompt override program for a change command (if one exists)

CHKOBJ

Check Object

ALCOBJ

Allocate Object

CPROBJ

Compress Object

DCPOBJ

Decompress Object

DLC OBJ

Deallocate Object

1. A prompt override program displays the current values when prompting is requested for a command. For example, if you type CHGURSPRF USERA and press F4 (prompt), the Change User Profile display shows the current values for the USERA user profile.

DSPOBJD
Display Object Description

DSPOBJAUT
Display Object Authority

EDTOBJAUT
Edit Object Authority

Note: If object authority is changed and action auditing includes *SECURITY, or the object is being audited, an audit record is written.

QSYCUSRA
Check User's Authority to an Object API

QSYLUSRA
List Users Authorized to an Object API. An audit record is not written for the object whose authority is being listed. An audit record is written for the user space used to contain information.

QSYRUSRA
Retrieve User's Authority to Object API

RCLTMPSTG
Reclaim Temporary Storage

RMVDFRID
Remove Defer ID

RSTDFROBJ
Restore Deferred Object

RTVOBJD
Retrieve Object Description

SAVSTG
Save Storage (audit of SAVSTG command only)

WRKOBJLCK
Work with Object Lock

WRKOBJOWN
Work with Objects by Owner

WRKxxx
Work with object commands

Operations for Access Path Recovery Times

This list describes the operations that you can perform against the Access Path Recovery Times object, and whether those operations are audited.

Note: Changes to access path recovery times are audited if the action auditing (QAUDLVL) system value or the action auditing (AUDLVL) parameter in the user profile includes *SYSMGT.

- Operations that are audited

CHGRCYAP
Change Recovery for Access Paths

EDTRCYAP
Edit Recovery for Access Paths

- Operations that are not audited

DSPRCYAP

Display Recovery for Access Paths

Operations for Alert Table (*ALRTBL)

This list describes the operations that you can perform against Alert Table (*ALRTBL), and whether those operations are audited.

- Read operation

None

- Change operation

ADDALRD

Add Alert Description

CHGALRD

Change Alert Description

CHGALRTBL

Change Alert Table

RMVALRD

Remove Alert Description

- Operations that are not audited

Print Print alert description

WRKALRD

Work with Alert Description

WRKALRTBL

Work with Alert Table

Operations for Authorization List (*AUTL)

This list describes the operations that you can perform against Authorization List (*AUTL), and whether those operations are audited.

- Read operation

None

- Change operation

ADDAUTLE

Add Authorization List Entry

CHGAUTLE

Change Authorization List Entry

EDTAUTL

Edit Authorization List

RMVAUTLE

Remove Authorization List Entry

- Operations that are not audited

DSPAUTL

Display Authorization List

DSPAUTOBJ

Display Authorization List Objects

DSPAUTLDLO
Display Authorization List DLO

RTVAUTLE
Retrieve Authorization List Entry

QSYLATLO
List Objects Secured by *AUTL API

WRKAUTL
Work with authorization list

Operations for Authority Holder (*AUTHLR)

This list describes the operations that you can perform against Authority Holder (*AUTHLR), and whether those operations are audited.

- Read operation

None

- Change operation

Associated

When used to secure an object.

- Operations that are not audited

DSPAUTHLR

Display Authority Holder

Operations for Binding Directory (*BNDDIR)

This list describes the operations that you can perform against Binding Directory (*BNDDIR), and whether those operations are audited.

- Read operation

CRTPGM

Create Program

CRTSRVPGM

Create Service Program

RTVBNSRC

Retrieve Binder Source

UPDPGM

Update Program

UPDSRVPGM

Update Service Program

- Change operation

ADDBNDDIRE

Add Binding Directory Entries

RMVBNDDIRE

Remove Binding Directory Entries

- Operations that are not audited

DSPBNDDIR

Display the contents of a binding directory

WRKBNDDIR

Work with Binding Directory

WRKBNDDIRE

Work with Binding Directory Entry

Operations for Configuration List (*CFGL)

This list describes the operations that you can perform against Configuration List (*CFGL), and whether those operations are audited.

- Read operation

CPYCFGL

Copy Configuration List. An entry is written for the *from-configuration-list*.

- Change operation

ADDCFGLE

Add Configuration List Entries

CHGCFGL

Change Configuration List

CHGCFGLE

Change Configuration List Entry

RMVCFGLE

Remove Configuration List Entry

- Operations that are not audited

DSPCFGL

Display Configuration List

WRKCFGL

Work with Configuration List

Operations for Special Files (*CHRSF)

This list describes the operations that you can perform against Special Files (*CHRSF), and whether those operations are audited.

See Operations for Stream File (*STMF) for *CHRSF auditing.

Operations for Chart Format (*CHTFMT)

This list describes the operations that you can perform against Chart Format (*CHTFMT), and whether those operations are audited.

- Read operation

Display

DSPCHT command or option F10 from the BGU menu

Print/Plot

DSPCHT command or option F15 from the BGU menu

Save/Create

Save or create graphics data file (GDF) using CRTGDF command or option F13 from the BGU menu

- Change operation

None

- Operations that are not audited

None

Operations for C Locale Description (*CLD)

This list describes the operations that you can perform against C Locale Description (*CLD), and whether those operations are audited.

- Read operation

RTVCLDSRC

Retrieve C Locale Source

Setlocale

Use the C locale object during C program run time using the Set locale function.

- Change operation

None

- Operations that are not audited

None

Operations for Change Request Description (*CRQD)

This list describes the operations that you can perform against Change Request Description (*CRQD), and whether those operations are audited.

- Read operation

QFVLSTA

List Change Request Description Activities API

QFVRTVCD

Retrieve Change Request Description API

SBMCRQ

Submit Change Request

- Change operation

ADDCMDCRQA

Add Command Change Request Activity

ADDOBJCRQA

Add Object Change Request Activity

ADDPRDCRQA

Add Product Change Request Activity

ADDPTFCRQA

Add PTF Change Request Activity

ADDRSCCRQA

Add Resource Change Request Activity

CHGCMDCRQA

Change Command Change Request Activity

CHGCRQD

Change Change Request Description

CHGOBJCRQA

Change Object Change Request Activity

CHGPRDCRQA

Change Product Change Request Activity

CHGPTFCRQA

Change PTF Change Request Activity

CHGRSCCRQA

Change Resource Change Request Activity

QFVADDA

Add Change Request Description Activity API

QFVRMVA

Remove Change Request Description Activity API

RMVCRQDA

Remove Change Request Description Activity

- Operations that are not audited

WRKCRQD

Work with Change Request Descriptions

Operations for Class (*CLS)

This list describes the operations that you can perform against Class (*CLS), and whether those operations are audited.

- Read operation

None

- Change operation

CHGCLS

Change Class

- Operations that are not audited

Job start

When used by work management to start a job

DSPCLS

Display Class

WRKCLS

Work with Class

Operations for Command (*CMD)

This list describes the operations that you can perform against Command (*CMD), and whether those operations are audited.

- Read operation

Run When command is run

- Change operation

CHGCMD

Change Command

CHGCMDDFT

Change Command Default

- Operations that are not audited

DSPCMD

Display Command

PRTCMDUSG

Print Command Usage

QCDRCMDI

Retrieve Command Information API

WRKCMD

Work with Command

The following commands are used within CL programs to control processing and to manipulate data within the program. The use of these commands is not audited.

CALL ¹ CALLPRC CHGVAR COPYRIGHT DCL DCLF DO ELSE ENDDO	ENDPGM ENDRCV GOTO IF MONMSG PGM	RCVF RETURN SNDF SNDRCVF TFRCTL WAIT
¹ CALL is audited if it is run interactively. It is not audited if it is run within a CL program.		

Operations for Connection List (*C>NNL)

This list describes the operations that you can perform against Connection List (*C>NNL), and whether those operations are audited.

- Read operation

None

- Change operation

ADDC>NNLE

Add Connection List Entry

CHGC>NNL

Change Connection List

CHGC>NNLE

Change Connection List Entry

RMVC>NNLE

Remove Connection List Entry

RNMC>NNLE

Rename Connection List Entry

- Operations that are not audited

Copy Option 3 of WRKC>NNL

DSPC>NNL

Display Connection List

RTVCFGSRC

Retrieve source of connection list

WRKC>NNL

Work with Connection List

WRKC>NNLE

Work with Connection List Entry

Operations for Class-of-Service Description (*COSD)

This list describes the operations that you can perform against Class-of-Service Description (*COSD), and whether those operations are audited.

- Read operation
 - None**
- Change operation
 - CHGCOSD**
Change Class-of-Service Description
- Operations that are not audited
 - DSPCOSD**
Display Class-of-Service Description
 - RTVCFGSRC**
Retrieve source of class-of-service description
 - WRKCOSD**
Copy class-of-service description
 - WRKCOSD**
Work with Class-of-Service Description

Operations for Communications Side Information (*CSI)

This list describes the operations that you can perform against Communications Side Information (*CSI), and whether those operations are audited.

- Read operation
 - DSPCSI**
Display Communications Side Information
 - Initialize**
Initialize conversation
- Change operation
 - CHGCSI**
Change Communications Side Information
- Operations that are not audited
 - WRKCSI**
Work with Communications Side Information

Operations for Cross System Product Map (*CSPMAP)

This list describes the operations that you can perform against Cross System Product Map (*CSPMAP), and whether those operations are audited.

- Read operation
 - Reference**
When referred to in a CSP application
- Change operation
 - None**
- Operations that are not audited
 - DSPCSPOBJ**
Display CSP Object

Operations for Cross System Product Table (*CSPTBL)

This list describes the operations that you can perform against Cross System Product Table (*CSPTBL), and whether those operations are audited.

- Read operation

Reference

When referred to in a CSP application

- Change operation

None

- Operations that are not audited

DSPCSPOBJ

Display CSP Object

WRKOBJCSP

Work with Objects for CSP

Operations for Controller Description (*CTLDD)

This list describes the operations that you can perform against Controller Description (*CTLDD), and whether those operations are audited.

- Read operation

SAVCFG

Save Configuration

VFYCMN

Link test

- Change operation

CHGCTLxxx

Change controller description

VRYCFG

Vary controller description on or off

- Operations that are not audited

DSPCTLD

Display Controller Description

ENDCTLRCY

End Controller Recovery

PRTDEVADR

Print Device Address

RSMCTLRCY

Resume Controller Recovery

RTVCFGSRC

Retrieve source of controller description

RTVCFGSTS

Retrieve controller description status

WRKCTLD

Copy controller description

WRKCTLD

Work with Controller Description

Operations for Device Description (*DEV D)

This list describes the operations that you can perform against Device Description (*DEV D), and whether those operations are audited.

- Read operation

Acquire

First acquisition of the device during open operation or explicit acquire operation

Allocate

Allocate conversation

SAVCFG

Save Configuration

STRPASTHR

Start pass-through session

Start of the second session for intermediate pass-through

VFYCMN

Link test

- Change operation

CHGDEVxxx

Change device description

HLDDDEVxxx

Hold device description

RLSDEVxxx

Release device description

QWSSETWS

Change type-ahead setting for a device

VRYCFG

Vary device description on or off

- Operations that are not audited

DSPDEV D

Display Device Description

DSPMODSTS

Display Mode Status

ENDDEVRCY

End Device Recovery

HLDCMNDEV

Hold Communications Device

RLSCMNDEV

Release Communications Device

RSMDEVRCY

Resume Device Recovery

RTVCFG SRC

Retrieve source of device description

RTVCFGSTS
Retrieve device description status

WRKCFGSTS
Work with device status

WRKDEVD
Copy device description

WRKDEVD
Work with Device Description

Operations for Directory (*DIR)

This list describes the operations that you can perform against Directory (*DIR) objects, and whether those operations are audited.

- Read/search operations
 - access, accessx, QlgAccess, QlgAccessx**
Determine file accessibility
 - CHGATR**
Change Attribute
 - CPY** Copy Object
 - DSPCURDIR**
Display Current Directory
 - DSPLNK**
Display Object Links
 - faccessx**
Determine file accessibility for a class of users by descriptor
 - getcwd, qlgGetcwd**
Get Path Name of Current Directory API
 - Qp0lGetAttr, QlgGetAttr**
Get attributes APIs
 - Qp0lGetPathFromFileID, QlgGetPathFromFileID**
Get Path From File Identifier APIs
 - Qp0lProcessSubtree, QlgProcessSubtree**
Process a Path Name APIs
 - open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
Open File APIs
 - Qp0lSetAttr, QlgSetAttr**
Set Attributes APIs
 - opendir, QlgOpendir**
Open Directory APIs
 - RTVCURDIR**
Retrieve Current Directory
 - SAV** Save Object
 - WRKLNK**
Work with Links
- Change operation

- CHGATR**
Change Attributes
- CHGAUD**
Change Auditing Value
- CHGAUT**
Change Authority
- CHGOWN**
Change Owner
- CHGPGP**
Change Primary Group
- chmod, QlgChmod**
Change File Authorizations API
- chown, QlgChown**
Change Owner and Group API
- CPY** Copy Object
- CRTDIR**
Make Directory
- fchmod**
Change File Authorizations by Descriptor API
- fchown**
Change Owner and Group of File by Descriptor API
- mkdir, QlgMkdir**
Make Directory API
- MOV** Move Object
- Qp0lRenameKeep, QlgRenameKeep**
Rename File or Directory, Keep New APIs
- Qp0lRenameUnlink, QlgRenameUnlink**
Rename File or Directory, Unlink New APIs
- Qp0lSetAttr, QlgSetAttr**
Set Attribute APIs
- rmdir, QlgRmdir**
Remove Directory API
- RMVDIR**
Remove Directory
- RNM** Rename Object
- RST** Restore Object
- utime, QlgUtime**
Set File Access and Modification Times API
- WRKAUT**
Work with Authority
- WRKLNK**
Work with Object Links
- Operations that are not audited

chdir, QlgChdir
Change Directory API

CHGCURDIR
Change Current Directory

close Close File Descriptor API

closedir
Close Directory API

DSPAUT
Display Authority

dup Duplicate Open File Descriptor API

dup2 Duplicate Open File Descriptor to Another Descriptor API

faccessx
Determine file accessibility for a class of users by descriptor

fchdir Change current directory by descriptor

fcntl Perform File Control Command API

fpathconf
Get Configurable Path Name Variables by Descriptor API

fstat, fstat64
Get File Information by Descriptor APIs

givedescriptor
Give File Access API

ioctl Perform I/O Control Request API

lseek, lseek64
Set File Read/Write Offset APIs

lstat, lstat64, QlgLstat, QlgLstat64
Get File or Link Information APIs

pathconf, QlgPathconf
Get Configurable Path Name Variables API

readdir
Read Directory Entry API

rewinddir
Reset Directory Stream API

select Check I/O Status of Multiple File Descriptors API

stat, QlgStat
Get File Information API

takedescriptor
Take File Access API

Operations for Directory Server

This list describes the operations that you can perform against Directory Server, and whether those operations are audited.

Note: Directory Server actions are audited if the action auditing (QAUDLVL) system value or the action auditing (AUDLVL) parameter in the user profile includes *OFCSRV.

- Operations that are audited
 - Add** Adding new directory entries
 - Change** Changing directory entry details
 - Delete** Deleting directory entries
 - Rename** Renaming directory entries
 - Print** Displaying or printing directory entry details
 - Displaying or printing department details
 - Displaying or printing directory entries as the result of a search
 - RTVDIRE** Retrieve Directory Entry
 - Collect** Collecting directory entry data using directory shadowing
 - Supply** Supplying directory entry data using directory shadowing
- Operations that are not audited
 - CL commands** CL commands that work on the directory can be audited separately using the object auditing function.
 - Note:** Some CL directory commands cause an audit record because they perform a function that is audited by *OFCSR action auditing, such as adding a directory entry.
 - CHGSYSDIRA** Change System Directory Attributes
 - Departments** Adding, changing, deleting, or displaying directory department data
 - Descriptions** Assigning a description to a different directory entry using option 8 from the WRKDIR panel.
 - Adding, changing, or deleting directory entry descriptions
 - Distribution lists** Adding, changing, renaming, or deleting distribution lists
 - ENDDIRSHD** End Directory Shadowing
 - List** Displaying or printing a list of directory entries that does not include directory entry details, such as using the WRKDIRE command or using F4 to select entries for sending a note.
 - Locations** Adding, changing, deleting, or displaying directory location data
 - Nickname** Adding, changing, renaming or deleting nicknames
 - Search** Searching for directory entries
 - STRDIRSHD** Start Directory Shadowing

Operations for Document Library Object (*DOC or *FLR)

This list describes the operations that you can perform against document library objects (*DOC or *FLR), and whether those operations are audited.

- Read operation

CHKDOC

Check document spelling

CPYDOC

Copy Document

DMPDLO

Dump DLO

DSPDLOAUD

Display DLO Auditing

Note: If auditing information is displayed for all documents in a folder and object auditing is specified for the folder, an audit record is written. Displaying object auditing for individual documents does not result in an audit record.

DSPDLOAUT

Display DLO Authority

DSPDOC

Display Document

DSPHLPDOC

Display Help Document

EDTDLOAUT

Edit DLO Authority

MRGDOC

Merge Document

PRTDOC

Print Document

QHFCPYSF

Copy Stream File API

QHFGETSZ

Get Stream File Size API

QHFRDDR

Read Directory Entry API

QHFRDSF

Read Stream File API

RTVDOC

Retrieve Document

SAVDLO

Save DLO

SAVSHF

Save Bookshelf

SNDDOC

Send Document

SNDDST
Send Distribution

WRKDOC
Work with Document

Note: A read entry is written for the folder containing the documents.

- Change operation

ADDDLOAUT
Add DLO Authority

ADDOFCENR
Add Office Enrollment

CHGDLOAUD
Change DLO Auditing

CHGDLOAUT
Change DLO Authority

CHGDLOOWN
Change DLO Ownership

CHGDLOPGP
Change DLO Primary Group

CHGDOCD
Change Document Description

CHGDSTD
Change Distribution Description

CPYDOC²
Copy Document

Note: A change entry is written if the target document already exists.

CRTFLR
Create Folder

CVTTOFLR²
Convert to Folder

DLTDLO²
Delete DLO

DLTSHF
Delete Bookshelf

DTLDOCL²
Delete Document List

DLTDST²
Delete Distribution

EDTDLOAUT
Edit DLO Authority

EDTDOC
Edit Document

2. A change entry is written for both the document and the folder if the target of the operation is in a folder.

FILDOC ²
File Document

GRTACCAUT
Grant Access Code Authority

GRTUSRPMN
Grant User Permission

MOVDOC ²
Move Document

MRGDOC ²
Merge Document

PAGDOC
Paginate Document

QHFCHGAT
Change Directory Entry Attributes API

QHFSETSZ
Set Stream File Size API

QHFWRFSF
Write Stream File API

QRYDOCLIB ²
Query Document Library

Note: A change entry is written if an existing document resulting from a search is replaced.

RCVDST ²
Receive Distribution

RGZDLO
Reorganize DLO

RMVACC
Remove access code, for any DLO to which the access code is attached

RMVDLOAUT
Remove DLO authority

RNMDLO ²
Rename DLO

RPLDOC
Replace Document

RSTDLO ²
Restore DLO

RSTSHF
Restore Bookshelf

RTVDOC
Retrieve Document (check out)

RVKACCAUT
Revoke Access Code Authority

RVKUSRPMN
Revoke User Permission

- SAVDLO ²
Save DLO
- Operations that are not audited
 - ADDACC
Add Access Code
 - DSPACC
Display Access Code
 - DSPUSRPMN
Display User Permission
 - QHFCHGFP
Change File Pointer API
 - QHFCLODR
Close Directory API
 - QHFCLOSF
Close Stream File API
 - QHFFRCSE
Force Buffered Data API
 - QHFLULSF
Lock/Unlock Stream File Range API
 - QHFRVAT
Retrieve Directory Entry Attributes API
 - RCLDLO
Reclaim DLO (*ALL or *INT)
 - WRKDOCLIB
Work with Document Library
 - WRKDOCPTQ
Work with Document Print Queue

Operations for Data Area (*DTAARA)

This list describes the operations that you can perform against Data Area (*DTAARA), and whether those operations are audited.

- Read operation
 - DSPDTAARA
Display Data Area
 - RCVDTAARA
Receive Data Area (S/38 command)
 - RTVDTAARA
Retrieve Data Area
 - QWCRDTAA
Retrieve Data Area API
- Change operation
 - CHGDTAARA
Change Data Area
 - SNDDTAARA
Send Data Area

- Operations that are not audited

Data Areas

Local Data Area, Group Data Area, PIP (Program Initialization Parameter) Data Area

WRKDTAARA

Work with Data Area

Operations for Interactive Data Definition Utility (*DTADCT)

This list describes the operations that you can perform against Interactive Data Definition Utility (*DTADCT), and whether those operations are audited.

- Read operation

None

- Change operation

Create Data dictionary and data definitions

Change

Data dictionary and data definitions

Copy Data definitions (recorded as create)

Delete Data dictionary and data definitions

Rename

Data definitions

- Operations that are not audited

Display

Data dictionary and data definitions

LNKDTADFN

Linking and unlinking file definitions

Print Data dictionary, data definitions, and where-used information for data definitions

Operations for Data Queue (*DTAQ)

This list describes the operations that you can perform against Data Queue (*DTAQ), and whether those operations are audited.

- Read operation

QMHRDQM

Retrieve Data Queue Message API

- Change operation

QRCVDTAQ

Receive Data Queue API

QSNDDTAQ

Send Data Queue API

QCLRDTAQ

Clear Data Queue API

QMHQCDQ

Change Data Queue API

- Operations that are not audited

WRKDTAQ

Work with Data Queue

QMHQRDQD

Retrieve Data Queue Description API

Operations for Edit Description (*EDTD)

This list describes the operations that you can perform against Edit Description (*EDTD), and whether those operations are audited.

- Read operation

DSPEDTD

Display Edit Description

QECCVTEC

Edit code expansion API (via routine QECEDITU)

- Change operation

None

- Operations that are not audited

WRKEDTD

Work with Edit Descriptions

QECEDT

Edit API

QECCVTEW

API for translating Edit Work into Edit Mask

Operations for Exit Registration (*EXITRG)

This list describes the operations that you can perform against Exit Registration (*EXITRG), and whether those operations are audited.

- Read operation

QUSRTVEI

Retrieve Exit Information API

QusRetrieveExitInformation

Retrieve Exit Information API

- Change operation

ADDEXITPGM

Add Exit Program

QUSADDEP

Add Exit Program API

QusAddExitProgram

Add Exit Program API

QUSDRGPT

Unregister Exit Point API

QusDeregisterExitPoint

Unregister Exit Point API

QUSRGPT

Register Exit Point API

QusRegisterExitPoint

Register Exit Point API

QUSRMVEP

Remove Exit Program API

QusRemoveExitProgram

Remove Exit Program API

RMVEXITPGM

Remove Exit Program

WRKREGINF

Work with Registration Information

- Operations that are not audited

None

Operations for Forms Control Table (*FCT)

This list describes the operations that you can perform against Forms Control Table (*FCT), and whether those operations are audited.

- No Read or Change operations are audited for the *FCT object type.

Operations for File (*FILE)

This list describes the operations that you can perform against File (*FILE), and whether those operations are audited.

- Read operation

CPYF Copy File (uses open operation)**Open** Open of a file for read**DSPPFM**

Display Physical File Member (uses open operation)

Open Open of MRTs after the initial open**CRTBSCF**

Create BSC File (uses open operation)

CRTC MNF

Create Communications File (uses open operation)

CRTDSPF

Create Display File (uses open operation)

CRTICFF

Create ICF File (uses open operation)

CRTMXDF

Create MXD File (uses open operation)

CRTPRTF

Create Printer File (uses open operation)

CRTPF

Create Physical File (uses open operation)

CRTL F

Create Logical File (uses open operation)

DSPMODSRC

Display Module Source (uses open operation)

- STRDBG**
Start Debug (uses open operation)
- QTEDBGS**
Retrieve View Text API
- Change operation
 - Open** Open a file for modification
 - ADDBSCDEVE**
(S/38E) Add Bisync Device Entry to a mixed device file
 - ADDCMNDEVE**
(S/38E) Add Communications Device Entry to a mixed device file
 - ADDDSPDEVE**
(S/38E) Add Display Device Entry to a mixed device file
 - ADDICFDEVE**
(S/38E) Add ICF Device Entry to a mixed device file
 - ADDLFM**
Add Logical File Member
 - ADDPFCST**
Add Physical File Constraint
 - ADDPFM**
Add Physical File Member
 - ADDPFTRG**
Add Physical File Trigger
 - ADDPFVLM**
Add Physical File Variable Length Member
 - APYJRNCHGX**
Apply Journal Changes Extend
 - CHGBSCF**
Change Bisync function
 - CHGCMNF**
(S/38E) Change Communications File
 - CHGDDMF**
Change DDM File
 - CHGDKTF**
Change Diskette File
 - CHGDSPF**
Change Display File
 - CHGICFDEVE**
Change ICF Device File Entry
 - CHGICFF**
Change ICF File
 - CHGMXDF**
(S/38E) Change Mixed Device File
 - CHGLF**
Change Logical File

CHGLFM
Change Logical File Member

CHGPF
Change Physical File

CHGPFCST
Change Physical File Constraint

CHGPFM
Change Physical File Member

CHGPRTF
Change Printer Device GQle

CHGSAVF
Change Save File

CHGS36PRCA
Change S/36 Procedure Attributes

CHGS36SRCA
Change S/36 Source Attributes

CHGTAPF
Change Tape Device File

CLRPFM
Clear Physical File Member

CPYF Copy File (open file for modification, such as adding records, clearing a member, or saving a member)

EDTS36PRCA
Edit S/36 Procedure Attributes

EDTS36SRCA
Edit S/36 Source Attributes

INZPFM
Initialize Physical File Member

JRNAP
(S/38E) Start Journal Access Path (entry per file)

JRNPF
(S/38E) Start Journal Physical File (entry per file)

RGZPFM
Reorganize Physical File Member

RMVBSCDEVE
(S/38E) Remove BSC Device Entry from a mixed dev file

RMVCMNDEVE
(S/38E) Remove CMN Device Entry from a mixed dev file

RMVDSPDEVE
(S/38E) Remove DSP Device Entry from a mixed dev file

RMVICFDEVE
(S/38E) Remove ICF Device Entry from an ICM dev file

RMVM
Remove Member

- RMVFCST**
Remove Physical File Constraint
- RMVFTGR**
Remove Physical File Trigger
- RNMM**
Rename Member
- WRKS36PRCA**
Work with S/36 Procedure Attributes
- WRKS36SRCA**
Work with S/36 Source Attributes
- Operations that are not audited
 - CHGPFTRG**
Change Physical File Trigger
 - DSPCPCST**
Display Check Pending Constraints
 - DSPFD**
Display File Description
 - DSPFFD**
Display File Field Description
 - DSPDBR**
Display Database Relations
 - DSPPGMREF**
Display Program File References
 - EDTCPCST**
Edit Check Pending Constraints
 - OVRxxx**
Override file
 - RTVMBRD**
Retrieve Member Description
 - WRKFCST**
Work with Physical File Constraints
 - WRKF**
Work with File

Operations for First-in First-out Files (*FIFO)

This list describes the operations that you can perform against first-in first-out (*FIFO) objects, and whether those operations are audited.

See Operations for Stream File (*STMF) for the *FIFO auditing.

Operations for Folder (*FLR)

This list describes the operations that you can perform against folder (*FLR) objects, and whether those operations are audited.

See operations for “Operations for Document Library Object (*DOC or *FLR)” on page 516

Operations for Font Resource (*FNTRSC)

This list describes the operations that you can perform against Font Resource (*FNTRSC), and whether those operations are audited.

- Read operation
 - Print** Printing a spooled file that refers to the font resource
- Change operation
 - None**
- Operations that are not audited
 - WRKFNTRSC**
Work with Font Resource
 - Print** Referring to the font resource when creating a spooled file

Operations for Form Definition (*FORMDF)

This list describes the operations that you can perform against Form Definition (*FORMDF), and whether those operations are audited.

- Read operation
 - Print** Printing a spooled file that refers to the form definition
- Change operation
 - None**
- Operations that are not audited
 - WRKFORMDF**
Work with Form Definition
 - Print** Referring to the form definition when creating a spooled file

Operations for Filter Object (*FTR)

This list describes the operations that you can perform against Filter Object (*FTR), and whether those operations are audited.

- Read operation
 - None**
- Change operation
 - ADDALRACNE**
Add Alert Action Entry
 - ADDALRSLTE**
Add Alert Selection Entry
 - ADDPRBACNE**
Add Problem Action Entry
 - ADDPRBSLTE**
Add Problem Selection Entry
 - CHGALRACNE**
Change Alert Action Entry
 - CHGALRSLTE**
Change Alert Selection Entry

CHGPRBACNE

Change Problem Action Entry

CHGPRBSLTE

Change Problem Selection Entry

CHGFTR

Change Filter

RMVFTRACNE

Remove Alert Action Entry

RMVFTRSLTE

Remove Alert Selection Entry

WRKFTRACNE

Work with Alert Action Entry

WRKFTRSLTE

Work with Alert Selection Entry

- Operations that are not audited

WRKFTR

Work with Filter

WRKFTRACNE

Work with Filter Action Entries

WRKFTRSLTE

Work with Filter Selection Entries

Operations for Graphics Symbols Set (*GSS)

This list describes the operations that you can perform against Graphics Symbols Set (*GSS), and whether those operations are audited.

- Read operation

Loaded

When it is loaded

Font When it is used as a font in an externally described printer file

- Change operation

None.

- Operations that are not audited

WRKGSS

Work with Graphic Symbol Set

Operations for Double-byte Character Set Dictionary (*IGCDCT)

This list describes the operations that you can perform against Double-byte Character Set Dictionary (*IGCDCT), and whether those operations are audited.

- Read operation

DSPIGCDCT

Display IGC Dictionary

- Change operation

EDTIGCDCT

Edit IGC Dictionary

Operations for Double-byte Character Set Sort (*IGCSRT)

This list describes the operations that you can perform against Double-byte Character Set Sort (*IGCSRT), and whether those operations are audited.

- Read operation

CPYIGCSRT

Copy IGC Sort (*from-*IGCSRT-object*)

Conversion

Conversion to V3R1 format, if necessary

Print Print character to register in sort table (option 1 from CGU menu)

Print before deleting character from sort table (option 2 from CGU menu)

- Change operation

CPYIGCSRT

Copy IGC Sort (*to-*IGCSRT-object*)

Conversion

Conversion to V3R1 format, if necessary

Create Create a user-defined character (option 1 from CGU menu)

Delete Delete a user-defined character (option 2 from CGU menu)

Update

Update the active sort table (option 5 from CGU menu)

- Operations that are not audited

FMTDTA

Sort records or fields in a file

Operations for Double-byte Character Set Table (*IGCTBL)

This list describes the operations that you can perform against Double-byte Character Set Table (*IGCTBL), and whether those operations are audited.

- Read operation

CPYIGCTBL

Copy IGC Table

STRFMA

Start Font Management Aid

- Change operation

STRFMA

Start Font Management Aid

- Operations that are not audited

CHKIGCTBL

Check IGC Table

Operations for Job Description (*JOBDD)

This list describes the operations that you can perform against Job Description (*JOBDD), and whether those operations are audited.

- Read operation

None

- Change operation
CHGJOB
Change Job Description
- Operations that are not audited
DSPJOB
Display Job Description
- WRKJOB**
Work with Job Description
- QWDRJOB**
Retrieve Job Description API
- Batch job**
When used to establish a job

Operations for Job Queue (*JOBQ)

This list describes the operations that you can perform against Job Queue (*JOBQ), and whether those operations are audited.

- Read operation
None
- Change operation
Entry When an entry is placed on or removed from the queue
CHGJOBQ
Change Job Queue
- CLRJOBQ**
Clear Job Queue
- HLDJOBQ**
Hold Job Queue
- RLSJOBQ**
Release Job Queue
- Operations that are not audited
ADDJOBQE “Subsystem descriptions” on page 205
Add Job Queue Entry
- CHGJOB**
Change Job from one JOBQ to another JOBQ
- CHGJOBQE** “Subsystem descriptions” on page 205
Change Job Queue Entry
- QSPRJOBQ**
Retrieve job queue information
- RMVJOBQE** “Subsystem descriptions” on page 205
Remove Job Queue Entry
- TFRJOB**
Transfer Job
- TFRBCHJOB**
Transfer Batch Job

WRKJOBQ
Work with Job Queue for a specific job queue

WRKJOBQ
Work with Job Queue for all job queues

WRKJOBQD
Work with Job Queue Description

Operations for Job Scheduler Object (*JOBSCD)

This list describes the operations that you can perform against Job Scheduler Object (*JOBSCD), and whether those operations are audited.

- Read operation

None

- Change operation

ADDJOBSCDE
Add Job Schedule Entry

CHGJOBSCDE
Change Job Schedule Entry

RMVJOBSCDE
Remove Job Schedule Entry

HLDJOBSCDE
Hold Job Schedule Entry

RLSJOBSCDE
Release Job Schedule Entry

- Operations that are not audited

Display
Display details of scheduled job entry

WRKJOBSCDE
Work with Job Schedule Entries

Work with ...
Work with previously submitted jobs from job schedule entry

QWCLSCDE
List job schedule entry API

Operations for Journal (*JRN)

This list describes the operations that you can perform against Journal (*JRN), and whether those operations are audited.

- Read operation

CMPJRNIMG
Compare Journal Images

DSPJRN
Display Journal Entry for user journals

QJORJIDI
Retrieve Journal Identifier (JID) Information

3. An audit record is written if object auditing is specified for the subsystem description (*SBSD).

- QjoRetrieveJournalEntries**
Retrieve Journal Entries
- RCVJRNE**
Receive Journal Entry
- RTVJRNE**
Retrieve Journal Entry
- Change operation
- ADDRMTJRN**
Add Remote Journal
- APYJRNCHG**
Apply Journal Changes
- APYJRNCHGX**
Apply Journal Changes Extend
- CHGJRN**
Change Journal
- CHGRMTJRN**
Change Remote Journal
- ENDJRNxxx**
End Journaling
- JRNAP**
(S/38E) Start Journal Access Path
- JRNPF**
(S/38E) Start Journal Physical File
- QjoAddRemoteJournal**
Add Remote Journal API
- QjoChangeJournalState**
Change Journal State API
- QjoEndJournal**
End Journaling API
- QjoRemoveRemoteJournal**
Remove Remote Journal API
- QJOSJRNE**
Send Journal Entry API (user entries only via QJOSJRNE API)
- QjoStartJournal**
Start Journaling API
- RMVJRNCHG**
Remove Journal Changes
- RMVRMTJRN**
Remove Remote Journal
- SNDJRNE**
Send Journal Entry (user entries only via SNDJRNE command)
- STRJRNxxx**
Start Journaling
- Operations that are not audited

DSPJRN

Display Journal Entry for internal system journals, JRN(*INTSYSJRN)

DSPJRNA

(S/38E) Work with Journal Attributes

DSPJRNMNU

(S/38E) Work with Journal

QjoRetrieveJournalInformation

Retrieve Journal Information API

WRKJRN

Work with Journal (DSPJRNMNU in S/38 environment)

WRKJRNA

Work with Journal Attributes (DSPJRNA in S/38 environment)

Operations for Journal Receiver (*JRNRCV)

This list describes the operations that you can perform against Journal Receiver (*JRNRCV), and whether those operations are audited.

- Read operation

None

- Change operation

CHGJRN

Change Journal (when attaching new receivers)

- Operations that are not audited

DSPJRNRCVA

Display Journal Receiver Attributes

QjoRtvJrnReceiverInformation

Retrieve Journal Receiver Information API

WRKJRNRCV

Work with Journal Receiver

Operations for Library (*LIB)

This list describes the operations that you can perform against Library (*LIB), and whether those operations are audited.

- Read operation

DSPLIB

Display Library (when library is not empty. If library is empty, no audit is performed.)

Locate When a library is accessed to find an object

Note:

1. Several audit entries might be written for a library for a single command. For example, when you open a file, a ZR audit journal entry for the library is written when the system locates the file and each member in the file.
2. No audit entry is written if the locate function is not successful. For example, you run a command using a generic parameter, such as:

```
DSPOBJD OBJ(AR/WRK*) OBJTYPE(*FILE)
```

If a library named "AR" does not have any file names beginning with "WRK", no audit record is written for that library.

Library list

Adding library to a library list

- Change operation

CHGLIB

Change Library

CLRLIB

Clear Library

MOVOBJ

Move Object

RNMOBJ

Rename Object

Add Add object to library**Delete** Delete object from library

- Operations that are not audited

None

Operations for Line Description (*LIND)

This list describes the operations that you can perform against Line Description (*LIND), and whether those operations are audited.

- Read operation

SAVCFG

Save Configuration

RUNLPDA

Run LPDA-2 operational commands

VFYCMN

Link test

VFYLNKLPDA

LPDA-2 link test

- Change operation

CHGLINxxx

Change Line Description

VRYCFG

Vary on/off line description

- Operations that are not audited

ANSLIN

Answer Line

Copy Option 3 from WRKLIND**DSPLIND**

Display Line Description

ENDLINRCY

End Line Recovery

RLSCMNDEV

Release Communications Device

RSMLINRCY
Resume Line Recovery

RTVCFGSRC
Retrieve Source of line description

RTVCFGSTS
Retrieve line description status

WRKLIND
Work with Line Description

WRKCFGSTS
Work with line description status

Operations for Mail Services

This list describes the operations that you can perform against Mail Services, and whether those operations are audited.

Note: Mail services actions are audited if the action auditing (QAUDLVL) system value or the action auditing (AUDLVL) parameter in the user profile includes *OFCSRV.

- Operations that are audited

Change

Changes to the system distribution directory

On behalf

Working on behalf of another user

Note: Working on behalf of another user is audited if the AUDLVL in the user profile or the QAUDLVL system value includes *SECURITY.

Open An audit record is written when the mail log is opened

- Operations that are not audited

Change

Change details of a mail item

Delete Delete a mail item

File File a mail item into a document or folder

Note: When a mail item is filed, it becomes a document library object (DLO). Object auditing can be specified for a DLO.

Forward

Forward a mail item

Print Print a mail item

Note: Printing of mail items can be audited using the *SPLFDTA or *PRTDTA audit level.

Receive

Receive a mail item

Reply Reply to a mail item

Send Send a mail item

View View a mail item

Operations for Menu (*MENU)

This list describes the operations that you can perform against Menu (*MENU), and whether those operations are audited.

- Read operation

Display

Displaying a menu through the GO MENU command or UIM dialog box command

- Change operation

CHGMNU

Change menu

- Operations that are not audited

Return

Returning to a menu in the menu stack that has already been displayed

DSPMNUA

Display menu attributes

WRKMNU

Work with menu

Operations for Mode Description (*MODD)

This list describes the operations that you can perform against Mode Description (*MODD), and whether those operations are audited.

- Read operation

None

- Change operation

CHGMODD

Change Mode Description

- Operations that are not audited

CHGSSNMAX

Change session maximum

DSPMODD

Display Mode Description

ENDMOD

End Mode

STRMOD

Start Mode

WRKMODD

Work with Mode Descriptions

Operations for Module Object (*MODULE)

This list describes the operations that you can perform against Module Object (*MODULE), and whether those operations are audited.

- Read operation

CRTPGM

An audit entry for each module object used during a CRTPGM.

CRTSRVPGM

An audit entry for each module object used during a CRTSRVPGM

RTVCLSRC

An audit entry for each module object used during a RTVCLSRC

UPDPGM

An audit entry for each module object used during an UPDPGM

UPDSRVPGM

An audit entry for each module object used during an UPDSRVPGM

- Change operation

CHGMOD

Change Module

- Operations that are not audited

DSPMOD

Display Module

Module Conversion

Machine-initiated conversion for compatibility with the current machine

RTVBNDSRC

Retrieve Binder Source

WRKMOD

Work with Module

Operations for Message File (*MSGF)

This list describes the operations that you can perform against Message File (*MSGF), and whether those operations are audited.

- Read operation

DSPMSGD

Display Message Description

MRGMSGF

Merge Message File from-file

Print Print message description

RTVMSG

Retrieve information from a message file

QMHRTVM

Retrieve Message API

WRKMSGD

Work with Message Description

- Change operation

ADDMSGD

Add Message Description

CHGMSGD

Change Message Description

CHGMSGF

Change Message File

MRGMSGF

Merge Message File (to-file and replace MSGF)

- RMVMSGD**
Remove Message Description
- Operations that are not audited
 - OVRMSGF**
Override Message File
 - WRKMSGF**
Work with Message File
 - QMHRMFAT**
Retrieve Message File Attributes API

Operations for Message Queue (*MSGQ)

This list describes the operations that you can perform against Message Queue (*MSGQ), and whether those operations are audited.

- Read operation
 - QMHLSTM**
List Nonprogram Messages API
 - QMHRMQAT**
Retrieve Nonprogram Message Queue Attributes API
 - DSPLOG**
Display Log
 - DSPMSG**
Display Message
 - Print** Print Messages
 - RCVMSG**
Receive Message RMV(*NO)
 - QMHRCVM**
Receive Nonprogram Messages API when message action is not *REMOVE.
- Change operation
 - CHGMSGQ**
Change Message Queue
 - CLRMSGQ**
Clear Message Queue
 - RCVMSG**
Receive Message RMV(*YES)
 - QMHRCVM**
Receive Nonprogram Messages API when message action is *REMOVE.
 - RMVMSG**
Remove Message
 - QMHRCVM**
Remove Nonprogram Messages API
 - SNDxxxMSG**
Send a Message to a message queue
 - QMHSNDBM**
Send Break Message API

QMHSNDM
Send Nonprogram Message API

QMHSNDRM
Send Reply Message API

SNDRPY
Send Reply

WRKMSG
Work with Message

- Operations that are not audited

WRKMSGQ
Work with Message Queue

Program
Program message queue operations

Operations for Node Group (*NODGRP)

This list describes the operations that you can perform against Node Group (*NODGRP), and whether those operations are audited.

- Read operation

DSPNODGRP
Display Node Group

- Change operation

CHGNODGRPA
Change Node Group

Operations for Node List (*NODL)

This list describes the operations that you can perform against Node List (*NODL), and whether those operations are audited.

- Read operation

QFVLSTNL
List node list entries

- Change operation

ADDNODLE
Add Node List Entry

RMVNODLE
Remove Node List Entry

- Operations that are not audited

WRKNODL
Work with Node List

WRKNODLE
Work with Node List Entries

Operations for NetBIOS Description (*NTBD)

This list describes the operations that you can perform against NetBIOS Description (*NTBD), and whether those operations are audited.

- Read operation

SAVCFG

Save Configuration

- Change operation

CHGNTBD

Change NetBIOS Description

- Operations that are not audited

Copy Option 3 of WRKNTBD**DSPNTBD**

Display NetBIOS Description

RTVCFGSRC

Retrieve Configuration Source of NetBIOS description

WRKNTBD

Work with NetBIOS Description

Operations for Network Interface (*NWID)

This list describes the operations that you can perform against Network Interface (*NWID), and whether those operations are audited.

- Read operation

SAVCFG

Save Configuration

- Change operation

CHGNWIISDN

Change Network Interface Description

VRYCFG

Vary network interface description on or off

- Operations that are not audited

Copy Option 3 of WRKNWID**DSPNWID**

Display Network Interface Description

ENDNWIRCY

End Network Interface Recovery

RSMNWIRCY

Resume Network Interface Recovery

RTVCFGSRC

Retrieve Source of Network Interface Description

RTVCFGSTS

Retrieve Status of Network Interface Description

WRKNWID

Work with Network Interface Description

WRKCFGSTS

Work with network interface description status

Operations for Network Server Description (*NWSD)

This list describes the operations that you can perform against Network Server Description (*NWSD), and whether those operations are audited.

- Read operation
 - SAVCFG**
Save Configuration
- Change operation
 - CHGNWSD**
Change Network Server Description
 - VRFCFG**
Vary Configuration
- Operations that are not audited
 - Copy** Option 3 of WRKNWSD
 - DSPNWSD**
Display Network Server Description
 - RTVCFGSRC**
Retrieve Configuration Source for *NWSD
 - RTVCFGSTS**
Retrieve Configuration Status for *NWSD
 - WRKNWSD**
Work with Network Server Description

Operations for Output Queue (*OUTQ)

This list describes the operations that you can perform against Output Queue (*OUTQ), and whether those operations are audited.

- Read operation
 - STRPRTWTR**
Start a Printer Writer to an OUTQ
 - STRRMTWTR**
Start a Remote Writer to an OUTQ
- Change operation
 - Placement**
When an entry is placed on or removed from the queue
 - CHGOUTQ**
Change Output Queue
 - CHGSPLFA** ⁴
Change Spooled File Attributes, if moved to a different output queue and either output queue is audited
 - CLROUTQ**
Clear Output Queue
 - DLTSPLF** ⁴
Delete Spooled File
 - HLDOUTQ**
Hold Output Queue

- RLSOUTQ**
Release Output Queue
- Operations that are not audited
- CHGSPLFA**⁴
Change Spooled File Attributes
- CPYSPLF**⁴
Copy Spooled File
- Create**⁴
Create a spooled file
- DSPSPLF**⁴
Display Spooled File
- HLDSPLF**⁴
Hold Spooled File
- QSPROUTQ**
Retrieve output queue information
- RLSSPLF**⁴
Release Spooled File
- SNDNETSPLF**⁴
Send Network Spooled File
- WRKOUTQ**
Work with Output Queue
- WRKOUTQD**
Work with Output Queue Description
- WRKSPLF**
Work with Spooled File
- WRKSPLFA**
Work with Spooled File Attributes

Operations for Overlay (*OVL)

This list describes the operations that you can perform against Overlay (*OVL), and whether those operations are audited.

- Read operation
 - Print** Printing a spooled file that refers to the overlay
- Change operation
 - None**
- Operations that are not audited
 - WRKOVL**
Work with overlay
 - Print** Referring to the overlay when creating a spooled file

4. This is also audited if action auditing (QAUDLVL system value or AUDLVL user profile value) includes *SPLFDA.

Operations for Page Definition (*PAGDFN)

This list describes the operations that you can perform against Page Definition (*PAGDFN), and whether those operations are audited.

- Read operation
 - Print** Printing a spooled file that refers to the page definition
- Change operation
 - None**
- Operations that are not audited
 - WRKPAGDFN**
Work with Page Definition
 - Print** Referring to the form definition when creating a spooled file

Operations for Page Segment (*PAGSEG)

This list describes the operations that you can perform against Page Segment (*PAGSEG), and whether those operations are audited.

- Read operation
 - Print** Printing a spooled file that refers to the page segment
- Change operation
 - None**
- Operations that are not audited
 - WRKPAGSEG**
Work with Page Segment
 - Print** Referring to the page segment when creating a spooled file

Operations for Print Descriptor Group (*PDG)

This list describes the operations that you can perform against Print Descriptor Group (*PDG), and whether those operations are audited.

- Read operation
 - Open** When the page descriptor group is opened for read access by a PrintManager™ API or CPI verb.
- Change operation
 - Open** When the page descriptor group is opened for change access by a PrintManager* API or CPI verb.
- Operations that are not audited
 - CHGPDGPRF**
Change Print Descriptor Group Profile
 - WRKPDG**
Work with Print Descriptor Group

Operations for Program (*PGM)

This list describes the operations that you can perform against Program (*PGM), and whether those operations are audited.

- Read operation

Activation

Program activation

Call Call program that is not already activated

ADDPGM

Add program to debug

QTEDBGS

Qte Register Debug View API

QTEDBGS

Qte Retrieve Module Views API

// RUN

Run program in S/36 environment

RTVCLSRC

Retrieve CL Source

STRDBG

Start Debug

- Create operation

CRTPGM

Create Program

UPDPGM

Update Program

- Change operation

CHGCSPPGM

Change CSP/AE Program

CHGPGM

Change Program

CHGS36PGMA

Change S/36 Program Attributes

EDTS36PGMA

Edit S/36 Program Attributes

WRKS36PGMA

Work with S/36 Program Attributes

- Operations that are not audited

ANZPGM

Analyze Program

DMPCLPGM

Dump CL Program

DSPCSPOBJ

Display CSP Object

DSPPGM

Display Program

Program Conversion

Machine-initiated conversion for compatibility with the current machine

PRTCMDUSG

Print Command Usage

PRTCSPAPP
Print CSP Application

PRTSQLINF
Print SQL Information

QBNLPGMI
List ILE Program Information API

QCLRPGMI
Retrieve Program Information API

STRCSP
Start CSP Utilities

TRCCSP
Trace CSP Application

WRKOBJCSP
Work with Objects for CSP

WRKPGM
Work with Program

Operations for Panel Group (*PNLGRP)

This list describes the operations that you can perform against Panel Group (*PNLGRP), and whether those operations are audited.

- Read operation

ADDSCHIDX
Add Search Index Entry

QUIOPNDA
Open Panel Group for Display API

QUIOPNPA
Open Panel Group for Print API

QUHDSPH
Display Help API

- Change operation

None

- Operations that are not audited

WRKPNLGRP
Work with Panel Group

Operations for Product Availability (*PRDAVL)

This list describes the operations that you can perform against Product Availability (*PRDAVL), and whether those operations are audited.

- Change operation

WRKSPTPRD
Work with Supported Products, when support is added or removed

- Operations that are not audited

Read No read operations are audited

Operations for Product Definition (*PRDDFN)

This list describes the operations that you can perform against Product Definition (*PRDDFN), and whether those operations are audited.

- Change operation

ADDPRDLICI

Add Product License Information

WRKSPTPRD

Work with Supported Products, when support is added or removed

- Operations that are not audited

Read No read operations are audited

Operations for Product Load (*PRDLOD)

This list describes the operations that you can perform against Product Load (*PRDLOD), and whether those operations are audited.

- Change operation

Change

Product load state, product load library list, product load folder list, primary language

- Operations that are not audited

Read No read operations are audited

Operations for Query Manager Form (*QMFORM)

This list describes the operations that you can perform against Query Manager Form (*QMFORM), and whether those operations are audited.

- Read operation

STRQMORY

Start Query Management Query

RTVQMFORM

Retrieve Query Management Form

Run Run a query

Export Export a Query Management form

Print Print a Query Management form

Print a Query Management report using the form

Use Access the form using option 2, 5, 6, or 9 or function F13 from the DB2 Query Manager and SQL Development Kit for IBM i.

- Change operation

CRTQMFORM

Create Query Management Form

IMPORT

Import Query Management form

Save Save the form using a menu option or a command

Copy Option 3 from the Work with Query Manager Forms function

- Operations that are not audited

Work with

When *QMFORMs are listed in a Work with display

Active Any form operation that is done against the 'active' form.

Operations for Query Manager Query (*QMQRy)

This list describes the operations that you can perform against Query Manager Query (*QMQRy), and whether those operations are audited.

- Read operation

RTVQMQRy

Retrieve Query Manager Query

Run Run Query Manager Query

STRQMQRy

Start Query Manager Query

Export Export Query Manager query

Print Print Query Manager query

Use Access the query using function F13 or option 2, 5, 6, or 9 from the Work with Query Manager queries function

- Change operation

CRTQMQRy

Create Query Management Query

Convert

Option 10 (Convert to SQL) from the Work with Query Manager Queries function

Copy Option 3 from the Work with Query Manager Queries function

Save Save the query using a menu or command

- Operations that are not audited

Work with

When *QMQRys are listed in a Work with display

Active Any query operation that is done against the 'active' query.

Operations for Query Definition (*QRyDFN)

This list describes the operations that you can perform against Query Definition (*QRyDFN), and whether those operations are audited.

- Read operation

ANZQRy

Analyze Query

Change

Change a query using a prompt display presented by WRKQRy or QRy.

Display

Display a query using WRKQRy prompt display

Export Export form using Query Manager

Export Export query using Query Manager

Print Print query definition using WRKQRy prompt display

Print Query Management form

Print Query Management query

Print Query Management report

QRYRUN

Run Query

RTVQMFORM

Retrieve Query Management Form

RTVQMQR

Retrieve Query Management Query

Run Run query using WRKQRY prompt display

Run (Query Management command)

RUNQRY

Run Query

STRQMQR

Start Query Management Query

Submit

Submit a query (run request) to batch using WRKQRY prompt display or Exit This Query prompt display

- Change operation

Change

Save a changed query using the Query/400 licensed program

- Operations that are not audited

Copy Copy a query using option 3 on the "Work with Queries" display

Create Create a query using option 1 on the "Work with Queries" display

Delete Delete a query using option 4 on the "Work with Queries" display

Run Run a query using option 1 on the "Exit this Query" display when creating or changing a query using the Query/400 licensed program; Run a query interactively using PF5 while creating, displaying, or changing a query using the Query/400 licensed program

DLTQRY

Delete a query

Operations for Reference Code Translate Table (*RCT)

This list describes the operations that you can perform against Reference Code Translate Table (*RCT), and whether those operations are audited.

- Read operation

None

- Change operation

None

- Operations that are not audited

None

Operations for Reply List

This list describes the operations that you can perform against Reply List, and whether those operations are audited.

Note: Reply list actions are audited if the action auditing (QAUDLVL) system value or the action auditing (AUDLVL) parameter in the user profile includes *SYSMGT.

- Operations that are audited

ADDRPYLE

Add Reply List Entry

CHGRPYLE

Change Reply List Entry

RMVRPYLE

Remove Reply List Entry

WRKRPYLE

Work with Reply List Entry

- Operations that are not audited

None

Operations for Subsystem Description (*SBSD)

This list describes the operations that you can perform against Subsystem Description (*SBSD), and whether those operations are audited.

- Read operation

ENDSBS

End Subsystem

STRSBS

Start Subsystem

- Change operation

ADDAJE

Add Autostart Job Entry

ADDCMNE

Add Communications Entry

ADDJOBQE

Add Job Queue Entry

ADDPJE

Add Prestart Job Entry

ADDRTGE

Add Routing Entry

ADDWSE

Add Workstation Entry

CHGAJE

Change Autostart Job Entry

CHGCMNE

Change Communications Entry

CHGJOBQE

Change Job Queue Entry

CHGPJE

Change Prestart Job Entry

CHGRTGE

Change Routing Entry

CHGSBSD
Change Subsystem Description

CHGWSE
Change Workstation Entry

RMVAJE
Remove Autostart Job Entry

RMVCMNE
Remove Communications Entry

RMVJOBQE
Remove Job Queue Entry

RMVPJE
Remove Prestart Job Entry

RMVRTGE
Remove Routing Entry

RMVWSE
Remove Workstation Entry

- Operations that are not audited

DSPSBSD
Display Subsystem Description

QWCLASBS
List Active Subsystem API

QWDLSJBQ
List Subsystem Job Queue API

QWDRSBSD
Retrieve Subsystem Description API

WRKSBSD
Work with Subsystem Description

WRKSBS
Work with Subsystem

WRKSBSJOB
Work with Subsystem Job

Operations for Information Search Index (*SCHIDX)

This list describes the operations that you can perform against Information Search Index (*SCHIDX), and whether those operations are audited.

- Read operation

STRSCHIDX
Start Index Search

WRKSCHIDX
Work with Search Index Entry

- Change operation (audited if OBJAUD is *CHANGE or *ALL)

ADDSCHIDX
Add Search Index Entry

CHGSCHIDX
Change Search Index

RMVSDCHIDX

Remove Search Index Entry

- Operations that are not audited

WRKSDCHIDX

Work with Search Index

Operations for Local Socket (*SOCKET)

This list describes the operations that you can perform against Local Socket (*SOCKET), and whether those operations are audited.

- Read operation

connect

Bind a permanent destination to a socket and establish a connection.

DSPLNK

Display Links

givedescriptor

Give File Access API

Qp01GetPathFromFileID

Get Path Name of Object from File ID API

Qp01RenameKeep

Rename File or Directory, Keep New API

Qp01RenameUnlink

Rename File or Directory, Unlink New API

sendmsg

Send a datagram in connectionless mode. Can use multiple buffers.

sendto

Send a datagram in connectionless mode.

WRKLNK

Work with Links

- Change operation

ADDLNK

Add Link

bind Establish a local address for a socket.**CHGAUD**

Change Auditing

CHGAUT

Change Authority

CHGOWN

Change Owner

CHGPGP

Change Primary Group

CHKIN

Check In

CHKOUT

Check Out

- chmod** Change File Authorizations API
- chown** Change Owner and Group API
- givedescriptor** Give File Access API
- link** Create Link to File API
- Qp0lRenameKeep** Rename File or Directory, Keep New API
- Qp0lRenameUnlink** Rename File or Directory, Unlink New API
- RMVLNK** Remove Link
- RNM** Rename
- RST** Restore
- unlink** Remove Link to File API
- utime** Set File Access and Modification Times API
- WRKAUT** Work with Authority
- WRKLNK** Work with Links
- Operations that are not audited
 - close** Close File API
 - Note:** Close is not audited, but if there were a failure or modification in a close scan_related exit program, then an audit record is cut.
 - DSPAUT** Display Authority
 - dup** Duplicate Open File Descriptor API
 - dup2** Duplicate Open File Descriptor to Another Descriptor API
 - fcntl** Perform File Control Command API
 - fstat** Get File Information by Descriptor API
 - fsync** Synchronize Changes to File API
 - ioctl** Perform I/O Control Request API
 - lstat** Get File or Link Information API
 - pathconf** Get Configurable Path Name Variables API
 - read** Read from File API
 - readv** Read from File (Vector) API
 - select** Check I/O Status of Multiple File Descriptors API
 - stat** Get File Information API

takedescriptor

Take File Access API

write Write to File API**writew** Write to File (Vector) API

Operations for Spelling Aid Dictionary (*SPADCT)

This list describes the operations that you can perform against Spelling Aid Dictionary (*SPADCT), and whether those operations are audited.

- Read operation

Verify Spell verify function**Aid** Spell aid function**Hyphenation**

Hyphenation function

Dehyphenation

Dehyphenation function

Synonyms

Synonym function

Base Use dictionary as base when creating another dictionary**Verify** Use as verify dictionary when creating another dictionary**Retrieve**

Retrieve Stop Word List Source

Print Print Stop Word List Source

- Change operation

CRTSPADCT

Create Spelling Aid Dictionary with REPLACE(*YES)

- Operations that are not audited

None

Operations for Spooled Files

This list describes the operations that you can perform against Spooled Files, and whether those operations are audited.

Note: Spooled file actions are audited if the action auditing (QAUDLVL) system value or the action auditing (AUDLVL) parameter in the user profile includes *SPLFDTA.

- Operations that are audited

Access

Each access by any user that is not the owner of the spooled file, including:

- CPYSPLF
- DSPSPLF
- SNDNETSPLF
- SNDTCPSPLF
- STRRMTWTR
- QSPOPNSP API

Change

Changing any of the following spooled file attributes with CHGSPLFA:

- COPIES
- DEV
- FORMTYPE
- RESTART
- PAGERANGE
- OUTQ
- DRAWER
- PAGDFN
- FORMDF
- USRDFNOPT
- USRDFNOBJ
- USRDFNDTA
- EXPDATE
- SAVE

Changing any other spooled file attributes with CHGSPLFA:

Create Creating a spooled file using print operations

Creating a spooled file using the QSPCRTSP API

Delete Deleting a spooled file using any of the following operations:

- Printing a spooled file by a printer or diskette writer
- Clearing the output queue (CLRROUTQ)
- Deleting the spooled file using the DLTSPFLF command or the delete option from a spooled files display
- Deleting spooled files when a job ends (ENDJOB SPLFILE(*YES))
- Deleting spooled files when a print job ends (ENDPJ SPLFILE(*YES))
- Sending a spooled file to a remote system by a remote writer
- Deleting of spooled files that have expired using the DLTEXPSPLF command
- Deleting of spooled files through the operational assist cleanup function

Hold Holding a spooled file by any of the following operations:

- Using the HLDSPLF command
- Using the hold option from a spooled files display
- Printing a spooled file that specifies SAVE(*YES)
- Sending a spooled file to a remote system by a remote writer when the spooled file specifies SAVE(*YES)
- Having a writer hold a spooled file after an error occurs when processing the spooled file

Read Reading a spooled file by a printer or diskette writer

Release

Releasing a spooled file

Restore

Restoring a spooled file

Save Saving a spooled file

Operations for SQL Package (*SQLPKG)

This list describes the operations that you can perform against SQL Package (*SQLPKG), and whether those operations are audited.

- Read operation
 - Run** When *SQLPKG object is run
- Change operation
 - None**
- Operations that are not audited
 - PRTSQLINF**
Print SQL Information

Operations for Service Program (*SRVPGM)

This list describes the operations that you can perform against Service Program (*SRVPGM), and whether those operations are audited.

- Read operation
 - CRTPGM**
An audit entry for each service program used during a CRTPGM command
 - CRTSRVPGM**
An audit entry for each service program used during a CRTSRVPGM command
 - QTEDBGS**
Register Debug View API
 - QTEDBGS**
Retrieve Module Views API
 - RTVBNDSRC**
Retrieve Binder Source
 - RTVCLSRC**
An audit entry for each service program used during a RTVCLSRC command
 - UPDPGM**
An audit entry for each service program used during a UPDPGM command.
 - UPDSRVPGM**
An audit entry for each service program used during a UPDSRVPGM command.
- Create operation
 - CRTSRVPGM**
Create Service Program
 - UPDSRVPGM**
Update Service Program
- Change operation
 - CHGSRVPGM**
Change Service Program
- Operations that are not audited
 - DSPSRVPGM**
Display Service Program
 - PRTSQLINF**
Print SQL Information

- | **Service Program Conversion**
Machine-initiated conversion for compatibility with the current machine
- QBNLSPGM**
List Service Program Information API
- QBNRSPGM**
Retrieve Service Program Information API
- WRKSRVPGM**
Work with Service Program

Operations for Session Description (*SSND)

This list describes the operations that you can perform against Session Description (*SSND), and whether those operations are audited.

No Read or Change operations are audited for the *SSND object type.

Operations for Server Storage Space (*SVRSTG)

This list describes the operations that you can perform against Server Storage Space (*SVRSTG), and whether those operations are audited.

No Read or Change operations are audited for the *SVRSTG object type.

Operations for Stream File (*STMF)

This list describes the operations that you can perform against Stream File (*STMF) objects, and whether those operations are audited.

- Read operation
 - CPY** Copy Object
 - DSPLNK**
Display Object Links
 - givedescriptor**
Give File Access API
 - MOV** Move Object
 - open, open64, QlgOpen, QlgOpen64, Qp0lOpen**
Open File APIs
 - SAV** Save Object
 - WRKLNK**
Work with Object Links
- Change operation
 - ADDLNK**
Add Link
 - CHGAUD**
Change Auditing
 - CHGAUT**
Change Authority
 - CHGOWN**
Change Owner

CHGPGP
Change Primary Group

CHKIN
Check In Object

CHKOUT
Check Out Object

chmod, QlgChmod
Change File Authorizations APIs

chown, QlgChown
Change Owner and Group APIs

CPY Copy Object

creat, creat64, QlgCreat, QlgCreat64
Create New File or Rewrite Existing File APIs

fchmod
Change File Authorizations by Descriptor API

fchown
Change Owner and Group of File by Descriptor API

givedescriptor
Give File Access API

link Create Link to File API

MOV Move Object

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
When opened for write APIs

Qp0lGetPathFromFileID, QlgGetPathFromFileID
Get Path Name of Object from File ID APIs

Qp0lRenameKeep, QlgRenameKeep
Rename File or Directory, Keep New APIs

Qp0lRenameUnlink, QlgRenameUnlink
Rename File or Directory, Unlink New APIs

RMVLNK
Remove Link

RNM Rename Object

RST Restore Object

unlink, QlgUnlink
Remove Link to File APIs

utime, QlgUtime
Set File Access and Modification Times APIs

WRKAUT
Work with Authority

WRKLNK
Work with Links

- Operations that are not audited

close Close File API

DSPAUT Display Authority

dup Duplicate Open File Descriptor API

dup2 Duplicate Open File Descriptor to Another Descriptor API

faccessx Determine file accessibility

fclear, fclear64 Clear a file

fcntl Perform File Control Command API

fpathconf Get Configurable Path Name Variables by Descriptor API

fstat, fstat64 Get File Information by Descriptor APIs

fsync Synchronize Changes to File API

ftruncate, ftruncate64 Truncate File APIs

ioctl Perform I/O Control Request API

lseek, lseek64 Set File Read/Write Offset APIs

lstat, lstat64 Get File or Link Information APIs

pathconf, QlgPathconf Get Configurable Path Name Variables APIs

pread, pread64 Read from Descriptor with Offset APIs

pwrite, pwrite64 Write to Descriptor with Offset APIs

read Read from File API

readv Read from File (Vector) API

select Check I/O Status of Multiple File Descriptors API

stat, stat64, QlgStat, QlgStat64 Get File Information APIs

takedescriptor Take File Access API

write Write to File API

writv Write to File (Vector) API

Operations for Symbolic Link (*SYMLNK)

This list describes the operations that you can perform against symbolic link (*SYMLNK) objects, and whether those operations are audited.

- Read operation
 - CPY** Copy Object

- DSPLNK**
Display Object Links
- MOV** Move Object
- readlink**
Read Value of Symbolic Link API
- SAV** Save Object
- WRKLNK**
Work with Object Links
- Change operation
- CHGOWN**
Change Owner
- CHGPGP**
Change Primary Group
- CPY** Copy Object
- MOV** Move Object
- Qp0IRenameKeep, QlgRenameKeep**
Rename File or Directory, Keep New APIs
- Qp0IRenameUnlink, QlgRenameUnlink**
Rename File or Directory, Unlink New APIs
- RMVLNK**
Remove Link
- RNM** Rename Object
- RST** Restore Object
- symlink, QlgSymlink**
Make Symbolic Link APIs
- unlink, QlgUnlink**
Remove Link to File APIs
- WRKLNK**
Work with Object Links
- Operations that are not audited
- lstat, lstat64, QlgLstat, QlgLstat64**
Link Status APIs

Operations for S/36 Machine Description (*S36)

This list describes the operations that you can perform against S/36 Machine Description (*S36), and whether those operations are audited.

- Read operation
 - None**
- Change operation
 - CHGS36**
Change S/36 configuration
 - CHGS36A**
Change S/36 configuration attributes

SET SET procedure

CRTDEVXXX

When a device is added to the configuration table

DLTDEVD

When a device is deleted from the configuration table

RNMOBJ

Rename device description

- Operations that are not audited

DSPS36

Display S/36 configuration

RTVS36A

Retrieve S/36 Configuration Attributes

STRS36

Start S/36

ENDS36

End S/36

Operations for Table (*TBL)

This list describes the operations that you can perform against Table (*TBL), and whether those operations are audited.

- Read operation

QDCXLATE

Translate character string

QTBXLATE

Translate character string

QLGRTVSS

Retrieve sort sequence table

CRTL

Translation Table during CTRL command

Read Use of Sort Sequence Table when running any command that can specify a sort sequence

- Change operation

None

- Operations that are not audited

WRKTBL

Work with table

Operations for User Index (*USRIDX)

This list describes the operations that you can perform against User Index (*USRIDX), and whether those operations are audited.

- Read operation

QUSRTVUI

Retrieve user index entries API

- Change operation

QUSADDUI

Add User Index Entries API

QUSRMVUI

Remove User Index Entries API

- Operations that are not audited

Access

Direct access to a user index using MI instructions (only allowed for a user domain user index in a library specified in the QALWUSRDMN system value.

QUSRUIAT

Retrieve User Index Attributes API

Operations for User Profile (*USRPRF)

This list describes the operations that you can perform against User Profile (*USRPRF), and whether those operations are audited.

- Read operation

RCLOBJOWN

Reclaim Objects by Owner

- Change operation

CHGPRF

Change Profile

CHGPWD

Change Password

CHGUSRPRF

Change User Profile

CHKPWD

Check Password

DLTUSRPRF

Delete User Profile

GRTUSRAUTGrant User Authority (*to-user-profile*)**QSYCHGPW**

Change Password API

RSTUSRPRF

Restore User Profile

- Operations that are not audited

DSPPGMADP

Display Programs that Adopt

DSPUSRPRF

Display User Profile

GRTUSRAUTGrant User Authority (*from-user-profile*)**PRTPRFINT**

Print Profile Internals

PRTUSRPRF

Print User Profile

QSYCUSRS	Check User Special Authorities API
QSYLOBJA	List Authorized Objects API
QSYLOBJP	List Objects That Adopt API
QSYRUSRI	Retrieve User Information API
RTVUSRPRF	Retrieve User Profile
WRKOBJOWN	Work with Owned Objects
WRKUSRPRF	Work with User Profiles

Operations for User Queue (*USRQ)

This list describes the operations that you can perform against User Queue (*USRQ), and whether those operations are audited.

- No Read or Change operations are audited for the *USRQ object type.
- Operations that are not audited

Access

Direct access to user queues using MI instructions (only allowed for a user domain user queue in a library specified in the QALWUSRDMN system value).

Operations for User Space (*USRSPC)

This list describes the operations that you can perform against User Space (*USRSPC), and whether those operations are audited.

- Read operation

QUSRTVUS

Retrieve User Space API

- Change operation

QUSCHGUS

Change User Space API

QUSCUSAT

Change User Space Attributes API

- Operations that are not audited

Access

Direct access to user space using MI instructions (only allowed for user domain user spaces in libraries specified in the QALWUSRDMN system value).

QUSRUSAT

Retrieve User Space Attributes API

Operations for Validation List (*VLDL)

This list describes the operations that you can perform against Validation List (*VLDL), and whether those operations are audited.

- Read operation
 - QSYFDVLE**
Find Validation List Entry API
- Change operation
 - QSYADVLE**
Add Validation List Entry API
 - QSYCHVLE**
Change Validation List Entry API
 - QSYRMVLE**
Remove Validation List Entry API

Operations for Workstation Customizing Object (*WSCST)

This list describes the operations that you can perform against Workstation Customizing Object (*WSCST), and whether those operations are audited.

- Read operation
 - Vary** When a customized device is varied on
 - RTVWSCST**
Retrieve Workstation Customizing Object Source (only when *TRANSFORM is specified for the device type)
 - SNDTCPSPLF**
Send TCP/IP Spooled File (only when TRANSFORM(*YES) is specified)
 - STRPRTWTR**
Start Printer Writer (only for spooled files that are printed to a customized printer using the host print transform function)
 - STRRMTWTR**
Start Remote Writer (only when output queue is configured with CNNTYPE(*IP) and TRANSFORM(*YES))
 - Print** When output is printed directly (not spooled) to a customized printer using the host print transform function
- Change operation
 - None**
- Operations that are not audited
 - None**

Appendix F. Layout of audit journal entries

This section contains layout information for all entry types with journal code T in the audit (QAUDJRN) journal. These entries are controlled by the action and object auditing you define.

The journal entry layouts described in this appendix are similar to how one can define a physical file using DDS. For instance, a Binary (4) is defined to hold from 1 to 4 digits information with the storage requirement of two bytes, while a Binary (5) holds from 1 to 5 digits information with the storage requirement of 4 bytes. Languages such as RPG use and enforce these definitions. The system writes additional entries to the audit journal for such events as a system IPL or saving the journal receiver. The layouts for these entry types can be found in the Journal management topic.

“Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)” on page 567 contains the layout for fields that are common to all entry types when `OUTFILFMT(*TYPE2)` is specified on the `DSPJRN` command. This layout, which is called `QJORDJE2`, is defined in the `QADSPJR2` file in the `QSYS` library.

“Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)” on page 565 contains the layout for fields that are common to all entry types when `OUTFILFMT(*TYPE4)` is specified on the `DSPJRN` command. This layout, which is called `QJORDJE4`, is defined in the `QADSPJR4` file in the `QSYS` library. The `*TYPE4` output includes all of the `*TYPE2` information, plus information about journal identifiers, triggers, and referential constraints.

Note: `TYPE2` and `*TYPE4` output formats are no longer updated; therefore, it is recommended that you stop using `*TYPE2` and `*TYPE4` formats and use only `*TYPE5` formats.

“Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” on page 564 contains the layout for fields that are common to all entry types when `OUTFILFMT(*TYPE5)` is specified on the `DSPJRN` command. This layout, which is called `QJORDJE5`, is defined in the `QADSPJR5` file in the `QSYS` library. The `*TYPE5` output includes all of the `*TYPE4` information, plus information about the program library, program ASP device name, program ASP device number, receiver, receiver library, receiver ASP device name, receiver ASP device number, arm number, thread ID, address family, remote port, and remote address.

“AD (Auditing Change) journal entries” on page 570 through “ZR (Read of Object) journal entries” on page 703 contain layouts for the model database outfiles provided to define entry-specific data. You can use the `CRTDUPOBJ` command to create any empty output file with the same layout as one of the model database outfiles. You can use the `DSPJRN` command to copy selected entries from the audit journal to the output file for analysis. “Analyzing audit journal entries with query or a program” on page 296 provides examples of using the model database outfiles. See also the Journal management topic.

Note: In these journal entries tables, you might see a blank column under the offset, JE or J4, column. It means there is no model outfile for that audit journal type.

Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)

This table lists all possible values for the fields that are common to all entry types when OUTFILFMT(*TYPE5) is specified on the DSPJRN command.

Table 158. Standard heading fields for audit journal entries. QJORDJE5 Record Format (*TYPE5)

Offset	Field	Format	Description
1	Length of Entry	Zoned(5,0)	Total length of the journal entry including the entry length field.
6	Sequence Number	Char(20)	Applied to each journal entry. Initially set to 1 for each new or restored journal. Optionally, reset to 1 when a new receiver is attached.
26	Journal Code	Char(1)	Always T.
27	Entry Type	Char(2)	See "Audit Journal (QAUDJRN) entry types" on page 568 for a list of entry types and descriptions.
29	Timestamp of Entry	Char(26)	Date and time that the entry was made in SAA timestamp format.
55	Name of Job	Char(10)	The name of the job that caused the entry to be generated.
65	User Name	Char(10)	The user profile name associated with the job ¹ .
75	Job Number	Zoned(6,0)	The job number.
81	Program Name	Char(10)	The name of the program that made the journal entry. This can also be the name of a service program or the partial name of a class file used in a compiled Java program. If an application program or CL program did not cause the entry, the field contains the name of a system-supplied program such as QCMD. The field has the value *NONE if one of the following conditions is true: <ul style="list-style-type: none"> • The program name does not apply to this entry type. • The program name was not available.
91	Program library	Char(10)	Name of the library that contains the program that added the journal entry.
101	Program ASP device	Char(10)	Name of ASP device that contains the program that added the journal entry.
111	Program ASP number	Zoned(5,0)	Number of the ASP that contains the program that added the journal entry.
116	Name of object	Char(10)	Used for journaled objects. Not used for audit journal entries.
126	Objects Library	Char(10)	Used for journaled objects. Not used for audit journal entries.
136	Member Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
146	Count/RRN	Char(20)	Used for journaled objects. Not used for audit journal entries.
166	Flag	Char(1)	Used for journaled objects. Not used for audit journal entries.
167	Commit Cycle identifier	Char(20)	Used for journaled objects. Not used for audit journal entries.
187	User Profile	Char(10)	The name of the current user profile ¹ .
197	System Name	Char(8)	The name of the system.
205	Journal identifier	Char(10)	Used for journaled objects. Not used for audit journal entries.
215	Referential Constraint	Char(1)	Used for journaled objects. Not used for audit journal entries.
216	Trigger	Char(1)	Used for journaled objects. Not used for audit journal entries.
217	Incomplete Data	Char(1)	Used for journaled objects. Not used for audit journal entries.

Table 158. Standard heading fields for audit journal entries (continued). QJORDJE5 Record Format (*TYPE5)

Offset	Field	Format	Description
218	Ignored by APY/ RMVJRNCHG	Char(1)	Used for journaled objects. Not used for audit journal entries.
219	Minimized ESD	Char(1)	Used for journaled objects. Not used for audit journal entries.
220	Object indicator	Char(1)	Used for journaled objects. Not used for audit journal entries.
221	System sequence	Char(20)	A number assigned by the system to each journal entry.
241	Receiver	Char(10)	The name of the receiver holding the journal entry.
251	Receiver library	Char(10)	The name of the library containing the receiver that holds the journal entry.
261	Receiver ASP device	Char(10)	Name of ASP device that contains the receiver.
271	Receiver ASP number	Zoned(5,0)	Number of the ASP that contains the receiver that holds the journal entry.
276	Arm number	Zoned(5,0)	The number of the disk arm that contains the journal entry.
281	Thread identifier	Hex(8)	Identifies the thread within the process that added the journal entry.
289	Thread identifier hex	Char(16)	Displayable hex version of the thread identifier.
305	Address family	Char(1)	The format of the remote address for this journal entry.
306	Remote port	Zoned(5,0)	The port number of the remote address associated with the journal entry.
311	Remote address	Char(46)	The remote address associated with the journal entry.
357	Logical unit of work	Char(39)	Used for journaled objects. Not used for audit journal entries.
396	Transaction ID	Char(140)	Used for journaled objects. Not used for audit journal entries.
536	Reserved	Char(20)	Used for journaled objects. Not used for audit journal entries.
556	Null value indicators	Char(50)	Used for journaled objects. Not used for audit journal entries.
606	Entry specific data length	Binary(5)	Length of the entry specific data.
<p>Note: The three fields beginning at offset 55 make up the system job name. In most cases, the User name field at offset 65 and the User profile name field at offset 187 have the same value. For prestarted jobs, the User profile name field contains the name of the user starting the transaction. For some jobs, both these fields contain QSYS as the user name. The User profile name field in the entry-specific data contains the actual user who caused the entry. If an API is used to exchange user profiles, the User profile name field contains the name of the new (swapped) user profile.</p>			

Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)

This table lists all possible values for the fields that are common to all entry types when OUTFILFMT(*TYPE4) is specified on the DSPJRN command.

Table 159. Standard heading fields for audit journal entries. QJORDJE4 Record Format (*TYPE4)

Offset	Field	Format	Description
1	Length of Entry	Zoned(5,0)	Total length of the journal entry including the entry length field.
6	Sequence Number	Zoned(10,0)	Applied to each journal entry. Initially set to 1 for each new or restored journal. Optionally, reset to 1 when a new receiver is attached.

Table 159. Standard heading fields for audit journal entries (continued). QJORDJE4 Record Format (*TYPE4)

Offset	Field	Format	Description
16	Journal Code	Char(1)	Always T.
17	Entry Type	Char(2)	See "Audit Journal (QAUDJRN) entry types" on page 568 for a list of entry types and descriptions.
19	Timestamp of Entry	Char(26)	Date and time that the entry was made in SAA timestamp format.
45	Name of Job	Char(10)	The name of the job that caused the entry to be generated.
55	User Name	Char(10)	The user profile name associated with the job ¹ .
65	Job Number	Zoned(6,0)	The job number.
71	Program Name	Char(10)	The name of the program that made the journal entry. This can also be the name of a service program or the partial name of a class file used in a compiled Java program. If an application program or CL program did not cause the entry, the field contains the name of a system-supplied program such as QCMD. The field has the value *NONE if one of the following is true: <ul style="list-style-type: none"> • The program name does not apply to this entry type. • The program name was not available.
81	Object Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
91	Library Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
101	Member Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
111	Count/RRN	Zoned(10)	Used for journaled objects. Not used for audit journal entries.
121	Flag	Char(1)	Used for journaled objects. Not used for audit journal entries.
122	Commit Cycle ID	Zoned(10)	Used for journaled objects. Not used for audit journal entries.
132	User Profile	Char(10)	The name of the current user profile ¹ .
142	System Name	Char(8)	The name of the system.
150	Journal Identifier	Char(10)	Used for journaled objects. Not used for audit journal entries.
160	Referential Constraint	Char(1)	Used for journaled objects. Not used for audit journal entries.
161	Trigger	Char(1)	Used for journaled objects. Not used for audit journal entries.
162	(Reserved Area)	Char(8)	
170	Null Value Indicators	Char(50)	Used for journaled objects. Not used for audit journal entries.
220	Entry Specific Data Length	Binary (4)	Length of the entry specific data.
<p>Note: The three fields beginning at offset 45 make up the system job name. In most cases, the User name field at offset 55 and the User profile name field at offset 132 have the same value. For prestarted jobs, the User profile name field contains the name of the user starting the transaction. For some jobs, both these fields contain QSYS as the user name. The User profile name field in the entry-specific data contains the actual user who caused the entry. If an API is used to exchange user profiles, the User profile name field contains the name of the new (swapped) user profile.</p>			

Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)

This table lists all possible values for the fields that are common to all entry types when OUTFILFMT(*TYPE2) is specified on the DSPJRN command.

Table 160. Standard heading fields for audit journal entries. QJORDJE2 Record Format (*TYPE2)

Offset	Field	Format	Description
1	Length of Entry	Zoned(5,0)	Total length of the journal entry including the entry length field.
6	Sequence Number	Zoned(10,0)	Applied to each journal entry. Initially set to 1 for each new or restored journal. Optionally, reset to 1 when a new receiver is attached.
16	Journal Code	Char(1)	Always T.
17	Entry Type	Char(2)	See "Audit Journal (QAUDJRN) entry types" on page 568 for a list of entry types and descriptions.
19	Timestamp	Char(6)	The system date that the entry was made.
25	Time of entry	Zoned(6,0)	The system time that the entry was made.
31	Name of Job	Char(10)	The name of the job that caused the entry to be generated.
41	User Name	Char(10)	The user profile name associated with the job ¹ .
51	Job Number	Zoned(6,0)	The job number.
57	Program Name	Char(10)	The name of the program that made the journal entry. This can also be the name of a service program or the partial name of a class file used in a compiled Java program. If an application program or CL program did not cause the entry, the field contains the name of a system-supplied program such as QCMD. The field has the value *NONE if one of the following is true: <ul style="list-style-type: none"> • The program name does not apply to this entry type. • The program name was not available.
67	Object Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
77	Library Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
87	Member Name	Char(10)	Used for journaled objects. Not used for audit journal entries.
97	Count/RRN	Zoned(10)	Used for journaled objects. Not used for audit journal entries.
107	Flag	Char(1)	Used for journaled objects. Not used for audit journal entries.
108	Commit Cycle ID	Zoned(10)	Used for journaled objects. Not used for audit journal entries.
118	User Profile	Char(10)	The name of the current user profile ¹ .
128	System Name	Char(8)	The name of the system.
136	(Reserved Area)	Char(20)	
¹	The three fields beginning at offset 31 make up the system job name. In most cases, the <i>User name</i> field at offset 41 and the <i>User profile name</i> field at offset 118 have the same value. For prestarted jobs, the <i>User profile name</i> field contains the name of the user starting the transaction. For some jobs, both these fields contain QSYS as the user name. The <i>User profile name</i> field in the entry-specific data contains the actual user who caused the entry. If an API is used to exchange user profiles, the <i>User profile name</i> field contains the name of the new (swapped) user profile.		

Audit Journal (QAUDJRN) entry types

This table introduces all available entry types for the audit journal.

Table 161. Audit Journal (QAUDJRN) entry types

Entry type	Description
AD	Auditing changes
AF	Authority failure
AP	Obtaining adopted authority
AU	Attribute changes
CA	Authority changes
CD	Command string audit
CO	Create object
CP	User profile changed, created, or restored
CQ	Change of *CRQD object
CU	Cluster Operations
CV	Connection verification
CY	Cryptographic Configuration
DI	Directory Server
DO	Delete object
DS	DST security password reset
EV	System environment variables
GR	Generic record
GS	Socket description was given to another job
IM	Intrusion monitor
IP	Interprocess Communication
IR	IP Rules Actions
IS	Internet security management
JD	Change to user parameter of a job description
JS	Actions that affect jobs
KF	Key ring file
LD	Link, unlink, or look up directory entry
ML	Office services mail actions
NA	Network attribute changed
ND	APPN directory search filter violation
NE	APPN end point filter violation
OM	Object move or rename
OR	Object restore
OW	Object ownership changed
O1	(Optical Access) Single File or Directory
O2	(Optical Access) Dual File or Directory
O3	(Optical Access) Volume

Table 161. Audit Journal (QAUDJRN) entry types (continued)

Entry type	Description
PA	Program changed to adopt authority
PG	Change of an object's primary group
PO	Printed output
PS	Profile swap
PW	Invalid password
RA	Authority change during restore
RJ	Restoring job description with user profile specified
RO	Change of object owner during restore
RP	Restoring adopted authority program
RQ	Restoring a *CRQD object
RU	Restoring user profile authority
RZ	Changing a primary group during restore
SD	Changes to system distribution directory
SE	Subsystem routing entry changed
SF	Actions to spooled files
SG	Asynchronous Signals
SK	Secure sockets connections
SM	Systems management changes
SO	Server security user information actions
ST	Use of service tools
SV	System value changed
VA	Changing an access control list
VC	Starting or ending a connection
VF	Closing server files
VL	Account limit exceeded
VN	Logging on and off the network
VO	Validation list actions
VP	Network password error
VR	Network resource access
VS	Starting or ending a server session
VU	Changing a network profile
VV	Changing service status
X0	Network Authentication
X1	Identify Token
XD	Directory server extension
YC	DLO object accessed (change)
YR	DLO object accessed (read)
ZC	Object accessed (change)
ZR	Object accessed (read)

AD (Auditing Change) journal entries

This table provides the format of the AD (Auditing Change) journal entries.

Table 162. AD (Auditing Change) journal entries. QASYADJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	<p>D CHGDLOAUD command</p> <p>O CHGOBJAUD or CHGAUD command</p> <p>S The scan attribute was changed using CHGATR command or the Qp0lSetAttr API, or when the object was created.</p> <p>U CHGUSRAUD command</p>
157	225	611	Object Name	Char(10)	Name of the object for which auditing was changed.
167	235	621	Library Name	Char(10)	Name of the library for the object.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Object Audit Value	Char(10)	If the entry type is D, O, or U, the field contains the audit value specified. If the entry type is S, the field contains the scan attribute value.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = Audit commands for this user.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = Write an audit record when this user creates an object.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = Write an audit record when this user deletes an object.
198	266	652	CHGUSRAUD *JOBDA	Char(1)	Y = Write an audit record when this user changes a job.
199	267	653	CHGUSRAUD *OBJMGT	Char(1)	Y = Write an audit record when this user moves or renames an object.
200	268	654	CHGUSRAUD *OFCSR	Char(1)	Y = Write an audit record when this user performs office functions.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = Write an audit record when this user obtains authority through adopted authority.
202	270	656	CHGUSRAUD *SAVRST	Char(1)	Y = Write an audit record when this user saves or restores objects.
203	271	657	CHGUSRAUD *SECURITY	Char(1)	Y = Write an audit record when this user performs security-relevant actions.
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = Write an audit record when this user performs service functions.
205	273	659	CHGUSRAUD *SPLFDA	Char(1)	Y = Write an audit record when this user manipulates spooled files.

Table 162. AD (Auditing Change) journal entries (continued). QASYADJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = Write an audit record when this user makes systems management changes.
207	275	661	CHGUSRAUD *OPTICAL	Char (1)	Y = Write an audit record when this user accesses optical devices.
208	276	662	CHGUSRAUD *AUTFAIL	Char(1)	Y = Write an audit record when this user has an authorization failure.
		663	CHGUSRAUD *JOBBAS	Char(1)	Y = Write an audit record when this user performs a job base function.
		664	CHGUSRAUD *JOBCHGUSR	Char(1)	Y = Write an audit record when this user changes a thread's active user profile or its group file.
		665	CHGUSRAUD *NETBAS	Char(1)	Y = Write an audit record when this user performs network base functions.
		666	CHGUSRAUD *NETCLU	Char(1)	Y = Write an audit record when this user performs cluster or cluster resource group functions.
		667	CHGUSRAUD *NETCMN	Char(1)	Y = Write an audit record when this user performs network communications functions.
		668	CHGUSRAUD *NETFAIL	Char(1)	Y = Write an audit record when this user has a network failure.
		669	CHGUSRAUD *NETSCK	Char(1)	Y = Write an audit record when this user performs sockets tasks.
		670	CHGUSRAUD *PGMFAIL	Char(1)	Y = Write an audit record when this user has a program failure.
		671	CHGUSRAUD *PRTDTA	Char(1)	Y = Write an audit record when this user performs a print function with parameter SPOOL(*NO).
		672	CHGUSRAUD *SECCFG	Char(1)	Y = Write an audit record when this user performs security configuration.
		673	CHGUSRAUD *SECDIRSRV	Char(1)	Y = Write an audit record when this user makes changes or updates using directory service functions.
		674	CHGUSRAUD *SECIPC	Char(1)	Y = Write an audit record when this user makes changes to interprocess communications.
		675	CHGUSRAUD *SECNAS	Char(1)	Y = Write an audit record when this user performs network authentication service actions.
		676	CHGUSRAUD *SECRUN	Char(1)	Y = Write an audit record when this user performs security run time functions.
		677	CHGUSRAUD *SECCKD	Char(1)	Y = Write an audit record when this user performs socket descriptor functions.
		678	CHGUSRAUD *SECVFY	Char(1)	Y = Write an audit record when this user uses verification functions.
		679	CHGUSRAUD *SECVLDL	Char(1)	Y = Write an audit record when this user manipulates validation lists.
		680	(Reserved Area)	Char(19)	

Table 162. AD (Auditing Change) journal entries (continued). QASYADJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
227	295	681	DLO Name	Char(12)	Name of the DLO object for which auditing was changed.
239	307	693	(Reserved Area)	Char(8)	
247	315	701	Folder Path	Char(63)	Path of the folder.
310			(Reserved Area)	Char(20)	
	378	764	(Reserved Area)	Char(18)	
	396	782	Object Name Length ¹	Binary(4)	The length of the object name.
330	398	784	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
334	402	788	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
336	404	790	Object Name Language ID ¹	Char(3)	The language ID for the object name.
339	407	793	(Reserved area)	Char(3)	
342	410	796	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
358	426	812	Object File ID ^{1,2}	Char(16)	The file ID of the object.
374	442	828	Object Name ¹	Char(512)	The name of the object.
	954	1340	Object File ID ¹	Char(16)	The file ID of the object.
	970	1356	ASP Name ⁵	Char(10)	The name of the ASP device.
	980	1366	ASP Number ⁵	Char(5)	The number of the ASP device.
	985	1371	Path Name CCSID ¹	Binary(5)	The coded character set identifier for the path name.
	989	1375	Path Name Country or Region ID ¹	Char(2)	The Country or Region ID for the path name.
	991	1377	Path Name Language ID ¹	Char(3)	The language ID for the path name.
	994	1380	Path Name Length ¹	Binary(4)	The length of the path name.
	996	1382	Path Name Indicator ¹	Char(1)	<p>Path name indicator:</p> <p>Y The Path Name field contains complete absolute path name for the object.</p> <p>N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.</p>

Table 162. AD (Auditing Change) journal entries (continued). QASYADJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	997	1383	Relative Directory File ID ^{1, 3}	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1013	1399	Path Name ^{1, 4}	Char(5002)	The path name of the object.
<p>¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.</p> <p>² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.</p> <p>³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.</p> <p>⁴ This is a variable length field. The first two bytes contain the length of the path name.</p> <p>⁵ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.</p>					

AF (Authority Failure) journal entries

This table provides the format of the AF (Authority Failure) journal entries.

Table 163. AF (Authority Failure) journal entries. QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 163. AF (Authority Failure) journal entries (continued). QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Violation Type ¹	Char(1)	<p>A Not authorized to object</p> <p>B Restricted instruction</p> <p>C Validation failure (see J5 offset 639)</p> <p>D Use of unsupported interface, object domain failure</p> <p>E Hardware storage protection error, program constant space violation</p> <p>F ICAPI authorization error</p> <p>G ICAPI authentication error</p> <p>H Scan exit program action (see J5 offset 639)</p> <p>I⁷ System Java inheritance not allowed</p> <p>J Submit job profile error</p> <p>K Special authority violation</p> <p>N Profile token not a regenerable token</p> <p>O Optical Object Authority Failure</p> <p>P Profile swap error</p> <p>R Hardware protection error</p> <p>S Default sign-on attempt</p> <p>T Not authorized to TCP/IP port</p> <p>U User permission request not valid</p> <p>V Profile token not valid for generating new profile token</p> <p>W Profile token not valid for swap</p> <p>X System violation — see J5 offset 723 for violation codes</p> <p>Y Not authorized to the current JUID field during a clear JUID operation.</p> <p>Z Not authorized to the current JUID field during a set JUID operation.</p>
157	225	611	Object Name ^{1, 5, 12, 17}	Char(10)	The name of the object.
167	235	621	Library Name ¹³	Char(10)	The name of the library where the object is stored or the Licensed Internal Code fix number that failed to apply. ¹¹
177	245	631	Object Type ^{14, 17}	Char(8)	The type of object.

Table 163. AF (Authority Failure) journal entries (continued). QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
185	253	639	Validation Error Action	Char(1)	<p>Action taken after validation error detected, set only if the violation type (J5 offset 610) is C or H.</p> <p>A The translation of the object was not attempted or it failed. The QALWOBJRST system value setting allowed the object to be restored. The user doing the restore did not have *ALLOBJ special authority and the system security level is set to 10, 20, or 30. Therefore, all authorities to the object were retained.</p> <p>B The translation of the object was not attempted or it failed. The QALWOBJRST system value setting allowed the object to be restored. The user doing the restore did not have *ALLOBJ special authority and the system security level is set to 40 or above. Therefore, all authorities to the object were revoked.</p> <p>C The translation of the object was successful. The translated copy was restored on the system.</p> <p>D The translation of the object was not attempted or it failed. The QALWOBJRST system value setting allowed the object to be restored. The user doing the restore had *ALLOBJ special authority. Therefore, all authorities to the object were retained.</p> <p>E System install time error detected.</p> <p>F The object was not restored because the signature is not i5/OS format.</p> <p>G Unsigned system or inherit state object found when checking system.</p> <p>H Unsigned user state object found when checking system.</p> <p>I Mismatch between object and its signature found when checking system.</p> <p>J IBM certificate not found when checking system.</p> <p>K Invalid signature format found when checking system.</p> <p>M Scan exit program modified the object that was scanned</p> <p>X Scan exit program wanted object marked as having a scan failure</p>
186	254	640	Job Name	Char(10)	The name of the job.

Table 163. AF (Authority Failure) journal entries (continued). QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
196	264	650	User Name	Char(10)	The job user name.
206	274	660	Job Number	Zoned(6,0)	The job number.
212	280	666	Program Name	Char(10)	The name of the program.
222	290	676	Program Library	Char(10)	The name of the library where the program is found.
232	300	686	User Profile ²	Char(10)	The name of the user that caused the authority failure.
242	310	696	Workstation Name	Char(10)	The name of the workstation or workstation type.
252	320	706	Program Instruction Number	Zoned(7,0)	The instruction number of the program.
259	327	713	Field name	Char(10)	The name of the field.
269	337	723	Operation Violation Code	Char(3)	The type of operation violation that occurred, set only if the violation type (J5 offset 610) is X. AAC Not authorized to use SST Advanced Analysis Command. HCA Service tool user profile not authorized to perform hardware configuration operation (QYHCHCOP). LIC LIC indicates that a Licensed Internal Code fix was not applied because of a signature violation. SFA Not authorized to activate the environment attribute for system file access. CMD An attempt was made to use a command that has been disabled by a system administrator.
272	340	726	Office User	Char(10)	The name of the office user.
282	350	736	DLO Name	Char(12)	The name of the document library object.
294	362	748	(Reserved Area)	Char(8)	
302	370	756	Folder Path ^{15, 16}	Char(63)	The path of the folder.
365	433	819	Office on Behalf of User	Char(10)	User working on behalf of another user.
375			(Reserved Area)	Char(20)	
	443	829	(Reserved Area)	Char(18)	
	461	847	Object Name Length ³	Binary(4)	The length of the object name.
395	463	849	Object Name CCSID ³	Binary(5)	The coded character set identifier for the object name.

Table 163. AF (Authority Failure) journal entries (continued). QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
399	467	853	Object Name Country or Region ID ³	Char(2)	The Country or Region ID for the object name.
401	469	855	Object Name Language ID ³	Char(3)	The language ID for the object name.
404	472	858	(Reserved area)	Char(3)	
407	475	861	Parent File ID ^{3,4}	Char(16)	The file ID of the parent directory.
423	491	877	Object File ID ^{3,4}	Char(16)	The file ID of the object.
439	507	893	Object Name ^{3,6}	Char(512)	The name of the object.
	1019	1405	Object File ID ³	Char(16)	The file ID of the object.
	1035	1421	ASP Name ¹⁰	Char(10)	The name of the ASP device.
	1045	1431	ASP Number ¹⁰	Char(5)	The number of the ASP device.
	1050	1436	Path Name CCSID ³	Binary(5)	The coded character set identifier for the path name.
	1054	1440	Path Name Country or Region ID ³	Char(2)	The Country or Region ID for the path name.
	1056	1442	Path Name Language ID ³	Char(3)	The language ID for the path name.
	1059	1445	Path Name Length ³	Binary(4)	The length of the path name.
	1061	1447	Path Name Indicator ³	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	1062	1448	Relative Directory File ID ^{3,8}	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ⁸
	1078	1464	Path Name ^{3,9}	Char(5002)	The path name of the object.
		6466	ASP Program Library Name	Char(10)	ASP name for program library
		6476	ASP Program Library Number	Char(5)	ASP number for program library

Table 163. AF (Authority Failure) journal entries (continued). QASYAFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1					When the violation type is for description G, the object name contains the name of the *SRVPGM that contained the exit that detected the error. For more information about the violation types, see "Security auditing journal entries" on page 269.
2					This field contains the name of the user that caused the entry. QSYS might be the user for the following entries: <ul style="list-style-type: none"> • offsets 41 and 118 for *TYPE2 records • offsets 55 and 132 for *TYPE4 records • offsets 65 and 187 for *TYPE5 records
3					These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.
4					An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
5					When the violation type is T, the object name contains the TCP/IP port the user is not authorized to use. The value is left justified and blank filled. The object library and object type fields will be blank.
6					When the violation type is O, the optical object name is contained in the integrated file system object name field. The Country or Region ID, language ID, parent file ID, and object file ID fields will all contain blanks.
7					The Java class object being created can not extend its base class because the base class has system Java attributes.
8					If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.
9					This is a variable length field. The first two bytes contain the length of the path name.
10					If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.
11					When the violation type is X and the Operation Violation code value is LIC, this indicates that a Licensed Internal Code fix was not applied because of a signature violation. This field will contain the Licensed Internal Code fix number that failed to apply.
12					When the violation type is K, the object name contains the name of the command or program that detected the error. If the command has several alternative names, the command name in the audit record might not match the specific command name used but will be one of the equivalent alternatives. A special value of *INSTR indicates that a machine instruction detected the error.
13					When the violation type is K, the library name contains the name of the program's library or *N for the command's library that detected the error.
14					When the violation type is K, the object type contains the object type of the command or program that detected the error.
15					When the violation type is K, the Folder Path might contain the full API name of the API or exit point name that detected the error.
16					When the violation type is X and the Operation Violation Code is AAC, the Folder Path will contain the 30 character Advanced Analysis Command name.
17					When the object type is *LIC and the object library is *N, the object name is a Licensed Internal Code Ru name.

AP (Adopted Authority) journal entries

This table provides the format of the AP (Adopted Authority) journal entries.

Table 164. AP (Adopted Authority) journal entries. QASYAPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	S Start E End A Adopted authority used during program activation
157	225	611	Object Name	Char(10)	The name of the program, service program, or SQL package
167	235	621	Library Name	Char(10)	The name of the library.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Owning User Profile	Char(10)	The name of the user profile whose authority is adopted.
195	263	649	Object File ID	Char(16)	The file ID of the object.
	279	665	ASP Name ¹	Char(10)	The name of the ASP device.
	289	675	ASP Number ¹	Char(5)	The number of the ASP device.
¹ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.					

AU (Attribute Changes) journal entries

This table provides the format of the AU (Attribute Changes) journal entries.

Table 165. AU (Attribute Changes) journal entries. QASYAUJ5 Field Description File

Offset		Field	Format	Description
J5				
610		Entry type	Char(1)	The type of entry. E EIM configuration attributes
611		Action	Char(3)	Action CHG Attributes changed
614		Name	Char(100)	Attribute name
714		New Value Length	Binary(4)	New value length
716		New Value CCSID	Binary(5)	New value CCSID

Table 165. AU (Attribute Changes) journal entries (continued). QASYAUJ5 Field Description File

Offset		Field	Format	Description
J5				
720		New Value Country or Region ID	Char(2)	New value Country or Region ID
722		New Value Language ID	Char(3)	New value language ID
725		New Value	Char(2002) ¹	New value
2727		Old Value Length	Binary(4)	Old value length
2729		Old Value CCSID	Binary(5)	Old value CCSID
2733		Old Value Country or Region ID	Char(2)	Old value Country or Region ID
2735		Old Value Language ID	Char(3)	Old value language ID
2738		Old Value	Char(2002) ¹	Old value
1 This is a variable length field. The first two bytes contain the length of the field.				

CA (Authority Changes) journal entries

This table provides the format of the CA (Authority Changes) journal entries.

Table 166. CA (Authority Changes) journal entries. QASYCAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Changes to authority
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	User Name	Char(10)	The name of the user profile whose authority is being granted or revoked.
195	263	649	Authorization List Name	Char(10)	The name of the authorization list.
					Authorities granted or removed:
205	273	659	Object Existence	Char(1)	Y *OBJEXIST
206	274	660	Object Management	Char(1)	Y *OBJMGT

Table 166. CA (Authority Changes) journal entries (continued). QASYCAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
207	275	661	Object Operational	Char(1)	Y *OBJOPR
208	276	662	Authorization List Management	Char(1)	Y *AUTLMGT
209	277	663	Authorization List	Char(1)	Y *AUTL public authority
210	278	664	Read Authority	Char(1)	Y *READ
211	279	665	Add Authority	Char(1)	Y *ADD
212	280	666	Update Authority	Char(1)	Y *UPD
213	281	667	Delete Authority	Char(1)	Y *DLT
214	282	668	Exclude Authority	Char(1)	Y *EXCLUDE
215	283	669	Execute Authority	Char(1)	Y *EXECUTE
216	284	670	Object Alter Authority	Char(1)	Y *OBJALTER
217	285	671	Object Reference Authority	Char(1)	Y *OBJREF
218	286	672	(Reserved Area)	Char(4)	
222	290	676	Command Type	Char(3)	The type of command used. GRT Grant RPL Grant with replace RVK Revoke USR GRTUSRAUT operation
225	293	679	Field name	Char(10)	The name of the field.
235	303		(Reserved Area)	Char(10)	
		689	Object Attribute	Char(10)	The attribute of the object.
245	313	699	Office User	Char(10)	The name of the office user.
255	323	709	DLO Name	Char(12)	The name of the DLO.
267	335	721	(Reserved Area)	Char(8)	
275	343	729	Folder Path	Char(63)	The path of the folder.
338	406	792	Office on Behalf of User	Char(10)	User working on behalf of another user.
348	416	802	Personal Status	Char(1)	Y Personal status changed

Table 166. CA (Authority Changes) journal entries (continued). QASYCAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
349	417	803	Access Code	Char(1)	A Access code added R Access code removed
350	418	804	Access Code	Char(4)	Access code.
354			(Reserved Area)	Char(20)	
	422	808	(Reserved Area)	Char(18)	
	440	826	Object Name Length ¹	Binary(4)	The length of the object name.
374	442	828	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
378	446	832	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
380	448	834	Object Name Language ID ¹	Char(3)	The language ID for the object name.
383	451	837	(Reserved area)	Char(3)	
386	454	840	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
402	470	856	Object File ID ^{1,2}	Char(16)	The file ID of the object.
418	486	872	Object Name ¹	Char(512)	The name of the object.
	998	1384	Object File ID	Char(16)	The file ID of the object.
	1014	1400	ASP Name ⁵	Char(10)	The name of the ASP device.
	1024	1410	ASP Number ⁵	Char(5)	The number of the ASP device.
	1029	1415	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	1033	1419	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	1035	1421	Path Name Language ID	Char(3)	The language ID for the path name.
	1038	1424	Path Name Length	Binary(4)	The length of the path name.
	1040	1426	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.

Table 166. CA (Authority Changes) journal entries (continued). QASYCAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1041	1427	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1057	1443	Path Name ⁴	Char(5002)	The path name of the object.
<p>¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.</p> <p>² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.</p> <p>³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.</p> <p>⁴ This is a variable length field. The first two bytes contain the length of the path name.</p> <p>⁵ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.</p>					

CD (Command String) journal entries

This table provides the format of the CD (Command String) journal entries.

Table 167. CD (Command String) journal entries. QASYCDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. C Command run L OCL statement O Operator control command P S/36 procedure S Command run after command substitution took place U Utility control statement
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Run from a CL program	Char(1)	Y Yes N No

Table 167. CD (Command String) journal entries (continued). QASYCDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
186	254	640	Command String	Char(6000)	The command that was run, with parameters.
		6640	ASP Name for Command Library	Char(10)	ASP name for command library
		6650	ASP Number for Command Library	Char(5)	ASP number for command library

CO (Create Object) journal entries

This table provides the format of the CO (Create Object) journal entries.

Table 168. CO (Create Object) journal entries. QASYCOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. N Create of new object R Replacement of existing object
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library the object is in.
177	245	631	Object Type	Char(8)	The type of object.
185	253		(Reserved Area)	Char(20)	
		639	Object Attribute	Char(10)	The attribute of the object.
		649	(Reserved Area)	Char(10)	
205	273	659	Office User	Char(10)	The name of the office user.
215	283	669	DLO Name	Char(12)	The name of the document library object created.
227	295	681	(Reserved Area)	Char(8)	
235	303	689	Folder Path	Char(63)	The path of the folder.
298	366	752	Office on Behalf of User	Char(10)	User working on behalf of another user.
308			(Reserved Area)	Char(20)	

Table 168. CO (Create Object) journal entries (continued). QASYCOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID ¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID ^{1,2}	Char(16)	The file ID of the object.
372	440	826	Object Name ¹	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name ⁵	Char(10)	The name of the ASP device.
	978	1364	ASP Number ⁵	Char(5)	The number of the ASP device.
	983	1369	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	987	1373	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the path name.
	992	1378	Path Name Length	Binary(4)	The length of the path name.
	994	1380	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	995	1381	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1011	1397	Path Name ⁴	Char(5002)	The path name of the object.

Table 168. CO (Create Object) journal entries (continued). QASYCOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1					These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.
2					An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
3					If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.
4					This is a variable length field. The first 2 bytes contain the length of the path name.
5					If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.

CP (User Profile Changes) journal entries

This table provides the format of the CP (User Profile Changes) journal entries.

Table 169. CP (User Profile Changes) journal entries. QASYCPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change to a user profile
157	225	611	User Profile Name	Char(10)	The name of the user profile that was changed.
167	235	621	Library Name	Char(10)	The name of the library.
177	245	631	Object Type	Char(8)	The type of object.
185	256	639	Command Name	Char(3)	The type of command used. CRT CRTUSRPRF CHG CHGUSRPRF RST RSTUSRPRF DST QSECOFR password reset using DST RPA QSYRESPI API
188	256	642	Password Changed	Char(1)	Y Password changed
189	257	643	Password *NONE	Char(1)	Y Password is *NONE.
190	258	644	Password Expired	Char(1)	Y Password expired is *YES N Password expired is *NO

Table 169. CP (User Profile Changes) journal entries (continued). QASYCPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
191	259	645	All Object Special Authority	Char(1)	Y *ALLOBJ special authority
192	260	646	Job Control Special Authority	Char(1)	Y *JOBCTL special authority
193	261	647	Save System Special Authority	Char(1)	Y *SAVSYS special authority
194	262	648	Security Administrator Special Authority	Char(1)	Y *SECADM special authority
195	263	649	Spool Control Special Authority	Char(1)	Y *SPLCTL special authority
196	264	650	Service Special Authority	Char(1)	Y *SERVICE special authority
197	265	651	Audit Special Authority	Char(1)	Y *AUDIT special authority
198	266	652	System Configuration Special Authority	Char(1)	Y *IOSYSCFG special authority
199	267	653	(Reserved Area)	Char(13)	
212	280	666	Group Profile	Char(10)	The name of a group profile.
222	290	676	Owner	Char(10)	Owner of objects created as a member of a group profile.
232	300	686	Group Authority	Char(10)	Group profile authority.
242	310	696	Initial Program	Char(10)	The name of the user's initial program.
252	320	706	Initial Program Library	Char(10)	The name of the library where the initial program is found.
262	330	716	Initial Menu	Char(10)	The name of the user's initial menu.
272	340	726	Initial Menu Library	Char(10)	The name of the library where the initial menu is found.
282	350	736	Current Library	Char(10)	The name of the user's current library.
292	360	746	Limited Capabilities	Char(10)	The value of limited capabilities parameter.
302	370	756	User Class	Char(10)	The user class of the user.
312	380	766	Priority Limit	Char(1)	The value of the priority limit parameter.
313	381	767	Profile Status	Char(10)	User profile status.
323	391	777	Group Authority Type	Char(10)	The value of the GRPAUTTYP parameter.

Table 169. CP (User Profile Changes) journal entries (continued). QASYCPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
333	401	787	Supplemental Group Profiles	Char(150)	The names of up to 15 supplemental group profiles for the user.
483	551	937	User Identification	Char(10)	The uid for the user.
493	561	947	Group Identification	Char(10)	The gid for the user.
503	571	957	Local Password Management	Char(10)	The value of the LCLPWDMGT parameter.
		967	Password Composition Conformance	Char(10)	Indicates whether the new password conforms to the password composition rules. *PASSED Checked and conforms. *SYSVAL Checked but does not conform because of a system value based rule. *EXITPGM Checked but does not conform because of an exit program response. *NONE Not checked; *NONE was specified for the new password. *NOCHECK Not checked; password was changed. This field has meaning only when the Password Changed field contains a Y.
		977	Password Expiration Interval	Char(7)	Specifies the value that the password expiration interval has been changed to. *NOMAX No expiration interval. *SYSVAL The system value QPWDEXPITV is used. number The size of the expiration interval in days.
		984	Block Password Change	Char(10)	Specifies the value that the block password change has been changed to. *SYSVAL The system value QPWDCHGBLK is used. *NONE No block period. 1-99 Blocked hours.

Table 169. CP (User Profile Changes) journal entries (continued). QASYCPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		994	User expiration date	Char(7)	Specifies the date when the user profile expires (CYYMMDD). The user profile is automatically disabled or deleted on this date.

CQ (*CRQD Changes) journal entries

This table provides the format of the CQ (*CRQD Changes) journal entries.

Table 170. CQ (*CRQD Changes) journal entries. QASYCQJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change to a *CRQD object
157	225	611	Object Name	Char(10)	The name of the object that was changed.
167	235	621	Library Name	Char(10)	The name of the object library.
177	245	631	Object Type	Char(8)	The type of object.
		639	ASP Name	Char(10)	ASP name for CRQD library
		649	ASP Number	Char(5)	ASP number for CRQD library

CU (Cluster Operations) journal entries

This table provides the format of the CU (Cluster Operations) journal entries.

Table 171. CU (Cluster Operations) journal entries. QASYCUJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. M Cluster control operation R Cluster Resource Group (*GRP) management operation

Table 171. CU (Cluster Operations) journal entries (continued). QASYCUJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	225	611	Entry Action	Char(3)	The type of action. ADD Add CRT Create DLT Delete DST Distribute END End FLO Fail over LST List information RMV Remove RSC Report state change STR Start SWT Switch UPC Update attributes
	228	614	Status	Char(3)	The status of the request. ABN The request ended abnormally AUT Authority Failure, *IOSYSCFG is required END The request ended successfully STR The request was started
	231	617	CRG Object Name	Char(10)	The Cluster Resource Group object name. Note: This value is filled in when the entry type is R.
	241	627	CRG Library Name	Char(10)	The Cluster Resource Group object library. Note: This value is filled in when the entry type is R.
	251	637	Cluster Name	Char(10)	The name of the cluster.
	261	647	Node ID	Char(8)	The node ID.
	269	655	Source Node ID	Char(8)	The source node ID.
	277	663	Source User Name	Char(10)	Name of the source system user that initiated the request.
	287	673	User Queue Name	Char(10)	Name of the user queue where responses are sent.
	297	683	User Queue Library	Char(10)	The user queue library.
		693	ASP Name	Char(10)	ASP name for user queue library
		703	ASP Number	Char(5)	ASP number for user queue library

CV (Connection Verification) journal entries

This table provides the format of the CV (Connection Verification) journal entries.

Table 172. CV (Connection Verification) journal entries. QASYCVJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. C Connection established E Connection ended R Connection rejected
	225	611	Action	Char(1)	Action taken for the connection type. " " Connection established or ended normally. Used for Entry Type C or E. A Peer was not authenticated. Used for Entry Type E or R. C No response from the authentication server. Used for Entry Type R. L LCP configuration error. Used for Entry Type R. N NCP configuration error. Used for Entry Type R. P Password is not valid. Used for Entry Type E or R. R Authentication was rejected by peer. Used for Entry Type R. T L2TP configuration error. Used for Entry Type E or R. U User is not valid. Used for Entry Type E or R.
	226	612	Point to Point Profile Name	Char(10)	The point-to-point profile name.
	236	622	Protocol	Char(10)	The type of entry. L2TP Layer Two Tunneling protocol PPP Point-to-Point protocol. SLIP Serial Line Internet Protocol.

Table 172. CV (Connection Verification) journal entries (continued). QASYCVJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	246	632	Local Authentication Method	Char(10)	The type of entry. CHAP Challenge Handshake Authentication Protocol. PAP Password Authentication Protocol. SCRIPT Script method.
	256	642	Remote Authentication Method	Char(10)	The type of entry. CHAP Challenge Handshake Authentication Protocol. PAP Password Authentication Protocol. RADIUS Radius method. SCRIPT Script method.
	266	652	Object Name	Char(10)	The *VLDL object name.
	276	662	Library Name	Char(10)	The *VLDL object library name.
	286	672	*VLDL User Name	Char(100)	The *VLDL user name.
	386	772	Local IP Address	Char(40)	The local IP address.
	426	812	Remote IP Address	Char(40)	The remote IP address.
	466	852	IP Forwarding	Char(1)	The type of entry. Y IP forwarding is on. N IP forwarding is off.

Table 172. CV (Connection Verification) journal entries (continued). QASYCVJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	467	853	Proxy ARP	Char(1)	The type of entry. Y Proxy ARP is enabled. N Proxy ARP is not enabled.
	468	854	Radius Name	Char(10)	The AAA profile name.
	478	864	Authenticating IP Address	Char(40)	The authenticating IP address.
	518	904	Account Session ID	Char(14)	The account session ID.
	532	918	Account Multi-Session ID	Char(14)	The account multi-session ID.
	546	932	Account Link Count	Binary(4)	The account link count.
	548	934	Tunnel Type	Char(1)	The tunnel type: 0 Not tunneled 3 L2TP 6 AH 9 ESP
	549	935	Tunnel Client Endpoint	Char(40)	Tunnel client endpoint.
	589	975	Tunnel Server Endpoint	Char(40)	Tunnel server endpoint.
	629	1015	Account Session Time	Char(8)	The account session time. Used for Entry Type E or R.
	637	1023	Reserved	Binary(4)	Always zero
		1025	ASP Name	Char(10)	ASP name for validation list library
		1035	ASP Number	Char(5)	ASP number for validation list library

CY (Cryptographic Configuration) journal entries

This table provides the format of the CY (Cryptographic Configuration) journal entries.

Table 173. CY (Cryptographic Configuration) journal entries. QASYCYJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 173. CY (Cryptographic Configuration) journal entries (continued). QASYCYJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	224	610	Entry Type	Char(1)	The type of entry. A Cryptographic Coprocessor Access Control Function F Cryptographic Coprocessor Facility Control Function K Cryptographic Services Master Key Function M Cryptographic Coprocessor Master Key Function
	225	611	Action	Char(3)	The cryptographic configuration function performed: CCP Define a card profile. CCR Define a card role. CLK Set clock. CLR Clear master keys. CRT Create master keys. DCP Delete a card profile. DCR Delete a card role. DST Distribute master keys. EID Set environment ID. FCV Load or clear FCV. INI Reinitialize card. LOD Load master key. QRY Query role or profile information. RCP Replace a card profile. RCR Replace a card role. RCV Receive master keys. SET Set master keys. SHR Cloning shares. TST Test master key.
	228	614	Card Profile	Char(8)	The name of the card profile. ²
	236	622	Card Role	Char(8)	The role of the card profile. ²
	244	630	Device Name	Char(10)	The name of the cryptographic device. ²

Table 173. CY (Cryptographic Configuration) journal entries (continued). QASYCYJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		640	Master Key ID ¹	Binary(4)	The cryptographic services Master Key ID ³ . Possible values are as follows: -2 Save/restore master key -1 ASP master key 1 Master key 1 2 Master key 2 3 Master key 3 4 Master key 4 5 Master key 5 6 Master key 6 7 Master key 7 8 Master key 8
		644	Master key encryption	Char(1)	Master Key encrypted with default S/R Master Key. Y The master key was set and encrypted with the default Save/Restore Master Key. N The master key was set and encrypted with a user-set Save/Restore Master Key.
		645	Master key version	Char(8)	The version of the master key that was cleared. NEW The new version was cleared. CURRENT The current version was cleared. OLD The old version was cleared. PENDING The pending version was cleared.
¹ When the entry type (J5 offset 610) is K, the card profile (J5 offset 614), card role (J5 offset 622), and device name (J5 offset 630) is set to blanks. ² When the entry type is K, this field is blank. ³ When the entry type is not K, this field is blank.					

DI (Directory Server) journal entries

This table provides the format of the DI (Directory Server) journal entries.

Table 174. DI (Directory Server) journal entries. QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. L LDAP Operation
	225	611	Operation Type	Char(2)	The type of LDAP operation: AD Audit attribute change. AF Authority failure. BN Successful bind. CA Object authority change. CF Configuration change. CI Create instance CO Object creation. CP Password change. DI Delete instance DO Object delete. EX LDAP directory export. IM LDAP directory import. OM Object management (rename). OW Ownership change. PO Policy change. PW Password fail. RM Replication management UB Successful unbind. ZC Object change. ZR Object read.

Table 174. DI (Directory Server) journal entries (continued). QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	227	613	Authority Failure Code	Char(1)	<p>Code for authority failures. This field is used only if the operation type (J5 offset 611) is AF.</p> <p>A Unauthorized attempt to change audit value.</p> <p>B Unauthorized bind attempt.</p> <p>C Unauthorized object create attempt.</p> <p>D Unauthorized object delete attempt.</p> <p>E Unauthorized export attempt.</p> <p>F Unauthorized configuration change (administrator, change log, backend library, replicas, publishing).</p> <p>G Unauthorized replication management attempt.</p> <p>I Unauthorized import attempt.</p> <p>M Unauthorized change attempt.</p> <p>P Unauthorized policy change attempt.</p> <p>R Unauthorized read (search) attempt.</p> <p>U Unauthorized attempt to read the audit configuration.</p> <p>X Unauthorized proxy authorization attempt.</p>
	228	614	Configuration Change	Char(1)	<p>Configuration changes. This field is only used if the operation type (J5 offset 611) is CF.</p> <p>A Administrator ND change.</p> <p>C Change log on or off.</p> <p>L Backend library name change.</p> <p>P Publishing agent change.</p> <p>R Replica server change.</p> <p>If the operation type (J5 offset 611) is RM the following values might be present:</p> <p>U Suspend replication.</p> <p>V Resume replication.</p> <p>W Replicate pending changes now.</p> <p>X Skip one or more pending changes.</p> <p>Y Quiesce replication context.</p> <p>Z Unquiesce replication context.</p>

Table 174. DI (Directory Server) journal entries (continued). QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	229	615	Configuration Change Code	Char(1)	Code for configuration changes. This field is used only if the operation type (J5 offset 611) is CF. A Item added to configuration D Item deleted from configuration M Item modified
	230	616	Propagate Flag	Char(1)	Indicates the new setting of the owner or ACL propagate value. This field is used only if the operation type (J5 offset 611) is CA or OW. T True F False
	231	617	Bind Authentication Choice	Char(20)	The bind authentication choice. This field is used only if the operation type (J5 offset 611) is BN.
	251	637	LDAP Version	Char(4)	Version of client making request. This field is used only if the operation was done through the LDAP server. 2 LDAP Version 2 3 LDAP Version 3
	255	641	SSL Indicator	Char(1)	Indicates if SSL was used on the request. This field is used only if the operation was done through the LDAP server. 0 No 1 Yes
	256	642	Request Type	Char(1)	The type of request. This field is used only if the operation was done through the LDAP server. A Authenticated N Anonymous U Unauthenticated
	257	643	Connection ID	Char(20)	Connection ID of the request. This field is used only if the operation was done through the LDAP server.
	277	663	Client IP Address	Char(50)	IP address and port number of the client request. This field is used only if the operation was done through the LDAP server.
	327	713	User Name CCSID	Bin(5)	The coded character set identifier of the user name.
	331	717	User Name Length	Bin(4)	The length of the user name.
	333	719	User Name ¹	Char(2002)	The name of the LDAP user.
	2335	2721	Object Name CCSID	Bin(5)	The coded character set identifier of the object name.
	2339	2725	Object Name Length	Bin(4)	The length of the object name.

Table 174. DI (Directory Server) journal entries (continued). QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	2341	2727	Object Name ¹	Char(2002)	The name of the LDAP object.
	4343	4729	Owner Name CCSID	Bin(5)	The coded character set identifier of the owner name. This field is used only if the operation type (J5 offset 611) is OW.
	4347	4733	Owner Name Length	Bin(4)	The length of the owner name. This field is used only if the operation type is OW.
	4349	4735	Owner Name ¹	Char(2002)	The name of the owner. This field is used only if the operation type (J5 offset 611) is OW.
	6351	6737	New Name CCSID	Bin(5)	The coded character set identifier of the new name. This field is used only if the operation type (J5 offset 611) is OM, OW, PO, ZC, AF+M, or AF+P. <ul style="list-style-type: none"> • For operation type OM, this field will contain the CCSID of the new object name. • For operation type OW, this field will contain the CCSID of the new owner name. • For operation types PO, ZC, AF+M, or AF+P, this field will contain the CCSID of the list of changed attribute types in the New Name field.
	6355	6741	New Name Length	Bin(4)	The length of the new name. This field is used only if the operation type (J5 offset 611) is OM, OW, PO, ZC, AF+M, or AF+P. <ul style="list-style-type: none"> • For operation type OM, this field will contain the length of the new object name. • For operation type OW, this field will contain the length of the new owner name. • For operation types PO, ZC, AF+M, or AF+P, this field will contain the length of the list of changed attribute types in the New Name field.
	6357	6743	New Name ¹	Char(2002)	The new name. This field is used only if the operation type (J5 offset 611) is OM, OW, PO, ZC, AF+M, or AF+P. <ul style="list-style-type: none"> • For operation type OM, this field will contain the new object name. • For operation type OW, this field will contain the new owner name. • For operation types PO, ZC, AF+M, or AF+P, this field will contain a list of changed attribute types.
	8359	8745	Object File ID ²	Char(16)	The file ID of the object for export.
	8375	8761	ASP Name ²	Char(10)	The name of the ASP device.
	8385	8771	ASP Number ²	Char(5)	The number of the ASP device.
	8390	8776	Path Name CCSID ²	Bin(5)	The coded character set identifier of the path name.
	8394	8780	Path Name Country or Region ID ²	Char(2)	The Country or Region ID of the path name.

Table 174. DI (Directory Server) journal entries (continued). QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	8396	8782	Path Name Language ID ²	Char(3)	The language ID of the path name.
	8399	8785	Path Name Length ²	Bin(4)	The length of the path name.
	8401	8787	Path Name Indicator ²	Char(1)	Path name indicator. Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	8402	8788	Relative Directory File ID ^{2,3}	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	8418	8804	Path Name ^{1,2}	Char(5002)	The path name of the object.
		13806	Local User Profile	Char(10)	The local user profile name that is mapped to the LDAP user name (J5 offset 719). Blank indicates no user profile is mapped.
		13816	Administrator Indicator	Char(1)	Administrator indicator for the LDAP user name (J5 offset 719). Y The LDAP user is an administrator. N The LDAP user is not an administrator. U It is unknown at this time if the LDAP user is an administrator.
		13817	Proxy ID CCSID	Bin(5)	The coded character set identifier (CCSID) of the proxy ID.
		13821	Proxy ID Length	Bin(4)	The length of the proxy ID.
		13823	Proxy ID ¹	Char(2002)	The name of the proxy ID. This field is used when the proxy authorization control is used to request that an operation be done under the authority of the proxy ID, or for a SASL bind in which the client has specified an authorization ID different from the bind ID.
		15825	Group Assertion	Char(1)	Group membership assertion 0 Groups were not specified by client. 1 Groups were specified by client.
		15826	Cross Reference	Char(36)	Cross reference string used to correlate this entry with the XD entry/entries listing the groups.
		15862	Instance Name	Char(8)	Instance name
		15870	Route CCSID	Bin(5)	CCSID of route

Table 174. DI (Directory Server) journal entries (continued). QASYDIJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		15874	Route Length	Bin(4)	Length of route
		15876	Route	Char(502)	Request route
¹	This is a variable length field. The first two bytes contain the length of the value in the field.				
²	These fields are used only if the operation type (J5 offset 611) is EX or IM.				
³	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				

DO (Delete Operation) journal entries

This table provides the format of the DO (Delete Operation) journal entries.

Table 175. DO (Delete Operation) journal entries. QASYDOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Object was deleted not under commitment control) C A pending object delete was committed D A pending object create was rolled back I Initialize environment variable space P The object delete is pending (the delete was performed under commitment control) R A pending object delete was rolled back
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253		(Reserved Area)	Char(20)	
		639	Object Attribute	Char(10)	The attribute of the object.
		649	(Reserved Area)	Char(10)	

Table 175. DO (Delete Operation) journal entries (continued). QASYDOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
205	273	659	Office User	Char(10)	The name of the office user.
215	283	669	DLO Name	Char(12)	The name of the document library object.
227	295	681	(Reserved Area)	Char(8)	
235	303	689	Folder Path	Char(63)	The path of the folder.
298	366	752	Office on Behalf of User	Char(10)	User working on behalf of another user.
308			(Reserved Area)	Char(20)	
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length ¹	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID ¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID ^{1,2}	Char(16)	The file ID of the object.
372	440	826	Object Name ¹	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name ⁵	Char(10)	The name of the ASP device.
	978	1364	ASP Number ⁵	Char(5)	The number of the ASP device.
	983	1369	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	987	1373	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the path name.
	992	1378	Path Name Length	Binary(4)	The length of the path name.

Table 175. DO (Delete Operation) journal entries (continued). QASYDOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	994	1380	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	995	1381	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1011	1397	Path Name ⁴	Char(5002)	The path name of the object.
¹	These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.				
²	An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.				
³	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				
⁴	This is a variable length field. The first two bytes contain the length of the path name.				
⁵	If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.				

DS (IBM-Supplied Service Tools User ID Reset) journal entries

This table provides the format of the DS (IBM-Supplied Service Tools User ID Reset) journal entries.

Table 176. DS (IBM-Supplied Service Tools User ID Reset) journal entries. QASYDSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Reset of a service tools user ID password. C Changed to a service tools user ID. P Service tools user ID password was changed.

Table 176. DS (IBM-Supplied Service Tools User ID Reset) journal entries (continued). QASYDSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
157	225	611	IBM-Supplied Service Tools User ID Reset	Char(1)	Y Request to reset an IBM-supplied service tools user ID.
158	226	612	Service Tools User ID Type	Char(10)	The type of service tools user ID *SECURITY *FULL *BASIC
168	236	622	Service Tools User ID New Name	Char(8)	The name of the service tools user ID.
176	244	630	Service Tools User ID Password Change	Char(1)	Request to change the service tools user ID password. Y Request to change service tools user ID password.
	245	631	Service Tools User ID New Name	Char(10)	The name of the service tools user ID.
	255	641	Service Tools User ID Requesting Profile	Char(10)	The name of the service tools user ID that requested the change.

EV (Environment Variable) journal entries

This table provides the format of the EV (Environment Variable) journal entries.

Table 177. EV (Environment Variable) journal entries. QASYEVJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. A Add C Change D Delete I Initialize Environment Variable Space

Table 177. EV (Environment Variable) journal entries (continued). QASYEVJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	225	611	Name Truncated	Char(1)	Indicates whether the environment variable name (offset 232) is truncated. Y Environment variable name truncated. N Environment variable name not truncated.
	226	612	CCSID	Binary(5)	The CCSID of the environment variable name.
	230	616	Length	Binary(4)	The length of the environment variable name.
	232	618	Environment Variable Name ²	Char(1002)	The name of the environment variable.
	1234	1620	New Name Truncated ¹	Char(1)	Indicates whether the new environment variable name (offset 1241) is truncated. Y Environment variable value truncated. N Environment variable value not truncated.
	1235	1621	New Name CCSID ¹	Binary(5)	The CCSID of the new environment variable name.
	1239	1625	New Name Length ¹	Binary(4)	The length of the new environment variable name.
	1241	1627	New Environment Variable Name ^{1,2}	Char (1002)	The new environment variable name.
¹ These fields are used when the entry type is C.					
² This is a variable length field. The first two bytes contain the length of the environment variable name.					

GR (Generic Record) journal entries

This table provides the format of the GR (Generic Record) journal entries.

Table 178. GR (Generic Record) journal entries. QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.

Table 178. GR (Generic Record) journal entries (continued). QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	224	610	Entry Type	Char(1)	The type of entry. A Exit program added C Operations Resource Monitoring and Control Operations D Exit program removed F Function registration operations R Exit program replaced
	225	611	Action	Char(2)	The action performed. ZC Change ZR Read
	227	613	User Name	Char(10)	User profile name For entry type F, this field contains the name of the user the function registration operation was performed against.
	237	623	Field 1 CCSID	Binary (5)	The CCSID value for field 1.
	241	627	Field 1 Length	Binary (4)	The length of the data in field 1.

Table 178. GR (Generic Record) journal entries (continued). QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	243	629	Field 1	Char(102) ¹	<p>Field 1 data</p> <p>For entry type F, this field contains the description of the function registration operation that was performed. The possible values are:</p> <p>*REGISTER: Function has been registered</p> <p>*REREGISTER: Function has been updated</p> <p>*DEREGISTER: Function has been de-registered</p> <p>*CHGUSAGE: Function usage information has been changed</p> <p>*CHKUSAGE: Function usage was checked for a user and the check passed</p> <p>*USAGEFAILURE: Function usage was checked for a user and the check failed</p> <p>For entry types A, D, and R, this field will contain the exit program information for the specific function that was performed.</p> <p>For entry type C, this field contains the name of the RMC function that is being attempted. The possible values are:</p> <ul style="list-style-type: none"> • mc_reg_event_select Register event using attribute selection • mc_reg_event_handle Register event using resource handle • mc_reg_class_event Register event for a resource class • mc_unreg_event Unregister event • mc_define_resource Define new resource • mc_undefine_resource Undefine resource • mc_set_select Set resource attribute values using attribute selection • mc_set_handle Set resource attribute values using resource handle • mc_class_set Set resource class attribute values • mc_query_p_select Query resource persistent attributes using attribute selection • mc_query_d_select Query resource dynamic attributes using attribute selection

Table 178. GR (Generic Record) journal entries (continued). QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
243 (cont)					<ul style="list-style-type: none"> • mc_query_p_handle Query resource persistent attributes using resource handle mc_query_d_handle Query resource dynamic attributes using resource handle mc_class_query_p Query resource class persistent attributes mc_class_query_d Query resource class dynamic attributes mc_qdef_resource_class Query resource class definition mc_qdef_p_attribute Query persistent attribute definition mc_qdef_d_attribute Query dynamic attribute definition mc_qdef_sd Query Structured Data definition mc_qdef_valid_values Query definition of a persistent attribute's valid values mc_qdef_actions Query definition of a resource's actions mc_invoke_action Invoke action on a resource mc_invoke_class_action Invoke action on a resource class
	345	731	Field 2 CCSID	Binary (5)	The CCSID value for field 2.
	349	735	Field 2 Length	Binary (4)	The length of the data in field 2.
	351	737	Field 2	Char (102) ¹	<p>Field 2 data</p> <p>For entry type F, this field contains the name of the function that was operated on.</p> <p>For entry type C, this field contains the name of the resource or resource class against which the operation was attempted.</p>
	453	839	Field 3 CCSID	Binary (5)	The CCSID value for field 3.
	457	843	Field 3 Length	Binary (4)	The length of the data in field 3.

Table 178. GR (Generic Record) journal entries (continued). QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	459	845	Field 3	Char(102) ¹	<p>Field 3 data.</p> <p>For entry type F, this field contains the usage setting for a user. There is a value for this field only if the function registration operation is one of the following values:</p> <p>*REGISTER: When the operation is *REGISTER, this field contains the default usage value. The user name will be *DEFAULT.</p> <p>*REREGISTER: When the operation is *REREGISTER, this field contains the default usage value. The user name will be *DEFAULT.</p> <p>*CHGUSAGE: When the operation is *CHGUSAGE, this field contains the usage value for the user specified in the user name field.</p> <p>For entry type C, this field contains the result of any authorization check that was made for the operation indicated in field 1. The following are possible values:</p> <ul style="list-style-type: none"> • *NOAUTHORITYCHECKED: When either the operation indicated in field 1 does not require an authorization check, or if for any other reason an authorization check was not attempted. • *AUTHORITYPASSED: When the mapped user ID indicated in the User Profile Name has successfully passed the appropriate authorization check for the operation indicated in field 1 against the resource or resource class indicated in field 2. • *AUTHORITYFAILED: When the mapped user ID indicated in the User Profile Name has failed the appropriate authorization check for the operation indicated in field 1 against the resource or resource class indicated in field 2.
	561	947	Field 4 CCSID	Binary (5)	The CCSID value for field 4.
	565	951	Field 4 Length	Binary (4)	The length of the data in field 4.

Table 178. GR (Generic Record) journal entries (continued). QASYGRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	567	953	Field 4	Char(102) ¹	Field 4 data. For entry type F, this field contains the allow *ALLOBJ setting for the function. There is a value for this field only if the function registration operation is one of the following values: *REGISTER *REREGISTER
¹ This is a variable length field. The first two bytes contain the length of the field.					

GS (Give Descriptor) journal entries

This table provides the format of the GS (Give Descriptor) journal entries.

Table 179. GS (Give Descriptor) journal entries. QASYGSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. G Give descriptor R Received descriptor U Unable to use descriptor
157	225	611	Job Name	Char(10)	The name of the job.
167	235	621	User Name	Char(10)	The name of the user.
177	245	631	Job Number	Zoned (6,0)	The number of the job.
183	251	637	User Profile Name	Char (10)	The name of the user profile.
	261	647	JUID	Char (10)	The Job User ID of the target job. (This value applies only to subtype G audit records.)

IM (Intrusion Monitor) journal entries

This table provides the format of the IM (Intrusion Monitor) journal entries.

Table 180. IM (Intrusion Monitor) journal entries. QASYIMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		1			Heading fields common to all entry types.
		610	Entry Type	Char(1)	The type of entry. P Potential intrusion event detected
		611	Time of Event	TIMESTAMP	The time that the event was detected, in SAA timestamp format.
		637	Detection Point Identifier	Char(4)	A unique identifier for the processing location that detected the intrusion event. This field is intended for use by service personnel.
		641	Local Address Family	Char(1)	Local IP address family associated with the detected event.
		642	Local Port Number	Zone(5, 0)	Local port number associated with the detected event.
		647	Local IP Address	Char(46)	Local IP address associated with the detected event.
		693	Remote Address Family	Char(1)	Remote address family associated with the detected event.
		694	Remote Port Number	Zoned(5, 0)	Remote port number associated with the detected event.
		699	Remote IP Address	Char(46)	Remote IP address associated with the detected event.

Table 180. IM (Intrusion Monitor) journal entries (continued). QASYIMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		745	Probe Type Identifier	Char(6)	<p>Identifies the type of probe used to detect the potential intrusion. Possible values are as follows:</p> <p>ATTACK Attack action detected event</p> <p>TR-TCP Traffic Regulation action detected event over TCP</p> <p>TR-UDP Traffic Regulation action detected event over UDP</p> <p>SCANE Scan event action detected event</p> <p>SCANG Scan global action detected event</p> <p>XATTACK Possible extrusion attack</p> <p>XTRTCP Outbound TR detected event (TCP)</p> <p>XTRUDP Outbound TR detected event (UDP)</p> <p>XSCAN Outbound scan event detected</p>
		751	Event Correlator	Char(4)	<p>Unique identifier for this specific intrusion event. This identifier can be used to correlate this audit record with other intrusion detection information.</p>

Table 180. IM (Intrusion Monitor) journal entries (continued). QASYIMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		755	Event type	Char(8)	<p>Identifies the type of potential intrusion that was detected. The possible values are as follows:</p> <p>ACKSTORM TCP ACK storm</p> <p>ADRPOISN Address poisoning</p> <p>FLOOD Flood event</p> <p>FRAGGLE Fraggle attack</p> <p>ICMPRED ICMP (Internet Control Message Protocol) redirect</p> <p>IPFRAG IP fragment</p> <p>MALFPKT Malformed packet</p> <p>OUTRAW Outbound Raw</p> <p>PERPECH Perpetual echo</p> <p>PNGDEATH Ping of death</p> <p>RESTOPT Restricted IP options</p> <p>RESTPROT Restricted IP protocol</p> <p>SMURF Smurf attack</p>
		763	Protocol	Char(3)	Protocol number
		766	Condition	Char(4)	Condition number from IDS policy file
		770	Throttling	Char(1)	<ul style="list-style-type: none"> • 0 = not active • 1 = active
		771	Discarded Packets	Zoned(5,0)	Number of discarded packets when throttled
		776	Target TCP/IP Stack	Char(1)	<p>P Production Stack</p> <p>S Service Stack</p>
		777	Reserved	Char(6)	Reserved for future use
		783	Suspected Packet	Char(1002) ¹	A variable length field which can contain up to the first 1000 bytes of the IP packet associated with the detected event. This field contains binary data and should be treated as if it has a CCSID of 65 535.

Table 180. IM (Intrusion Monitor) journal entries (continued). QASYIMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
¹ This is a variable length field. The first 2 bytes contain the length of the suspected packet information.					

IP (Interprocess Communication) journal entries

This table provides the format of the IP (Interprocess Communication) journal entries.

Table 181. IP (Interprocess Communication) journal entries. QASYIPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Ownership and/or authority changes C Create D Delete F Authority failure G Get M Shared memory attach Z Normal semaphore close or shared memory detach
157	225	611	IPC Type	Char(1)	IPC Type M Shared memory N Normal semaphore Q Message queue S Semaphore
158	226	612	IPC Handle	Binary(5)	IPC handle ID
162	230	616	New Owner	Char(10)	New owner of IPC entity
172	240	626	Old Owner	Char(10)	Old owner of IPC entity
182	250	636	Owner Authority	Char(3)	Owner's authority to IPC entity *R read *W write *RW read and write
185	253	639	New Group	Char(10)	Group associated with IPC entity
195	263	649	Old Group	Char(10)	Previous group associated with IPC entity

Table 181. IP (Interprocess Communication) journal entries (continued). QASYIPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
205	273	659	Group Authority	Char(3)	Group's authority to IPC entity *R read *W write *RW read and write
208	276	662	Public Authority	Char(3)	Public's authority to IPC entity *R read *W write *RW read and write
211	279	665	CCSID Semaphore Name	Binary(5)	The CCSID of the semaphore name.
216	283	669	Length Semaphore Name	Binary(4)	The length of the semaphore name.
218	285	671	Semaphore Name	Char(2050)	The semaphore name. Note: This is a variable length field. The first two characters contain the length of the semaphore name.

IR (IP Rules Actions) journal entries

This table provides the format of the IR (IP Rules Actions) journal entries.

Table 182. IR (IP Rules Actions) journal entries. QASYIRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. L IP rules have been loaded from a file. N IP rules have been unloaded for an IP Security connection P IP rules have been loaded for an IP Security connection R IP rules have been read and copied to a file. U IP rules have been unloaded (removed).

Table 182. IR (IP Rules Actions) journal entries (continued). QASYIRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	225	611	File Name	Char(10)	The name of the QSYS file used to load or receive the IP rules. This value is blank if the file used was not in the QSYS file system.
	235	621	File Library	Char(10)	The name of the QSYS file library.
	245	631	Reserved	Char(18)	
	263	649	File Name Length	Binary (4)	The length of the file name.
	265	651	File Name CCSID ¹	Binary (5)	The coded character set identifier for the file name.
	269	655	File Country or Region ID ¹	Char(2)	The Country or Region ID for the file name.
	271	657	File Language ID ¹	Char(3)	The language ID for the file name.
	274	660	Reserved	Char(3)	
	277	663	Parent File ID ^{1, 2}	Char(16)	The file ID of the parent directory.
	293	679	Object File ID ^{1, 2}	Char(16)	The file ID of the file.
	309	695	File Name ¹	Char(512)	The name of the file.
	821	1207	Connection sequence	Char(40)	The connection name.
	861	1247	Object File ID	Char(16)	The file ID of the object.
	877	1263	ASP Name	Char(10)	The name of the ASP device.
	887	1273	ASP Number ⁵	Char(5)	The number of the ASP device.
	892	1278	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	896	1282	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	898	1284	Path Name Language ID	Char(3)	The language ID for the path name.
	901	1287	Path Name Length	Binary(4)	The length of the path name.
	903	1289	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.

Table 182. IR (IP Rules Actions) journal entries (continued). QASYIRJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	904	1290	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	920	1306	Path Name ⁴	Char(5002)	The path name of the object.
<p>¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file system.</p> <p>² If the ID has the left-most bit set and the rest of the bits zero, the ID is not set.</p> <p>³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.</p> <p>⁴ This is a variable length field. The first two bytes contain the length of the field.</p> <p>⁵ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.</p>					

IS (Internet Security Management) journal entries

This table provides the format of the IS (Internet Security Management) journal entries.

Table 183. IS (Internet Security Management) journal entries. QASYISJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. A Fail (this type no longer used) C Normal (this type no longer used) U Mobile User (this type no longer used) 1 IKE Phase 1 SA Negotiation 2 IKE Phase 2 SA Negotiation
	225	611	Local IP Address ¹	Char(15)	Local IP Address.
	240	626	Local Client ID Port	Char(5)	Local Client ID port.
	245	631	Remote IP Address ¹	Char (15)	Remote IP address.
	260	646	Remote Client ID Port	Char (5)	Remote Client ID Port (valid for phase 2).
	265	651	Local IP Address Family	Char (1)	Local IP address family 4 IPv4 6 IPv6

Table 183. IS (Internet Security Management) journal entries (continued). QASYISJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		652	Local IP Address	Char (46)	Local IP address
		698	Remote IP Address Family	Char (1)	Remote IP address family 4 IPv4 6 IPv6
		699	Remote IP Address	Char (46)	Remote IP address
		745	Reserved	Char (162)	Reserved
	521	907	Result Code	Char(4)	Negotiation Result: 0 Successful 1-30 Protocol specific errors (documented in ISAKMP RFC2408, found at: http://www.ietf.org) 82xx IBM i VPN Key Manager specific errors
	525	911	CCSID	Bin(5)	The coded character set identifier for the following fields: <ul style="list-style-type: none"> • Local ID • Local Client ID Value • Remote ID • Remote Client ID Value
	529	915	Local ID	Char(256)	Local IKE identifier
	785	1171	Local Client ID Type	Char(2)	Type of client ID (valid for phase 2): 1 IP version 4 address 2 Fully qualified domain name 3 User fully qualified domain name 4 IP version 4 subnet 5 IP version 6 address 6 IP version 6 subnet 7 IP version 4 address range 8 IP version 6 address range 9 Distinguished name 11 Key identifier
	787	1173	Local Client ID Value	Char(256)	Local client ID (valid for phase 2)
	1043	1429	Local Client ID Protocol	Char(4)	Local client ID protocol (valid for phase 2)
	1047	1433	Remote ID	Char(256)	Remote IKE identifier

Table 183. IS (Internet Security Management) journal entries (continued). QASYISJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1303	1689	Remote Client ID Type	Char(2)	Type of client ID (valid for phase 2) 1 IP version 4 address 2 Fully qualified domain name 3 User fully qualified domain name 4 IP version 4 subnet 5 IP version 6 address 6 IP version 6 subnet 7 IP version 4 address range 8 IP version 6 address range 9 Distinguished name 11 Key identifier
	1305	1691	Remote Client ID Value	Char(256)	Remote client ID (valid for phase 2)
	1561	1947	Remote Client ID Protocol	Char(4)	Remote client ID protocol (valid for phase 2)
¹ This field only supports IPv4 addresses.					

JD (Job Description Change) journal entries

This table provides the format of the JD (Job Description Change) journal entries.

Table 184. JD (Job Description Change) journal entries. QASYJDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A User profile specified for the USER parameter of a job description
157	225	611	Job Description	Char(10)	The name of the job description that had the USER parameter changed.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.

Table 184. JD (Job Description Change) journal entries (continued). QASYJDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
185	253	639	Command Type	Char(3)	The type of command used. CHG Change Job Description (CHGJOBDD) command. CRT Create Job Description (CRTJOBDD) command.
188	256	642	Old User	Char(10)	The name of the user profile specified for the USER parameter before the job description was changed.
198	266	652	New User	Char(10)	The name of the USER profile specified for the user parameter when the job description was changed.
		662	ASP name	Char(10)	ASP name for JOBDD library
		672	ASP number	Char(5)	ASP number for JOBDD library

JS (Job Change) journal entries

This table provides the format of the JS (Job Change) journal entries.

Table 185. JS (Job Change) journal entries. QASYJSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 185. JS (Job Change) journal entries (continued). QASYJSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Entry Type	Char(1)	<p>The type of entry.</p> <p>A ENDJOBABN command</p> <p>B Submit</p> <p>C Change</p> <p>E End</p> <p>H Hold</p> <p>I Disconnect</p> <p>J The current job is attempting to interrupt another job</p> <p>K The current job is about to be interrupted</p> <p>L The interruption of the current job has completed</p> <p>M Change profile or group profile</p> <p>N ENDJOB command</p> <p>P Attach prestart or batch immediate job</p> <p>Q Change query attributes</p> <p>R Release</p> <p>S Start</p> <p>T Change profile or group profile using a profile token.</p> <p>U CHGUSRTRC</p> <p>V Virtual device changed by QWSACCD5 API.</p>
157	225	611	Job Type	Char(1)	<p>The type of job.</p> <p>A Autostart</p> <p>B Batch</p> <p>I Interactive</p> <p>M Subsystem monitor</p> <p>R Reader</p> <p>S System</p> <p>W Writer</p> <p>X SCPF</p>

Table 185. JS (Job Change) journal entries (continued). QASYJSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
158	226	612	Job Subtype	Char(1)	The subtype of the job. ' ' No subtype D Batch immediate E Procedure start request J Prestart P Print device driver Q Query T MRT U Alternate spool user
159	227	613	Job Name	Char(10)	The first part of the qualified job name being operated on
169	237	623	Job User Name	Char(10)	The second part of the qualified job name being operated on
179	247	633	Job Number	Char(6)	The third part of the qualified job name being operated on
185	253	639	Device Name	Char(10)	The name of the device
195	263	649	Effective User Profile ²	Char(10)	The name of the effective user profile for the thread
205	273	659	Job Description Name	Char(10)	The name of the job description for the job
215	283	669	Job Description Library	Char(10)	The name of the library for the job description
225	293	679	Job Queue Name	Char(10)	The name of the job queue for the job
235	303	689	Job Queue Library	Char(10)	The name of the library for the job queue
245	313	699	Output Queue Name	Char(10)	The name of the output queue for the job
255	323	709	Output Queue Library	Char(10)	The name of the library for the output queue
265	333	719	Printer Device	Char(10)	The name of the printer device for the job
275	343	729	Library List ²	Char(430)	The library list for the job
705	773	1159	Effective Group Profile Name ²	Char(10)	The name of the effective group profile for the thread
715	783	1169	Supplemental Group Profiles ²	Char(150)	The names of the supplemental group profiles for the thread.
	933	1319	JUID Description	Char(1)	Describes the meaning of the JUID field: ' ' The JUID field contains the value for the JOB. C The clear JUID API was called. The JUID field contains the new value. S The set JUID API was called. The JUID field contains the new value.

Table 185. JS (Job Change) journal entries (continued). QASYJSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	934	1320	JUID Field	Char(10)	Contains the JUID value
	944	1330	Real User Profile	Char(10)	The name of the real user profile for the thread.
	954	1340	Saved User Profile	Char(10)	The name of the saved user profile for the thread.
	964	1350	Real Group Profile	Char(10)	The name of the real group profile for the thread.
	974	1360	Saved Group Profile	Char(10)	The name of the saved group profile for the thread.
	984	1370	Real User Changed ³	Char(1)	The real user profile was changed. Y Yes N No
	985	1371	Effective User Changed ³	Char(1)	The effective user profile was changed. Y Yes N No
	986	1372	Saved User Changed ³	Char(1)	The saved user profile was changed Y Yes N No
	987	1373	Real Group Changed ³	Char(1)	The real group profile was changed. Y Yes N No
	988	1374	Effective Group Changed ³	Char(1)	The effective group profile was changed Y Yes N No
	989	1375	Saved Group Changed ³	Char(1)	The saved group profile was changed. Y Yes N No
	990	1376	Supplemental Groups Changed ³	Char(1)	The supplemental group profiles were changed. Y Yes N No
	991	1377	Library list Number ⁴	Bin(4)	The number of libraries in the library list extension field (offset 993).
	993	1379	Library List Extension ^{4,5}	Char(2252)	The extension to the library list for the job.
		3631	Library ASP group	Char(10)	Library ASP group
		3641	ASP name	Char(10)	ASP name for JOBD library
		3651	ASP number	Char(5)	ASP number for JOBD library
		3656	Time Zone Name	Char(10)	The time zone description name

Table 185. JS (Job Change) journal entries (continued). QASYJSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		3666	Exit Job Name or Workload Capping Group Name ^{6,7,8}	Char(10)	Can contain any of the following values: <ul style="list-style-type: none"> The name of the job that interrupted the current job The name of the job that was interrupted by the current job The name of the workload capping group associated with the job
		3676	Exit Job User	Char(10)	The user of the job that interrupted the current job, or the user of the job that was interrupted by the current job
		3686	Exit Job Number ^{6,7}	Char(6)	The number of the job that interrupted the current job, or the job number of the job that was interrupted by the current job
		3692	Exit Program Name ⁶	Char(10)	The exit program used to interrupt the job
		3702	Exit Program Library ⁶	Char(10)	The library name of the exit program used to interrupt the job
		3712	JOBQ Library ASP Name	Char(10)	ASP name for JOBQ library
		3722	JOBQ Library ASP Number	Char(5)	ASP numer of JOBQ library

¹ This field is blank if the job is on the job queue and has not run.

² When the JS audit record is generated because one job performs an operation on another job then this field will contain data from the initial thread of the job that is being operated on. In all other cases, the field will contain data from the thread that performed the operation.

³ This field is used only when entry type (offset 610) is M or T.

⁴ This field is used only if the number of libraries in the library list exceeds the size of the field at offset 729.

⁵ This is a variable length field. The first two bytes contain the length of the data in the field.

⁶ This field is used only when entry type (offset 610) is J, K, or L.

⁷ When the entry type is J, this field contains information about the job that will be interrupted. When the entry type is K or L, this field contains information about the job that requested the interruption of the current job.

⁸ When the entry type is C, E, or S, this field contains the Workload Capping Group Name.

KF (Key Ring File) journal entries

This table provides the format of the KF (Key Ring File) journal entries.

Table 186. KF (Key Ring File) journal entries. QASYKFJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. C Certificate operation K Key ring file operation P Password incorrect T Trusted root operation
	225	611	Certificate Operation	Char(3)	Type of action ⁴ . ADK Certificate with private key added ADD Certificate added REQ Certificate requested SGN Certificate signed
	228	614	Key Ring Operation	Char(3)	Type of action ⁵ . ADD Key ring pair added DFT Key ring pair designated as default. EXP Key ring pair exported IMP Key ring pair imported LST List the key ring pair labels in a file PWD Change key ring file password RMV Key ring pair removed INF Key ring pair information retrieval 2DB Key ring file converted to key database file format 2YR Key database file converted to key ring file
	231	617	Trusted Root Operation	Char(3)	Type of action ⁶ . TRS Key ring pair designated as trusted root RMV Trusted root designation removed LST List trusted roots
	234	620	Reserved	Char(18)	
	252	638	Object Name Length	Binary(4)	Key ring file name length.

Table 186. KF (Key Ring File) journal entries (continued). QASYKFJ4/J5 Field Description File

JE	Offset		Field	Format	Description
	J4	J5			
	254	640	Object Name CCSID	Binary(5)	Key ring file name CCSID.
	258	644	Object Name Country or Region ID	Char(2)	Key ring file name Country or Region ID.
	260	646	Object Name Language ID	Char(3)	Key ring file name language ID.
	263	649	Reserved	Char(3)	
	266	652	Parent File ID	Char(16)	Key ring parent directory file ID.
	282	668	Object File ID	Char(16)	Key ring directory file name.
	298	684	Object Name	Char(512)	Key ring file name.
	810	1196	Reserved	Char(18)	
	828	1214	Object Name length	Binary(4)	Source or destination file name length.
	830	1216	Object Name CCSID	Binary(5)	Source or destination file name CCSID.
	834	1220	Object Name Country or Region ID	Char(2)	Source or destination file name Country or Region ID.
	836	1222	Object Name Language ID	Char(3)	Source or destination file name language ID.
	839	1225	Reserved	Char(3)	
	842	1228	Parent File ID	Char(16)	Source or destination parent directory file ID.
	858	1244	Object File ID	Char(16)	Source or destination directory file ID.
	874	1260	Object Name	Char(512)	Source or destination file name.
	1386	1772	Certificate Label Length	Binary(4)	The length of the certificate label.
	1388	1774	Certificate Label ¹	Char(1026)	The certificate label.
	2414	2800	Object File ID	Char(16)	The file ID of the key ring file.
	2430	2816	ASP Name	Char(10)	The name of the ASP device.
	2440	2826	ASP Number	Char(5)	The number of the ASP device.
	2445	2831	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	2449	2835	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	2451	2837	Path Name Language ID	Char(3)	The language ID for the path name.
	2454	2840	Path Name Length	Binary(4)	The length of the path name.

Table 186. KF (Key Ring File) journal entries (continued). QASYKFJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	2456	2842	Path Name Indicator	Char(1)	<p>Path name indicator:</p> <p>Y The Path Name field contains complete absolute path name for the key ring file.</p> <p>N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.</p>
	2457	2843	Relative Directory File ID ²	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ²
	2473	2859	Absolute Path Name ¹	Char(5002)	The absolute path name of the key ring file.
	7475	7861	Object File ID	Char(16)	The file ID of the source or destination file.
	7491	7877	ASP Name	Char(10)	Source or destination file ASP name
	7501	7887	ASP Number	Char(5)	Source or destination file ASP number
	7506	7892	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	7510	7896	Path name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	7512	7898	Path Name Language ID	Char(3)	The language ID for the path name.
	7515	7901	Path Name Length	Binary(4)	The length of the path name.
	7517	7903	Path Name Indicator	Char(1)	<p>Path name indicator:</p> <p>Y The Path Name field contains complete absolute path name for the source or destination file.</p> <p>N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.</p>
	7518	7904	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ²
	7534	7920	Absolute Path Name ¹	Char(5002)	The absolute path name of the source or destination file.

Table 186. KF (Key Ring File) journal entries (continued). QASYKFJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1					This is a variable length field. The first 2 bytes contain the length of the path name.
2					If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.
3					When the path name indicator (offset 7517) is N, this field will contain the relative file ID of the absolute path name at offset 7534. When the path name indicator is Y, this field will contain 16 bytes of hex zeros.
4					The field will be blanks when it is not a certificate operation.
5					The field will be blanks when it is not a key ring file operation.
6					The field will be blanks when it is not a trusted root operation.

LD (Link, Unlink, Search Directory) journal entries

This table provides the format of the LD (Link, Unlink, Search Directory) journal entries.

Table 187. LD (Link, Unlink, Search Directory) journal entries. QASYLDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. L Link directory U Unlink directory K Search directory
157			(Reserved area)	Char(20)	
	225	611	(Reserved area)	Char(18)	
	243	629	Object Name Length ¹	Binary (4)	The length of the object name.
177	245	631	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
181	249	635	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
183	251	637	Object Name Language ID ¹	Char(3)	The language ID for the object name.
186	254	640	(Reserved area)	Char(3)	

Table 187. LD (Link, Unlink, Search Directory) journal entries (continued). QASYLDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
189	257	643	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
205	273	659	Object File ID ^{1,2}	Char(16)	The file ID of the object.
221	289	675	Object Name ¹	Char(512)	The name of the object.
	801	1187	Object File ID	Char(16)	The file ID of the object.
	817	1203	ASP Name	Char(10)	The name of the ASP device.
	827	1213	ASP Number	Char(5)	The number of the ASP device.
	832	1218	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	836	1222	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	838	1224	Path Name Language ID	Char(3)	The language ID for the path name.
	841	1227	Path Name Length	Binary(4)	The length of the path name.
	843	1229	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	844	1230	Relative Directory File ID ¹	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ¹
	860	1246	Path Name ²	Char(5002)	The path name of the object.
¹ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information. ² This is a variable length field. The first 2 bytes contain the length of the path name.					

ML (Mail Actions) journal entries

This table provides the format of the ML (Mail Actions) journal entries.

Table 188. ML (Mail Actions) journal entries. QASYMLJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. O Mail log opened
157	225	611	User Profile	Char(10)	User profile name.
167	235	621	User ID	Char(8)	User identifier
175	243	629	Address	Char(8)	User address

NA (Attribute Change) journal entries

This table provides the format of the NA (Attribute Change) journal entries.

Table 189. NA (Attribute Change) journal entries. QASYNaje/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change to network attribute. T Change to TCP/IP attribute.
157	225	611	Attribute	Char(10)	The name of the attribute.
167	235	621	New Attribute Value	Char(250)	The value of the attribute after it was changed.
417	485	871	Old Attribute Value	Char(250)	The value of the attribute before it was changed.

ND (APPN Directory Search Filter) journal entries

This table provides the format of the ND (APPN Directory Search Filter) journal entries.

Table 190. ND (APPN Directory Search Filter) journal entries. QASYNDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See “Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” on page 564, “Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)” on page 565, and “Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)” on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Directory search filter violation
157	225	611	Filtered control point name	Char(8)	Filtered control point name
165	233	619	Filtered control point NETID.	Char(8)	Filtered control point NETID.
173	241	627	Filtered CP location name	Char(8)	Filtered CP location name.
181	249	635	Filtered CP location NETID	Char(8)	Filtered CP location NETID.
189	257	643	Partner location name	Char(8)	Partner location name.
197	265	651	Partner location NETID	Char(8)	Partner location NETID.
205	273	659	Inbound session	Char(1)	Inbound session. Y This is an inbound session N This is not an inbound session
206	274	660	Outbound session	Char(1)	Outbound session. Y This is an outbound session N This is not an outbound session

For more information about APPN Directory Search Filter and APPN End point, see Protection of your system in an APPN and HPR environment for details.

NE (APPN End Point Filter) journal entries

This table provides the format of the NE (APPN End Point Filter) journal entries.

Table 191. NE (APPN End Point Filter) journal entries. QASYNEJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A End point filter violation
157	225	611	Local location name	Char(8)	Local location name.
165	233	619	Remote location name	Char(8)	Remote location name.
173	241	627	Remote NETID	Char(8)	Remote NETID.
181	249	635	Inbound session	Char(1)	Inbound session. Y This is an inbound session N This is not an inbound session
182	250	636	Outbound session	Char(1)	Outbound session. Y This is an outbound session N This is not an outbound session

For more information about APPN Directory Search Filter and APPN End point, see Protection of your system in an APPN and HPR environment for details.

OM (Object Management Change) journal entries

This table provides the format of the OM (Object Management Change) journal entries.

Table 192. OM (Object Management Change) journal entries. QASYOMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 192. OM (Object Management Change) journal entries (continued). QASYOMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Entry Type	Char(1)	The type of entry. M Object moved to a different library. R Object renamed.
157	225	611	Old Object Name	Char(10)	The old name of the object.
167	235	621	Old Library Name	Char(10)	The name of the library in which the old object resides.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	New Object Name	Char(10)	The new name of the object.
195	263	649	New Library Name	Char(10)	The name of the library to which the object was moved.
205	273		(Reserved Area)	Char(20)	
		659	Object Attribute	Char(10)	The attribute of the object.
		669	(Reserved Area)	Char(10)	
225	293	679	Office User	Char(10)	The name of the office user.
235	303	689	Old Folder or Document Name	Char(12)	The old name of the folder or document.
247	315	701	(Reserved Area)	Char(8)	
255	323	709	Old Folder Path	Char(63)	The old path of the folder.
318	386	772	New Folder or Document Name	Char(12)	The new name of the folder or document.
330	398	784	(Reserved Area)	Char(8)	
338	406	792	New Folder Path	Char(63)	The new path of the folder.
401	469	855	Office on Behalf of User	Char(10)	User working on behalf of another user.
411			(Reserved Area)	Char(20)	
	479	865	(Reserved Area)	Char (18)	
	497	883	Object Name Length	Binary (4)	The length of the old object name field.
431	499	885	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.

Table 192. OM (Object Management Change) journal entries (continued). QASYOMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
435	503	889	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
437	505	891	Object Name Language ID ¹	Char(3)	The language ID for the object name.
440	508	894	(Reserved area)	Char(3)	
443	511	897	Old Parent File ID ^{1,2}	Char(16)	The file ID of the old parent directory.
459	527	913	Old Object File ID ^{1,2}	Char(16)	The file ID of the old object.
475	543	929	Old Object Name ¹	Char(512)	The name of the old object.
987	1055	1441	New Parent File ID ^{1,2}	Char(16)	The file ID of the new parent directory.
1003	1071	1457	New Object Name ^{1, 2, 6}	Char(512)	The new name of the object.
	1583	1969	Object File ID ^{1,2}	Char(16)	The file ID of the object.
	1599	1985	ASP Name ⁷	Char(10)	The name of the ASP device.
	1609	1995	ASP Number ⁷	Char(5)	The number of the ASP device.
	1614	2000	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	1618	2004	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	1620	2006	Path Name Language ID	Char(3)	The language ID for the path name.
	1623	2009	Path Name Length	Binary(4)	The length of the path name.
	1625	2011	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	1626	2012	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1642	2028	Absolute Path Name ⁵	Char(5002)	The old absolute path name of the object.
	6644	7030	Object File ID	Char(16)	The file ID of the object.

Table 192. OM (Object Management Change) journal entries (continued). QASYOMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	6660	7046	ASP Name ⁸	Char(10)	The name of the ASP device.
	6670	7056	ASP Number ⁸	Char(5)	The number of the ASP device.
	6675	7061	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	6679	7065	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	6681	7067	Path Name Language ID	Char(3)	The language ID for the path name.
	6684	7070	Path Name Length	Binary(4)	The length of the path name.
	6686	7072	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	6687	7073	Relative Directory File ID ⁴	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	6703	7089	Absolute Path Name ⁵	Char(5002)	The new absolute path name of the object.
¹	These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.				
²	An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.				
³	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				
⁴	When the path name indicator (offset 6686) is N, this field will contain the relative file ID of the absolute path name at offset 6703. When the path name indicator is Y, this field will contain 16 bytes of hex zeros.				
⁵	This is a variable length field. The first 2 bytes contain the length of the path name.				
⁶	There is no associated length field for this value. The string is null padded unless it is the full 512 characters long.				
⁷	If the old object is in a library, this is the ASP information of the object's library. If the old object is not in a library, this is the ASP information of the object.				
⁸	If the new object is in a library, this is the ASP information of the object's library. If the new object is not in a library, this is the ASP information of the object.				

OR (Object Restore) journal entries

This table provides the format of the OR (Object Restore) journal entries.

Table 193. OR (Object Restore) journal entries. QASYORJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. N A new object was restored to the system. E An existing object was restored to the system.
157	225	611	Restored Object Name	Char(10)	The name of the restored object.
167	235	621	Restored Library Name	Char(10)	The name of the library of the restored object.
177	245	631	Object Type.	Char(8)	The type of object.
185	253	639	Save Object Name	Char(10)	The name of the save object.
195	263	649	Save Library Name	Char(10)	The name of the library from which the object was saved.
205	273	659	Program State ¹	Char(1)	I An inherit state program was restored. Y A system state program was restored. N A user state program was restored.
206	274	660	System Command ²	Char(1)	Y A system command was restored. N A user state command was restored.
207			(Reserved Area)	Char(18)	
	275	661	SETUID Mode	Char(1)	The SETUID mode indicator. Y The SETUID mode bit for the restored object is on. N The SETUID mode bit for the restored object is not on.
	276	662	SETGID Mode	Char(1)	The SETGID mode indicator. Y The SETGID mode bit for the restored object is on. N The SETGID mode bit for the restored object is not on.

Table 193. OR (Object Restore) journal entries (continued). QASYORJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	277	663	Signature Status	Char(1)	The signature status of the restored object. B Signature was not in i5/OS format E Signature exists but is not verified F Signature does not match object content I Signature ignored N Unsignable object S Signature is valid T Untrusted signature U Object unsigned
	278	664	Scan attribute	Char(1)	If the file was an integrated file system object, the value of the scan attribute for that object where Y *YES N *NO C *CHGONLY See the CHGATR command for descriptions of these values.
	279		(Reserved Area)	Char(14)	
		665	Object Attribute	Char(10)	The attribute of the object.
		675	(Reserved Area)	Char(4)	
225	293	679	Office User	Char(10)	The name of the office user.
235	303	689	Restore DLO Name	Char(12)	The document library object name of the restored object.
247	315	701	(Reserved Area)	Char(8)	
255	323	709	Restore Folder Path	Char(63)	The folder into which the DLO was restored.
318	386	772	Save DLO Name	Char(12)	The DLO name of the saved object.
330	398	784	(Reserved Area)	Char(8)	
338	406	792	Save Folder Path	Char(63)	The folder from which the DLO was saved.
401	469	855	Office on Behalf of User	Char(10)	User working on behalf of another user.
411			(Reserved Area)	Char(20)	
	479		(Reserved Area)	Char(18)	

Table 193. OR (Object Restore) journal entries (continued). QASYORJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		865	Restore Private Authorities	Char(1)	Private authorities requested to be restored (PVTAUT(*YES) specified on restore command) Y PVTAUT(*YES) specified on restore command N PVTAUT(*NO) specified on restore command
		866	Private Authorities Saved ⁸	Binary(5)	Number of private authorities saved
		870	Private Authorities Restored ⁸	Binary(5) ⁸	Number of private authorities restored
		874	(Reserved Area)	Char(9)	
	497	883	Object Name Length	Binary (4)	The length of the Old Object Name field.
431	499	885	Object Name CCSID ³	Binary(5)	The coded character set identifier for the object name.
435	503	889	Object Name Country or Region ID ³	Char(2)	The Country or Region ID for the object name.
437	505	891	Object Name Language ID ³	Char(3)	The language ID for the object name.
440	508	894	(Reserved area)	Char(3)	
443	511	897	Parent File ID ^{3,4}	Char(16)	The file ID of the parent directory.
459	527	913	Object File ID ^{3,4}	Char(16)	The file ID of the object.
475	543	929	Object Name ³	Char(512)	The name of the object.
	1055	1441	Old File ID	Char(16)	The file ID for the old object.
	1071	1457	Media File ID	Char(16)	The file ID (FID) that was stored on the media file. Note: The FID stored on the media is the FID the object had on the source system.
	1087	1473	Object File ID	Char(16)	The file ID of the object.
	1103	1489	ASP Name ⁷	Char(10)	The name of the ASP device.
	1113	1499	ASP Number ⁷	Char(5)	The number of the ASP device.
	1118	1504	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	1122	1508	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.

Table 193. OR (Object Restore) journal entries (continued). QASYORJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1124	1510	Path Name Language ID	Char(3)	The language ID for the path name.
	1127	1513	Path Name Length	Binary(4)	The length of the path name.
	1129	1515	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	1130	1516	Relative Directory File ID ⁵	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ⁵
	1146	1532	Path Name ⁶	Char(5002)	The path name of the object.
¹	This field has an entry only if the object being restored is a program.				
²	This field has an entry only if the object being restored is a command.				
³	This field is used only for objects in the "root" (/) ,QOpenSys, and user-defined file system.				
⁴	An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.				
⁵	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				
⁶	This is a variable length field. The first 2 bytes contain the length of the path name.				
⁷	If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.				
⁸	This field is zero if Restore Private Authorities (offset 865) is N.				

OW (Ownership Change) journal entries

This table provides the format of the OW (Ownership Change) journal entries.

Table 194. OW (Ownership Change) journal entries. QASYOWJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change of object owner
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Old Owner	Char(10)	Old owner of the object.
195	263	649	New Owner	Char(10)	New owner of the object.
205	273	659	(Reserved Area)	Char(20)	
225	293	679	Office User	Char(10)	The name of the office user.
235	303	689	DLO Name	Char(12)	The name of the document library object.
247	315	701	(Reserved Area)	Char(8)	
255	323	709	Folder Path	Char(63)	The path of the folder.
318	386	772	Office on Behalf of User	Char(10)	User working on behalf of another user.
328			(Reserved Area)	Char(20)	
	396	782	(Reserved Area)	Char(18)	
	414	800	Object Name Length	Binary (4)	The length of the new object name.
348	416	802	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
352	420	806	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
354	422	808	Object Name Language ID ¹	Char(3)	The language ID for the object name.
357	425	811	(Reserved area)	Char(3)	
360	428	814	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.

Table 194. OW (Ownership Change) journal entries (continued). QASYOWJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
376	444	830	Object File ID ^{1,2}	Char(16)	The file ID of the object.
392	460	846	Object Name ¹	Char(512)	The name of the object.
	972	1358	Object File ID	Char(16)	The file ID of the object.
	988	1374	ASP Name ⁵	Char(10)	The name of the ASP device.
	998	1384	ASP Number ⁵	Char(5)	The number of the ASP device.
	1003	1389	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	1007	1393	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	1009	1395	Path Name Language ID	Char(3)	The language ID for the path name.
	1012	1398	Path Name Length	Binary(4)	The length of the path name.
	1014	1400	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and may be used to form an absolute path name with this relative path name.
	1015	1401	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1031	1417	Path Name ⁴	Char(5002)	The path name of the object.
¹	These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file system.				
²	An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.				
³	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				
⁴	This is a variable length field. The first 2 bytes contain the length of the path name.				
⁵	If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.				

O1 (Optical Access) journal entries

This table provides the format of the O1 (Optical Access) journal entries.

Table 195. O1 (Optical Access) journal entries. QASY01JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	R-Read U-Update D-Delete C-Creat Dir X-Release Held File
157	225	611	Object Type	Char(1)	F-File D-Directory End S-Storage
158	226	612	Access Type	Char(1)	D-File Data A-File Directory Attributes R-Restore operation S-Save operation
159	227	613	Device Name	Char(10)	Library LUD name
169	237	623	CSI Name	Char(8)	Side Object Name
177	245	631	CSI Library	Char(10)	Side Object Library
187	255	641	Volume Name	Char(32)	Optical volume name
219	287	673	Object Name	Char(256)	Optical directory/file name
		929	ASP name	Char(10)	ASP name for CSI library
		939	ASP number	Char(5)	ASP number for CSI library
<p>Note: This entry is used to audit the following optical functions:</p> <ul style="list-style-type: none"> • Open File or Directory • Create Directory • Delete File Directory • Change or Retrieve Attributes • Release Held Optical File 					

O2 (Optical Access) journal entries

This table provides the format of the O2 (Optical Access) journal entries.

Table 196. O2 (Optical Access) journal entries. QASY02JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	C-Copy R-Rename B-Backup Dir or File S-Save Held File M-Move File
157	225	611	Object Type	Char(1)	F-File D-Directory
158	226	612	Src Device Name	Char(10)	Source library LUD name
168	236	622	Src CSI Name	Char(8)	Source Side Object Name
176	244	630	Src CSI Library	Char(10)	Source Side Object Library
186	254	640	Src Volume Name	Char(32)	Source Optical volume name
218	286	672	Src Obj Name	Char(256)	Source Optical directory/file name
474	542	928	Tgt Device Name	Char(10)	Target library LUD name
484	552	938	Tgt CSI Name	Char(8)	Target Side Object Name
492	560	946	Tgt CSI Library	Char(10)	Target Side Object Library
502	570	956	Tgt Volume Name	Char(32)	Target Optical volume name
534	602	988	Tgt Obj Name	Char(256)	Target Optical directory/file name
		1244	ASP name	Char(10)	ASP name for source CSI library
		1254	ASP number	Char(5)	ASP number for source CSI library
		1259	ASP name for target CSI library	Char(10)	ASP name for target CSI library
		1269	ASP number for target CSI library	Char(5)	ASP number for target CSI library

O3 (Optical Access) journal entries

This table provides the format of the O3 (Optical Access) journal entries.

Table 197. O3 (Optical Access) journal entries. QASY03JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for the field listing.
156	224	610	Entry Type	Char(1)	A Change Volume Attributes B Backup Volume C Convert Backup Volume to Primary E Export I Initialize K Check Volume L Change Authorization List M Import N Rename R Absolute Read
157	225	611	Device Name	Char(10)	Library LUD name
167	235	621	CSI Name	Char(8)	Side Object Name
175	243	629	CSI Library	Char(10)	Side Object Library
185	253	639	Old Volume Name	Char(32)	Old Optical volume name
217	285	671	New Volume Name ¹	Char(32)	New Optical volume name
249	317	703	Old Auth List ²	Char(10)	Old Authorization List
259	327	713	New Auth List ³	Char(10)	New Authorization List
269	337	723	Address ⁴	Binary(5)	Starting Block
273	341	727	Length ⁴	Binary(5)	Length read
		731	ASP name	Char(10)	ASP name for CSI library
		741	ASP number	Char(5)	ASP number for CSI library

Table 197. O3 (Optical Access) journal entries (continued). QASY03JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	This field contains the new volume name for Initialize, Rename, and Convert functions; it contains the backup volume name for Backup functions. It contains volume name for Import, Export, Change Authorization List, Change Volume Attributes, and Sector Read.				
2	Used for Import, Export, and Change Authorization List only.				
3	Used for Change Authorization List only.				
4	Used for Sector Read only.				

PA (Program Adopt) journal entries

This table provides the format of the PA (Program Adopt) journal entries.

Table 198. PA (Program Adopt) journal entries. QASYPAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change program to adopt owner's authority. J Java program adopts owner's authority. M Change object's SETUID, SETGID, or Restricted rename and unlink mode indicator.
157	225	611	Program Name ³	Char(10)	The name of the program.
167	235	621	Program Library ³	Char(10)	The name of the library where the program is found.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Owner	Char(10)	The name of the owner.
	263	649	IXVTX mode	Char(1)	The restricted rename and unlink (ISVTX) mode indicator. Y The ISVTX mode indicator is on for the object. N The ISVTX mode indicator is not on for the object.
	263	649	Reserved	Char(17)	
	281	667	Object Name Length ¹	Binary (4)	The length of the object name.
	283	669	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.

Table 198. PA (Program Adopt) journal entries (continued). QASYPAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	287	673	Object Name Country or Region ID	Char(2)	The Country or Region ID for the object name.
	289	675	Object Name Language ID ¹	Char(3)	The language ID for the object name.
	292	678	Reserved	Char(3)	
	295	681	Parent ID ^{1, 2, 3}	Char(16)	Parent File ID.
	311	697	Object File ID ³	Char(16)	File ID for the object
	327	713	Object Name ¹	Char(512)	Object name for the object.
	839	1225	SETUID Mode	Char(1)	The Set effective user ID (SETUID) mode indicator. Y The SETUID mode bit is on for the object. N The SETUID mode bit is not on for the object.
	840	1226	SETGID Mode	Char(1)	The Set effective group ID (SETGID) mode indicator. Y The SETGID mode bit is on for the object. N The SETGID mode bit is not on for the object.
	841	1227	Primary Group Owner	Char(10)	The name of the primary group owner.
	851	1237	Object File ID	Char(16)	The file ID of the object.
	867	1253	ASP Name ⁶	Char(10)	The name of the ASP device.
	877	1263	ASP Number ⁶	Char(5)	The number of the ASP device.
	882	1268	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	886	1272	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	888	1274	Path Name Language ID	Char(3)	The language ID for the path name.
	891	1277	Path Name Length	Binary(4)	The length of the path name.
	893	1279	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.

Table 198. PA (Program Adopt) journal entries (continued). QASYPAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	894	1280	Relative Directory File ID ⁴	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ⁴
	910	1296	Path Name ⁵	Char(5002)	The path name of the object.
<p>¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.</p> <p>² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.</p> <p>³ When the entry type is J, the program name and the library name fields will contain *N. In addition, the parent file ID and the object file ID fields will contain binary zeros.</p> <p>⁴ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.</p> <p>⁵ This is a variable length field. The first 2 bytes contain the length of the path name.</p> <p>⁶ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.</p>					

PG (Primary Group Change) journal entries

This table provides the format of the PG (Primary Group Change) journal entries.

Table 199. PG (Primary Group Change) journal entries. QASYPGJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change primary group.
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Object Library	Char(10)	The name of the library where the object is found.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Old Primary Group	Char(10)	The previous primary group for the object. ⁵
195	263	649	New Primary Group	Char(10)	The new primary group for the object.
					Authorities for new primary group:
205	273	659	Object Existence	Char(1)	Y *OBJEXIST
206	274	660	Object Management	Char(1)	Y *OBJMGT

Table 199. PG (Primary Group Change) journal entries (continued). QASYPGJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
207	275	661	Object Operational	Char(1)	Y *OBJOPR
208	276	662	Object Alter	Char(1)	Y *OBJALTER
209	277	663	Object Reference	Char(1)	Y *OBJREF
210	278	664	(Reserved Area)	Char(10)	
220	288	674	Authorization List Management	Char(1)	Y *AUTLMGT
221	289	675	Read Authority	Char(1)	Y *READ
222	290	676	Add Authority	Char(1)	Y *ADD
223	291	677	Update Authority	Char(1)	Y *UPD
224	292	678	Delete Authority	Char(1)	Y *DLT
225	293	679	Execute Authority	Char(1)	Y *EXECUTE
226	294	680	(Reserved Area)	Char(10)	
236	304	690	Exclude Authority	Char(1)	Y *EXCLUDE
237	305	691	Revoke Old Primary Group	Char(1)	Y Revoke authority for previous primary group. ' ' Do not revoke authority for previous primary group.
238	306	692	(Reserved Area)	Char (20)	
258	326	712	Office User	Char(10)	The name of the office user.
268	336	722	DLO Name	Char(12)	The name of the document library object or folder.
280	348	734	(Reserved Area)	Char(8)	
288	356	742	Folder Path	Char(63)	The path of the folder.
351	419	805	Office on Behalf of User	Char(10)	User working on behalf of another user.
361			(Reserved Area)	Char(20)	
	429	815	(Reserved Area)	Char(18)	
	447	833	Object Name Length ¹	Binary (4)	The length of the object name.
381	449	835	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
385	453	839	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.

Table 199. PG (Primary Group Change) journal entries (continued). QASYPGJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
387	455	841	Object Name Language ID ¹	Char(3)	The language ID for the object name.
390	458	844	(Reserved area)	Char(3)	
393	461	847	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
409	477	863	Object File ID ^{1,2}	Char(16)	The file ID of the object.
425	493	879	Object Name ¹	Char(512)	The name of the object.
	1005	1391	Object File ID	Char(16)	The file ID of the object.
		1407	ASP Name ⁶	Char(10)	The name of the ASP device.
		1417	ASP Number ⁶	Char(5)	The number of the ASP device.
	1035	1422	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	1040	1426	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	1042	1428	Path Name Language ID	Char(3)	The language ID for the path name.
	1045	1431	Path Name Length	Binary(4)	The length of the path name.
	1047	1433	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	1048	1434	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1064	1450	Path Name ⁴	Char(5002)	The path name of the object.

¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.

² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.

⁴ This is a variable length field. The first 2 bytes contain the length of the path name.

⁵ A value of *N implies that the value of the Old Primary Group was not available.

⁶ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.

PO (Printer Output) journal entries

This table provides the format of the PO (Printer Output) journal entries.

Table 200. PO (Printer Output) journal entries. QASYPOJE/J4/J5 Field Description File

JE	Offset		Field	Format	Description
	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Output Type	Char(1)	The type of output. D Direct print R Sent to remote system for printing S Spooled file printed
157	225	611	Status After Printing	Char(1)	D Deleted after printed H Held after printed S Saved after printed ' ' Direct print
158	226	612	Job Name	Char(10)	The first part of the qualified job name.
168	236	622	Job User Name	Char(10)	The second part of the qualified job name.
178	246	632	Job Number	Zoned(6,0)	The third part of the qualified job name.
184	252	638	User Profile	Char(10)	The user profile that created the output.
194	262	648	Output Queue	Char(10)	The output queue containing the spooled file. ¹
204	272	658	Output Queue Library Name	Char(10)	The name of the library containing the output queue. ¹
214	282	668	Device Name	Char(10)	The device where the output was printed ² .
224	292	678	Device Type	Char(4)	The type of printer device ² .
228	296	682	Device Model	Char(4)	The model of the printer device ² .
232	300	686	Device File Name	Char(10)	The name of the device file used to access the printer.
242	310	696	Device File Library	Char(10)	The name of the library for the device file.
252	320	706	Spooled File Name	Char(10)	The name of the spooled file ¹
262	330	716	Short Spooled File Number	Char(4)	The number of the spooled file ¹ . Set to blank if too long.
266	334	720	Form Type	Char(10)	The form type of the spooled file.
276	344	730	User Data	Char(10)	The user data associated with the spooled file ¹ .
286			(Reserved area)	Char(20)	

Table 200. PO (Printer Output) journal entries (continued). QASYPOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	354	740	Spooled File Number	Char(6)	The number of the spooled file.
	360	746	Reserved Area	Char(14)	
306	374	760	Remote System	Char(255)	Name of the remote system to which printing was sent.
561	629	1015	Remote System Print Queue	Char(128)	The name of the output queue on the remote system.
	757	1143	Spooled File Job system Name	Char (8)	The name of the system on which the spooled file resides.
	765	1151	Spooled File Create Date	Char (7)	The spooled file create date (CYMMDD)
	772	1158	Spooled File Create Time	Char(6)	The spooled file create time (HHMMSS).
		1164	ASP Name	Char(10)	ASP name for the device library
		1174	ASP number	Char(5)	ASP number for device file library
		1179	Output Queue ASP Name	Char(10)	ASP name for output queue library.
		1189	Output Queue ASP Number	Char(5)	ASP number for output queue library.
		1194	Spooled File Create Date UTC	Char(7)	The spooled file create date in UTC (This is the same date as the Spool File Create Date (offset 1151) only in UTC).
		1201	Spooled File Create Time UTC	Char(6)	The spooled file create time in UTC (This is the same time as the Spool File Create Time (offset 1158) only in UTC)
¹ This field is blank if the type of output is direct print. ² This field is blank if the type of output is remote print.					

PS (Profile Swap) journal entries

This table provides the format of the PS (Profile Swap) journal entries.

Table 201. PS (Profile Swap) journal entries. QASYPSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 201. PS (Profile Swap) journal entries (continued). QASYPSJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Entry Type	Char(1)	The type of entry. A Profile swap during pass-through. E End work on behalf of relationship. H Profile handle generated by the QSYGETPH API. I All profile tokens were invalidated M Maximum number of profile tokens have been generated. P Profile token generated for user. R All profile tokens for a user have been removed. S Start work on behalf of relationship V User profile authenticated
157	225	611	User Profile	Char(10)	User profile name.
167	235	621	Source Location	Char(8)	Pass-through source location.
175	243	629	Original Target User Profile	Char(10)	Original pass-through target user profile.
185	253	639	New Target User Profile	Char(10)	New pass-through target user profile.
195	263	649	Office User	Char(10)	Office user starting or ending on behalf of relationship.
205	273	659	On Behalf of User	Char(10)	User on behalf of whom the office user is working.
215	283	669	Profile Token Type	Char(1)	The type of the profile token that was generated. M Multiple-use profile token R Multiple-use regenerated profile token S Single-use profile token
216	284	670	Profile Token Timeout	Binary(4)	The number of seconds that the profile token is valid.

PW (Password) journal entries

This table provides the format of the PW (Password) journal entries.

Table 202. PW (Password) journal entries. QASYPWJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Violation Entry Type	Char(1)	<p>The type of violation</p> <p>A APPC bind failure.</p> <p>C User authentication with the CHKPWD command failed.</p> <p>D Service tools user ID name not valid.</p> <p>E Service tools user ID password not valid.</p> <p>P Password not valid.</p> <p>Q Attempted signon (user authentication) failed because user profile is disabled.</p> <p>R Attempted signon (user authentication) failed because password was expired. This audit record might not occur for some user authentication mechanisms. Some authentication mechanisms do not check for expired passwords.</p> <p>S SQL Decryption password is not valid.</p> <p>U User name not valid.</p> <p>X Service tools user ID is disabled.</p> <p>Y Service tools user ID not valid.</p> <p>Z Service tools user ID password not valid.</p>
157	225	611	User Name	Char(10)	The job user name or the service tools user ID name.
167	235	621	Device name	Char(40)	The name of the device or communications device on which the password or user ID was entered. If the entry type is X, Y, or Z, this field will contain the name of the service tool being accessed.
207	275	661	Remote Location Name	Char(8)	Name of the remote location for the APPC bind.
215	283	669	Local Location Name	Char(8)	Name of the local location for the APPC bind.
223	291	677	Network ID	Char(8)	Network ID for the APPC bind.

Table 202. PW (Password) journal entries (continued). QASYPWJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		685 ²	Object Name	Char(10)	The name of the object being decrypted.
		695	Object Library	Char(10)	The library for the object being decrypted.
		705	Object Type	Char(8)	The type of object being decrypted.
		713	ASP Name ¹	Char(10)	The name of the ASP device.
		723	ASP Number ¹	Char(5)	The number of the ASP device.
¹ If the object is in a library, this is the ASP information for the object's library. If the object is not in a library, this is the ASP information for the object.					
² If the object name is *N and the violation type is S, the user attempted to decrypt data in a host variable.					

RA (Authority Change for Restored Object) journal entries

This table provides the format of the RA (Authority Change for Restored Object) journal entries.

Table 203. RA (Authority Change for Restored Object) journal entries. QASYRAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Changes to authority for object restored
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Authorization List Name	Char(10)	The name of the authorization list.
195	263	649	Public Authority	Char(1)	Y Public authority set to *EXCLUDE.
196	264	650	Private Authority	Char(1)	Y Private authority removed.
197	265	651	AUTL Removed	Char(1)	Y Authorization list removed from object.
198	266	652	(Reserved Area)	Char(20)	
218	286	672	DLO Name	Char(12)	The name of the document library object.

Table 203. RA (Authority Change for Restored Object) journal entries (continued). QASYRAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
230	298	684	(Reserved Area)	Char(8)	
238	306	692	Folder Path	Char(63)	The folder containing the document library object.
301			(Reserved Area)	Char(20)	
	369	755	(Reserved Area)	Char(18)	
	387	773	Object Name Length	Binary(4)	The length of the object name.
321	389	775	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
325	393	779	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
327	395	781	Object Name Language ID ¹	Char(3)	The language ID for the object name.
330	398	784	(Reserved area)	Char(3)	
333	401	787	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
349	417	803	Object File ID ^{1,2}	Char(16)	The file ID of the object.
365	433	819	Object Name ¹	Char(512)	The name of the object.
	945	1331	Object File ID	Char(16)	The file ID of the object.
	961	1347	ASP Name ⁵	Char(10)	The name of the ASP device.
	971	1357	ASP Number ⁵	Char(5)	The number of the ASP device.
	976	1362	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	980	1366	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	982	1368	Path Name Language ID	Char(3)	The language ID for the path name.
	985	1371	Path Name Length	Binary(4)	The length of the path name.

Table 203. RA (Authority Change for Restored Object) journal entries (continued). QASYRAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	987	1373	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	988	1374	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1004	1390	Path Name ⁴	Char(5002)	The path name of the object.
<p>¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.</p> <p>² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.</p> <p>³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.</p> <p>⁴ This is a variable length field. The first 2 bytes contain the length of the path name.</p> <p>⁵ If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.</p>					

RJ (Restoring Job Description) journal entries

This table provides the format of the RJ (Restoring Job Description) journal entries.

Table 204. RJ (Restoring Job Description) journal entries. QASYRJJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Restoring a job description that had a user profile specified in the USER parameter.

Table 204. RJ (Restoring Job Description) journal entries (continued). QASYRJJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
157	225	611	Job Description Name	Char(10)	The name of the job description restored.
167	235	621	Library Name	Char(10)	The name of the library the job description was restored to.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	User Name	Char(10)	The name of the user profile specified in the job description.
		649	ASP name	Char(10)	ASP name for JOBD library
		659	ASP number	Char(5)	ASP number for JOBD library

RO (Ownership Change for Restored Object) journal entries

This table provides the format of the RO (Ownership Change for Restored Object) journal entries.

Table 205. RO (Ownership Change for Restored Object) journal entries. QASYROJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Restoring objects that had ownership changed when restored
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Library Name	Char(10)	The name of the library the object is in.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Old Owner	Char(10)	The name of the owner before ownership was changed.
195	263	649	New Owner	Char(10)	The name of the owner after ownership was changed.
205	273	659	(Reserved Area)	Char(20)	
225	293	679	DLO Name	Char(12)	The name of the document library object.
237	305	691	(Reserved Area)	Char(8)	
245	313	699	Folder Path	Char(63)	The folder into which the object was restored.
308			(Reserved Area)	Char(20)	

Table 205. RO (Ownership Change for Restored Object) journal entries (continued). QASYROJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length ¹	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID ¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID ^{1,2}	Char(16)	The file ID of the object.
372	440	826	Object Name ¹	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name ⁵	Char(10)	The name of the ASP device.
	978	1364	ASP Number ⁵	Char(5)	The number of the ASP device.
	983	1369	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	987	1373	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the path name.
	992	1378	Path Name Length	Binary(4)	The length of the path name.
	994	1380	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	995	1381	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1011	1397	Path Name ⁴	Char(5002)	The path name of the object.

Table 205. RO (Ownership Change for Restored Object) journal entries (continued). QASYROJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1					These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.
2					An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
3					If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.
4					This is a variable length field. The first 2 bytes contain the length of the path name.
5					If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.

RP (Restoring Programs that Adopt Authority) journal entries

This table provides the format of the RP (Restoring Programs that Adopt Authority) journal entries.

Table 206. RP (Restoring Programs that Adopt Authority) journal entries. QASYRPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Restoring programs that adopt the owner's authority
157	225	611	Program Name	Char(10)	The name of the program
167	235	621	Program Library	Char(10)	The name of the library where the program is located
177	245	631	Object Type	Char(8)	The type of object
185	253	639	Owner Name	Char(10)	Name of the owner
	263	649	(Reserved Area)	Char(18)	
	281	667	Object Name Length ¹	Binary (4)	The length of the object name.
	283	669	Object Name CCSID ¹	Binary (5)	The coded character set identifier for the object name.
	287	673	Object Name Country or Region ID ¹	Char (2)	The Country or Region ID for the object name.
	289	675	Object name Language ID ¹	Char (3)	The language ID for the object name.
	292	678	(Reserved Area)	Char (3)	
	295	681	Parent File ID ^{1,2}	Char (16)	The file ID of the parent directory.

Table 206. RP (Restoring Programs that Adopt Authority) journal entries (continued). QASYRPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	311	697	Object File ID ^{1,2}	Char (16)	The file ID of the object.
	327	713	Object Name ¹	Char (512)	The name of the object.
	839	1225	Object File ID	Char(16)	The file ID of the object.
	855	1241	ASP Name ⁵	Char(10)	The name of the ASP device.
	865	1251	ASP Number ⁵	Char(5)	The number of the ASP device.
	870	1256	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	874	1260	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	876	1262	Path Name Language ID	Char(3)	The language ID for the path name.
	879	1265	Path Name Length	Binary(4)	The length of the path name.
	881	1267	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	882	1268	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	898	1284	Path Name ⁴	Char(5002)	The path name of the object.
¹	These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file system.				
²	If an ID that has the left-most bit set and the rest of the bits are zero, the ID is not set.				
³	If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.				
⁴	This is a variable length field. The first 2 bytes contain the length of the path name.				
⁵	If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.				

RQ (Restoring Change Request Descriptor Object) journal entries

This table provides the format of the RQ (Restoring Change Request Descriptor Object) journal entries.

Table 207. RQ (Restoring Change Request Descriptor Object) journal entries. QASYRQJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See “Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” on page 564, “Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)” on page 565, and “Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)” on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Restore *CRQD object that adopts authority.
157	225	611	Object Name	Char(10)	The name of the change request descriptor.
167	235	621	Object Library	Char(10)	The name of the library where the change request descriptor is found.
177	245	631	Object Type	Char(8)	The type of object.
		639	ASP name	Char(10)	ASP name for CRQD library
		649	ASP number	Char(5)	ASP number for CRQD library

RU (Restore Authority for User Profile) journal entries

This table provides the format of the RU (Restore Authority for User Profile) journal entries.

Table 208. RU (Restore Authority for User Profile) journal entries. QASYRUJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See “Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)” on page 564, “Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)” on page 565, and “Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)” on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Restoring authority to user profiles
157	225	611	User Name	Char(10)	The name of the user profile whose authority was restored.
167	235	621	Library Name	Char(10)	The name of the library.
177	245	631	Object Type	Char(8)	The type of object.

Table 208. RU (Restore Authority for User Profile) journal entries (continued). QASYRUJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	253	639	Authority Restored	Char(1)	Indicates whether all authorities were restored for the user. A All authorities were restored S Some authorities not restored

RZ (Primary Group Change for Restored Object) journal entries

This table provides the format of the RZ (Primary Group Change for Restored Object) journal entries.

Table 209. RZ (Primary Group Change for Restored Object) journal entries. QASYRZJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Primary group changed.
157	225	611	Object Name	Char(10)	The name of the object.
167	235	621	Object Library	Char(10)	The name of the library where the object is found.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Old Primary Group	Char(10)	The previous primary group for the object.
195	263	649	New Primary Group	Char(10)	The new primary group for the object.
205	273	659	(Reserved Area)	Char(20)	
225	293	679	DLO Name	Char(12)	The name of the document library object.
237	305	691	(Reserved Area)	Char(8)	
245	313	699	Folder Path	Char(63)	The folder into which the object was restored.
308			(Reserved Area)	Char(20)	
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length ¹	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID ¹	Binary(5)	The coded character set identifier for the object name.

Table 209. RZ (Primary Group Change for Restored Object) journal entries (continued). QASYRZJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
332	400	786	Object Name Country or Region ID ¹	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID ¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID ^{1,2}	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID ^{1,2}	Char(16)	The file ID of the object.
372	440	826	Object Name ¹	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name	Char(10)	The name of the ASP device.
	978	1364	ASP Number	Char(5)	The number of the ASP device.
	983	1369	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	987	1373	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the path name.
	992	1378	Path Name Length	Binary(4)	The length of the path name.
	994	1380	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	995	1381	Relative Directory File ID ³	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ³
	1011	1397	Path Name ⁴	Char(5002)	The path name of the object.

¹ These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.

² An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

³ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.

⁴ This is a variable length field. The first 2 bytes contain the length of the path name.

SD (Change System Distribution Directory) journal entries

This table provides the format of the SD (Change System Distribution Directory) journal entries.

Table 210. SD (Change System Distribution Directory) journal entries. QASYSDJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. S System directory change
157	225	611	Type of Change	Char(3)	ADD Add directory entry CHG Change directory entry COL Collector entry DSP Display directory entry OUT Output file request PRT Print directory entry RMV Remove directory entry RNM Rename directory entry RTV Retrieve details SUP Supplier entry
160	228	614	Type of record	Char(4)	DIRE Directory DPTD Department details SHDW Directory shadow SRCH Directory search
164	232	618	Originating System	Char(8)	The system originating the change
172	240	626	User Profile	Char(10)	The user profile making the change
182	250	636	Requesting system	Char(8)	The system requesting the change
190	258	644	Function Requested	Char(6)	INIT Initialization OFFLIN Offline initialization REINIT Reinitialization SHADOW Normal shadowing STPSHD Stop shadowing

Table 210. SD (Change System Distribution Directory) journal entries (continued). QASYSdje/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
196	264	650	User ID	Char(8)	The user ID being changed
204	272	658	Address	Char(8)	The address being changed
212	280	666	Network User ID	Char(47)	The network user ID being changed

SE (Change of Subsystem Routing Entry) journal entries

This table provides the format of the SE (Change of Subsystem Routing Entry) journal entries.

Table 211. SE (Change of Subsystem Routing Entry) journal entries. QASYSEJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Subsystem routing entry changed
157	225	611	Subsystem Name	Char(10)	The name of the object
167	235	621	Library Name	Char(10)	The name of the library where the object is stored.
177	245	631	Object Type	Char(8)	The type of object.
185	253	639	Program Name	Char(10)	The name of the program that changed the routing entry
195	263	649	Library Name	Char(10)	The name of the library for the program
205	273	659	Sequence Number	Char(4)	The sequence number
209	277	663	Command Name	Char(3)	The type of command used ADD ADDRTGE CHG CHGRTGE RMV RMVRTGE
		666	ASP name for SBSDB library	Char(10)	ASP name for SBSDB library
		676	ASP number for SBSDB library	Char(5)	ASP number for SBSDB library
		681	ASP name for program library	Char(10)	ASP name for program library

Table 211. SE (Change of Subsystem Routing Entry) journal entries (continued). QASYSEJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		691	ASP number for program library	Char(5)	ASP number for program library

SF (Action to Spooled File) journal entries

This table provides the format of the SF (Action to Spooled File) journal entries.

Table 212. SF (Action to Spooled File) journal entries. QASYSFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Access Type	Char(1)	The type of entry A Spooled file read by someone other than the owner of the spooled file. C Spooled file created. D Spooled file deleted. H Spooled file held. I Create of inline file. R Spooled file released. S Spooled file saved. T Spooled file restored. U Security-relevant spooled file attributes changed. V Only non-security-relevant spooled file attributes changed. X Spooled file operation rejected by exit program.
157	225	611	Database File Name	Char(10)	The name of the database file containing the spooled file
167	235	621	Library Name	Char(10)	The name of the library for the database file
177	245	631	Object Type	Char(8)	The object type of the database file
185	253	639	Reserved area	Char(10)	
195	263	649	Member Name	Char(10)	The name of the file member.
205	273	659	Spooled File Name	Char(10)	The name of the spooled file ¹ .

Table 212. SF (Action to Spooled File) journal entries (continued). QASYSFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
215	283	669	Short Spooled File Number	Char(4)	The number of the spooled file ¹ . If the spooled file number is larger than 4 bytes, this field will be blank and the Spooled File Number field (J5 offset 693) will be used.
219	287	673	Output Queue Name	Char(10)	The name of the output queue containing the spooled file.
229	297	683	Output Queue Library	Char(10)	The name of the library for the output queue.
239			Reserved area	Char(20)	
	307	693	Spooled File Number	Char(6)	The number of the spooled file.
	313	699	Reserved Area	Char(14)	
259	327	713	Old Copies	Char(3)	Number of old copies of the spooled file
262	330	716	New Copies	Char(3)	Number of new copies of the spooled file
265	333	719	Old Printer	Char(10)	Old printer for the spooled file
275	343	729	New Printer	Char(10)	New printer for the spooled file
285	353	739	New Output Queue	Char(10)	New output queue for the spooled file
295	363	749	New Output Queue Library	Char(10)	Library for the new output queue
305	373	759	Old Form Type	Char(10)	Old form type of the spooled file
315	383	769	New Form Type	Char(10)	New form type of the spooled file
325	393	779	Old Restart Page	Char(8)	Old restart page for the spooled file
333	401	787	New Restart Page	Char(8)	New restart page for the spooled file
341	409	795	Old Page Range Start	Char(8)	Old page range start of the spooled file
349	417	803	New Page Range Start	Char(8)	New page range start of the spooled file
357	425	811	Old Page Range End	Char(8)	Old page range end of the spooled file
365	433	819	New Page Range End	Char(8)	New page range end of the spooled file
	441	827	Spooled File Job Name	Char(10)	The name of the spooled file job.
	451	837	Spooled File Job User	Char(10)	The user for the spooled file job.
	461	847	Spooled File Job Number	Char(6)	The number for the spooled file job.
	467	853	Old Drawer	Char(8)	Old source drawer.
	475	861	New Drawer	Char(8)	New source drawer.

Table 212. SF (Action to Spooled File) journal entries (continued). QASYSFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	483	869	Old Page Definition Name	Char(10)	Old page definition name.
	493	879	Old Page Definition Library	Char(10)	Old page definition library name.
	503	889	New Page Definition Name	Char(10)	New page definition name.
	513	899	New Page Definition Library	Char(10)	New page definition library.
	523	909	Old Form Definition Name	Char(10)	Old form definition name.
	533	919	Old Form Definition library	Char(10)	Old form definition library name.
	543	929	Name of new form definition	Char(10)	Name of new form definition
	553	939	New Form Definition Library	Char(10)	New form definition library name.
	563	949	Old User Defined Option 1	Char(10)	Old user-defined option 1.
	573	959	Old User Defined Option 2	Char(10)	Old user-defined option 2.
	583	969	Old User Defined Option 3	Char(10)	Old user-defined option 3.
	593	979	Old User Defined Option 4	Char(10)	Old user-defined option 4.
	603	989	New User Defined Option 1	Char(10)	New user-defined option 1.
	613	999	New User Defined Option 2	Char(10)	New user-defined option 2.
	623	1009	New User Defined Option 3	Char(10)	New user-defined option 3.
	633	1019	New User Defined Option 4	Char(10)	New user-defined option 4.
	643	1029	Old User Defined Object	Char(10)	Old user-defined object name.

Table 212. SF (Action to Spooled File) journal entries (continued). QASYSFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	653	1039	Old User Defined Object Library	Char(10)	Old user-defined library name.
	663	1049	Old User Defined Object Type	Char(10)	Old user-defined object type.
	673	1059	New User Defined Object	Char(10)	New user-defined object.
	683	1069	New User Defined Object Library	Char(10)	New user-defined object library name.
	693	1079	New User Defined Object Type	Char(10)	New user-defined object type.
	703	1089	Spooled File Job System Name	Char(8)	The name of the system on which the spooled file resides.
	711	1097	Spooled File Create Date	Char(7)	The spooled file create date (CYMMDD).
	718	1104	Spooled File Create Time	Char(6)	The spooled file create time (HHMMSS).
		1110	Name of old user defined data	Char(255)	Name of old user defined data
		1365	Name of new user defined data	Char(255)	Name of new user defined data
		1620	File ASP Name	Char(10)	ASP name for database file library.
		1630	File ASP Number	Char(5)	ASP number for database file library.
		1635	Output Queue ASP name	Char(10)	ASP name for output queue library.
		1645	Output Queue ASP number	Char(5)	ASP number for output queue library.
		1650	New Output Queue ASP Name	Char(10)	ASP name for new output queue library.
		1660	New Output Queue ASP Number	Char(5)	ASP number for new output queue library.
		1665	Old Spooled File Status	Char(3)	Old spooled file status.
		1668	New Spooled File Status	Char(3)	New spooled file status.
		1671	Original Creation Date	Char(7)	Original creation date.

Table 212. SF (Action to Spooled File) journal entries (continued). QASYSFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		1678	Original Creation Time	Char(6)	Original creation time.
		1684	Old Spooled File Expiration Date	Char(7)	Old spooled file expiration date
		1687	New Spooled File Expiration Date	Char(7)	New spooled file expiration date
		1694	Spooled File Create Date UTC	Char(7)	The spooled file create date in UTC (This is the same date as the Spool File Create Date (offset 1097) only in UTC)
		1701	Spooled File Create Time UTC	Char(6)	The spooled file create time in UTC (This is the same time as the Spool File Create Time (offset 1104) only in UTC)
		1707	Registered security exit program	Char(10)	The name of the registered security exit program.
		1717	Registered security exit program library	Char(10)	The library name of the registered security exit program.
		1727	Registered security exit program ASP name	Char(10)	The ASP name of the registered security exit program.
		1737	Registered security exit program ASP number	Char(5)	The ASP number of the registered security exit program.
¹ This field is blank when the type of entry is I (inline print).					

SG (Asynchronous Signals) journal entries

This table provides the format of the SG (Asynchronous Signals) journal entries.

Table 213. SG (Asynchronous Signals) journal entries. QASYSGJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.

Table 213. SG (Asynchronous Signals) journal entries (continued). QASYSJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	224	610	Entry Type	Char(1)	The type of entry. A Asynchronous IBM i signal processed P Asynchronous Private Address Space Environment (PASE) signal processed
	225	611	Signal Number	Char(4)	The signal number that was processed.
	229	615	Handle action	Char(1)	The action taken on this signal. C Continue the process E Signal exception H Handle by invoking the signal catching function S Stop the process T End the process U End the request
	230	616	Signal Source	Char(1)	The source of the signal. M Machine source P Process source Note: When the signal source value is machine, the source job values are blank.
	231	617	Source Job Name	Char(10)	The first part of the source job's qualified name.
	241	627	Source Job User Name	Char(10)	The second part of the source job's qualified name.
	251	637	Source Job Number	Char(6)	The third part of the source jobs's qualified name.
	257	643	Source Job Current User	Char(10)	The current user profile for the source job.
	267	653	Generation Timestamp	Char(8)	The *DTS format of the time when the signal was generated. Note: The QWCCVTDT API can be used to convert a *DTS time stamp to other formats.

SK (Secure Sockets Connections) journal entries

This table provides the format of the SK (Secure Sockets Connections) journal entries.

Table 214. SK (Secure Sockets Connections) journal entries. QASYSKJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.

Table 214. SK (Secure Sockets Connections) journal entries (continued). QASYSKJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	224	610	Entry type	Char(1)	A Accept C Connect D DHCP address assigned F Filtered mail P Port unavailable R Reject mail U DHCP address not assigned
	225	611	Local IP Address ³	Char(15)	The local IP address.
	240	626	Local port	Char(5)	The local port.
	245	631	Remote IP Address ³	Char(15)	The remote IP address.
	260	646	Remote port	Char(5)	The remote port.
	265	651	Socket Descriptor	Bin(5)	The socket descriptor.
	269	655	Filter Description	Char(10)	The mail filter specified.
	279	665	Filter Data Length	Bin(4)	The length of the filter data.
	281	667	Filter Data ¹	Char(514)	The filter data.
	795	1181	Address Family	Char(10)	The address family. *IPV4 Internet Protocol Version 4 *IPV6 Internet Protocol Version 6
	805	1191	Local IP address	Char(46)	The local IP address.
	851	1237	Remote IP address ²	Char(46)	The remote IP address
	897	1283	MAC address	Char(32)	The MAC address of the requesting client.
	929	1315	Host name	Char(255)	The host name of the requesting client.
¹	This is a variable length field. The first two bytes contain the length of the field.				
²	When the entry type is D, this field contains the IP address that the DHCP server assigned to the requesting client.				
³	These fields only support IPv4 addresses.				

SM (Systems Management Change) journal entries

This table provides the format of the SM (Systems Management Change) journal entries.

Table 215. SM (Systems Management Change) journal entries. QASYSMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	Function accessed B Backup list changed C Automatic cleanup options D DRDA F HFS file system N Network file operation O Backup options changed P Power on/off schedule S System reply list T Access path recovery times changed
157	225	611	Access Type	Char(1)	A Add C Change D Delete R Remove S Display T Retrieve or receive
158	226	612	Sequence Number	Char(4)	Sequence number of the action
162	230	616	Message ID	Char(7)	Message ID associated with the action
169	237	623	Relational Database Name	Char(18)	Name of the relational database
187	255	641	File System Name	Char(10)	Name of the file system
197	265	651	Backup Option Changed	Char(10)	The backup option that was changed
207	275	661	Backup List Change	Char(10)	The name of the backup list that was changed
217	285	671	Network File Name	Char(10)	The name of the network file that was used

Table 215. SM (Systems Management Change) journal entries (continued). QASYSMJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
227	295	681	Network File Member	Char(10)	The name of the member of the network file
237	305	691	Network File Number	Zoned(6,0)	The number of the network file
243	311	697	Network File Owner	Char(10)	The name of the user profile that owns the network file
253	321	707	Network File Originating User	Char(8)	The name of the user profile that originated the network file
261	329	715	Network File Originating Address	Char(8)	The address that originated the network file

SO (Server Security User Information Actions) journal entries

This table provides the format of the SO (Server Security User Information Actions) journal entries.

Table 216. SO (Server Security User Information Actions) journal entries. QASYSOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry A Add entry C Change entry R Remove entry T Retrieve entry
157	225	611	User Profile	Char(10)	The name of the user profile.
	235	621	User Information Entry Type	Char(1)	N Entry type not specified. U Entry is a user application information entry. Y Entry is a server authentication entry.
	236	622	Password Stored	Char(1)	N Password not stored S No change Y Password is stored.
	237	623	Server Name	Char(200)	The name of the server.

Table 216. SO (Server Security User Information Actions) journal entries (continued). QASYSOJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	437	823	(Reserved Area)	Char(3)	
	440	826	User ID Length	Binary (4)	The length of the user ID.
	442	828	(Reserved Area)	Char(20)	
	462	848	User ID	Char(1002) ¹	The ID for the user.
¹ This is a variable length field. The first 2 bytes contain the length of the field.					

ST (Service Tools Action) journal entries

This table provides the format of the ST (Service Tools Action) journal entries.

Table 217. ST (Service Tools Action) journal entries. QASYSTJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry A Service record
157	225	611	Service Tool	Char(2)	The type of entry. AN ANZJVM AR ARM diagnostic trace (see ARMSRV QShell command) CD QTACTLDV, QTADMPDV CE QWTCTLTR CS STRCPYSCN CT DMPCLUTRC DC DLTCMNTRC DD DMPDLO DF QWTDMPFR, QWTDMPFL DI QSCDIRD DJ DMPJVM, QPYRTJVM DM DMPMEMINF DO DMPOBJ

Table 217. ST (Service Tools Action) journal entries (continued). QASYSTJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
					DS DMPYSOBY, QTADMPTS, QTADMPDV, QWIDMPLF DU DMPUSRPRF DW STRDW, ENDDW, ADDDWDFN, RMVDWDFN EC ENDCMNTRC ER ENDRMTSPT FF FFDC (First Failure Data Capture) GS QSMGSSTD HD QYHCHCOP (DASD) HL QYHCHCOP (LPAR)
					JW STRJW, ENDJW, ADDJWDFN, RMVJWDFN LC EPT created LD EPT deleted LE EPT for the job has been changed LF System EPT has been fixed up LG Entries in the EPT have been changed LH EPT compared
					LI EPT entries displayed MC QWTMAINT (change) MD QWTMAINT (dump) MP End system job MQ Restart system job OP Operations console PC PRTCMNTRC
					PE PRERRLOG, QTADMPDV PI PRTINTDTA, QTADMPDV PS QP0FPTOS SC STRCMNTRC, QSCCHGCT SE QWTSETTR

Table 217. ST (Service Tools Action) journal entries (continued). QASYSTJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
					SF QWCCDSIC, QWVRCSTK (Display internal stack entry) SJ STRSRVJOB SN QPZSYNC SR STRRMTSPT SS QFPHPSF ST STRSST SV QSRSRV TA TRCTCPAPP
					TC TRCCNN (*FORMAT specified) TE ENDTRC, ENDPEX, TRCJOB(*OFF or *END specified) TI TRCINT, or TRCCNN with SET(*ON), SET(*OFF), or SET(*END) TO QTOBSRV TQ QWCTMQTM TS STRTRC, STRPEX, TRCJOB(*ON specified)
					UD QTAUPDDV WE ENDWCH, QSCEWCH WS STRWCH, QSCSWCH WT WRKTRC WW WRKWCH, QSCRWCHI, QSCRWCHL
159	227	613	Object Name	Char(10)	Name of the object accessed
169	237	623	Library Name	Char(10)	Name of the library for the object
179	247	633	Object Type	Char(8)	Type of object
187	255	641	Job Name	Char(10)	The first part of the qualified job name
197	265	651	Job User Name	Char(10)	The second part of the qualified job name
207	275	661	Job Number	Zoned(6,0)	The third part of the qualified job name
213	281	667	Object Name	Char(30)	Name of the object for DMPSYSOBJ
243	311	697	Library Name	Char(30)	Name of the library for the object for DMPSYSOBJ
273	341	727	Object Type	Char(8)	Type of the object
281	349	735	DLO Name	Char(12)	Name of the document library object
293	361	747	(Reserved Area)	Char(8)	
301	369	755	Folder Path ⁸	Char(63)	The folder containing the document library object
	432	818	JUID Field	Char(10)	The JUID of the target job

Table 217. ST (Service Tools Action) journal entries (continued). QASYSTJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	442	828	Early Trace Action ¹	Char(10)	The action requested for early job tracing *ON Early tracing turned on *OFF Early tracing turned off *RESET Early tracing turned off and trace information deleted.
	452	838	Application Trace Option ²	Char(1)	The trace option specified on TRCTCPAPP. A ⁶ Activate D ⁶ Deactivate Y ⁷ Collection of trace information started N ⁷ Collection of trace information stopped and trace information written to spooled file E ⁷ Collection of trace information ended and all trace information purged (no output created)
	453	839	Application Traced ²	Char(10)	The name of the application being traced.
	463	849	Service Tools Profile ³	Char(10)	The name of the service tools profile used for STRSST.
		859	Source node ID	Char(8)	Source node ID
		867	Source user	Char(10)	Source user
		877	ASP name for object library	Char(10)	ASP name for object library
		887	ASP number for object library	Char(5)	ASP number for object library
		892	ASP name for DMPSYSOBJ object library	Char(10)	ASP name for DMPSYSOBJ object library
		902	ASP number for DMPSYSOBJ object library	Char(5)	ASP number for DMPSYSOBJ object library
		907	Console Type ⁴	Char(10)	The console type. Possible values are: • *DIRECT • *LAN • *HMC
		917	Console action ⁴	Char(10)	The console action. Possible values are: • *RECOVERY • *TAKEOVER
		927	Address family ⁴	Char(10)	The address family. • *IPv4 • *IPv6

Table 217. ST (Service Tools Action) journal entries (continued). QASYSTJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		937	Previous IP address ⁴	Char(46)	The IP address of the previous console device for *LAN.
		938	Previous device ID ⁴	Char(10)	The service tools device ID of the previous console device for *LAN.
		993	Current IP address ⁴	Char(46)	The IP address of the current console device for *LAN.
		1039	Current device ID ⁴	Char(10)	The service tools device ID of the current console device for *LAN.
		1049	Watch session ⁵	Char(10)	Watch session ID.
		1059	Entry ⁹	Char(10)	Name of the entry in the entry point table that was changed.
		1069	Related Object ¹⁰	Char(10)	Name of related object. <ul style="list-style-type: none"> • For Service Tool value LC, this field contains the name of the base entry point table. • For Service Tool value LG, this field contains the name of the replacement program. • For Service Tool value LH, this field contains the name of the compare entry point table.
		1079	Related Object Library ¹⁰	Char(10)	Name of related object library. <ul style="list-style-type: none"> • For Service Tool value LC, this field contains the name of the base entry point table library. • For Service Tool value LG, this field contains the name of the replacement program library. • For Service Tool value LH, this field contains the name of the compare entry point table library.
¹	This field is only used when the Service Tool value (offset 611) is CE.				
²	This field is only used when the Service Tool value (offset 611) is AR or TA.				
³	This field is only used when the Service Tool value (offset 611) is ST or OP.				
⁴	This field is only used when the Service Tool value (offset 611) is OP.				
⁵	This field is only used when the Service Tool value (offset 611) is WS or WE.				
⁶	This field is only used when the Service Tool value (offset 611) is AR.				
⁷	This field is only used when the Service Tool value (offset 611) is TA.				
⁸	The Folder Path will contain the 30 character Advanced Analysis Command name when the Service Tool value (offset 611) is GS.				
⁹	This field is only used when the Service Tool value (offset 611) is LG.				
¹⁰	This field is only used when the Service Tool value (offset 611) is LC, LG, or LH.				

SV (Action to System Value) journal entries

This table provides the format of the SV (Action to System Value) journal entries.

Table 218. SV (Action to System Value) journal entries. QASYSVJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry. A Change to system values B Change to service attributes C Change to system clock D Adjustment to Coordinated Universal Time (UTC) E Change to option F Change to system-wide journal attribute
157	225	611	System Value or Service Attribute	Char(10)	JRNRCVCNT Changed journal recovery count value MAXCCHWAIT Changed journal maximum cache wait time QINPIDCO Change the current install disk configuration option with QINPIDCO API.
167	235	621	New Value	Char(250)	The value to which the system value or service attribute was changed
417	485	871	Old Value	Char(250)	The value of the system value or service attribute before it was changed
667	735	1121	New Value Continued	Char(250)	Continuation of the value to which the system value or service attribute was changed.
917	985	1371	Old Value Continued	Char(250)	Continuation of the value of the system value or service attribute before it was changed.
		1621	New Value Continued Extension	Char(1000)	Second continuation of the value to which the system value or service attribute was changed.
		2621	Old Value Continued Extension	Char(1000)	Second continuation of the value of the system value or service attribute before it was changed.

VA (Change of Access Control List) journal entries

This table provides the format of the VA (Change of Access Control List) journal entries.

Table 219. VA (Change of Access Control List) journal entries. QASYVAJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Status	Char(1)	Status of request. S Successful F Failed
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer issuing the request to change the access control list.
187	255	641	Requester Name	Char(10)	The name of the user issuing the request.
197	265	651	Action Performed	Char(1)	The action performed on the access control profile: A Addition C Modification D Deletion
198	266	652	Resource Name	Char(260)	The name of the resource to be changed.

VC (Connection Start and End) journal entries

This table provides the format of the VC (Connection Start and End) journal entries.

Table 220. VC (Connection Start and End) journal entries. QASYVCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 220. VC (Connection Start and End) journal entries (continued). QASYVCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Connect Action.	Char(1)	The connection action that occurred. S Start E End R Reject
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer associated with the connection request.
187	255	641	Connection User	Char(10)	The name of the user associated with the connection request.
197	265	651	Connect ID	Char(5)	The start or stop connection ID.
202	270	656	Rejection Reason	Char(1)	The reason why the connection was rejected: A Automatic disconnect (timeout), share removed, or administrative permissions lacking E Error, session disconnect, or incorrect password N Normal disconnection or user name limit P No access permission to shared resource
203	271	657	Network Name	Char(12)	The network name associated with the connection.

VF (Close of Server Files) journal entries

This table provides the format of the VF (Close of Server Files) journal entries.

Table 221. VF (Close of Server Files) journal entries. QASYVFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 221. VF (Close of Server Files) journal entries (continued). QASYVFJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Close Reason	Char(1)	The reason why the file was closed. A Administrative disconnection N Normal client disconnection S Session disconnection
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer requesting the close.
187	255	641	Connection User	Char(10)	The name of the user requesting the close.
197	265	651	File ID	Char(5)	The ID of the file being closed.
202	270	656	Duration	Char(6)	The number of seconds the file was open.
208	276	662	Resource Name	Char(260)	The name of the resource owning the accessed file.

VL (Account Limit Exceeded) journal entries

This table provides the format of the VL (Account Limit Exceeded) journal entries.

Table 222. VL (Account Limit Exceeded) journal entries. QASYVLJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Reason	Char(1)	The reason why the limit was exceeded. A Account expired D Account disabled L Logon hours exceeded U Unknown or unavailable W Workstation not valid
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.

Table 222. VL (Account Limit Exceeded) journal entries (continued). QASYVLJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer with the account limit violation.
187	255	641	User	Char(10)	The name of the user with the account limit violation.
197	265	651	Resource Name	Char(260)	The name of the resource being used.

VN (Network Log On and Off) journal entries

This table provides the format of the VN (Network Log On and Off) journal entries.

Table 223. VN (Network Log On and Off) journal entries. QASYVNJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Log Type	Char(1)	The type of event that occurred: F Logoff requested O Logon requested R Logon rejected
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer for the event.
187	255	641	User	Char(10)	The user who logged on or off.
197	265	651	User Privilege	Char(1)	Privilege of user logging on: A Administrator G Guest U User
198	266	652	Reject Reason	Char(1)	The reason why the log on attempt was rejected: A Access denied F Forced off due to logon limit P Incorrect password

Table 223. VN (Network Log On and Off) journal entries (continued). QASYVNJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
199	267	653	Additional Reason	Char(1)	Details of why access was denied: A Account expired D Account disabled L Logon hours not valid R Requester ID not valid U Unknown or unavailable

VO (Validation List) journal entries

This table provides the format of the VO (Validation List) journal entries.

Table 224. VO (Validation List) journal entries. QASYVOJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564 and "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565 for field listing.
	224	610	Entry Type	Char(1)	The type of entry. A Add validation list entry C Change validation list entry F Find validation list entry R Remove validation list entry U Unsuccessful verify of a validation list entry V Successful verify of a validation list entry
	225	611	Unsuccessful Type	Char(1)	Type of unsuccessful verify. E Encrypted data is incorrect I Entry ID was not found V Validation list was not found
	226	612	Validation List	Char(10)	The name of the validation list.
	236	622	Library Name	Char(10)	The name of the library that the validation list is in.
	246	632	Encrypted Data	Char(1)	Data value to be encrypted. Y Data to be encrypted was specified on the request. N Data to be encrypted was not specified on the request.

Table 224. VO (Validation List) journal entries (continued). QASYVOJ4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	247	633	Entry Data	Char(1)	Entry data value. Y Entry data was specified on the request. N Entry data was not specified on the request.
	248	634	Entry ID Length	Binary(4)	The length of the entry ID.
	250	636	Data length	Binary(4)	The length of the entry data.
	252	638	Encrypted Data Attribute	Char (1)	Encrypted data. ' ' An encrypted data attribute was not specified. 0 The data to be encrypted can only be used to verify an entry. This is the default. 1 The data to be encrypted can be used to verify an entry and the data can be returned on a find operation.
	253	639	X.509 Certificate attribute	Char (1)	X.509 Certificate.
	254	640	(Reserved Area)	Char (28)	
	282	668	Entry ID	Byte(100)	The entry ID.
	382	768	Entry Data	Byte(1000)	The entry data.
		1768	ASP name for validation list library	Char(10)	ASP name for validation list library
		1778	ASP number for validation list library	Char(5)	ASP number for validation list library

VP (Network Password Error) journal entries

This table provides the format of the VP (Network Password Error) journal entries.

Table 225. VP (Network Password Error) journal entries. QASYVPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 225. VP (Network Password Error) journal entries (continued). QASYVPJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Error Type	Char(1)	The type of error that occurred. P Password error
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer initiating the request.
187	255	641	User	Char(10)	The name of the user who attempted to log on.

VR (Network Resource Access) journal entries

This table provides the format of the VR (Network Resource Access) journal entries.

Table 226. VR (Network Resource Access) journal entries. QASYVRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Status	Char(1)	The status of the access. F Resource access failed S Resource access succeeded
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer requesting the resource.
187	255	641	User	Char(10)	The name of the user requesting the resource.

Table 226. VR (Network Resource Access) journal entries (continued). QASYVRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
197	265	651	Operation Type	Char(1)	The type of operation being performed: A Resource attributes modified C Instance of the resource created D Resource deleted P Resource permissions modified R Data read or run from a resource W Data written to resource X Resource was run
198	266	652	Return Code	Char(4)	The return code received if resource access is granted.
202	270	656	Server Message	Char(4)	The message code sent when access is granted.
206	274	660	File ID	Char(5)	The ID of the file being accessed.
211	279	665	Resource Name	Char(260)	Name of the resource being used.

VS (Server Session) journal entries

This table provides the format of the VS (Server Session) journal entries.

Table 227. VS (Server Session) journal entries. QASYVSJE/J4/J5 field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Session Action	Char(1)	The session action that occurred. E End session S Start session
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer requesting the session.
187	255	641	User	Char(10)	The name of the user requesting the session.

Table 227. VS (Server Session) journal entries (continued). QASYVSJE/J4/J5 field Description File

Offset			Field	Format	Description
JE	J4	J5			
197	265	651	User Privilege	Char(1)	The privilege level of the user for session start: A Administrator G Guest U User
198	266	652	Reason Code	Char(1)	The reason code for ending the session. A Administrator disconnect D Automatic disconnect (timeout), share removed, or administrative permissions lacking E Error, session disconnect, or incorrect password N Normal disconnection or user name limit R Account restriction

VU (Network Profile Change) journal entries

This table provides the format of the VU (Network Profile Change) journal entries.

Table 228. VU (Network Profile Change) journal entries. QASYVUJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Type	Char(1)	The type of record that was changed. G Group record U User record M User profile global information
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer requesting the user profile change.
187	255	641	User	Char(10)	The name of the user requesting the user profile change.

Table 228. VU (Network Profile Change) journal entries (continued). QASYVUJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
197	265	651	Action	Char(1)	Action requested: A Addition C Change D Deletion P Incorrect password
198	266	652	Resource Name	Char(260)	Name of the resource.

VV (Service Status Change) journal entries

This table provides the format of the VV (Service Status Change) journal entries.

Table 229. VV (Service Status Change) journal entries. QASYVVJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	The type of entry: C Service status changed E Server stopped P Server paused R Server restarted S Server started
157	225	611	Server Name	Char(10)	The name of the network server description that registered the event.
167	235	621	Server Date	Char(6)	The date on which the event was logged on the network server.
173	241	627	Server Time	Zoned(6,0)	The time when the event was logged on the network server.
179	247	633	Computer Name	Char(8)	The name of the computer requesting the change.
187	255	641	User	Char(10)	The name of the user requesting the change.

Table 229. VV (Service Status Change) journal entries (continued). QASYVVJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
197	265	651	Status	Char(1)	Status of the service request: A Service active B Start service pending C Continue paused service E Stop pending for service H Service pausing I Service paused S Service stopped
198	266	652	Service Code	Char(8)	The code of the service requested.
206	274	660	Text Set	Char(80)	The text being set by the service request.
286	354	740	Return Value	Char(4)	The return value from the change operation.
290	358	744	Service	Char(20)	The service that was changed.

X0 (Network Authentication) journal entries

This table provides the format of the X0 (Network Authentication) journal entries.

Table 230. X0 (Network Authentication) journal entries. QASYX0JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 230. X0 (Network Authentication) journal entries (continued). QASYX0JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Entry Type	Char(1)	The type of entry: 1 Service ticket valid 2 Service principals do not match 3 Client principals do not match 4 Ticket IP address mismatch 5 Decryption of the ticket failed 6 Decryption of authenticator failed 7 Realm is not within client local realms 8 Ticket is a replay attempt 9 Ticket not yet valid A Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error B Remote IP address mismatch C Local IP address mismatch D KRB_AP_PRIV or KRB_AP_SAFE timestamp error E KRB_AP_PRIV or KRB_AP_SAFE replay error F KRB_AP_PRIV or KRB_AP_SAFE sequence order error K GSS accept — expired credential L GSS accept — checksum error M GSS accept — channel bindingst N GSS unwrap or GSS verify expired context O GSS unwrap or GSS verify decrypt/decode P GSS unwrap or GSS verify checksum error Q GSS unwrap or GSS verify sequence error
	225	611	Status Code	Char(8)	The status of the request
	233	619	GSS Status Value	Char(8)	GSS status value
	241	627	Remote IP Address	Char(21)	Remote IP address
	262	648	Local IP Address	Char(21)	Local IP address
	283	669	Encrypted Addresses	Char(256)	Encrypted IP addresses

Table 230. X0 (Network Authentication) journal entries (continued). QASYX0JE/J4/J5 Field Description File

JE	Offset		Field	Format	Description
	J4	J5			
	539	925	Encrypted Addresses Indicator	Char(1)	Encrypted IP addresses indicator Y all addresses included N not all addresses included X not provided
	540	926	Ticket flags	Char(8)	Ticket flags
	548	934	Ticket Authentication Time	Char(8)	Ticket authentication time
	556	942	Ticket Start Time	Char(8)	Ticket start time
	564	950	Ticket End Time	Char(8)	Ticket end time
	572	958	Ticket Renew Time	Char(8)	Ticket renew until time
	580	966	Message Time Stamp	Char(8)	X0E time stamp
	588	974	GSS Expiration Time Stamp	Char(8)	GSS credential expiration time stamp or context expiration time stamp
	596	982	Server Principal CCSID	Binary(5)	Server principal (from ticket) CCSID
	600	986	Server Principal Length	Binary(4)	Server principal (from ticket) length
	602	988	Server Principal Indicator	Char(1)	Server principal (from ticket) indicator Y server principal complete N server principal not complete X not provided
	603	989	Server Principal	Char(512)	Server principal (from ticket)
	1115	1501	Server Principal Parameter CCSID	Binary(5)	Server principal (from ticket) parameter CCSID
	1119	1505	Server Principal Parameter Length	Binary(4)	Server principal (from ticket) parameter length
	1121	1507	Server Principal Parameter Indicator	Char(1)	Server principal (from ticket) parameter indicator Y server principal complete N server principal not complete X not provided
	1122	1508	Server Principal Parameter	Char(512)	Server principal parameter that ticket must match
	1634	2020	Client Principal CCSID	Binary(5)	Client principal (from authenticator) CCSID
	1638	2024	Client Principal Length	Binary(4)	Client principal (from authenticator) length

Table 230. X0 (Network Authentication) journal entries (continued). QASYX0JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	1640	2026	Client Principal Indicator	Char(1)	Client principal (from authenticator) indicator Y client principal complete N client principal not complete X not provided
	1641	2027	Client Principal	Char(512)	Client principal from authenticator
	2153	2539	Client Principal CCSID	Binary(5)	Client principal (from ticket) CCSID
	2157	2543	Client Principal Length	Binary(4)	Client principal (from ticket) length
	2159	2545	Client Principal Indicator	Char(1)	Client principal (from ticket) indicator Y client principal complete N client principal not complete X not provided
	2160	2546	Client Principal	Char(512)	Client principal from ticket
	2672	3058	GSS Server Principal CCSID	Binary(5)	Server principal (from GSS credential) CCSID
	2676	3062	GSS Server Principal Length	Binary(4)	Server principal (from GSS credential) length
	2678	3064	GSS Server Principal Indicator	Char(1)	Server principal (from GSS credential) indicator Y server principal complete N server principal not complete X not provided
	2679	3065	GSS Server Principal	Char(512)	Server principal from GSS credential
	3191	3577	GSS Local Principal CCSID	Binary(5)	GSS local principal name CCSID
	3195	3581	GSS Local Principal Length	Binary(4)	GSS local principal name length
	3197	3583	GSS Local Principal Indicator	Char(1)	GSS local principal name indicator Y local principal complete N local principal not complete X not provided
	3198	3584	GSS Local Principal	Char(512)	GSS local principal
	3710	4096	GSS Remote Principal CCSID	Binary(5)	GSS remote principal name CCSID

Table 230. X0 (Network Authentication) journal entries (continued). QASYX0JE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	3714	4100	GSS Remote Principal Length	Binary(4)	GSS remote principal name length
	3716	4102	GSS Remote Principal Indicator	Char(1)	GSS remote principal name indicator Y remote principal complete N remote principal not complete X not provided
	3717	4103	GSS Remote Principal	Char(512)	GSS remote principal

X1 (Identity Token) journal entries

This table provides the format of the X1 (Identity Token) journal entries.

Table 231. X1 (Identity Token) journal entries. QASYX1J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564,"Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
		610	Entry Type	Char(1)	The type of entry: D Delegate of identity token was successful F Delegate of identity token failed G Get user from identity token was successful U Get user from identity token failed
		611	Reason Code	Binary (5)	Reason code for failed request: 9 Token length mismatch 10 EIM identifier mismatch 11 Application instance ID mismatch 12 Token signature not valid 13 Identity token not valid 14 Target user not found 16 Key handle not valid 17 Token version not supported 18 Public key not found Note: On a failure, only the information that has been validated up to the point of failure will be filled in the text fields.

Table 231. X1 (Identity Token) journal entries (continued). QASYX1J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		615	Reserved	Char(7)	Reserved
		622	Data CCSID	Binary(5)	The CCSID of the data in the text fields
		626	Receiver length	Binary(5)	The length of the data in the receiver field.
		630	Receiver	Char(508)	The receiver of the identity token that either failed the request or was successful. The data in this field will be in the format: <EIMID>receiver_eimID </EIMID> <APPID>RECEIVER_appID </APPID> <TIMESTAMP>receiver_timestamp </TIMESTAMP>. The timestamp will only be included on delegate requests.
		1138	Sender Length	Binary(5)	The length of the data in the sender field.
		1142		Char(508)	The last sender of the identity token that either failed the request or was successful. The data in this field will be in the format The data in this field will be in the format: <EIMID>sender_eimID</EIMID> <APPID>sender_appID</APPID> <TIMESTAMP>sender_timestamp</TIMESTAMP>
		1650	Initiator Length	Binary(5)	The length of the data in the initiator field.
		1654	Initiator	Char(508)	The initiator of the identity token request. If the sender and initiator are the same, the initiator length field will be 0. The data in this field will be in the format: <EIMID>initiator_eimID</EIMID> <APPID>initiator_appID</APPID> <TIMESTAMP>initiator_timestamp</TIMESTAMP>
		2162	Chain Length	Binary(5)	The length of the data in the chain field.
		2166	Chain	Char(2036)	The chain of senders between the initiator and the last sender. The chain will be in the order of latest to earliest. If there are no other senders, then the chain length field will be 0. This field will be truncated if the chain is longer than the length of this field. The data in this field will be in the format: <SNDRz><EIMID>sndrz_eimID</EIMID> <APPID>sndrz_appID</APPID> <TIMESTAMP>sndrz_timestamp </TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Chain Entries	Binary(5)	The number of entries in the chain field.
		4206	Chain Entries Available	Binary(5)	The number of available entries for the chain of senders. This number might be greater than the number of entries in the field if the chain field is truncated.
		4210	Source Registry Length	Binary(5)	The length of the data in the source registry field.
		4214	Source Registry	Char(508)	The source registry specified in the identity token.

Table 231. X1 (Identity Token) journal entries (continued). QASYX1J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		4722	Source Registry User Length	Binary(5)	The length of the data in the source registry user field.
		4726	Source Registry User	Char(508)	The source registry user specified in the identity token.
		5234	Target Registry Length	Binary(5)	The length of the data in the target registry field.
		5238	Target Registry	Char(508)	The target registry specified.
		5746	Target Registry User Length	Binary(5)	The length of the data in the target registry user field.
		5750	Target Registry User	Char(508)	The target registry user to which the identity token maps.

XD (Directory Server Extension) journal entries

This table provides the format of the XD (Directory Server Extension) journal entries.

Table 232. XD (Directory Server Extension) journal entries. QASYXDJ5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
		610	Entry Type	Char(1)	The type of entry: G Group names. Field 1 through Field 5 contain group names.
		611	Cross Reference	Char(36)	Cross reference string used to correlate this entry with the DI entry using these groups. More than one DI entry can refer to this XD entry if multiple LDAP requests use the same set of groups.
		647	Reserved	Char(100)	
		747	Field 1 CCSID	Bin(5)	The CCSID value for field 1.
		751	Field 1 Length	Bin(4)	The length of the data in field 1.
		753	Field 1	Char(2002)	Field 1 data For entry type G, this field will contain a group name from a group membership assertion.

Table 232. XD (Directory Server Extension) journal entries (continued). QASYXDJ5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
		2755	Field 2 CCSID	Bin(5)	The CCSID value for field 2.
		2759	Field 2 Length	Bin(4)	The length of the data in field 2.
		2761	Field 2	Char(2002)	Field 2 data For entry type G, this field will contain a group name from a group membership assertion.
		4763	Field 3 CCSID	Bin(5)	The CCSID value for field 3.
		4767	Field 3 Length	Bin(4)	The length of the data in field 3.
		4769	Field 3	Char(2002)	Field 3 data For entry type G, this field will contain a group name from a group membership assertion.
		6771	Field 4 CCSID	Bin(5)	The CCSID value for field 4.
		6775	Field 4 Length	Bin(4)	The length of the data in field 4.
		6777	Field 4	Char(2002)	Field 4 data For entry type G, this field will contain a group name from a group membership assertion.
		8779	Field 5 CCSID	Bin(5)	The CCSID value for field 5.
		8783	Field 5 Length	Bin(4)	The length of the data in field 5.
		8785	Field 5	Char(2002)	Field 5 data For entry type G, this field will contain a group name from a group membership assertion.

YC (Change to DLO Object) journal entries

This table provides the format of the YC (Change to DLO Object) journal entries.

Table 233. YC (Change to DLO Object) journal entries. QASYJCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.

Table 233. YC (Change to DLO Object) journal entries (continued). QASYCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
156	224	610	Entry Type	Char(1)	Object access C Change of a DLO object
157	225	611	Object Name	Char(10)	Name of the object
167	235	621	Library Name	Char(10)	Name of the library
177	245	631	Object Type	Char(8)	Type of object
185	253	639	Office User	Char(10)	User profile of the office user
195	263	649	Folder or Document Name	Char(12)	Name of the document or folder
207	275	661	(Reserved Area)	Char(8)	
215	283	669	Folder Path	Char(63)	The folder containing the document library object
278	346	732	On Behalf of User	Char(10)	User working on behalf of another user
288	356	742	Access Type	Packed(5,0)	Type of access ¹
¹ See "Numeric codes for access types" on page 706 for a list of the codes for access types.					

YR (Read of DLO Object) journal entries

This table provides the format of the YR (Read of DLO Object) journal entries.

Table 234. YR (Read of DLO Object) journal entries. QASYRJE/J4/J5 Field Description File

Offstes			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	Object access R Read of a DLO object
157	225	611	Object Name	Char(10)	Name of the object
167	235	621	Library Name	Char(10)	Name of the library
177	245	631	Object Type	Char(8)	Type of object
185	253	639	Office User	Char(10)	User profile of the office user
195	263	649	Folder or Document Name	Char(12)	Name of the document library object
207	275	661	(Reserved Area)	Char(8)	
215	283	669	Folder Path	Char(63)	The folder containing the document library object

Table 234. YR (Read of DLO Object) journal entries (continued). QASYRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
278	346	732	On Behalf of User	Char(10)	User working on behalf of another user
288	356	742	Access Type	Packed(5,0)	Type of access ¹

¹ See "Numeric codes for access types" on page 706 for a list of the codes for access types.

ZC (Change to Object) journal entries

This table provides the format of the ZC (Change to Object) journal entries.

Table 235. ZC (Change to Object) journal entries. QASYZCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	Object access C Change of an object U Upgrade of open access to an object
157	225	611	Object Name	Char(10)	Name of the object
167	235	621	Library Name	Char(10)	Name of the library in which the object is located
177	245	631	Object Type	Char(8)	Type of object
185	253	639	Access Type	Packed(5,0)	Type of access ¹

Table 235. ZC (Change to Object) journal entries (continued). QASYZCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
188	256	642	Access Specific Data	Char(50)	<p>Specific data about the access</p> <p>When the object type is *IMGCLG, this field contains the following format:</p> <p>Char 3 Index number of the image catalog entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Char 32 Volume ID of the image catalog entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Char 1 Access type for the entry. The possible values are listed below.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>R The file containing the image catalog entry is read-only.</p> <p>W The file containing the image catalog entry is read/write capable.</p> <p>Char 1 The write protection for the entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Y The file containing the image catalog entry is write protected.</p> <p>N The file containing the image catalog entry is not write protected.</p> <p>Char 10 The name of the virtual device.</p> <p>Blank Indicates the operation was against an image catalog or the image catalog is not in Ready status.</p> <p>Char 3 Not used.</p> <p>When the object type is an integrated file system object, this field contains further information identifying the change request. See the QSYSINC include file, QPOLJRNL.H for the possible values.</p>
238			(Reserved Area)	Char(20)	
	306	692	(Reserved Area)	Char(18)	

Table 235. ZC (Change to Object) journal entries (continued). QASYZCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
	324	710	Object Name Length ²	Binary (4)	The length of the object name.
258	326	712	Object Name CCSID ²	Binary(5)	The coded character set identifier for the object name.
262	330	716	Object Name Country or Region ID ²	Char(2)	The Country or Region ID for the object name.
264	332	718	Object Name Language ID ²	Char(3)	The language ID for the object name.
267	335	721	(Reserved area)	Char(3)	
270	338	724	Parent File ID ² ₃	Char(16)	The file ID of the parent directory.
286	354	740	Object File ID ² ₃	Char(16)	The file ID of the object.
302	370	756	Object Name ²	Char(512)	The name of the object.
	882	1268	Object File ID	Char(16)	The file ID of the object.
	898	1284	ASP Name ⁶	Char(10)	The name of the ASP device.
	908	1294	ASP Number ⁶	Char(5)	The number of the ASP device.
	913	1299	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	917	1303	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	919	1305	Path Name Language ID	Char(3)	The language ID for the path name.
	922	1308	Path Name Length	Binary(4)	The length of the path name.
	924	1310	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	925	1311	Relative Directory File ID ⁴	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ⁴
	941	1327	Path Name ⁵	Char(5002)	The path name of the object.

Table 235. ZC (Change to Object) journal entries (continued). QASYZCJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1					See "Numeric codes for access types" on page 706 for a list of the codes for access types.
2					These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.
3					An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
4					If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.
5					This is a variable length field. The first 2 bytes contain the length of the path name.
6					If the object is in a library, this is the ASP information of the object's library. If the object is not in a library, this is the ASP information of the object.

ZR (Read of Object) journal entries

This table provides the format of the ZR (Read of Object) journal entries.

Table 236. ZR (Read of Object) journal entries. QASYZRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
1	1	1			Heading fields common to all entry types. See "Standard heading fields for audit journal entries QJORDJE5 Record Format (*TYPE5)" on page 564, "Standard heading fields for audit journal entries QJORDJE4 Record Format (*TYPE4)" on page 565, and "Standard heading fields for audit journal entries QJORDJE2 Record Format (*TYPE2)" on page 567 for field listing.
156	224	610	Entry Type	Char(1)	Object access R Read of an object
157	225	611	Object Name	Char(10)	Name of the object
167	235	621	Library Name	Char(10)	Name of the library in which the object is located
177	245	631	Object Type	Char(8)	Type of object
185	253	639	Access Type	Packed(5,0)	Type of access ¹

Table 236. ZR (Read of Object) journal entries (continued). QASYZRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
188	256	642	Access Specific Data	Char(50)	<p>Specific data about the access.</p> <p>When the object type is *IMGCLG, this field contains the following format:</p> <p>Char 3 Index number of the image catalog entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Char 32 Volume ID of the image catalog entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Char 1 Access type for the entry. The possible values are listed below.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>R The file containing the image catalog entry is read-only.</p> <p>W The file containing the image catalog entry is read/write capable.</p> <p>Char 1 The write protection for the entry.</p> <p>Blank Indicates the operation was against an image catalog.</p> <p>Y The file containing the image catalog entry is write protected.</p> <p>N The file containing the image catalog entry is not write protected.</p> <p>Char 10 The name of the virtual device.</p> <p>Blank Indicates the operation was against an image catalog or the image catalog is not in Ready status.</p> <p>Char 3 Not used.</p>
238			(Reserved Area)	Char(20)	
	306	692	(Reserved Area)	Char(18)	
	324	710	Object Name Length ²	Binary(4)	The length of the object name.
258	326	712	Object Name CCSID ²	Binary(5)	The coded character set identifier for the object name.
262	330	716	Object Name Country or Region ID ²	Char(2)	The Country or Region ID for the object name.

Table 236. ZR (Read of Object) journal entries (continued). QASYZRJE/J4/J5 Field Description File

Offset			Field	Format	Description
JE	J4	J5			
264	332	718	Object Name Language ID ²	Char(3)	The language ID for the object name.
267	335	721	(Reserved area)	Char(3)	
270	338	724	Parent File ID ^{2,3}	Char(16)	The file ID of the parent directory.
286	354	740	Object File ID ^{2,3}	Char(16)	The file ID of the object.
302	370	756	Object Name ²	Char(512)	The name of the object.
	882	1268	Object File ID	Char(16)	The file ID of the object.
	898	1284	ASP Name	Char(10)	The name of the ASP device.
	908	1294	ASP Number	Char(5)	The number of the ASP device.
	913	1299	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.
	917	1303	Path Name Country or Region ID	Char(2)	The Country or Region ID for the path name.
	919	1305	Path Name Language ID	Char(3)	The language ID for the path name.
	922	1308	Path Name Length	Binary(4)	The length of the path name.
	924	1310	Path Name Indicator	Char(1)	Path name indicator: Y The Path Name field contains complete absolute path name for the object. N The Path Name field does not contain an absolute path name for the object, instead it contains a relative path name. The Relative Directory File ID field is valid and can be used to form an absolute path name with this relative path name.
	925	1311	Relative Directory File ID ⁴	Char(16)	When the Path Name Indicator field is N, this field contains the file ID of the directory that contains the object identified in the Path Name field. Otherwise it contains hex zeros. ⁴
	941	1327	Path Name ⁵	Char(5002)	The path name of the object.

¹ See "Numeric codes for access types" on page 706 for a list of the codes for access types.

² These fields are used only for objects in the "root" (/), QOpenSys, and user-defined file systems.

³ An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

⁴ If the Path Name Indicator field is N, but the Relative Directory File ID is hex zeros, then there was some error in determining the path name information.

⁵ This is a variable length field. The first 2 bytes contain the length of the path name.

Numeric codes for access types

This table lists the access codes used for object auditing journal entries in files QASYJCJE/J4/J5, QASYRJE/J4/J5, QASYZCJE/J4/J5, and QASYZRJE/J4/J5.

Table 237. Numeric codes for access types

Code	Access type	Code	Access type	Code	Access type
1	Add	26	Load	51	Send
2	Activate Program	27	List	52	Start
3	Analyze	28	Move	53	Transfer
4	Apply	29	Merge	54	Trace
5	Call or TFRCTL	30	Open	55	Verify
6	Configure	31	Print	56	Vary
7	Change	32	Query	57	Work
8	Check	33	Reclaim	58	Read/Change DLO Attribute
9	Close	34	Receive	59	Read/Change DLO Security
10	Clear	35	Read	60	Read/Change DLO Content
11	Compare	36	Reorganize	61	Read/Change DLO all parts
12	Cancel	37	Release	62	Add Constraint
13	Copy	38	Remove	63	Change Constraint
14	Create	39	Rename	64	Remove Constraint
15	Convert	40	Replace	65	Start Procedure
16	Debug	41	Resume	66	Get Access on **OOPOOL
17	Delete	42	Restore	67	Sign object
18	Dump	43	Retrieve	68	Remove all signatures
19	Display	44	Run	69	Clear a signed object
20	Edit	45	Revoke	70	MOUNT
21	End	46	Save	71	Unload
22	File	47	Save with Storage Free	72	End Rollback
23	Grant	48	Save and Delete		
24	Hold	49	Submit		
25	Initialize	50	Set		

Appendix G. Commands and menus for security commands

The SECTOOLS (Security Tools) menu, the SECBATCH (Submit or Schedule Security Reports to Batch) menu, the Configure System Security (CFGSYSSEC) and Revoke Public Authority (RVKPUBAUT) commands are four security tools you can use to configure your system security.

Two menus are available for security tools:

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

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

Options on the Security Tools menu

You can use the Security Tools (SECTOOLS) menu to simplify the management and control of the security on your system with plenty of options and commands that it provides.

This figure shows the part of the SECTOOLS menu that relates to user profiles.

To access this menu, type GO SECTOOLS.

```
SECTOOLS                Security Tools
Select one of the following:

Work with profiles
  1. Analyze default passwords

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

  5. Display activation schedule
  6. Change activation schedule entry

  7. Display expiration schedule
  8. Change expiration schedule entry
  9. Print profile internals
```

Table 238 describes these menu options and the associated commands:

Table 238. Tool commands for user profiles

Menu ¹ option	Command name	Description	Database file used
1	ANZDFTPWD	Use the Analyze Default Passwords command to report on and take action on user profiles that have a password equal to the user profile name.	QASECPWD ²
2	DSPACTPRFL	Use the Display Active Profile List command to display or print the list of user profiles that are exempt from ANZPRFACT processing.	QASECIDL ²

Table 238. Tool commands for user profiles (continued)

Menu ¹ option	Command name	Description	Database file used
3	CHGACTPRFL	Use the Change Active Profile List command to add and remove user profiles from the exemption list for the ANZPRFACT command. A user profile that is on the active profile list is permanently active (until you remove the profile from the list). The ANZPRFACT command does not disable a profile that is on the active profile list, no matter how long the profile has been inactive.	QASECIDL ²
4	ANZPRFACT	Use the Analyze Profile Activity command to disable user profiles that have not been used for a specified number of days. After you use the ANZPRFACT command to specify the number of days, the system runs the ANZPRFACT job nightly. You can use the CHGACTPRFL command to exempt user profiles from being disabled.	QASECIDL ²
5	DSPACTSCD	Use the Display Activation Schedule command to display or print information about the schedule for enabling and disabling specific user profiles. You create the schedule with the CHGACTSCDE command.	QASECACT ²
6	CHGACTSCDE	Use the Change Activation Schedule Entry command to make a user profile available for sign on only at certain times of the day or week. For each user profile that you schedule, the system creates job schedule entries for the enable and disable times.	QASECACT ²
7	DSPEXPSCDE	Use the Display Expiration Schedule command to display or print the list of user profiles that are scheduled to be disabled or removed from the system in the future. You use the CHGEXPSCDE or CHGUSRPRF command to set up user profiles to expire.	
8	CHGEXPSCDE	Use the Change Expiration Schedule Entry command to schedule a user profile for removal. You can remove it temporarily (by disabling it) or you can delete it from the system. This command uses a job schedule entry that runs every day at 00:01 (1 minute after midnight). Use the DSPEXPSCD command to display the user profiles that are scheduled to expire.	
9	PRTPRFINT	Use the Print Profile Internals command to print a report of internal information about the number of entries in a user profile (*USRPRF) object.	

Notes:

1. Options are from the SECTOOLS menu.
2. This file is in the QUSRSYS library.

You can page down on the menu to see additional options. Table 239 describes the menu options and associated commands for security auditing:

Table 239. Tool commands for security auditing

Menu ¹ option	Command name	Description	Database file used
10	CHGSECAUD	Use the Change Security Auditing command to set up security auditing and to change the system values that control security auditing. When you run the CHGSECAUD command, the system creates the security audit (QAUDJRN) journal if it does not exist. The CHGSECAUD command provides options that make it simpler to set the QAUDLVL (audit level) and QAUDLVL2 (audit level extension) system values. You can specify *ALL to activate all of the possible audit level settings. Or, you can specify *DFTSET to activate the most commonly used settings (*AUTFAIL, *CREATE, *DELETE, *SECURITY, and *SAVRST). Note: If you use the security tools to set up auditing, make sure to plan for management of your audit journal receivers. Otherwise, you might quickly encounter problems with disk utilization.	
11	DSPSECAUD	Use the Display Security Auditing command to display information about the security audit journal and the system values that control security auditing.	
12	CPYAUDJRNE	Use the Copy Audit Journal Entries command to copy entries from the security audit journal to an output file.	QASYxxJ5 ²
¹	Options are from the SECTOOLS menu.		
²	xx is the two-character journal entry type. For example, the model output file for AE journal entries is QSYS/QASYAEJ5. The model output files are described in Appendix F, "Layout of audit journal entries," on page 563 of this topic collection.		

How to use the Security Batch menu

You can use the security batch menu to submit one or more of the Security Tools reports to a job queue to be run later as a batch job. You can also choose to schedule any of the Security Tools reports as batch jobs to be submitted once or to be submitted at regular intervals. Examples in this topic demonstrate how to use the security batch menu.

Here is the first part of the SECBATCH menu:

```

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

```

- ```

Submit Reports to Batch
 1. Adopting objects
 2. Audit journal entries
 3. Authorization list authorities
 4. Command authority
 5. Command private authorities
 6. Communications security
 7. Directory authority
 8. Directory private authority
 9. Document authority
10. Document private authority
11. File authority
12. File private authority
13. Folder authority

```

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

```

 Submit Job (SBMJOB)
Type choices, press Enter.
Command to run > PRTADPOBJ USRPRF(*ALL)

...
Job name *JOBD Name, *JOBD
Job description *USRPRF Name, *USRPRF
 Library Name, *LIBL, *CURLIB
Job queue *JOBD Name, *JOBD
 Library Name, *LIBL, *CURLIB
Job priority (on JOBQ) *JOBD 1-9, *JOBD
Output priority (on OUTQ) *JOBD 1-9, *JOBD
Print device *CURRENT Name, *CURRENT, *USRPRF...

```

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

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

```

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

```

- ```

 28. User objects
 29. User profile information
 30. User profile internals
 31. Check object integrity

Schedule Batch Reports
 40. Adopting objects
 41. Audit journal entries
 42. Authorization list authorities
 43. Command authority
 44. Command private authority
 45. Communications security
 46. Directory authority

```

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

```

Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . Name, *JOBID
Command to run . . . . . > PRTADPOBJ USRPRF(*ALL)

-----
-----
-----
-----
-----
Frequency . . . . . *ONCE, *WEEKLY, *MONTHLY
Schedule date, or . . . . . *CURRENT Date, *CURRENT, *MONTHST
Schedule day . . . . . *NONE *NONE, *ALL, *MON, *TUE.
+ for more values
Schedule time . . . . . *CURRENT Time, *CURRENT

```

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

Options on the security batch menu

This table describes the menu options and the associated commands for security reports.

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

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

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

Table 240. Commands for security reports

Menu ¹ option	Command name	Description	Database file used
1, 40	PRTADPOBJ	Use the Print Adopting Objects command to print a list of objects that adopt the authority of the specified user profile. You can specify a single profile, a generic profile name (such as all profiles that begin with Q), or all user profiles on the system. This report has two versions. The full report lists all adopted objects that meet the selection criteria. The changed report lists differences between adopted objects that are currently on the system and adopted objects that were on the system the last time that you ran the report.	QSECADPOLD ²
2, 41	DSPAUDJRNE ⁶	Use the Display Audit Journal Entries command to display or print information about entries in the security audit journal. You can select specific entry types, specific users, and a time period.	QASYxxJ5 ³

Table 240. Commands for security reports (continued)

Menu ¹ option	Command name	Description	Database file used
3, 42	PRTPVTAUT *AUTL	<p>When you use the Print Private Authorities command for *AUTL objects, you receive a list of all the authorization lists on the system. The report includes the users who are authorized to each list and what authority the users have for the list. Use this information to help you analyze sources of object authority on your system.</p> <p>This report has three versions. The full report lists all authorization lists on the system. The changed report lists additions and changes to authorization since you last ran the report. The deleted report lists users whose authority to the authorization list has been deleted since you last ran the report.</p> <p>When you print the full report, you have the option to print a list of objects that each authorization list secures. The system will create a separate report for each authorization list.</p>	QSECATLOLD ²
6, 45	PRTCMNSEC	<p>Use the Print Communications Security command to print the security-relevant settings for objects that affect communications on your system. These settings affect how users and jobs can enter your system.</p> <p>This command produces two reports: a report that displays the settings for configuration lists on the system and a report that lists security-relevant parameters for line descriptions, controllers, and device descriptions. Each of these reports has a full version and a changed version.</p>	QSECCMNOLD ²
15, 54	PRTJOBDAUT	<p>Use the Print Job Description Authority command to print a list of job descriptions that specify a user profile and have public authority that is not *EXCLUDE. The report shows the special authorities for the user profile that is specified in the job description.</p> <p>This report has two versions. The full report lists all job description objects that meet the selection criteria. The changed report lists differences between job description objects that are currently on the system and job description objects that were on the system the last time that you ran the report.</p>	QSECJBDOLD ²

Table 240. Commands for security reports (continued)

Menu ¹ option	Command name	Description	Database file used
See note 4	P RTPUBAUT	<p>Use the Print Publicly Authorized Objects command to print a list of objects whose public authority is not *EXCLUDE. When you run the command, you specify the type of object and the library or libraries for the report. Use the RTPUBAUT command to print information about objects that every user on the system can access.</p> <p>This report has two versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report.</p>	QPBxxxxx ⁵
See note 4.	P RTPVTAUT	<p>Use the Print Private Authorities command to print a list of the private authorities to objects of the specified type in the specified library. Use this report to help you determine the sources of authority to objects.</p> <p>This report has three versions. The full report lists all objects that meet the selection criteria. The changed report lists differences between the specified objects that are currently on the system and objects (of the same type in the same library) that were on the system the last time that you ran the report. The deleted report lists users whose authority to an object has been deleted since you last printed the report.</p>	QPVxxxxx ⁵
24, 63	P RTQAUT	<p>Use the Print Queue Authority command to print the security settings for output queues and job queues on your system. These settings control who can view and change entries in the output queue or job queue.</p> <p>This report has two versions. The full report lists all output queue and job queue objects that meet the selection criteria. The changed report lists differences between output queue and job queue objects that are currently on the system and output queue and job queue objects that were on the system the last time that you ran the report.</p>	QSECQOLD ²

Table 240. Commands for security reports (continued)

Menu ¹ option	Command name	Description	Database file used
25, 64	PRTSBSDAUT	<p>Use the Print Subsystem Description command to print the security-relevant communications entries for subsystem descriptions on your system. These settings control how work can enter your system and how jobs run. The report prints a subsystem description only if it has communications entries that specify a user profile name.</p> <p>This report has two versions. The full report lists all subsystem description objects that meet the selection criteria. The changed report lists differences between subsystem description objects that are currently on the system and subsystem description objects that were on the system the last time that you ran the report.</p>	QSECSBDOLD ²
26, 65	PRTSYSSECA	<p>Use the Print System Security Attributes command to print a list of security-relevant system values and network attributes. The report shows the current value and the recommended value.</p>	
27, 66	PRTRGPGM	<p>Use the Print Trigger Programs command to print a list of trigger programs that are associated with database files on your system.</p> <p>This report has two versions. The full report lists every trigger program that is assigned and meets your selection criteria. The changed report lists trigger programs that have been assigned since the last time that you ran the report.</p>	QSECTRGOLD ²
28, 67	PRTUSROBJ	<p>Use the Print User Objects command to print a list of the user objects (objects not supplied by IBM) that are in a library. You might use this report to print a list of user objects that are in a library (such as QSYS) that is in the system portion of the library list.</p> <p>This report has two versions. The full report lists all user objects that meet the selection criteria. The changed report lists differences between user objects that are currently on the system and user objects that were on the system the last time that you ran the report.</p>	QSECPUOLD ²
29, 68	PRTUSRPRF	<p>Use the Print User Profile command to analyze user profiles that meet specified criteria. You can select user profiles based on special authorities, user class, or a mismatch between special authorities and user class. You can print authority information, environment information, or password information.</p>	
30, 69	PRTPRFINT	<p>Use the Print Profile Internals command to print a report of internal information about the number of entries contained in a user profile (*USRPRF) object.</p>	

Table 240. Commands for security reports (continued)

Menu ¹ option	Command name	Description	Database file used
31, 70	CHKOBJITG	Use the Check Object Integrity command to determine whether operable objects (such as programs) have been changed without using a compiler. This command can help you to detect attempts to introduce a virus program on your system or to change a program to perform unauthorized instructions.	
¹	Options are from the SECBATCH menu.		
²	This file is in the QUSRSYS library.		
³	xx is the two-character journal entry type. For example, the model output file for AE journal entries is QSYS/QASYAEJ5. The model output files are described in Appendix F, "Layout of audit journal entries," on page 563 of this topic collection.		
⁴	The SECTOOLS menu contains options for the object types that are typically of concern to security administrators. For example, use options 11 or 50 to run the PRTPUBAUT command against *FILE objects. Use the general options (18 and 57) to specify the object type. Use options 12 and 51 to run the PRTPVTAUT command against *FILE objects. Use the general options (19 and 58) to specify the object type.		
⁵	The xxxxxx in the name of the file is the object type. For example, the file for program objects is called QPBPGM for public authorities and QPVPGM for private authorities. The files are in the QUSRSYS library. The file contains a member for each library for which you have printed the report. The member name is the same as the library name.		
⁶	The DSPAUDJRNE command cannot process all security audit record types, and the command does not list all the fields for the records it does support.		

Commands for customizing security

This table describes the commands that you can use to customize the security on your system, which are on the SECTOOLS menu.

Table 241. Commands for customizing your system

Menu ¹ option	Command name	Description	Database file used
60	CFGSYSSEC	Use the Configure System Security command to set security-relevant system values to their recommended settings. The command also sets up security auditing on your system. "Values that are set by the Configure System Security command" on page 716 describes what the command does.	
61	RVKPUBAUT	Use the Revoke Public Authority command to set the public authority to *EXCLUDE for a set of security-sensitive commands on your system. "What the Revoke Public Authority command does" on page 718 lists the actions that the RVKPUBAUT command performs.	
¹	Options are from the SECTOOLS menu.		

Values that are set by the Configure System Security command

This table lists the system values that are set when you run the Configure System Security (CFGSYSSEC) command that runs a program that is called QSYS/QSECCFGS.

Table 242. Values set by the CFGSYSSEC command

System value name	Setting	System value description
QAUTOCFG	0 (No)	Automatic configuration of new devices
QAUTOVRT	0	The number of virtual device descriptions that the system will automatically create if no device is available for use.
QALWOBJRST	*NONE	Whether system state programs and programs that adopt authority can be restored
QDEVRCYACN	*DSCMSG (Disconnect with message)	System action when communications is re-established
QDSCJOBITV	120	Time period before the system takes action on a disconnected job
QDSPSGNINF	1 (Yes)	Whether users see the sign-on information display
QINACTITV	60	Time period before the system takes action on an interactive job
QINACTMSGQ	*ENDJOB	Action that the system takes for an inactive job
QLMTDEVSSN	1 (Yes)	Whether users are limited to signing on at one device at a time
QLMTSECOFR	1 (Yes)	Whether *ALLOBJ and *SERVICE users are limited to specific devices
QMAXSIGN	3	How many consecutive, unsuccessful sign-on attempts are allowed
QMAXSGNACN	3 (Both)	Whether the system disables the workstation or the user profile when the QMAXSIGN limit is reached.
QPWDEXPITV	60	How often users must change their passwords
QPWDMINLEN	6 (See note 3 and 5)	Minimum length for passwords
QPWDMAXLEN	8 (See note 4 and 5)	Maximum length for passwords
QPWDPOSDIF	1 (Yes) (See note 5)	Whether every position in a new password must differ from the same position in the last password
QPWDLMTCHR	See note 2 and 5	Characters that are not allowed in passwords
QPWDLMTAJC	1 (Yes) (See note 5)	Whether adjacent numbers are prohibited in passwords
QPWDLMTREP	2 (Cannot be repeated consecutively) (See note 5)	Whether repeating characters in are prohibited in passwords
QPWDRQDDGT	1 (Yes) (See note 5)	Whether passwords must have at least one number
QPWDRQDDIF	1 (32 unique passwords)	How many unique passwords are required before a password can be repeated

Table 242. Values set by the CFGSYSSEC command (continued)

System value name	Setting	System value description
QPWDRULES	<ul style="list-style-type: none"> • *MINLEN6 • *MAXLEN10 • *LMTSAMPOS • *LMTPRFNAME • *DGTMIN1 • *CHRLMTAJC • *DGLMTAJC • *DGLMTFST • *DGLMTLST • *SPCCHRLMTAJC • *SPCCHRLMTFST • *SPCCHRLMTLST (see note 6)	Rules for forming a valid password.
QPWDVLDPGM	*NONE	The user exit program that the system calls to validate passwords
QRMTSIGN	*FRCSIGNON	How the system handles a remote (pass-through or TELNET) sign-on attempt.
QRMTSVRATR	0 (Off)	Allows the system to be analyzed remotely.
QSECURITY	50	The level of security that is enforced
QVFYOBJRST	3	Verify object on restore
<p>Notes:</p> <ol style="list-style-type: none"> 1. If you are currently running with a QSECURITY value of 30 or lower, be sure to review the information in Chapter 2, "Using System Security (QSecurity) system value," on page 9 before you change to a higher security level. 2. The restricted characters are stored in message ID CPXB302 in the message file QSYS/QCPFMSG. They are shipped as AEIOU@\$#. You can use the Change Message Description (CHGMSGD) command to change the restricted characters. 3. If the minimum length for passwords is already greater than 6, the QPWDMINLEN system value will not be changed. 4. If the maximum length for passwords is already greater than 8, the QPWDMAXLEN system value will not be changed. 5. This system value is only changed when the QPWDRULES system value currently specifies a value of *PWDSYSVAL. 6. This system value will not be changed if its current value is *PWDSYSVAL. 		

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

- QSYSOPR
- QPGMR
- QUSER
- QSRV
- QSRVBAS

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

Changing the program

If some system values of the settings are not appropriate for your installation, you can create your own version of the program that processes the Configure System Security (**CFGSYSSEC**) command.

To change the program, perform the following steps:

1. Use the Retrieve CL Source (**RTVCLSRC**) command to copy the source for the program that runs when you use the **CFGSYSSEC** command. The program to retrieve is QSYS/QSECCFGS. When you retrieve it, give it a different name.
2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you do not replace the IBM-supplied QSYS/QSECCFGS program. Your program should have a different name.
3. Use the Change Command (**CHGCMD**) command to change the program to process command (PGM) parameter for the **CFGSYSSEC** command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYSECCFG, you need to type the following command:

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

Notes:

- a. If you change the QSYS/QSECCFGS program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.
- b. If you change the **RVKPUBAUT** command to use a different command processing program, then the digital signature of this command will no longer be valid.

What the Revoke Public Authority command does

You can use the Revoke Public Authority (RVKPUBAUT) command to set the public authority to *EXCLUDE for a set of commands and programs.

The RVKPUBAUT command runs a program that is called QSYS/QSECRVKP. As it is shipped, the QSECRVKP revokes public authority (by setting public authority to *EXCLUDE) for the commands that are listed in Table 243 on page 719 and the application programming interfaces (APIs) that are listed in Table 244 on page 719. When your system arrives, these commands and APIs have their public authority set to *USE.

The commands that are listed in Table 243 on page 719 and the APIs that are listed in Table 244 on page 719 all perform functions on your system that might provide an opportunity for mischief. As security administrator, you should explicitly authorize users to run these commands and programs rather than make them available to all system users.

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

Table 243. Commands whose public authority is set by the RVKPUBAUT command

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

The APIs in Table 244 are all in the QSYS library:

Table 244. Programs whose public authority is set by the RVKPUBAUT command

QTIENDSUP		
QTISTRSUP		
QWTCTLTR		
QWTSETTR		
QY2FTML		

As of V3R7, when you run the RVKPUBAUT command, the system sets the public authority for the root directory to *USE (unless it is already *USE or less).

Changing the program

If some of the settings are not appropriate for your installation, you can create your own version of the program that processes the Revoke Public Authority (**RVKPUBAUT**) command.

To change the program, perform the following steps:

1. Use the Retrieve CL Source (**RTVCLSRC**) command to copy the source for the program that runs when you use the **RVKPUBAUT** command. The program to retrieve is QSYS/QSECRVKP. When you retrieve it, give it a *different name*.
2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you *do not* replace the IBM-supplied QSYS/QSECRVKP program. Your program should have a different name.
3. Use the Change Command (**CHGCMD**) command to change the program to process command (PGM) parameter for the **RVKPUBAUT** command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYRVKPGM, you need to type the following command:

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

Notes:

- a. If you change the QSYS/QSECRVKP program, IBM cannot guarantee or imply reliability, serviceability, performance or function of the program. The implied warranties of merchantability and fitness for a particular purpose are expressly disclaimed.
- b. If you change the **RVJPUAUT** command to use a different command processing program, then the digital signature of this command will no longer be valid.

Appendix H. Related information for IBM i security reference

Listed here are the product manuals and IBM Redbooks® (in PDF format), Web sites, and information center topics that relate to the security topic. You can view or print any of the PDFs.

Manuals

- Recovering your system (about 8.42 MB), provides information about planning a backup and recovery strategy, saving information from your system, and recovering your system, auxiliary storage pools, and disk protection options.
- Installing, upgrading, or deleting IBM i and related software (3,053 KB), provides step-by-step procedures for initial install, installing licensed programs, program temporary fixes (PTFs), and secondary languages from IBM.
- Remote Workstation Support  (1,636 KB), provides information about how to set up and use remote workstation support, such as display station pass-through, distributed host command facility, and 3270 remote attachment.
- Cryptographic Support/400  (448 KB), describes the data security capabilities of the Cryptographic Facility licensed program. It explains how to use the facility and provides reference information for programmers.
- Local Device Configuration  (763 KB), provides information about how to do an initial configuration and how to change that configuration. It also contains conceptual information about device configuration.
- *SNA Distribution Services, SC41-5410* (2,259 KB), provides information about configuring a network for Systems Network Architecture distribution services (SNADS) and the Virtual Machine/Multiple Virtual Storage (VM/MVS) bridge. In addition, object distribution functions, document library services, and system distribution directory services are discussed. (This manual is not included in this release of the IBM i Information Center. However, it might be a useful reference to you. The manual is available from the IBM Publications Center as a printed hardcopy that you can order or in an online format that you can download at no charge.)
- *ADTS for AS/400: Source Entry Utility, SC09-2605* (460 KB), provides information about using the Application Development Tools source entry utility (SEU) to create and edit source members. The book explains how to start and end an SEU session and how to use the many features of this full-screen text editor. The book contains examples to help both new and experienced users accomplish various editing tasks, from the simplest line commands to using pre-defined prompts for high-level languages and data formats. (This manual is not included in this release of the IBM i Information Center. However, it might be a useful reference to you. The manual is available from the IBM Publications Center as a printed hardcopy that you can order or in an online format that you can download at no charge.)

IBM Redbooks

- AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet  (2.1 MB) This IBM Redbook discusses the security issues and the risk associated with connecting your System i product to the Internet. It provides examples, recommendations, tips, and techniques for applications.
- Cool Title About the AS/400 and Internet  (7.36 MB) This IBM Redbook can help you understand and then use the Internet (or your own intranet) from your System i product. It helps you to understand how to use the functions and features. This book helps you to get started quickly using e-mail, file transfer, terminal emulation, gopher, HTTP, and 5250 to HTML Gateway.

Web sites

- Lotus Documentation  (<http://www.lotus.com/ldd/doc>)

This Web site provides information about Lotus Notes, Domino®, and IBM Domino for IBM i. From this Web site, you can download information in Domino database (.NSF) and Adobe Acrobat (.PDF) format, search databases, and find out how to obtain printed manuals.

Other information

- Planning and setting up system security provides a set of practical suggestions for using the security features of iSeries and for establishing operating procedures that are security-conscious. This book also describes how to set up and use security tools that are part of i5/OS.
- *Implementing AS/400 Security, 4th Edition* (October 15, 2000) by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press. Provides guidance and practical suggestions for planning, setting up, and managing your system security.

ISBN Order Number

1583040730

- IBM i Access for Windows provides technical information about the IBM i Access for Windows programs for all versions of IBM i Access for Windows
- TCP/IP setup provides information that describes how to use and configure TCP/IP.
- TCP/IP applications, protocols, and services provides information that describes how to use TCP/IP applications, such as FTP, SMTP, and TELNET.
- Basic system operations provides information about how to start and stop the system and work with system problems.
- Integrated file system provides an overview of the integrated file system, including what it is, how it can be used, and what interfaces are available.
- iSeries and Internet security helps you address potential security concerns you may have when connecting your iSeries to the Internet. For more information, visit the following IBM I/T (Information Technology) Security home page: <http://www.ibm.com/security>. Optical storage provides information about functions that are unique for *Optical Support*. It also contains helpful information for the use and understanding of; CD-Devices, Directly attached Optical Media Library Devices, and LAN attached Optical Media Library Devices.
- Printing provides information about printing elements and concepts of the system, printer file and print spooling support for printing operation, and printer connectivity.
- Control language provides a wide-ranging discussion of programming topics, including a general discussion of objects and libraries, CL programming, controlling flow and communicating between programs, working with objects in CL programs, and creating CL programs. Other topics include predefined and impromptu messages and message handling, defining and creating user-defined commands and menus, application testing, including debug mode, breakpoints, traces, and display functions.

It also provides a description of all the iSeries control language (CL) and its IBM i commands. The IBM i commands are used to request functions of the IBM i (5722-SS1) licensed program. All the non-IBM i CL commands—those associated with the other licensed programs, including all the various languages and utilities—are described in other books that support those licensed programs.

- Programming provides information about many of the languages and utilities available on the iSeries. It contains summaries of:
 - All iSeries CL commands (in IBM i program and in all other licensed programs), in various forms.
 - Information related to CL commands, such as the error messages that can be monitored by each command, and the IBM-supplied files that are used by some commands.
 - IBM-supplied objects, including libraries.
 - IBM-supplied system values.
 - DDS keywords for physical, logical, display, printer, and ICF files.

- REXX instructions and built-in functions.
- Other languages (like RPG) and utilities (like SEU and SDA).
- Systems management includes information about performance data collection, system values management, and storage management.
- Database file concepts provides an overview of how to design, write, run, and test the statements of DB2 Query Manger and SQL Development Kit for IBM i. It also describes interactive Structured Query Language (SQL), and provides examples of how to write SQL statements in COBOL, RPG, C, FORTRAN, and PL/I programs. It also provides information about how to:
 - Build, maintain, and run SQL queries
 - Create reports ranging from simple to complex
 - Build, update, manage, query, and report on database tables using a forms-based interface
 - Define and prototype SQL queries and reports for inclusion in application programs

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Appendix I. 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 grant 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:

- | Intellectual Property Licensing
- | Legal and Intellectual Property Law
- | IBM Japan, Ltd.
- | 3-2-12, Roppongi, Minato-ku, Tokyo 106-8711

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be
| liable for any damages arising out of your use of the sample 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 Security reference publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

| IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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.

Linux is a registered trademark of Linus Torvalds 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.

Index

Special characters

- (*Mgt) Management authority 132
- (*Ref) Reference authority 132
- (Display Link) command
 - object authority required 397
- (Move) command
 - object authority required 400
- *ADD (add) authority 132, 340
- *ADOPTED (adopted) authority 156
- *ADVANCED (advanced) assistance level 80
- *ALL (all) authority 134, 341
- *ALLOBJ
 - user class authority 10
- *ALLOBJ (all object) special authority
 - added by system
 - changing security levels 13
 - auditing 260
 - failed sign-on 201
 - functions allowed 85
 - removed by system
 - changing security levels 13
 - restoring profile 249
 - risks 85
- *ALRTBL (alert table) object auditing 503
- *ASSIST Attention-key-handling program 104
- *AUDIT (audit) special authority
 - functions allowed 88
 - risks 88
- *AUTFAIL (authority failure) audit level 270
- *AUTHLR (authority holder) object auditing 504
- *AUTL (authorization list) object auditing 503
- *AUTLMGT (authorization list management) authority 132, 340
- *BASIC (basic) assistance level 80
- *BNDDIR (binding directory) object auditing 504
- *BREAK (break) delivery mode user profile 102
- *CFGL (configuration list) object auditing 505
- *CHANGE (change) authority 134, 341
- *CHRSF (Special Files) object auditing 505
- *CHTFMT (chart format) object auditing 505
- *CLD (C locale description) object auditing 506
- *CLKWD (CL keyword) user option 106, 107, 108
- *CLS (Class) object auditing 507
- *CMD (command string) audit level 272
- *CMD (Command) object auditing 507
- *CNNL (connection list) object auditing 508
- *COSD (class-of-service description) object auditing 509
- *CREATE (create) audit level 272
- *CRQD
 - restoring
 - audit journal (QAUDJRN) entry 277
- *CRQD (change request description) object auditing 506
- *CRQD change (CQ) file layout 589
- *CSI (communications side information) object auditing 509
- *CSPMAP (cross system product map) object auditing 509
- *CSPTBL (cross system product table) object auditing 510
- *CTLD (controller description) object auditing 510
- *DELETE (delete) audit level 272
- *DEVD (device description) object auditing 511
- *DFT (default) delivery mode user profile 102
- *DIR (directory) object auditing 512
- *DISABLED (disabled) user profile status description 78
 - QSECOFR (security officer) user profile 78
- *DLT (delete) authority 132, 340
- *DOC (document) object auditing 516
- *DTAARA (data area) object auditing 519
- *DTADCT (data dictionary) object auditing 520
- *DTAQ (data queue) object auditing 520
- *EDTD (edit description) object auditing 521
- *ENABLED (enabled) user profile status 78
- *EXCLUDE (exclude) authority 133
- *EXECUTE (execute) authority 132, 340
- *EXITRG (exit registration) object auditing 521
- *EXPERT (expert) user option 106, 107, 108, 160
- *FCT (forms control table) object auditing 522
- *FILE (file) object auditing 522
- *FNTRSC (font resource) object auditing 526
- *FORMDF (form definition) object auditing 526
- *FTR (filter) object auditing 526
- *GROUP (group) authority 156
- *GSS (graphic symbols set) object auditing 527
- *HLPFULL (full-screen help) user option 108
- *HOLD (hold) delivery mode user profile 102
- *IGCDCT (double-byte character set dictionary) object auditing 527
- *IGCSRT (double-byte character set sort) object auditing 528
- *IGCTBL (double-byte character set table) object auditing 528
- *INTERMED (intermediate) assistance level 80
- *IOSYSCFG (system configuration) special authority
 - functions allowed 88
 - risks 88
- *JOBCTL (job control) special authority
 - functions allowed 86
 - output queue parameters 212
 - priority limit (PTYLMT) 95
 - risks 86
- *JOBDB (job description) object auditing 528
- *JOBDDTA (job change) audit level 273
- *JOBQ (job queue) object auditing 529
- *JOBSCD (job scheduler) object auditing 530
- *JRN (journal) object auditing 530
- *JRNRCV (journal receiver) object auditing 532
- *LIB (library) object auditing 532
- *LIND (line description) object auditing 533
- *MENU (menu) object auditing 535
- *Mgt (Management) authority 132
- *MODD (mode description) object auditing 535
- *MODULE (module) object auditing 535
- *MSGF (message file) object auditing 536
- *MSGQ (message queue) object auditing 537
- *NODGRP (node group) object auditing 538
- *NODL (node list) object auditing 538
- *NOSTMSG (no status message) user option 108
- *NOTIFY (notify) delivery mode user profile 102
- *NTBD (NetBIOS description) object auditing 538
- *NWID (network interface) object auditing 539
- *NWS (network server description) object auditing 540
- *OBJALTER (object alter) authority 132, 340
- *OBJEXIST (object existence) authority 132, 340
- *OBJMGT (object management) audit level 275
- *OBJMGT (object management) authority 132, 340
- *OBJOPR (object operational) authority 132, 339

- *OBJREF (object reference)
 - authority 132, 340
- *OFCSRV (office services) audit
 - level 275, 514, 534
- *OUTQ (output queue) object
 - auditing 540
- *OVL (overlay) object auditing 541
- *PAGDFN (page definition) object
 - auditing 542
- *PAGSEG (page segment) object
 - auditing 542
- *PARTIAL (partial) limit capabilities 83
- *PDG (print descriptor group) object
 - auditing 542
- *PGM (program) object 542
- *PGMADP (adopted authority) audit
 - level 275
- *PGMFAIL (program failure) audit
 - level 276
- *PNLGRP (panel group) object
 - auditing 544
- *PRDAVL (product availability) object
 - auditing 544
- *PRDDFN (product definition) object
 - auditing 545
- *PRDLOD (product load) object
 - auditing 545
- *PRTDTA (printer output) audit
 - level 276
- *PRTMSG (printing message) user
 - option 108
- *QMFORM (query manager form) object
 - auditing 545
- *QMQRV (query manager query) object
 - auditing 546
- *QRYDFN (query definition) object
 - auditing 546
- *R (read) 134, 341
- *RCT (reference code table) object
 - auditing 547
- *READ (read) authority 132, 340
- *Ref (Reference) authority 132
- *ROLLKEY (roll key) user option 108
- *RW (read, write) 134, 341
- *RWX (read, write, execute) 134, 341
- *RX (read, execute) 134, 341
- *S36 (S/36 machine description) object
 - auditing 558
- *S36 (System/36) special
 - environment 89
- *SAVRST (save/restore) audit level 276
- *SAVSYS (save system) special authority
 - *OBJEXIST authority 132, 340
 - description 256
 - functions allowed 86
 - removed by system
 - changing security levels 13
 - risks 86
- *SBSD (subsystem description) object
 - auditing 548
- *SCHIDX (search index) object
 - auditing 549
- *SECADM (security administrator)
 - special authority 85
 - functions allowed 85
- *SECURITY (security) audit level 280
- *SERVICE (service tools) audit level 283

- *SERVICE (service) special authority
 - failed sign-on 201
 - functions allowed 87
 - risks 87
- *SIGNOFF initial menu 82
- *SOCKET (local socket) object
 - auditing 550
- *SPADCT (spelling aid dictionary) object
 - auditing 552
- *SPLCTL (spool control) special authority
 - functions allowed 86
 - output queue parameters 213
 - risks 86
- *SPLFDTA (spooled file changes) audit
 - level 284, 552
- *SQLPKG (SQL package) object
 - auditing 554
- *SRVPGM (service program) object
 - auditing 554
- *SSND (session description) object
 - auditing 555
- *STMF (stream file) object auditing 555
- *STSMMSG (status message) user
 - option 108
- *SVRSTG (server storage space)
 - object 555
- *SYNLNK (symbolic link) object
 - auditing 557
- *SYSMTG (systems management) audit
 - level 284
- *SYSTEM (system) domain 15
- *SYSTEM (system) state 15
- *TBL (table) object auditing 559
- *TYPEAHEAD (type-ahead) keyboard
 - buffering 94
- *UPD (update) authority 132, 340
- *USE (use) authority 134, 341
- *USER (user) domain 15
- *USER (user) state 15
- *USRIDX (user index) object 19
- *USRIDX (user index) object
 - auditing 559
- *USRPRF (user profile) object
 - auditing 560
- *USRQ (user queue) object 19
- *USRQ (user queue) object auditing 561
- *USRSPC (user space) object 19
- *USRSPC (user space) object
 - auditing 561
- *VLDL (validation list) object
 - auditing 562
- *W (write) 134, 341
- *WX (write, execute) 134, 341
- *X (execute) 134, 341

A

- access
 - preventing
 - unauthorized 262
 - unsupported interface 15
 - restricting
 - console 258
 - workstations 258
- access code
 - object authority required for
 - commands 449

- access command (Determine File
 - Accessibility)
 - object auditing 512
- access control list
 - changing
 - audit journal (QAUDJRN)
 - entry 282
- access control list change (VA) journal
 - entry type 282
- access path recovery
 - action auditing 502
 - object authority required for
 - commands 350
- accessx command (Determine File
 - Accessibility)
 - object auditing 512
- account limit
 - exceeded
 - audit journal (QAUDJRN)
 - entry 284
- account limit exceeded (VL) file
 - layout 683
- account limit exceeded (VL) journal entry
 - type 284
- accounting code (ACGCDE) parameter
 - changing 100
 - user profile 100
- Accumulating Special Authorities 240
- ACGCDE (accounting code) parameter
 - changing 100
 - user profile 100
- action auditing
 - access path recovery 502
 - definition 263
 - Directory Server 514
 - mail services 534
 - office services 534
 - planning 263
 - reply list 548
 - spooled files 552
- action auditing (AUDLVL) parameter
 - user profile 113
- action to spooled file (SF) file layout 666
- action to system value (SV) file
 - layout 680
- action when sign-on attempts reached
 - (QMAXSGNACN) system value
 - description 30
 - value set by CFGSYSSEC
 - command 716
- activating
 - security auditing function 290
 - user profile 707
- active profile list
 - changing 707
- AD (auditing change) file layout 570
- AD (auditing change) journal entry
 - type 280
- add (*ADD) authority 132, 340
- Add Authorization List Entry
 - (ADDAUTLE) command 167, 309
- Add Directory Entry (ADDDIRE)
 - command 314
- Add Document Library Object Authority
 - (ADDDLOAUT) command 313

Add Job Schedule Entry (ADDJOBSCDE) command
 SECBATCH menu 710

Add Kerberos Keytab Entry (ADDKRBKTE) command
 object authority required 422

Add Kerberos Ticket (ADDKRBTKT) command
 object authority required 422

Add Library List Entry (ADDLIBLE) command 207, 210

Add User display sample 118

ADDACC (Add Access Code) command
 object auditing 519
 object authority required 449

ADDAJE (Add Autostart Job Entry) command
 object auditing 548
 object authority required 483

ADDALRACNE (Add Alert Action Entry) command
 object auditing 526
 object authority required 388

ADDALRD (Add Alert Description) command
 object auditing 503
 object authority required 352

ADDALRSLTE (Add Alert Selection Entry) command
 object auditing 526
 object authority required 388

ADDASPCPYD command
 authorized IBM-supplied user profiles 327

ADDAUTLE (Add Authorization List Entry) command
 description 309
 object auditing 503
 object authority required 354
 using 167

ADDDBKP (Add Breakpoint) command
 object authority required 463

ADDBNDDIRE (Add Binding Directory Entry) command
 object auditing 504
 object authority required 355

ADDBSCDEVE (Add BSC Device Entry) command
 object auditing 523

ADDCADMRE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADDCADNODE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADDCFGLE (Add Configuration List Entries) command
 object auditing 505
 object authority required 364

ADDCKMKSFE command
 object authority required 367

ADDCLUMON command
 authorized IBM-supplied user profiles 327

ADDCLUMON command (*continued*)
 object authority required 357

ADDCLUNODE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADDCMDCRQA (Add Command Change Request Activity) command
 authorized IBM-supplied user profiles 327
 object auditing 506
 object authority required 355

ADDCMNDEVE (Add Communications Device Entry) command
 object auditing 523

ADDCMNE (Add Communications Entry) command
 object auditing 548
 object authority required 483

ADDCNNLE (Add Connection List Entry) command
 object auditing 508

ADDCOMSNMP (Add Community for SNMP) command
 object authority required 490

ADDCRGDEVE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADDCRGNODE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADDCRSMDMNK (Add Cross Domain Key) command
 authorized IBM-supplied user profiles 327

ADDDEVDMNE command
 authorized IBM-supplied user profiles 327
 object authority required 357

ADD DIRE (Add Directory Entry) command
 description 314
 object authority required 371

ADDDIRSHD (Add Directory Shadow System) command
 object authority required 371

ADD DLOAUT (Add Document Library Object Authority) command
 description 313
 object auditing 517
 object authority required 374

ADD DSPDEVE (Add Display Device Entry) command
 object auditing 523

ADD DSTLE (Add Distribution List Entry) command
 object authority required 374

ADD DSTQ (Add Distribution Queue) command
 authorized IBM-supplied user profiles 327
 object authority required 373

ADDDSTRTE (Add Distribution Route) command
 authorized IBM-supplied user profiles 327
 object authority required 373

ADDDSTSYSN (Add Distribution Secondary System Name) command
 authorized IBM-supplied user profiles 327
 object authority required 373

ADDDTADFN (Add Data Definition) command
 object authority required 410

ADDDWDFN command
 authorized IBM-supplied user profiles 327

ADDEMLCFGE (Add Emulation Configuration Entry) command
 object authority required 370

ADDENVVAR (Add Environment Variable) command
 object authority required 380

ADDEWCBCDE (Add Extended Wireless Controller Bar Code Entry) command
 object authority required 381

ADDEWCM (Add Extended Wireless Controller Member) command
 object authority required 381

ADDEWCPTCE (Add Extended Wireless Controller PTC Entry) command
 object authority required 381

ADDEWLM (Add Extended Wireless Line Member) command
 object authority required 381

ADDEXITPGM (Add Exit Program) command
 authorized IBM-supplied user profiles 327
 object auditing 521
 object authority required 469

ADD FCTE (Add Forms Control Table Entry) command
 object authority required 470

ADD FNTBLE (Add DBCS Font Table Entry)
 object authority required for commands 351

ADD IC FDEVE (Add Intersystem Communications Function Program Device Entry) command
 object auditing 523
 object authority required 381

ADD IMGCLGE command
 object authority required 391

adding
 authorization list
 entries 167, 309
 objects 167
 users 167, 309
 directory entry 314
 document library object (DLO) authority 313
 library list entry 207, 210
 server authentication entry 314
 user authority 161
 user profiles 118

ADDIPSIFC (Add IP over SNA Interface) command
 object authority required 352

ADDIPSLOC (Add IP over SNA Location Entry) command
 object authority required 352

ADDIPSRTE (Add IP over SNA Route) command
 object authority required 352

ADDJOBQE (Add Job Queue Entry) command
 object auditing 529, 548
 object authority required 483

ADDJOBSCDE (Add Job Schedule Entry) command
 object auditing 530
 object authority required 417
 SECBATCH menu 710

ADDJWDFN command
 authorized IBM-supplied user profiles 327

ADDLANADPI (Add LAN Adapter Information) command
 object authority required 437

ADDLFM (Add Logical File Member) command
 object auditing 523
 object authority required 381

ADDLIBLE (Add Library List Entry) command 207, 210
 object authority required 430

ADDLICENSE (Add License Key) command
 object authority required 434

ADDLNK (Add Link) command
 object auditing 550, 555
 object authority required 392

ADDMFS (Add Mounted File System) command
 authorized IBM-supplied user profiles 327
 object authority required 491

ADDMFS (Add Mounted File System) command) command
 object authority required 445

ADDMSGD (Add Message Description) command
 object auditing 536
 object authority required 441

ADDMSTPART command
 authorized IBM-supplied user profiles 327
 object authority required 367

ADDNETJOB (Add Network Job Entry) command
 authorized IBM-supplied user profiles 327
 object authority required 444

ADDNETTBLE (Add Network Table Entry) command
 object authority required 490

ADDNODLE (Add Node List Entry) command
 object auditing 538
 object authority required 449

ADDNWSSTGL (Add Network Server Storage Link) command
 object authority required 446

ADDOBJCRQA (Add Object Change Request Activity) command
 authorized IBM-supplied user profiles 328
 object auditing 506
 object authority required 355

ADDOFCENR (Add Office Enrollment) command
 object auditing 517

ADDOPTCTG (Add Optical Cartridge) command
 authorized IBM-supplied user profiles 328
 object authority required 451

ADDOPTSVR (Add Optical Server) command
 authorized IBM-supplied user profiles 328
 object authority required 451

ADDPFCST (Add Physical File Constraint) command
 object authority required 381

ADDPFXDFN () command
 authorized IBM-supplied user profiles 328

ADDPFXDFN (Add Performance Explorer Definition) command
 object authority required 455

ADDPFXFTR () command
 authorized IBM-supplied user profiles 328

ADDPFCST (Add Physical File Constraint) command
 object auditing 523

ADDPFPM (Add Physical File Member) command
 object auditing 523
 object authority required 381

ADDPFTRG (Add Physical File Trigger) command
 object auditing 523
 object authority required 382

ADDPFVLM (Add Physical File Variable-Length Member) command
 object auditing 523

ADDPGM (Add Program) command
 object authority required 463

ADDPJE (Add Prestart Job Entry) command
 object auditing 548
 object authority required 483

ADDPRBACNE (Add Problem Action Entry) command
 object auditing 526
 object authority required 388, 462

ADDPRBSLTE (Add Problem Selection Entry) command
 object auditing 526
 object authority required 388, 462

ADDPRDCRQA (Add Product Change Request Activity) command
 authorized IBM-supplied user profiles 328
 object auditing 506

ADDPRDCRQA (Add Product Change Request Activity) command (*continued*)
 object authority required 355

ADDPRDLICI (Add Product License Information) command
 object auditing 545

ADDPTFCRQA (Add PTF Change Request Activity) command
 authorized IBM-supplied user profiles 328
 object auditing 506
 object authority required 355

ADDRDBDIRE (Add Relational Database Directory Entry) command
 object authority required 469

ADDRJECMNE (Add RJE Communications Entry) command
 object authority required 470

ADDRJERDRE (Add RJE Reader Entry) command
 object authority required 470

ADDRJEWTRE (Add RJE Writer Entry) command
 object authority required 471

ADDRMTJRN (Add Remote Journal) command
 object auditing 531

ADDRMTSVR (Add Remote Server) command
 object authority required 447

ADDRPYLE (Add Reply List Entry) command
 authorized IBM-supplied user profiles 328
 object auditing 548
 object authority required 486

ADDRSCCRQA (Add Resource Change Request Activity) command
 authorized IBM-supplied user profiles 328
 object auditing 506
 object authority required 355

ADDRTGE (Add Routing Entry) command
 object auditing 548
 object authority required 483

ADDSCIDX (Add Search Index Entry) command
 object auditing 544, 549
 object authority required 411

ADDSOCE (Add Sphere of Control Entry) command
 object authority required 480

ADDSRVTBLE (Add Service Table Entry) command
 object authority required 490

ADDSVRAUTE (Add Server Authentication Entry) command
 object authority required 475

ADDTAPCTG (Add Tape Cartridge) command
 object authority required 438

ADDTCPHTE (Add TCP/IP Host Table Entry) command
 object authority required 490

ADDTCPIFC (Add TCP/IP Interface)
 command
 object authority required 490
 ADDTCPRT (Add TCP/IP Port Entry)
 command
 object authority required 490
 ADDTCPRSI (Add TCP/IP Remote System Information) command
 object authority required 490
 ADDTCPRTE (Add TCP/IP Route)
 command
 object authority required 490
 ADDTRC (Add Trace) command
 object authority required 463
 ADDTRCFTR
 authorized IBM-supplied user profiles 328
 ADDWSE (Add Workstation Entry) command
 object auditing 548
 object authority required 483
 adopted
 authority
 displaying 156
 adopted (*ADOPTED) authority 156
 adopted authority
 *PGMADP (program adopt) audit level 275
 AP (adopted authority) file layout 579
 AP (adopted authority) journal entry type 275
 application design 230, 232, 233
 Attention (ATTN) key 150
 audit journal (QAUDJRN) entry 275, 579
 auditing 261
 authority checking example 189, 192
 bound programs 151
 break-message-handling program 150
 changing
 audit journal (QAUDJRN) entry 281
 authority required 151
 job 151
 creating program 151
 debug functions 150
 definition 149
 displaying
 command description 312
 critical files 236
 programs that adopt a profile 151
 USRPRF parameter 151
 example 230, 232, 233
 flowchart 182
 group authority 150
 ignoring 152, 232
 job initiation 200
 library security 136
 object ownership 151
 printing list of objects 711
 purpose 149
 recommendations 152
 restoring programs
 changes to ownership and authority 253
 adopted authority (*continued*)
 risks 152
 service programs 151
 special authority 150
 system request function 150
 transferring to group job 150
 adopting owner's authority 261
 ADSM (QADSM) user profile 321
 advanced (*ADVANCED) assistance level 74, 80
 advanced function printing (AFP)
 object authority required for commands 351
 AF (authority failure) file layout 573
 AF (authority failure) journal entry type
 default sign-on violation 16
 description 270, 276
 hardware protection violation 17
 job description violation 16
 program validation 17, 18
 restricted instruction 18
 unsupported interface 16, 18
 AF_INET sockets over SNA
 object authority required for commands 352
 AFDFTUSR (QAFDFTUSR) user profile 321
 AFOWN (QAFOWN) user profile 321
 AFP (Advanced Function Printing)
 object authority required for commands 351
 AFUSR (QAFUSR) user profile 321
 ALCOBJ (Allocate Object) command
 object auditing 501
 object authority required 343
 alert
 object authority required for commands 352
 alert description
 object authority required for commands 352
 alert table
 object authority required for commands 352
 alert table (*ALRTBL) object auditing 503
 all (*ALL) authority 134, 341
 all object (*ALLOBJ) special authority
 added by system
 changing security levels 13
 auditing 260
 failed sign-on 201
 functions allowed 85
 removed by system
 changing security levels 13
 restoring profile 249
 risks 85
 all-numeric password 76
 allow limited user (ALWLMTUSR) parameter
 Change Command (CHGCMD) command 83
 Create Command (CRTCMD) command 83
 limit capabilities 83
 allow object difference (ALWOBJDIF) parameter 250
 allow object restore (QALWOBJRST) system value
 value set by CFGSYSSEC command 716
 allow object restore option (QALWOBJRST) system value 45
 allow remote sign-on (QRMTSIGN) system value
 value set by CFGSYSSEC command 716
 allow user objects (QALWUSRDMN) system value 19, 25
 allowed function
 limit capabilities (LMTCPB) 83
 allowing
 users to change passwords 259
 alter service function
 *SERVICE (service) special authority 87
 ALWLMTUSR (allow limited user) parameter
 Change Command (CHGCMD) command 83
 Create Command (CRTCMD) command 83
 limit capabilities 83
 ALWOBJDIF (allow object difference) parameter 250
 Analyze Default Passwords (ANZDFTPWD) command
 description 707
 Analyze Profile Activity (ANZPRFACT) command
 creating exempt users 707
 description 707
 analyzing
 audit journal entries, methods 295
 object authority 303
 program failure 303
 user profile
 by special authorities 711
 by user class 711
 user profiles 301
 ANSLIN (Answer Line) command
 object auditing 533
 ANSQST (Answer Questions) command
 authorized IBM-supplied user profiles 328
 object authority required 468
 ANZBESTMDL
 authorized IBM-supplied user profiles 328
 ANZBESTMDL (Analyze BEST/1 Model) command
 object authority required 456
 ANZCMDPFR command
 authorized IBM-supplied user profiles 328
 object authority required 456
 ANZDBF
 authorized IBM-supplied user profiles 328
 ANZDBF (Analyze Database File) command
 object authority required 456

ANZDBFKEY
 authorized IBM-supplied user profiles 328

ANZDBFKEY (Analyze Database File Keys) command
 object authority required 456

ANZDFTPWD (Analyze Default Password) command
 object authority required 492

ANZDFTPWD (Analyze Default Passwords) command
 authorized IBM-supplied user profiles 328
 description 707

ANZJVM
 authorized IBM-supplied user profiles 328

ANZJVM command
 object authority required 411

ANZOBJCVN
 authorized IBM-supplied user profiles 328

ANZOBJCVN command
 object authority required 343

ANZPFRDT2 (Analyze Performance Data) command
 object authority required 456

ANZPFRDTA
 authorized IBM-supplied user profiles 328

ANZPFRDTA (Analyze Performance Data) command
 object authority required 456

ANZPGM (Analyze Program) command
 object auditing 543
 object authority required 456

ANZPRB (Analyze Problem) command
 authorized IBM-supplied user profiles 328
 object authority required 462

ANZPRACT
 authorized IBM-supplied user profiles 328

ANZPRACT (Analyze Profile Activity) command
 creating exempt users 707
 description 707
 object authority required 492

ANZQRY (Analyze Query) command
 object auditing 546
 object authority required 466

ANZS34OCL (Analyze System/34 OCL) command
 authorized IBM-supplied user profiles 328
 object authority required 442

ANZS34OCL (Analyze System/36 OCL) command
 object authority required 442

ANZS36OCL (Analyze System/36 OCL) command
 authorized IBM-supplied user profiles 328

ANZUSROBJ command
 object authority required 343

AP (adopted authority) file layout 579

AP (adopted authority) journal entry type 275

API (application programming interface) security level 40 15

application design
 adopted authority 230, 233
 general security recommendations 220
 ignoring adopted authority 232
 libraries 225
 library lists 226
 menus 228
 profiles 226

Application development commands 353

application programming interface (API) security level 40 15

APPN directory (ND) file layout 631

APPN end point (NE) file layout 632

approval program, password 61, 62

approving password 60

APYJRNCHG (Apply Journalized Changes) command
 authorized IBM-supplied user profiles 328
 object auditing 500, 531
 object authority required 417

APYJRNCHGX (Apply Journal Changes Extend) command
 object auditing 523, 531

APYPTF (Apply Program Temporary Fix) command
 authorized IBM-supplied user profiles 328
 object authority required 475

APYRMPTPF (Apply Remote Program Temporary Fix) command
 authorized IBM-supplied user profiles 328

ASKQST (Ask Question) command
 object authority required 468

assistance level
 advanced 74, 80
 basic 74, 80
 definition 74
 example of changing 80
 intermediate 74, 80
 stored with user profile 80
 user profile 80

ASTLVL (assistance level) parameter
 user profile 80

ATNPGM (Attention-key-handling program) parameter
 user profile 104

Attention (ATTN) key
 adopted authority 150

Attention (ATTN) key buffering 93

Attention-key-handling program
 *ASSIST 104
 changing 104
 initial program 104
 job initiation 200
 QATNPGM system value 104
 QCMD command processor 104
 QEZMAIN program 104
 setting 104
 user profile 104

attribute change (AU) file layout 579

AU (attribute change) file layout 579

audit (*AUDIT) special authority functions allowed 88
 risks 88

audit (QAUDJRN) journal 499, 645
 AD (auditing change) entry type 280
 AD (auditing change) file layout 570
 AF (authority failure) entry type 276
 default sign-on violation 16
 description 270
 hardware protection violation 17
 job description violation 16
 program validation 18
 restricted instruction violation 18
 unsupported interface 16
 unsupported interface violation 18

AF (authority failure) file layout 573

analyzing
 with query 296

AP (adopted authority) entry type 275

AP (adopted authority) file layout 579

AU (attribute change) file layout 579

auditing level (QAUDLVL) system value 67

auditing level extension (QAUDLVL2) system value 69

automatic cleanup 293

CA (authority change) entry type 280

CA (authority change) file layout 580

CD (command string) entry type 272

CD (command string) file layout 583

changing receiver 294

CO (create object) entry type 144, 272

CO (create object) file layout 584

CP (user profile change) entry type 277

CP (user profile change) file layout 586

CQ (*CRQD change) file layout 589

CQ (change *CRQD object) entry type 277

creating 291

CU(Cluster Operations) file layout 589

CV(connection verification) file layout 591

CY(cryptographic configuration) file layout 593

damaged 292

detaching receiver 293, 294

DI(Directory Server) file layout 596

displaying entries 263, 295

DO (delete operation) entry type 272

DO (delete operation) file layout 601

DS (DST password reset) entry type 277

DS (IBM-Supplied Service Tools User ID Reset) file layout 603

error conditions 66

EV (Environment variable) file layout 604

force level 67

- audit (QAUDJRN) journal (*continued*)
 - GR(generic record) file layout 605
 - GS (give descriptor) entry type 281
 - GS (give descriptor) file layout 610
 - introduction 262
 - IP (change ownership) entry type 281
 - IP (interprocess communication actions) file layout 614
 - IP (interprocess communications) entry type 271
 - IR(IP rules actions) file layout 615
 - IS (Internet security management) file layout 617
 - JD (job description change) entry type 281
 - JD (job description change) file layout 619
 - JS (job change) entry type 273
 - JS (job change) file layout 620
 - KF (key ring file) file layout 625
 - LD (link, unlink, search directory) file layout 628
 - managing 292
 - methods for analyzing 295
 - ML (mail actions) entry type 275
 - ML (mail actions) file layout 630
 - NA (network attribute change) entry type 281
 - NA (network attribute change) file layout 630
 - ND (APPN directory) file layout 631
 - NE (APPN end point) file layout 632
 - O1 (optical access) file layout 642, 643
 - O3 (optical access) file layout 644
 - OM (object management) entry type 275
 - OM (object management) file layout 632
 - OR (object restore) entry type 276
 - OR (object restore) file layout 636
 - OW (ownership change) entry type 281
 - OW (ownership change) file layout 640
 - PA (program adopt) entry type 281
 - PG (primary group change) entry type 281
 - PG (primary group change) file layout 647
 - PO (printed output) entry type 276
 - PO (printer output) file layout 650
 - PS (profile swap) entry type 281
 - PS (profile swap) file layout 651
 - PW (password) entry type 271
 - PW (password) file layout 653
 - RA (authority change for restored object) entry type 276
 - RA (authority change for restored object) file layout 654
 - receiver storage threshold 293
 - RJ (restoring job description) entry type 276
 - RJ (restoring job description) file layout 656
- audit (QAUDJRN) journal (*continued*)
 - RO (ownership change for restored object) entry type 276
 - RO (ownership change for restored object) file layout 657
 - RP (restoring programs that adopt authority) entry type 276
 - RP (restoring programs that adopt authority) file layout 659
 - RQ (restoring *CRQD object that adopts authority) file layout 661
 - RQ (restoring *CRQD object) entry type 277
 - RU (restore authority for user profile) entry type 277
 - RU (restore authority for user profile) file layout 661
 - RZ (primary group change for restored object) entry type 277
 - RZ (primary group change for restored object) file layout 662
 - SD (change system distribution directory) entry type 275
 - SD (change system distribution directory) file layout 664
 - SE (change of subsystem routing entry) entry type 282
 - SE (change of subsystem routing entry) file layout 665
 - SF (action to spooled file) file layout 666
 - SF (change to spooled file) entry type 284
 - SG file layout 670, 671
 - SM (systems management change) entry type 284
 - SM (systems management change) file layout 673
 - SO (server security user information actions) file layout 674
 - ST (service tools action) entry type 283
 - ST (service tools action) file layout 675
 - stopping 295
 - SV (action to system value) entry type 282
 - SV (action to system value) file layout 680
 - system entries 292
 - VA (access control list change) entry type 282
 - VA (changing access control list) file layout 681
 - VC (connection start and end) file layout 681
 - VC (connection start or end) entry type 273
 - VF (close of server files) file layout 682
 - VL (account limit exceeded) entry type 284
 - VL (account limit exceeded) file layout 683
 - VN (network log on and off) file layout 684
- audit (QAUDJRN) journal (*continued*)
 - VN (network log on or off) entry type 273
 - VO (validation list) file layout 685
 - VP (network password error) entry type 271
 - VP (network password error) file layout 686
 - VR (network resource access) file layout 687
 - VS (server session) entry type 273
 - VS (server session) file layout 688
 - VU (network profile change) entry type 282
 - VU (network profile change) file layout 689
 - VV (service status change) entry type 283
 - VV (service status change) file layout 690
 - X0 (kerberos authentication) file layout 691
 - YC (change to DLO object) file layout 698
 - YR (read of DLO object) file layout 699
 - ZC (change to object) file layout 700
 - ZR (read of object) file layout 703
 - audit control (QAUDCTL) system value
 - changing 315, 709
 - displaying 315, 709
 - audit function
 - activating 290
 - starting 290
 - stopping 295
 - audit journal
 - displaying entries 315
 - printing entries 711
 - working with 294
 - audit journal receiver
 - creating 291
 - deleting 294
 - naming 291
 - saving 294
 - audit level (AUDLVL) parameter
 - *AUTFAIL (authority failure) value 270
 - *CMD (command string) value 272
 - *CREATE (create) value 272
 - *DELETE (delete) value 272
 - *JOBDDTA (job change) value 273
 - *OBJMGT (object management) value 275
 - *OFCSRVR (office services) value 275
 - *PGMADP (adopted authority) value 275
 - *PGMFAIL (program failure) value 276
 - *SAVRST (save/restore) value 276
 - *SECURITY (security) value 280
 - *SERVICE (service tools) value 283
 - *SPLFDDTA (spooled file changes) value 284
 - *SYSMGT (systems management) value 284
 - changing 127

- audit level (QAUDLVL) system value
 - *AUTFAIL (authority failure) value 270
 - *CREATE (create) value 272
 - *DELETE (delete) value 272
 - *JOBDDTA (job change) value 273
 - *OBJMGT (object management) value 275
 - *OFCSRV (office services) value 275
 - *PGMADP (adopted authority) value 275
 - *PGMFAIL (program failure) value 276
 - *PRTDDTA (printer output) value 276
 - *SAVRST (save/restore) value 276
 - *SECURITY (security) value 280
 - *SERVICE (service tools) value 283
 - *SPLFDDTA (spooled file changes) value 284
 - *SYSMGT (systems management) value 284
 - changing 292, 315, 709
 - displaying 315, 709
 - purpose 263
 - user profile 113
- auditing 290, 499
 - *ALLOBJ (all object) special authority 260
 - *AUDIT (audit) special authority 88
 - abnormal end 66
 - access path recovery 502
 - actions 263
 - activating 290
 - adopted authority 261
 - authority
 - user profiles 261
 - authorization 261
 - changing
 - command description 310, 313
 - checklist for 257
 - communications 262
 - controlling 66
 - Directory Server 514
 - encryption of sensitive data 262
 - ending 66
 - error conditions 66
 - group profile
 - *ALLOBJ (all object) special authority 260
 - membership 260
 - password 259
 - IBM-supplied user profiles 258
 - inactive users 260
 - job descriptions 261
 - library lists 261
 - limit capabilities 260
 - mail services 534
 - methods 299
 - network attributes 262
 - object
 - default 288
 - planning 286
 - object authority 303
 - object integrity 304
 - office services 534
 - overview 257
 - password controls 259

- auditing (*continued*)
 - physical security 258
 - planning
 - overview 263
 - system values 288
 - program failure 303
 - programmer authorities 260
 - QTEMP objects 290
 - remote sign-on 262
 - reply list 548
 - save operations 256
 - security officer 305
 - sensitive data
 - authority 261
 - encrypting 262
 - setting up 290
 - sign-on without user ID and password 261
 - spooled files 552
 - starting 290
 - steps to start 290
 - stopping 66, 295
 - system values 65, 258, 288
 - unauthorized access 262
 - unauthorized programs 262
 - unsupported interfaces 262
 - user profile
 - *ALLOBJ (all object) special authority 260
 - administration 260
 - using
 - journals 300
 - QHST (history) log 299
 - QSYSMSG message queue 262
 - working on behalf 534
 - working with user 127
 - auditing change (AD) file layout 570
 - auditing change (AD) journal entry type 280
 - auditing control (QAUDCTL) system value
 - overview 66
 - auditing end action (QAUDENDACN) system value 66, 289
 - auditing force level (QAUDFRCLVL) system value 67, 288
 - auditing level (QAUDLVL) system value 67
 - auditing level extension (QAUDLVL2) system value 69
 - AUDLVL (audit level) parameter
 - *CMD (command string) value 272
 - user profile 113
 - AUT (authority) parameter
 - creating libraries 157
 - creating objects 158
 - specifying authorization list (*AUTL) 166
 - user profile 112
 - AUTCHK (authority to check) parameter 212
 - authentication
 - digital ID 116
 - Authorities, Accumulating Special 240
 - authorities, field 136
 - Authorities, Special 240
 - authority 169

- authority (*continued*)
 - *ADD (add) 132, 340
 - *ALL (all) 134, 341
 - *ALLOBJ (all object) special authority 85
 - *AUDIT (audit) special authority 88
 - *AUTLMGT (authorization list management) 132, 139, 340
 - *CHANGE (change) 134, 341
 - *DLT (delete) 132, 340
 - *EXCLUDE (exclude) 133
 - *EXECUTE (execute) 132, 340
 - *IOSYSCFG (system configuration) special authority 88
 - *JOBCTL (job control) special authority 86
 - *Mgt 132
 - *OBJALTER (object alter) 132, 340
 - *OBJEXIST (object existence) 132, 340
 - *OBJMGT (object management) 132, 340
 - *OBJOPR (object operational) 132, 339
 - *OBJREF (object reference) 132, 340
 - *R (read) 134, 341
 - *READ (read) 132, 340
 - *Ref (Reference) 132
 - *RW (read, write) 134, 341
 - *RWX (read, write, execute) 134, 341
 - *RX (read, execute) 134, 341
 - *SAVSYS (save system) special authority 86
 - *SECADM (security administrator) special authority 85
 - *SERVICE (service) special authority 87
 - *SPLCTL (spool control) special authority 86
 - *UPD (update) 132, 340
 - *USE (use) 134, 341
 - *W (write) 134, 341
 - *WX (write, execute) 134, 341
 - *X (execute) 134, 341
 - adding users 161
 - adopted 579
 - application design 230, 232, 233
 - audit journal (QAUDJRN) entry 275
 - auditing 303
 - authority checking example 189, 192
 - displaying 156, 236
 - ignoring 232
 - purpose 149
 - assigning to new object 145
 - authorization for changing 159
 - authorization list
 - format on save media 247
 - management (*AUTLMGT) 132, 340
 - stored on save media 247
 - storing 247
 - changing 580
 - audit journal (QAUDJRN) entry 280
 - command description 310
 - procedures 159

- authority (*continued*)
 - checking 169
 - batch job initiation 200
 - interactive job initiation 199
 - sign-on process 199
 - commonly used subsets 133
 - copying
 - command description 311
 - example 121
 - recommendations 165
 - renaming profile 127
 - data
 - definition 132
 - definition 132
 - deleting user 161
 - detail, displaying (*EXPERT user option) 106, 107, 108
 - directory 5
 - displaying
 - command description 310
 - displaying detail (*EXPERT user option) 106, 107, 108
 - displays 154
 - field
 - definition 132
 - group
 - displaying 156
 - example 187, 191
 - holding when deleting file 153
 - ignoring adopted 152
 - introduction 5
 - library 5
 - Management authority
 - *Mgt(*) 132
 - multiple objects 162
 - new object
 - CRTAUT (create authority)
 - parameter 139, 157
 - example 145
 - GRPAUT (group authority)
 - parameter 98, 143
 - GRPAUTTYP (group authority type) parameter 98
 - QCRTAUT (create authority)
 - system value 26
 - QUSEADPAUT (use adopted authority) system value 35
 - object
 - *ADD (add) 132, 340
 - *DLT (delete) 132, 340
 - *EXECUTE (execute) 132, 340
 - *OBJEXIST (object existence) 132, 340
 - *OBJMGT (object management) 132, 340
 - *OBJOPR (object operational) 132, 339
 - *READ (read) 132, 340
 - *Ref (Reference) 132
 - *UPD (update) 132, 340
 - definition 132
 - exclude (*EXCLUDE) 133
 - format on save media 247
 - stored on save media 247
 - storing 246
 - object alter (*OBJALTER) 132, 340
 - object reference (*OBJREF) 132, 340
- authority (*continued*)
 - primary group 131, 144
 - example 187
 - working with 124
 - private
 - definition 131
 - restoring 245, 250
 - saving 245
 - public
 - definition 131
 - example 189, 191
 - restoring 245, 250
 - saving 245
 - referenced object
 - using 165
 - removing user 161
 - restoring
 - audit journal (QAUDJRN)
 - entry 277
 - command description 312
 - description of process 252
 - overview of commands 245
 - procedure 251
 - special (SPCAUT) authority
 - parameter 84
 - storing
 - authorization list 247
 - with object 246
 - with user profile 246
 - system-defined subsets 133
 - user profile
 - format on save media 247
 - stored on save media 247
 - storing 246
 - user-defined 160
 - using generic to grant 162
 - working with
 - command description 310
- authority (AUT) parameter
 - creating libraries 157
 - creating objects 158
 - specifying authorization list (*AUTL) 166
 - user profile 112
- authority cache
 - private authorities 197
- authority change (CA) file layout 580
- authority change (CA) journal entry
 - type 280
- authority change for restored object (RA)
 - file layout 654
- authority change for restored object (RA)
 - journal entry type 276
- authority checking 169
 - adopted authority
 - example 189, 192
 - flowchart 182
 - authorization list
 - example 193
 - group authority
 - example 187, 191
 - owner authority
 - flowchart 175
 - primary group
 - example 187
 - private authority
 - flowchart 174
- authority checking (*continued*)
 - public authority
 - example 189, 191
 - flowchart 181
 - sequence 169
- authority failure
 - audit journal (QAUDJRN) entry 276
 - default sign-on violation 16
 - device description 201
 - hardware protection violation 17
 - job description violation 16
 - job initiation 199
 - program validation 17, 18
 - restricted instruction 18
 - sign-on process 199
 - unsupported interface 16, 18
- authority failure (*AUTFAIL) audit
 - level 270
- authority failure (AF) file layout 573
- authority failure (AF) journal entry
 - type 270
 - description 276
- authority holder
 - automatically created 154
 - commands for working with 309, 314
 - creating 153, 309, 314
 - deleting 154, 309
 - description 153
 - displaying 153, 309
 - maximum storage limit exceeded 145
 - object auditing 504
 - object authority required for
 - commands 354
 - printing 316
 - restoring 245
 - risks 154
 - saving 245
 - System/36 migration 154
- authority profile (QAUTPROF) user
 - profile 321
- authority table 248
- authority, object 303
- authorization
 - auditing 261
- authorization list
 - adding
 - entries 167, 309
 - objects 167
 - users 167
 - authority
 - changing 167
 - storing 247
 - authority checking
 - example 193
 - changing
 - entry 309
 - comparison
 - group profile 241
 - creating 166, 309
 - damaged 254
 - deleting 169, 309
 - description 138
 - displaying
 - document library objects (DLO) 313
 - objects 168, 309

- authorization list (*continued*)
 - displaying (*continued*)
 - users 309
 - document library object (DLO)
 - displaying 313
 - editing 167, 309
 - entry
 - adding 167
 - group profile
 - comparison 241
 - introduction 5
 - management (*AUTLMGT)
 - authority 132, 139, 340
 - object auditing 503
 - object authority required for
 - commands 354
 - printing authority information 711
 - QRCLAUTL (reclaim storage) 255
 - reclaim storage (QRCLAUTL) 255
 - recovering damaged 254
 - removing
 - entries 309
 - objects 169
 - users 167, 309
 - restoring
 - association with object 250
 - description of process 254
 - overview of commands 245
 - retrieving entries 309
 - saving 245
 - securing IBM-supplied objects 139
 - securing objects 167
 - set up 168
 - storing
 - authority 247
 - user
 - adding 167
 - working with 309
- Authorization lists
 - advantages 166
 - planning 166
- authorization methods
 - combining
 - example 195
- authorized IBM-supplied user
 - profiles 330, 338
- authorized user
 - displaying 311
- AUTOCFG (automatic device configuration) value 37
- automatic configuration (QAUTOCFG)
 - system value
 - value set by CFGSYSSEC
 - command 716
- automatic configuration of virtual devices (QAUTOVRT) system value 37
- automatic creation
 - user profile 73
- automatic device configuration (AUTOCFG) value 37
- automatic device configuration (QAUTOCFG) system value
 - overview 37
- automatic install (QLPAUTO) user profile
 - default values 321

- automatic virtual-device configuration (QAUTOVRT) system value
 - value set by CFGSYSSEC
 - command 716
- availability 1

B

- backing up
 - security information 245
- backup
 - object authority required for
 - commands 450
- backup media
 - protecting 258
- basic (*BASIC) assistance level 74, 80
- basic service (QSRVBAS) user profile
 - authority to console 203
 - default values 321
- batch
 - restricting jobs 218
- batch job
 - *SPLCTL (spool control) special
 - authority 86
 - priority 95
 - security when starting 199, 200
- BCHJOB (Batch Job) command
 - object authority required 412
- binding directory
 - object authority required for
 - commands 355
- binding directory object auditing 504
- block
 - password change
 - QPWDCHGBLK system value 47
 - requiring
 - change (QPWDCHGBLK system value) 47
- bound program
 - adopted authority 151
 - definition 151
- break (*BREAK) delivery mode
 - user profile 102
- break-message-handling program
 - adopted authority 150
- BRM (QBRMS) user profile 321
- buffering
 - Attention key 93
 - keyboard 93

C

- C locale description (*CLD) auditing 506
- CA (authority change) file layout 580
- CA (authority change) journal entry
 - type 280
- CALL (Call Program) command
 - object authority required 463
 - transferring adopted authority 150
- Call Program (CALL) command
 - transferring adopted authority 150
- call-level interface
 - security level 40 15

- calling
 - program
 - transferring adopted
 - authority 150
- canceling
 - audit function 295
- cartridge
 - object authority required for
 - commands 438
- CCSID (coded character set identifier)
 - parameter
 - user profile 106
- CD (command string) file layout 583
- CD (command string) journal entry
 - type 272
- CFGDSTSRV (Configure Distribution Services) command
 - authorized IBM-supplied user
 - profiles 328
 - object authority required 373
- CFGIPS (Configure IP over SNA Interface) command
 - object authority required 352
- CFGRPDS (Configure VM/MVS Bridge) command
 - authorized IBM-supplied user
 - profiles 328
 - object authority required 373
- CFGSYSSEC (Configure System Security) command
 - authorized IBM-supplied user
 - profiles 328
 - description 316, 715
 - object authority required 474
- CFGTCP (Configure TCP/IP) command
 - object authority required 490
- CFGTCPAPP (Configure TCP/IP Applications) command
 - object authority required 490
- CFGTCPLPD (Configure TCP/IP LPD) command
 - object authority required 490
- CFGTCPSMTP (Configure TCP/IP SMTP) command
 - object authority required 490
- CFGTCPTELN (Change TCP/IP TELNET) command
 - object authority required 490
- change
 - password (QPWDCHGBLK system value) 47
 - change (*CHANGE) authority 134, 341
 - change *CRQD object (CQ) journal entry
 - type 277
- Change Accounting Code (CHGACGCDE) command 100
- Change Activation Schedule Entry (CHGACTSCDE) command
 - description 707
- Change Active Profile List (CHGACTPREFL) command
 - description 707
- Change Auditing (CHGAUD) command
 - description 310, 313
 - using 127
- Change Authority (CHGAUT)
 - command 159, 310

Change Authorization List Entry (CHGAUTLE) command
description 309
using 167

Change Command (CHGCMD) command
ALWLTUSR (allow limited user)
parameter 83
PRDLIB (product library)
parameter 210
security risks 210

Change Command Default (CHGCMDDFT) command 235

Change Current Library (CHGCURLIB) command
restricting 210

Change Dedicated Service Tools Password (CHGDSTPWD) command 311

Change Directory Entry (CHGDIRE) command 314

Change Document Library Object Auditing (CHGDLOAUD) command
*AUDIT (audit) special authority 88
description 313
QAUDCTL (Auditing Control) system value 66

Change Document Library Object Authority (CHGDLOAUT) command 313

Change Document Library Object Owner (CHGDLOOWN) command 313

Change Document Library Object Primary (CHGDLOPGP) command
description 313

Change Expiration Schedule Entry (CHGEXPSCDE) command
description 707

Change Job (CHGJOB) command
adopted authority 151

Change Journal (CHGJRN) command 293, 294

Change Kerberos Password (CHGKRBPWD) command
object authority required 422

Change Library List (CHGLIBL) command 207

Change Library Owner (CHGLIBOWN) tool 242

Change Menu (CHGMNU) command
PRDLIB (product library)
parameter 210
security risks 210

Change Network Attributes (CHGNETA) command 214

Change Node Group Attributes (Change Node Group Attributes) command
object auditing 538

Change Object Auditing (CHGOBJAUD) command
*AUDIT (audit) special authority 88
description 310, 313
QAUDCTL (Auditing Control) system value 66

Change Object Owner (CHGOBJOWN) command 163, 310

Change Object Primary Group (CHGOBJPGP) command 144, 164, 310

change of subsystem routing entry (SE) file layout 665

change of subsystem routing entry (SE) journal entry type 282

change of system value (SV) journal entry type 282

Change Output Queue (CHGOUTQ) command 211

Change Owner (CHGOWN) command 163, 310

change ownership (IP) journal entry type 281

Change Password (CHGPWD) command
auditing 259
description 311
enforcing password system values 47
setting password equal to profile name 76

Change Primary Group (CHGPGP) command 164, 310

Change Profile (CHGPRF) command 122, 311

Change Program (CHGPGM) command
specifying USEADPAUT
parameter 152

change request description
object authority required for
commands 355

change request description (*CRQD) object auditing 506

Change Security Auditing (CHGSECAUD) auditing
one-step 290

Change Security Auditing (CHGSECAUD) command
description 315, 709

Change Service Program (CHGSRVPGM) command
specifying USEADPAUT
parameter 152

Change Spooled File Attributes (CHGSPLFA) command 211

change system distribution directory (SD) file layout 664

change system distribution directory (SD) journal entry type 275

Change System Library List (CHGSYSLIBL) command 207, 227

change to DLO object (YC) file layout 698

change to object (ZC) file layout 700

change to spooled file (SF) journal entry type 284

Change User Audit (CHGUSRAUD) command 311
*AUDIT (audit) special authority 88
description 313
QAUDCTL (Auditing Control) system value 66
using 127

Change User Audit display 127

Change User Profile (CHGUSRPRF) command 311
description 311
password composition system values 47

Change User Profile (CHGUSRPRF) command (*continued*)
setting password equal to profile name 76
using 122

changing
access control list
audit journal (QAUDJRN) entry 282
accounting code 100
active profile list 707
adopted authority
authority required 151
audit journal receiver 293, 294
auditing
command description 310, 313
authority
audit journal (QAUDJRN) entry 280
command description 310
procedures 159
authorization list
entry 309
user authority 167

changing
audit journal (QAUDJRN) entry 281

command
ALWLTUSR (allow limited user)
parameter 83
defaults 235
current library 207, 210
device description
owner 203
directory entry 314
document library object (DLO) authority 313
owner 313
primary group 313
document library object auditing
command description 313

DST (dedicated service tools) password 129

DST (dedicated service tools) user ID 129

IBM-supplied user profile passwords 129

IPC object
audit journal (QAUDJRN) entry 281

job
adopted authority 151
audit journal (QAUDJRN) entry 273

job description
audit journal (QAUDJRN) entry 281

library list 207

menu
PRDLIB (product library)
parameter 210
security risks 210

network attribute
audit journal (QAUDJRN) entry 281
security-related 214

changing (*continued*)

- network profile
 - audit journal (QAUDJRN) entry 282
- object auditing 88, 310, 313
 - command description 313
- object owner 163, 310
- object ownership
 - moving application to production 242
- output queue 211
- ownership
 - device description 203
- password
 - description 311
 - DST (dedicated service tools) 129, 311
 - enforcing password system values 47
 - IBM-supplied user profiles 129
 - setting password equal to profile name 76
- primary group 144, 310
 - audit journal (QAUDJRN) entry 281
- primary group during restore
 - audit journal (QAUDJRN) entry 277
- profile 311
- program
 - specifying USEADPAUT parameter 152
- program adopt
 - audit journal (QAUDJRN) entry 281
- QAUDCTL (audit control) system value 315
- QAUDLVL (audit level) system value 315
- routing entry
 - audit journal (QAUDJRN) entry 282
- security auditing 315, 709
- security level (QSECURITY) system value
 - level 10 to level 20 12
 - level 20 to level 30 13
 - level 20 to level 40 18
 - level 20 to level 50 20
 - level 30 to level 20 13
 - level 30 to level 40 18
 - level 30 to level 50 20
 - level 40 to level 20 13
 - level 40 to level 30 19
 - level 50 to level 30 or 40 21
- server authentication entry 314
- spooled file
 - audit journal (QAUDJRN) entry 284
- system directory
 - audit journal (QAUDJRN) entry 275
- system library list 207, 227
- system value
 - audit journal (QAUDJRN) entry 282

changing (*continued*)

- systems management
 - audit journal (QAUDJRN) entry 284
- user auditing 88, 311, 313
 - user authority authorization list 167
- user ID
 - DST (dedicated service tools) 129
- user profile
 - audit journal (QAUDJRN) entry 277
 - command descriptions 311
 - methods 122
 - password composition system values 47
 - setting password equal to profile name 76
- changing access control list (VA) file layout 681
- characters
 - password 49
- chart format
 - object authority required for commands 356
- chart format (*CHTFMT) auditing 505
- Check Object Integrity (CHKOBJITG) command
 - auditing use 262
 - description 304, 311, 711
- Check Password (CHKPWD) command 128, 311
- checking 169
 - altered objects 304
 - default passwords 707
 - object integrity 711
 - auditing use 262
 - description 304, 311
 - password 128, 311
- checklist
 - auditing security 257
 - planning security 257
- CHGACGCDE (Change Accounting Code) command
 - object authority required 412
 - relationship to user profile 100
- CHGACTPRFL (Change Active Profile List) command
 - description 707
 - object authority required 492
- CHGACTSCDE
 - authorized IBM-supplied user profiles 328
- CHGACTSCDE (Change Activation Schedule Entry) command
 - description 707
- CHGACTSCDE (Change Activity Schedule Entry) command
 - object authority required 492
- CHGAJE (Change Autostart Job Entry) command
 - object auditing 548
 - object authority required 483
- CHGALRACNE (Change Alert Action Entry) command
 - object auditing 526
 - object authority required 388
- CHGALRD (Change Alert Description) command
 - object auditing 503
 - object authority required 352
- CHGALRSLTE (Change Alert Selection Entry) command
 - object auditing 526
 - object authority required 388
- CHGALRTBL (Change Alert Table) command
 - object auditing 503
 - object authority required 352
- CHGASPA
 - authorized IBM-supplied user profiles 328
- CHGASPA command 368
- CHGASPACT
 - authorized IBM-supplied user profiles 328
- CHGASPACT command
 - object authority required 368
- CHGASPCPYD
 - authorized IBM-supplied user profiles 328
- CHGASPSSN
 - authorized IBM-supplied user profiles 328
- CHGATR (Change Attribute) command
 - object auditing 512
- CHGATR (Change Attributes) command
 - object auditing 513
- CHGAUD (Change Audit) command using 127
- CHGAUD (Change Auditing) command
 - description 310, 313
 - object auditing 513, 550, 555
 - object authority required 392
- CHGAUT (Change Authority) command 159
 - description 310
 - object auditing 513, 550, 555
 - object authority required 393
- CHGAUTLE (Change Authorization List Entry) command
 - description 309
 - object auditing 503
 - object authority required 354
 - using 167
- CHGBCKUP (Change Backup Options) command
 - object authority required 450
- CHGCAD
 - authorized IBM-supplied user profiles 328
- CHGCAD command
 - object authority required 357
- CHGCDEFNT (Change Coded Font)
 - object authority required for commands 351
- CHGCFGL (Change Configuration List) command
 - object auditing 505
 - object authority required 364
- CHGCFGLE (Change Configuration List Entry) command
 - object auditing 505
 - object authority required 364

CHGCLNUP (Change Cleanup) command
 object authority required 450

CHGCLS (Change Class) command
 object auditing 507
 object authority required 356

CHGCLU
 authorized IBM-supplied user profiles 328

CHGCLU command
 object authority required 357

CHGCLUCFG
 authorized IBM-supplied user profiles 328

CHGCLUMON
 authorized IBM-supplied user profiles 328

CHGCLUMON command
 object authority required 357

CHGCLUNODE
 authorized IBM-supplied user profiles 328

CHGCLUNODE command
 object authority required 358

CHGCLURCY
 authorized IBM-supplied user profiles 329

CHGCLUVER
 authorized IBM-supplied user profiles 329

CHGCLUVER command
 object authority required 358

CHGCMD (Change Command) command
 ALWLMTUSR (allow limited user) parameter 83
 object auditing 507
 object authority required 361
 PRDLIB (product library) parameter 210
 security risks 210

CHGCMDCRQA (Change Command Change Request Activity) command
 authorized IBM-supplied user profiles 329
 object auditing 506
 object authority required 355

CHGCMDDDFT (Change Command Default) command
 object auditing 507
 object authority required 361
 using 235

CHGCMNE (Change Communications Entry) command
 object auditing 548
 object authority required 483

CHGCNNL (Change Connection List) command
 object auditing 508

CHGCNNLE (Change Connection List Entry) command
 object auditing 508

CHGCOMSNMP (Change Community for SNMP) command
 object authority required 490

CHGCOSD (Change Class-of-Service Description) command
 object auditing 509

CHGCOSD (Change Class-of-Service Description) command *(continued)*
 object authority required 356

CHGCRG
 authorized IBM-supplied user profiles 329

CHGCRG command
 object authority required 358

CHGCRGDEVE
 authorized IBM-supplied user profiles 329

CHGCRGDEVE command
 object authority required 358

CHGCRGPRI
 authorized IBM-supplied user profiles 329

CHGCRGPRI command
 object authority required 358

CHGCRQD (Change Change Request Description) command
 object auditing 506
 object authority required 355

CHGCRSDMNK (Change Cross Domain Key) command
 authorized IBM-supplied user profiles 329

CHGCSI (Change Communications Side Information) command
 object auditing 509
 object authority required 362

CHGCSPPGM (Change CSP/AE Program) command
 object auditing 543

CHGCTLAPPC (Change Controller Description (APPC)) command
 object authority required 365

CHGCTLASC (Change Controller Description (Async)) command
 object authority required 365

CHGCTLBSC (Change Controller Description (BSC)) command
 object authority required 365

CHGCTLFNC (Change Controller Description (Finance)) command
 object authority required 365

CHGCTLHOST (Change Controller Description (SNA Host)) command
 object authority required 365

CHGCTLLWS (Change Controller Description (Local Workstation)) command
 object authority required 365

CHGCTLNET (Change Controller Description (Network)) command
 object authority required 365

CHGCTLRIL (Change Controller Description (Retail)) command
 object authority required 365

CHGCTLRWS (Change Controller Description (Remote Workstation)) command
 object authority required 365

CHGCTLTAP (Change Controller Description (TAPE)) command
 object authority required 365

CHGCTLVWS (Change Controller Description (Virtual Workstation)) command
 object authority required 365

CHGCURDIR (Change Current Directory) command
 object auditing 514

CHGCURLIB (Change Current Library) command
 object authority required 430
 restricting 210

CHGDBG (Change Debug) command
 object authority required 463

CHGDMMF (Change Distributed Data Management File) command
 object auditing 523
 object authority required 382

CHGDEVAPPC (Change Device Description (APPC)) command
 object authority required 368

CHGDEVASC (Change Device Description (Async)) command
 object authority required 368

CHGDEVASP (Change Device Description for Auxiliary Storage Pool) command
 object authority required 368

CHGDEVBSC (Change Device Description (BSC)) command
 object authority required 368

CHGDEVCRP command
 object authority required 368

CHGDEVDSP (Change Device Description (Display)) command
 object authority required 368

CHGDEVFNC (Change Device Description (Finance)) command
 object authority required 368

CHGDEVHOST (Change Device Description (SNA Host)) command
 object authority required 368

CHGDEVINTR (Change Device Description (Intrasystem)) command
 object authority required 368

CHGDEVMLB command
 object authority required 368

CHGDEVNET (Change Device Description (Network)) command
 object authority required 368

CHGDEVNWSH command
 object authority required 368

CHGDEVOPT (Change Device Description (Optical)) command
 object authority required 368

CHGDEVOPT (Change Device Description (Optical)) command
 object authority required 451

CHGDEVPRT (Change Device Description (Printer)) command
 object authority required 368

CHGDEVRTL (Change Device Description (Retail)) command
 object authority required 368

CHGDEVSNPT (Change Device Description (SNPT)) command
 object authority required 369

CHGDEVSNUP (Change Device Description (SNUF)) command
 object authority required 369

CHGDEVTAP (Change Device Description (Tape)) command
 object authority required 369

CHGDIRE (Change Directory Entry) command
 description 314
 object authority required 371

CHGDIRSHD (Change Directory Shadow System) command
 object authority required 371

CHGDIRSRVA (Change Directory Server Attributes) command
 object authority required 371

CHGDIRSRVA command
 authorized IBM-supplied user profiles 329

CHGDKTF (Change Diskette File) command
 object auditing 523
 object authority required 382

CHGDLOAUD (Change Document Library Object Auditing) command
 *AUDIT (audit) special authority 88

CHGDLOAUD (Change Document Library Object Auditing) command
 description 313
 object auditing 517
 QAUDCTL (Auditing Control) system value 66

CHGDLOAUT (Change Document Library Object Auditing) command
 object authority required 374

CHGDLOAUT (Change Document Library Object Authority) command
 description 313
 object auditing 517
 object authority required 374

CHGDLOOWN (Change Document Library Object Owner) command
 description 313
 object auditing 517
 object authority required 374

CHGDLOPGP (Change Document Library Object Primary Group) command
 object auditing 517
 object authority required 374

CHGDLOPGP (Change Document Library Object Primary) command 313
 description 313

CHGDLOUAD (Change Document Library Object Auditing) command
 description 313

CHGDOCD (Change Document Description) command
 object auditing 517
 object authority required 374

CHGDSPF (Change Display File) command
 object auditing 523
 object authority required 382

CHGDSTD (Change Distribution Description) command
 object auditing 517

CHGDSTD (Change Distribution Description) command *(continued)*
 object authority required 373

CHGDSTL (Change Distribution List) command
 object authority required 374

CHGDSTPWD (Change Dedicated Service Tools Password) command
 description 311
 object authority required 492

CHGDSTQ (Change Distribution Queue) command
 authorized IBM-supplied user profiles 329
 object authority required 373

CHGDSTRTE (Change Distribution Route) command
 authorized IBM-supplied user profiles 329
 object authority required 373

CHGDTA (Change Data) command
 object authority required 382

CHGDTAARA (Change Data Area) command
 object auditing 519
 object authority required 367

CHGEMLCFGE (Change Emulation Configuration Entry) command
 object authority required 370

CHGENVVAR (Change Environment Variable) command
 object authority required 380

CHGEWCBCDE (Change Extended Wireless Controller Bar Code Entry) command
 object authority required 381

CHGEWCM (Change Extended Wireless Controller Member) command
 object authority required 381

CHGEWCPTCE (Change Extended Wireless Controller PTC Entry) command
 object authority required 381

CHGEWLM (Change Extended Wireless Line Member) command
 object authority required 381

CHGEXPSCDE (Change Expiration Schedule Entry) command
 authorized IBM-supplied user profiles 329
 description 707
 object authority required 493

CHGFCNARA
 authorized IBM-supplied user profiles 329

CHGFCT (Change Forms Control Table) command
 object authority required 471

CHGFCTE (Change Forms Control Table Entry) command
 object authority required 471

CHGFNTTBLE (Change DBCS Font Table Entry)
 object authority required for commands 351

CHGFTR (Change Filter) command
 object auditing 527

CHGFTR (Change Filter) command *(continued)*
 object authority required 388

CHGGPHFMT
 authorized IBM-supplied user profiles 329

CHGGPHFMT (Change Graph Format) command
 object authority required 456

CHGGPHPKG (Change Graph Package) command
 authorized IBM-supplied user profiles 329
 object authority required 456

CHGGRPA (Change Group Attributes) command
 object authority required 412

CHGHLLPTR (Change High-Level Language Pointer) command
 object authority required 463

CHGICFDEVE (Change Intersystem Communications Function Program Device Entry) command
 object authority required 382

CHGICFF (Change Intersystem Communications Function File) command
 object authority required 382

CHGIMGCLG command
 object authority required 391

CHGIMGCLGE command
 object authority required 391

CHGIPLA command 411

CHGIPSIFC (Change IP over SNA Interface) command
 object authority required 352

CHGIPSLOC (Change IP over SNA Location Entry) command
 object authority required 352

CHGIPSTOS (Change IP over SNA Type of Service) command
 object authority required 352

CHGJOB (Change Job) command
 adopted authority 151
 object auditing 529
 object authority required 412

CHGJOB (Change Job) command
 object auditing 529
 object authority required 415

CHGJOBQ (Change Job Queue) command
 object auditing 529
 object authority required 416

CHGJOBQE (Change Job Queue Entry) command
 object auditing 529, 548
 object authority required 484

CHGJOBSCDE (Change Job Schedule Entry) command
 object auditing 530
 object authority required 417

CHGJOBTRC
 authorized IBM-supplied user profiles 329

CHGJOBTYP (Change Job Type) command
 authorized IBM-supplied user profiles 329
 object authority required 456

CHGJRN (Change Journal) command
 authorized IBM-supplied user profiles 329
 detaching receiver 293, 294
 object auditing 531, 532
 object authority required 418

CHGJRNA (Change Journal Attributes) command
 authorized IBM-supplied user profiles 329
 object authority required 418

CHGJRNOBJ (Change Journaled Object) command
 object auditing 500

CHGLANADPI (Change LAN Adapter Information) command
 object authority required 437

CHGLF (Change Logical File) command
 object auditing 523
 object authority required 382

CHGLFM (Change Logical File Member) command
 object auditing 524
 object authority required 382

CHGLIB (Change Library) command
 object auditing 533
 object authority required 430

CHGLIBL (Change Library List) command
 object authority required 430
 using 207

CHGLIBOWN (Change Library Owner) tool 242

CHGLICINF (Change License Information) command
 authorized IBM-supplied user profiles 329
 object authority required 435

CHGLINASC (Change Line Description (Async)) command
 object authority required 435

CHGLINBSC (Change Line Description (BSC)) command
 object authority required 435

CHGLINETH (Change Line Description (Ethernet)) command
 object authority required 435

CHGLINFAX (Change Line Description (FAX)) command
 object authority required 435

CHGLINFR (Change Line Description (Frame Relay Network)) command
 object authority required 435

CHGLINIDD (Change Line Description (DDI Network)) command
 object authority required 435

CHGLINS DLC (Change Line Description (SDLC)) command
 object authority required 435

CHGLINTDLC (Change Line Description (TDLC)) command
 object authority required 435

CHGLINTRN (Change Line Description (Token-Ring Network)) command
 object authority required 435

CHGLINWLS (Change Line Description (Wireless)) command
 object authority required 436

CHGLINX25 (Change Line Description (X.25)) command
 object authority required 436

CHGLPDA (Change LPD Attributes) command
 object authority required 490

CHGMGDSYSA (Change Managed System Attributes) command
 authorized IBM-supplied user profiles 329

CHGMGRSRVA (Change Manager Service Attributes) command
 authorized IBM-supplied user profiles 329

CHGMGTCOL command
 object authority required 456

CHGMNU (Change Menu) command
 object auditing 535
 object authority required 439

PRDLIB (product library) parameter 210
 security risks 210

CHGMOD (Change Module) command
 object auditing 536
 object authority required 443

CHGMODD (Change Mode Description) command
 object auditing 535
 object authority required 442

CHGMSGD (Change Message Description) command
 object auditing 536
 object authority required 441

CHGMSGF (Change Message File) command
 object auditing 536
 object authority required 441

CHGMSGQ (Change Message Queue) command
 object auditing 537
 object authority required 441

CHGMSTK (Change Master Key) command
 authorized IBM-supplied user profiles 329

CHGMWSD (Change Network Server Description) command
 object auditing 540

CHGNETA (Change Network Attributes) command
 authorized IBM-supplied user profiles 329
 object authority required 444
 using 214

CHGNETJOBE (Change Network Job Entry) command
 authorized IBM-supplied user profiles 329
 object authority required 444

CHGNFSEXP (Change Network File System Export) command
 authorized IBM-supplied user profiles 329
 object authority required 445

CHGNTBD (Change NetBIOS Description) command
 object auditing 539
 object authority required 443

CHGNWIFR (Change Network Interface Description (Frame Relay Network)) command
 object authority required 446

CHGNWIISDN (Change Network Interface Description for ISDN) command
 object auditing 539

CHGNWSA (Change Network Server Attribute) command
 object authority required 447

CHGNWSA (Change Network Server Attributes) command
 authorized IBM-supplied user profiles 329

CHGNWSALS (Change Network Server Alias) command
 object authority required 447

CHGNWSCFG command
 authorized IBM-supplied user profiles 329
 object authority required 448

CHGNWSD (Change Network Server Description) command
 object authority required 448

CHGNWSSTG (Change Network Server Storage Space) command
 object authority required 446

CHGNWSVRA (Create Network Server Attribute) command
 object authority required 446

CHGOBJAUD (Change Object Audit) command
 object authority required 343

CHGOBJAUD (Change Object Auditing) command
 *AUDIT (audit) special authority 88

CHGOBJAUD (Change Object Auditing) command
 description 310
 QAUDCTL (Auditing Control) system value 66

CHGOBJCRQA (Change Object Change Request Activity) command
 authorized IBM-supplied user profiles 329
 object auditing 506
 object authority required 355

CHGOBJD (Change Object Description) command
 object auditing 500
 object authority required 343

CHGOBJOWN (Change Object Owner) command
 description 310
 object auditing 500
 object authority required 344
 using 163

CHGOBJPGP (Change Object Primary Group) command 144, 164
description 310

CHGOBJPGP (Change Object Primary) command
object authority required 344

CHGOBJUAD (Change Object Auditing) command
description 313

CHGOPTA (Change Optical Attributes) command
authorized IBM-supplied user profiles 329
object authority required 451

CHGOPTVOL (Change Optical Volume) command
object authority required 451

CHGOUTQ (Change Output Queue) command
object auditing 540
object authority required 454
using 211

CHGOWN (Change Owner) command 163
description 310
object auditing 513, 550, 555, 558
object authority required 393

CHGPCST (Change Physical File Constraint) command
object authority required 382

CHGPDGPRF (Change Print Descriptor Group Profile) command
object auditing 542
object authority required 461

CHGPXDFN (Change Performance Explorer Definition) command
authorized IBM-supplied user profiles 329
object authority required 456

CHGPF (Change Physical File) command
object auditing 524
object authority required 382

CHGPFCNARA (Change Functional Area) command
object authority required 456

CHGPFCST (Change Physical File Constraint) command
object auditing 524

CHGPFM (Change Physical File Member) command
object auditing 524
object authority required 382

CHGPFTRG (Change Physical File Trigger) command
object auditing 525
object authority required 382

CHGPGM (Change Program) command
object auditing 543
object authority required 463
specifying USEADPAUT parameter 152

CHGPGMVAR (Change Program Variable) command
object authority required 463

CHGPGP (Change Primary Group) command 164
description 310

CHGPGP (Change Primary Group) command (*continued*)
object auditing 513, 550, 556, 558
object authority required 393

CHGPJ (Change Prestart Job) command
object authority required 412

CHGPJE (Change Prestart Job Entry) command
object auditing 548
object authority required 484

CHGPRB (Change Problem) command
authorized IBM-supplied user profiles 329
object authority required 462

CHGPRBACNE (Change Problem Action Entry) command
object auditing 527
object authority required 388, 462

CHGPRBSLTE (Change Problem Selection Entry) command
object auditing 527
object authority required 388, 462

CHGPRDCRQA (Change Product Change Request Activity) command
authorized IBM-supplied user profiles 329
object auditing 506
object authority required 355

CHGPRF (Change Profile) command
description 311
object auditing 560
object authority required 493
using 122

CHGPRTF (Change Printer File) command
object auditing 524
object authority required 382

CHGPSFCFG (Change Print Services Facility Configuration) command
object authority required 461

CHGPTFCRQA (Change PTF Change Request Activity) command
authorized IBM-supplied user profiles 329
object auditing 506
object authority required 355

CHGPTR (Change Pointer) command
authorized IBM-supplied user profiles 329
object authority required 463

CHGPWD (Change Password) command
auditing 259
description 311
enforcing password system values 47
object auditing 560
object authority required 493
setting password equal to profile name 76

CHGPWRSCD (Change Power On/Off Schedule) command
object authority required 450

CHGPWRSCDE (Change Power On/Off Schedule Entry) command
object authority required 450

CHGQRYA (Change Query Attribute) command
object authority required 466

CHGQSTDB (Change Question-and-Answer Database) command
authorized IBM-supplied user profiles 329
object authority required 468

CHGRCYAP (Change Recovery for Access Paths) command
authorized IBM-supplied user profiles 329
object auditing 502
object authority required 350

CHGRDBDIRE (Change Relational Database Directory Entry) command
object authority required 469

CHGRJECMNE (Change RJE Communications Entry) command
object authority required 471

CHGRJERDRE (Change RJE Reader Entry) command
object authority required 471

CHGRJEWTR (Change RJE Writer Entry) command
object authority required 471

CHGRMTJRN (Change Remote Journal) command
object auditing 531

CHGRPYLE (Change Reply List Entry) command
authorized IBM-supplied user profiles 329
object auditing 548
object authority required 486

CHGRSCCRQA (Change Resource Change Request Activity) command
authorized IBM-supplied user profiles 329
object auditing 507
object authority required 355

CHGRTGE (Change Routing Entry) command
object auditing 548
object authority required 484

CHGS34LIBM (Change System/34 Library Members) command
authorized IBM-supplied user profiles 330
object authority required 442

CHGS36 (Change System/36) command
object auditing 558
object authority required 486

CHGS36A (Change System/36 Attributes) command
object auditing 558
object authority required 486

CHGS36PGMA (Change System/36 Program Attributes) command
object auditing 543
object authority required 486

CHGS36PRCA (Change System/36 Procedure Attributes) command
object auditing 524
object authority required 486

CHGS36SRCA (Change System/36 Source Attributes) command
object authority required 486

CHGSAVF (Change Save File) command
 object auditing 524
 object authority required 382

CHGSBSD (Change Subsystem Description) command
 object auditing 549
 object authority required 484

CHGSCHIDX (Change Search Index) command
 object auditing 549
 object authority required 411

CHGSECA (Change Security Attributes) command
 object authority required 474

CHGSECAUD (Change Security Audit) command
 object authority required 474

CHGSECAUD (Change Security Auditing) command
 security auditing function 290

CHGSECAUD (Change Security Auditing) command
 description 315, 709

CHGSHRPOOL (Change Shared Storage Pool) command
 object authority required 485

CHGSNMPA (Change SNMP Attributes) command
 object authority required 490

CHGSPLFA (Change Spooled File Attributes) command
 action auditing 553
 DSPDTA parameter of output queue 211
 object auditing 540, 541
 object authority required 481

CHGSRCPF (Change Source Physical File) command
 object authority required 382

CHGSRVA (Change Service Attributes) command
 object authority required 475

CHGSRVPGM (Change Service Program) command
 object auditing 554
 object authority required 463
 specifying USEADPAUT parameter 152

CHGSSND (Change Session Description) command
 object authority required 471

CHGSSNMAX (Change Session Maximum) command
 object auditing 535
 object authority required 442

CHGSVRAUTE (Change Server Authentication Entry) command
 object authority required 475

CHGSYSDIRA (Change System Directory Attributes) command
 object auditing 515
 object authority required 371

CHGSYSJOB (Change System Job) command
 object authority required 412

CHGSYSLIBL (Change System Library List) command
 authorized IBM-supplied user profiles 329
 object authority required 430
 programming example 227
 using 207

CHGYSVAL (Change System Value) command
 authorized IBM-supplied user profiles 329
 object authority required 486

CHGTAPCTG (Change Tape Cartridge) command
 object authority required 438

CHGTAPF (Change Tape File) command
 object auditing 524
 object authority required 382

CHGTCPA (Change TCP/IP Attributes) command
 object authority required 490

CHGTCPHTE (Change TCP/IP Host Table Entry) command
 object authority required 490

CHGTCPIFC (Change TCP/IP Interface) command
 object authority required 490

CHGTCPRTE (Change TCP/IP Route Entry) command
 object authority required 490

CHGTELNA (Change TELNET Attributes) command
 object authority required 490

CHGTIMZON command 491

CHGUSRAUD (Change User Audit) command
 *AUDIT (audit) special authority 88
 description 311, 313
 object authority required 493
 QAUDCTL (Auditing Control) system value 66
 using 127

CHGUSRPRF (Change User Profile) command
 description 311
 object auditing 560
 object authority required 493
 password composition system values 47
 setting password equal to profile name 76
 using 122

CHGUSRTRC (Change User Trace) command
 object authority required 412

CHGVTMAP (Change VT100 Keyboard Map) command
 object authority required 490

CHGWSE (Change Workstation Entry) command
 object auditing 549
 object authority required 484

CHGWTR (Change Writer) command
 object authority required 496

CHKASPBAL
 authorized IBM-supplied user profiles 330

CHKCMNTRC (Check Communications Trace) command
 authorized IBM-supplied user profiles 330
 object authority required 475

CHKDLO (Check Document Library Object) command
 object authority required 375

CHKDNSCFG (DNS Configuration Utility) command
 object authority required 378

CHKDNSZNE (DNS Zone Utility) command
 object authority required 378

CHKDOC (Check Document) command
 object auditing 516
 object authority required 375

CHKIGCTBL (Check DBCS Font Table) command
 object auditing 528

CHKIN (Check In) command
 object auditing 550, 556
 object authority required 394

CHKMSTKVV command
 authorized IBM-supplied user profiles 330
 object authority required 367

CHKOBJ (Check Object) command
 object auditing 501
 object authority required 344

CHKOBJITG (Check Object Integrity) command 3
 auditing use 262
 description 304, 311, 711
 object authority required 344

CHKOUT (Check Out) command
 object auditing 550, 556
 object authority required 394

CHKPRDOPT (Check Product Option) command
 authorized IBM-supplied user profiles 330
 object authority required 475

CHKPWD (Check Password) command
 description 311
 object auditing 560
 object authority required 493
 using 128

CHKTAP (Check Tape) command
 object authority required 438

CHRIDCTL (user options) parameter
 user profile 106

CL keyword (*CLKWD) user option 106, 107, 108

class
 object authority required for commands 356
 relationship to security 217

Class (*CLS) auditing 507

class files
 jar files 243

class-of-service description
 object authority required for commands 356

class-of-service description (*COSD)
 auditing 509

class, user 79

cleanup
 object authority required for
 commands 450

client request access (PCSACC) network
 attribute 215

close of server files (VF) file layout 682

CLP38 programs 137

CLRJOBQ (Clear Job Queue) command
 object auditing 529
 object authority required 416

CLRLIB (Clear Library) command
 object auditing 533
 object authority required 431

CLRMSGQ (Clear Message Queue)
 command
 object auditing 537
 object authority required 441

CLRMSTKEY (Clear Master Key)
 command
 authorized IBM-supplied user
 profiles 330

CLRMSTKEY command
 object authority required 367

CLROUTQ (Clear Output Queue)
 command
 action auditing 553
 object auditing 540
 object authority required 454

CLRPFM (Clear Physical File Member)
 command
 object auditing 524
 object authority required 383

CLRSVAV (Clear Save File) command
 object authority required 383

CLRTRCDTA (Clear Trace Data)
 command
 object authority required 463

cluster
 object authority required for
 commands 357

Cluster Operations(CU) file layout 589

CMPIJRNIMG (Compare Journal Images)
 command
 object auditing 530
 object authority required 418

CNLRJERDR (Cancel RJE Reader)
 command
 object authority required 471

CNLRJEWTR (Cancel RJE Writer)
 command
 object authority required 472

CNTRYID (country or region identifier)
 parameter
 user profile 105

CO (create object) file layout 584

CO (create object) journal entry
 type 144, 272

coded character set identifier
 CCSID user profile parameter 106
 QCCSID system value 106

combining authorization methods
 example 195

command
 auditing
 audit journal (QAUDJRN)
 entry 272

command (*continued*)
 changing
 ALWLMTUSR (allow limited user)
 parameter 83
 defaults 235
 PRDLIB (product library)
 parameter 210
 security risks 210

creating
 ALWLMTUSR (allow limited user)
 parameter 83
 PRDLIB (product library)
 parameter 210
 security risks 210

NLV (national language version)
 security 235

planning security 235

revoking public authority 316, 715

System/38
 security 235

command (*CMD object type)
 object authority required for
 commands 361

Command (*CMD) auditing 507

command capability
 listing users 302

command string
 audit journal (QAUDJRN) file
 layout 583

command string (*CMD) audit level 272

command string (CD) file layout 583

command string (CD) journal entry
 type 272

command, CL
 activation schedule 707
 Add Authorization List Entry
 (ADDAUTLE) 167, 309
 Add Directory Entry
 (ADDDIRE) 314
 Add Document Library Object
 Authority (ADDDLOAUT) 313
 Add Library List Entry
 (ADDLIBLE) 207, 210
 Add Server Authentication Entry
 (ADDSVRAUTE) 314
 ADDAUTLE (Add Authorization List
 Entry) 167, 309
 ADDDIRE (Add Directory
 Entry) 314
 ADDDLOAUT (Add Document
 Library Object Authority) 313
 ADDJOBSCDE (Add Job Schedule
 Entry)
 SECBATCH menu 710
 ADDLIBLE (Add Library List
 Entry) 207, 210
 ADDSVRAUTE (Add Server
 Authentication Entry) 314
 allowed for limit capabilities user 83
 ALWLMTUSR (allow limited user)
 parameter 83
 ANZDFTPWD (Analyze Default
 Passwords)
 description 707
 ANZPRFACT (Analyze Profile
 Activity)
 creating exempt users 707

command, CL (*continued*)
 ANZPRFACT (Analyze Profile
 Activity) (*continued*)
 description 707
 authority holders, table 309, 314
 authorization lists 309
 CALL (Call Program)
 transferring adopted
 authority 150
 Call Program (CALL)
 transferring adopted
 authority 150
 CFGSYSSEC (Configure System
 Security)
 description 316, 715
 Change Accounting Code
 (CHGACGCDE) 100
 Change Authorization List Entry
 (CHGAUTLE)
 description 309
 using 167
 Change Command (CHGCMD)
 ALWLMTUSR (allow limited user)
 parameter 83
 PRDLIB (product library)
 parameter 210
 security risks 210
 Change Command Default
 (CHGCMDDDFT) 235
 Change Current Library
 (CHGCURLIB)
 restricting 210
 Change Dedicated Service Tools
 Password (CHGDSTPWD) 311
 Change Directory Entry
 (CHGDIRE) 314
 Change Document Library Object
 Auditing (CHGDLOAUD) 313
 *AUDIT (audit) special
 authority 88
 description 313
 QAUDCTL (Auditing Control)
 system value 66
 Change Document Library Object
 Authority (CHGDLOAUT) 313
 Change Document Library Object
 Owner (CHGDLOOWN) 313
 Change Document Library Object
 Primary (CHGDLOPGP) 313
 Change Job (CHGJOB)
 adopted authority 151
 Change Journal (CHGJRN) 293, 294
 Change Library List (CHGLIBL) 207
 Change Menu (CHGMNU)
 PRDLIB (product library)
 parameter 210
 security risks 210
 Change Network Attributes
 (CHGNETA) 214
 Change Object Auditing
 (CHGOBJAUD) 310
 *AUDIT (audit) special
 authority 88
 description 313
 QAUDCTL (Auditing Control)
 system value 66

- command, CL (*continued*)
- Change Object Owner (CHGOBJOWN) 163, 310
 - Change Object Primary Group (CHGOBJPGP) 144, 164, 310
 - Change Output Queue (CHGOUTQ) 211
 - Change Password (CHGPWD)
 - auditing 259
 - description 311
 - enforcing password system values 47
 - setting password equal to profile name 76
 - Change Profile (CHGPRF) 122, 311
 - Change Program (CHGPGM)
 - specifying USEADPAUT parameter 152
 - Change Security Auditing (CHGSECAUD)
 - description 315
 - Change Server Authentication Entry (CHGSVRAUTE) 314
 - Change Service Program (CHGSRVPGM)
 - specifying USEADPAUT parameter 152
 - Change Spooled File Attributes (CHGSPLFA) 211
 - Change System Library List (CHGSYSLIBL) 207, 227
 - Change User Audit (CHGUSRAUD) 311
 - *AUDIT (audit) special authority 88
 - description 313
 - QAUDCTL (Auditing Control) system value 66
 - using 127
 - Change User Profile (CHGUSRPRF) 311
 - description 311
 - password composition system values 47
 - setting password equal to profile name 76
 - using 122
 - Check Object Integrity (CHKOBJITG)
 - auditing use 262
 - description 304, 311
 - Check Password (CHKPWD) 128, 311
 - CHGACGCDE (Change Accounting Code) 100
 - CHGACTPREF (Change Active Profile List)
 - description 707
 - CHGACTSCDE (Change Activation Schedule Entry)
 - description 707
 - CHGAUTLE (Change Authorization List Entry)
 - description 309
 - using 167
 - CHGCMD (Change Command)
 - ALWLMTUSR (allow limited user) parameter 83
- command, CL (*continued*)
- CHGCMD (Change Command) (*continued*)
 - PRDLIB (product library) parameter 210
 - security risks 210
 - CHGCMDDFT (Change Command Default) 235
 - CHGCURLIB (Change Current Library)
 - restricting 210
 - CHGDIRE (Change Directory Entry) 314
 - CHGDLOAUD (Change Document Library Object Auditing) 313
 - *AUDIT (audit) special authority 88
 - QAUDCTL (Auditing Control) system value 66
 - CHGDLOAUT (Change Document Library Object Authority) 313
 - CHGDLOOWN (Change Document Library Object Owner) 313
 - CHGDLOPGP (Change Document Library Object Primary) 313
 - CHGDLOUAD (Change Document Library Object Auditing)
 - description 313
 - CHGDSTPWD (Change Dedicated Service Tools Password) 311
 - CHGEXPCDE (Change Expiration Schedule Entry)
 - description 707
 - CHGJOB (Change Job)
 - adopted authority 151
 - CHGJRN (Change Journal) 293, 294
 - CHGLIBL (Change Library List) 207
 - CHGMNU (Change Menu)
 - PRDLIB (product library) parameter 210
 - security risks 210
 - CHGNETA (Change Network Attributes) 214
 - CHGOBJAUD (Change Object Auditing) 310
 - *AUDIT (audit) special authority 88
 - description 313
 - QAUDCTL (Auditing Control) system value 66
 - CHGOBJOWN (Change Object Owner) 163, 310
 - CHGOBJPGP (Change Object Primary Group) 144, 164, 310
 - CHGOUTQ (Change Output Queue) 211
 - CHGPGM (Change Program)
 - specifying USEADPAUT parameter 152
 - CHGPRF (Change Profile) 122, 311
 - CHGPWD (Change Password)
 - auditing 259
 - description 311
 - enforcing password system values 47
 - setting password equal to profile name 76
- command, CL (*continued*)
- CHGSECAUD (Change Security Auditing)
 - description 315, 709
 - CHGSPLFA (Change Spooled File Attributes) 211
 - CHGSRVPGM (Change Service Program)
 - specifying USEADPAUT parameter 152
 - CHGSVRAUTE (Change Server Authentication Entry) 314
 - CHGSYSLIBL (Change System Library List) 207, 227
 - CHGUSRAUD (Change User Audit) 311
 - *AUDIT (audit) special authority 88
 - description 313
 - QAUDCTL (Auditing Control) system value 66
 - using 127
 - CHGUSRPRF (Change User Profile) 311
 - description 311
 - password composition system values 47
 - setting password equal to profile name 76
 - using 122
 - CHKOBJITG (Check Object Integrity)
 - auditing use 262
 - description 304, 311, 711
 - CHKPWD (Check Password) 128, 311
 - Configure System Security (CFGSYSSEC)
 - description 316
 - Copy Spooled File (CPYSPLF) 211
 - CPYSPLF (Copy Spooled File) 211
 - Create Authority Holder (CRTAUTHLR) 153, 309, 314
 - Create Authorization List (CRTAUTL) 166, 309
 - Create Command (CRTCMD)
 - ALWLMTUSR (allow limited user) parameter 83
 - PRDLIB (product library) parameter 210
 - security risks 210
 - Create Journal (CRTJRN) 291
 - Create Journal Receiver (CRTJRNRCV) 291
 - Create Library (CRTLIB) 157
 - Create Menu (CRTMNU)
 - PRDLIB (product library) parameter 210
 - security risks 210
 - Create Output Queue (CRTOUTQ) 211, 214
 - Create User Profile (CRTUSRPRF)
 - description 118, 311
 - CRTAUTHLR (Create Authority Holder) 153, 309, 314
 - CRTAUTL (Create Authorization List) 166, 309

- command, CL (*continued*)
 - CRTCMD (Create Command)
 - ALWLMTUSR (allow limited user)
 - parameter 83
 - PRDLIB (product library)
 - parameter 210
 - security risks 210
 - CRTJRN (Create Journal) 291
 - CRTJRNRCV (Create Journal Receiver) 291
 - CRTLIB (Create Library) 157
 - CRTMNU (Create Menu)
 - PRDLIB (product library)
 - parameter 210
 - security risks 210
 - CRTOUTQ (Create Output Queue) 211, 214
 - CRTUSRPRF (Create User Profile)
 - description 118, 311
 - Delete Authority Holder (DLTAUTHLR) 154, 309
 - Delete Authorization List (DLTAUTL) 169, 309
 - Delete Journal Receiver (DLTJRNRCV) 294
 - Delete User Profile (DLTUSRPRF)
 - description 311
 - example 122
 - object ownership 143
 - Display Audit Journal Entries (DSPAUDJRNE)
 - description 315
 - Display Authority Holder (DSPAUTHLR) 153, 309
 - Display Authorization List (DSPAUTL) 309
 - Display Authorization List Document Library Objects (DSPAUTLDLO) 313
 - Display Authorization List Objects (DSPAUTLOBJ) 168, 309
 - Display Authorized Users (DSPAUTUSR)
 - auditing 301
 - description 311
 - example 125
 - Display Document Library Object Auditing (DSPDLOAUD) 288, 313
 - Display Document Library Object Authority (DSPDLOAUT) 313
 - Display Job Description (DSPJOB) 261
 - Display Journal (DSPJRN)
 - audit (QAUDJRN) journal
 - example 295
 - auditing file activity 236, 300
 - creating output file 296
 - displaying QAUDJRN (audit) journal 263
 - Display Library (DSPLIB) 303
 - Display Library Description (DSPLIBD)
 - CRTAUT parameter 158
 - Display Object Authority (DSPOBJAUT) 303, 310
 - Display Object Description (DSPOBJD) 288, 310
- command, CL (*continued*)
 - created by 144
 - object domain 15
 - program state 15
 - using output file 302
 - Display Program (DSPPGM)
 - adopted authority 151
 - program state 15
 - Display Programs That Adopt (DSPPGMADP)
 - auditing 303
 - description 312
 - using 151, 236
 - Display Security Auditing (DSPSECAUD Values)
 - description 315
 - Display Service Program (DPSRVPGM)
 - adopted authority 151
 - Display Spooled File (DSPSPLF) 211
 - Display User Profile (DSPUSRPRF)
 - description 311
 - using 125
 - using output file 302
 - displaying keywords (*CLKWD user option) 106, 107, 108
 - DLTAUTHLR (Delete Authority Holder) 154, 309
 - DLTAUTL (Delete Authorization List) 169, 309
 - DLTJRNRCV (Delete Journal Receiver) 294
 - DLTUSRPRF (Delete User Profile)
 - description 311
 - example 122
 - object ownership 143
 - document library object (DLO)
 - table 313
 - DSPACTPRFL (Display Active Profile List)
 - description 707
 - DSPACTSCD (Display Activation Schedule)
 - description 707
 - DSPAUDJRNE (Display Audit Journal Entries)
 - description 315, 711
 - DSPAUTHLR (Display Authority Holder) 153, 309
 - DSPAUTL (Display Authorization List) 309
 - DSPAUTLDLO (Display Authorization List Document Library Objects) 313
 - DSPAUTLOBJ (Display Authorization List Objects) 168, 309
 - DSPAUTUSR (Display Authorized Users)
 - auditing 301
 - description 311
 - example 125
 - DSPDLOAUD (Display Document Library Object Auditing) 288, 313
 - DSPDLOAUT (Display Document Library Object Authority) 313
 - DSPEXPSCD (Display Expiration Schedule)
 - description 707
- command, CL (*continued*)
 - DSPJOB (Display Job Description) 261
 - DSPJRN (Display Journal)
 - audit (QAUDJRN) journal
 - example 295
 - auditing file activity 236, 300
 - creating output file 296
 - displaying QAUDJRN (audit) journal 263
 - DSPLIB (Display Library) 303
 - DSPLIBD (Display Library Description)
 - CRTAUT parameter 158
 - DSPOBJAUT (Display Object Authority) 303, 310
 - DSPOBJD (Display Object Description) 288, 310
 - created by 144
 - object domain 15
 - program state 15
 - using output file 302
 - DSPPGM (Display Program)
 - adopted authority 151
 - program state 15
 - DSPPGMADP (Display Programs That Adopt)
 - auditing 303
 - description 312
 - using 151, 236
 - DSPSECAUD (Display Security Auditing Values)
 - description 315
 - DSPSECAUD (Display Security Auditing)
 - description 709
 - DSPSPLF (Display Spooled File) 211
 - DPSRVPGM (Display Service Program)
 - adopted authority 151
 - DSPUSRPRF (Display User Profile)
 - description 311
 - using 125
 - using output file 302
 - Edit Authorization List (EDTAUTL) 167, 309
 - Edit Document Library Object Authority (EDTDLOAUT) 313
 - Edit Library List (EDTLIBL) 207
 - Edit Object Authority (EDTOBJAUT) 159, 310
 - EDTAUTL (Edit Authorization List) 167, 309
 - EDTDLOAUT (Edit Document Library Object Authority) 313
 - EDTLIBL (Edit Library List) 207
 - EDTOBJAUT (Edit Object Authority) 159, 310
 - End Job (ENDJOB)
 - QINACTMSGQ system value 28
 - ENDJOB (End Job)
 - QINACTMSGQ system value 28
 - Grant Object Authority (GRTOBJAUT) 310
 - affect on previous authority 162
 - multiple objects 162

- command, CL (*continued*)
 - Grant User Authority (GRTUSRAUT)
 - copying authority 121
 - description 311
 - recommendations 165
 - renaming profile 127
 - Grant User Permission (GRTUSRPMN) 313
 - GRTOBJAUT (Grant Object Authority) 310
 - affect on previous authority 162
 - multiple objects 162
 - GRTUSRAUT (Grant User Authority)
 - copying authority 121
 - description 311
 - recommendations 165
 - renaming profile 127
 - GRTUSRPMN (Grant User Permission) 313
 - keywords, displaying (*CLKWD user option) 106, 107, 108
 - object authority, table 310
 - parameter names, displaying (*CLKWD user option) 106, 107, 108
 - passwords, table 311
 - Print Communications Security Attributes (PRTCMNSEC)
 - description 316
 - Print Job Description Authority (PRTJOBDAUT) 316
 - Print Private Authorities (PRTPVTAUT) 316
 - Print Publicly Authorized Objects (PRTPUBAUT) 316
 - Print Queue Authority (PRTQAUT)
 - description 316
 - Print Subsystem Description Authority (PRTSBSDAUT)
 - description 316
 - Print System Security Attributes (PRTSYSSECA)
 - description 316
 - Print Trigger Programs (PRTTRGPGM)
 - description 316
 - Print User Objects (PRTUSROBJ)
 - description 316
 - PRTADPOBJ (Print Adopting Objects)
 - description 711
 - PRTCMNSEC (Print Communications Security)
 - description 316, 711
 - PRTJOBDAUT (Print Job Description Authority) 316
 - description 711
 - PRTPUBAUT (Print Publicly Authorized Objects) 316
 - description 711
 - PRTPVTAUT (Print Private Authorities) 316
 - authorization list 711
 - description 713
 - PRTQAUT (Print Queue Authority)
 - description 316, 713
- command, CL (*continued*)
 - PRTSBSDAUT (Print Subsystem Description Authority)
 - description 316
 - PRTSBSDAUT (Print Subsystem Description)
 - description 711
 - PRTSYSSECA (Print System Security Attributes)
 - description 316, 711
 - PRTTRGPGM (Print Trigger Programs)
 - description 316, 711
 - PRTUSROBJ (Print User Objects)
 - description 316, 711
 - PRTUSRPRF (Print User Profile)
 - description 711
 - RCLSTG (Reclaim Storage) 19, 26, 145, 255
 - Reclaim Storage (RCLSTG) 19, 26, 145, 255
 - Remove Authorization List Entry (RMVAUTLE) 167, 309
 - Remove Directory Entry (RMVDIRE) 314
 - Remove Document Library Object Authority (RMVDLOAUT) 313
 - Remove Library List Entry (RMVLIBLE) 207
 - Remove Server Authentication Entry (RMVSVRAUTE) 314
 - Restore Authority (RSTAUT)
 - audit journal (QAUDJRN) entry 277
 - description 312
 - procedure 252
 - role in restoring security 245
 - using 251
 - Restore Document Library Object (RSTDLO) 245
 - Restore Library (RSTLIB) 245
 - Restore Licensed Program (RSTLICPGM)
 - recommendations 253
 - security risks 253
 - Restore Object (RSTOBJ)
 - using 245
 - Restore User Profiles (RSTUSRPRF) 245, 312
 - Retrieve Authorization List Entry (RTVAUTLE) 309
 - Retrieve User Profile (RTVUSRPRF) 128, 311
 - Revoke Object Authority (RVKOBJAUT) 169, 310
 - Revoke Public Authority (RVKPUBAUT)
 - description 316
 - Revoke User Permission (RVKUSRPMN) 313
 - RMVAUTLE (Remove Authorization List Entry) 167, 309
 - RMVDIRE (Remove Directory Entry) 314
 - RMVDLOAUT (Remove Document Library Object Authority) 313
- command, CL (*continued*)
 - RMVLIBLE (Remove Library List Entry) 207
 - RMVSVRAUTE (Remove Server Authentication Entry) 314
 - RSTAUT (Restore Authority)
 - audit journal (QAUDJRN) entry 277
 - description 312
 - procedure 252
 - role in restoring security 245
 - using 251
 - RSTDLO (Restore Document Library Object) 245
 - RSTLIB (Restore Library) 245
 - RSTLICPGM (Restore Licensed Program)
 - recommendations 253
 - security risks 253
 - RSTOBJ (Restore Object)
 - using 245
 - RSTUSRPRF (Restore User Profiles) 245, 312
 - RTVAUTLE (Retrieve Authorization List Entry) 309
 - RTVUSRPRF (Retrieve User Profile) 128, 311
 - RVKOBJAUT (Revoke Object Authority) 169, 310
 - RVKPUBAUT (Revoke Public Authority)
 - description 316, 715
 - details 718
 - RVKUSRPMN (Revoke User Permission) 313
 - SAVDLO (Save Document Library Object) 245
 - Save Document Library Object (SAVDLO) 245
 - Save Library (SAVLIB) 245
 - Save Object (SAVOBJ) 245, 294
 - Save Security Data (SAVSECDDTA) 245, 312
 - Save System (SAVSYS) 245, 312
 - SAVLIB (Save Library) 245
 - SAVOBJ (Save Object) 245, 294
 - SAVSECDDTA (Save Security Data) 245, 312
 - SAVSYS (Save System) 245, 312
 - SBMJOB (Submit Job) 200
 - SECBATCH menu 710
 - security tools 315, 707
 - security, list 309
 - Send Journal Entry (SNDJRNE) 292
 - Send Network Spooled File (SNDNETSPLF) 211
 - Set Attention Program (SETATNPGM) 104
 - SETATNPGM (Set Attention Program) 104
 - setting QALWUSRDMN (allow user objects) system value 26
 - SNDJRNE (Send Journal Entry) 292
 - SNDNETSPLF (Send Network Spooled File) 211

- command, CL (*continued*)
 - Start System/36 (STRS36)
 - user profile, special environment 89
 - STRS36 (Start System/36)
 - user profile, special environment 89
 - Submit Job (SBMJOB) 200
 - system distribution directory, table 314
 - TFRCTL (Transfer Control)
 - transferring adopted authority 150
 - TFRGRPJOB (Transfer to Group Job)
 - adopted authority 150
 - Transfer Control (TFRCTL)
 - transferring adopted authority 150
 - Transfer to Group Job (TFRGRPJOB)
 - adopted authority 150
 - user profiles (related), table 312
 - user profiles (working with), table 311
 - Work with Authorization Lists (WRKAUTL) 309
 - Work with Directory (WRKDIRE) 314
 - Work with Journal (WRKJRN) 294, 301
 - Work with Journal Attributes (WRKJRNA) 294, 301
 - Work with Objects (WRKOBJ) 310
 - Work with Objects by Owner (WRKOBJOWN)
 - auditing 261
 - description 310
 - using 163
 - Work with Objects by Primary Group (WRKOBJPGP) 144, 164
 - description 310
 - Work with Output Queue Description (WRKOUTQD) 211
 - Work with Spooled Files (WRKSPLF) 211
 - Work with System Status (WRKSYSSTS) 218
 - Work with System Values (WRKSYSVAL) 258
 - Work with User Profiles (WRKUSRPRF) 117, 311
 - WRKAUTL (Work with Authorization Lists) 309
 - WRKDIRE (Work with Directory) 314
 - WRKJRN (Work with Journal) 294, 301
 - WRKJRNA (Work with Journal Attributes) 294, 301
 - WRKOBJ (Work with Objects) 310
 - WRKOBJOWN (Work with Objects by Owner)
 - auditing 261
 - description 310
 - using 163
 - WRKOBJPGP (Work with Objects by Primary Group) 144, 164
 - description 310

- command, CL (*continued*)
 - WRKOUTQD (Work with Output Queue Description) 211
 - WRKSPLF (Work with Spooled Files) 211
 - WRKSYSSTS (Work with System Status) 218
 - WRKSYSVAL (Work with System Values) 258
 - WRKUSRPRF (Work with User Profiles) 117, 311
- command, generic
 - Change Authority (CHGAUT) 159
 - Change Owner (CHGOWN) 163
 - Change Primary Group (CHGPGP) 164
 - CHGAUT (Change Authority) 159
 - CHGOWN (Change Owner) 163
 - CHGPGP (Change Primary Group) 164
 - Grant Object Authority (GRTOBJAUT) 159
 - GRTOBJAUT (Grant Object Authority) 159
 - Revoke Object Authority (RVKOBJAUT) 159
 - RVKOBJAUT (Revoke Object Authority) 159
 - Work with Authority (WRKAUT) 159
 - WRKAUT (Work with Authority) 159
- command, generic object
 - Change Auditing (CHGAUD) 310
 - description 313
 - Change Authority (CHGAUT) 310
 - Change Owner (CHGOWN) 310
 - Change Primary Group (CHGPGP) 310
 - CHGAUD (Change Auditing) 310
 - description 313
 - CHGAUT (Change Authority) 310
 - CHGOWN (Change Owner) 310
 - CHGPGP (Change Primary Group) 310
 - Display Authority (DSPAUT) 310
 - DSPAUT (Display Authority) 310
 - Work with Authority (WRKAUT) 310
 - WRKAUT (Work with Authority) 310
- command, integrated file system
 - Change Auditing (CHGAUD)
 - using 127
 - CHGAUD (Change Auditing)
 - using 127
- commands
 - Application development 353
 - COMMIT (Commit) command
 - object authority required 362
 - commitment control
 - object authority required for commands 362
 - Common Criteria security
 - description 6
- communications
 - monitoring 262

- communications entry
 - job description 206
- communications side information
 - object authority required for commands 362
- communications side information (*CSI)
 - auditing 509
- comparison
 - group profile and authorization list 241
- complete change of password 53
- complex
 - authority
 - example 195
- confidential data
 - protecting 261
- confidentiality 1
- configuration
 - automatic
 - virtual devices (QAUTOVRT system value) 37
 - object authority required for commands 363
- configuration list
 - object authority required for commands 364
- configuration list object auditing 505
- Configure System Security (CFGSYSSEC)
 - command
 - description 316, 715
- connection
 - ending
 - audit journal (QAUDJRN) entry 273
 - starting
 - audit journal (QAUDJRN) entry 273
- connection list
 - object authority required for commands 364
- connection list (*CNL) auditing 508
- connection start and end (VC) file
 - layout 681
- connection start or end (VC) journal entry
 - type 273
- connection verification (CV) file
 - layout 591
- console
 - authority needed to sign on 203
 - QCONSOLE system value 203
 - QSECOFR (security officer) user profile 203
 - QSRV (service) user profile 203
 - QSRVBAS (basic service) user profile 203
 - restricting access 258
- contents
 - security tools 315, 707
- controller description
 - object authority required for commands 365
 - printing security-relevant parameters 711
- controller description (*CTLD)
 - auditing 510

controlling
 access
 DDM request (DDM) 216
 iSeries Access 215
 objects 15
 system programs 15
 auditing 66
 remote
 job submission 214
 sign-on (QRMTSIGN system value) 32
 restore operations 216
 save operations 216
 user library list 226

Convert Performance Collection (CVTPFRCOL) command
 authorized IBM-supplied user profiles 331
 object authority required 458

converting
 performance collection
 authorized IBM-supplied user profiles 331
 object authority required 458

Copy Performance Collection (CPYPFRCOL) command
 authorized IBM-supplied user profiles 330
 object authority required 457

Copy Spooled File (CPYSPLF) command 211

Copy User display 121

copying
 performance collection
 authorized IBM-supplied user profiles 330
 object authority required 457
 spooled file 211
 user authority
 command description 311
 example 121
 recommendations 165
 renaming profile 127
 user profile 119

country or region identifier
 QCNTYID system value 106

country region identifier
 CNTRYID user profile parameter 105

CP (user profile change) file layout 586

CP (user profile change) journal entry type 277

CPHDTA (Cipher Data) command
 authorized IBM-supplied user profiles 330

CPROBJ (Compress Object) command
 object auditing 501
 object authority required 344

CPY (Copy Object) command
 object auditing 512

CPY (Copy) command
 object auditing 513, 555, 556, 557, 558
 object authority required 395

CPYAUDJRNE command
 object authority required 418

CPYCFGL (Copy Configuration List) command
 object auditing 505
 object authority required 364

CPYCNARA (Copy Functional Area) command
 object authority required 456

CPYDOC (Copy Document) command
 object auditing 516, 517
 object authority required 375

CPYF (Copy File) command
 object auditing 522, 524
 object authority required 383

CPYFCNARA command
 authorized IBM-supplied user profiles 330

CPYFRMDIR (Copy from Directory) command
 object authority required 371

CPYFRMDKT (Copy from Diskette) command
 object authority required 383

CPYFRMIMPF (Copy from Import File) command
 object authority required 383

CPYFRMLDIF (Copy From LDIF) command
 object authority required 372

CPYFRMLDIF command
 authorized IBM-supplied user profiles 330

CPYFRMQRYF (Copy from Query File) command
 object authority required 383

CPYFRMSTMF (Copy from Stream File) command
 object authority required 383

CPYFRMTAP (Copy from Tape) command
 object authority required 383

CPYGPHFMT
 authorized IBM-supplied user profiles 330

CPYGPHFMT (Copy Graph Format) command
 object authority required 457

CPYGPHPKG
 authorized IBM-supplied user profiles 330

CPYGPHPKG (Copy Graph Package) command
 object authority required 457

CPYIGCSRT (Copy DBCS Sort Table) command
 object auditing 528

CPYIGCTBL (Copy DBCS Font Table) command
 object auditing 528
 object authority required 380

CPYLIB (Copy Library) command
 object authority required 431

CPYOPT (Copy Optical) command
 object authority required 451

CPYPFRCOL (Copy Performance Collection) command
 authorized IBM-supplied user profiles 330

CPYPFRCOL (Copy Performance Collection) command (*continued*)
 object authority required 457

CPYPFRTA
 authorized IBM-supplied user profiles 330

CPYPFRTA (Copy Performance Data) command
 object authority required 457

CPYPTF (Copy Program Temporary Fix) command
 authorized IBM-supplied user profiles 330
 object authority required 475

CPYPTFGRP (Copy Program Temporary Fix Group) 330

CPYPTFGRP (Copy PTF Group) command
 object authority required 475

CPYSPLF (Copy Spooled File) command
 action auditing 552
 DSPDATA parameter of output queue 211
 object auditing 541
 object authority required 481

CPYSRCF (Copy Source File) command
 object authority required 383

CPYTCPHT command
 object authority required 489

CPYTODIR (Copy to Directory) command
 object authority required 371

CPYTODKT (Copy to Diskette) command
 object authority required 384

CPYTOIMPF (Copy to Import File) command
 object authority required 384

CPYTOLDIF (Copy To LDIF) command
 object authority required 372

CPYTOLDIF command 330

CPYTOSTMF (Copy to Stream File) command
 object authority required 384

CPYTOTAP (Copy to Tape) command
 object authority required 384

CQ (*CRQD change) file layout 589

CQ (change *CRQD object) journal entry type 277

create (*CREATE) audit level 272

create authority (CRTAUT) parameter
 description 139
 displaying 158
 risks 140

create authority (QCRTAUT) system value
 description 26
 risk of changing 26
 using 139

Create Authority Holder (CRTAUTHLR) command 153, 309, 314

Create Authorization List (CRAUTL) command 166, 309

Create Command (CRTCMD) command
 ALWLMTUSR (allow limited user) parameter 83
 PRDLIB (product library) parameter 210

Create Command (CRTCMD) command
(continued)
security risks 210

Create Journal (CRTJRN) command 291

Create Journal Receiver (CRTJRNRCV) command 291

Create Library (CRTLIB) command 157

Create Menu (CRTMNU) command
PRDLIB (product library)
parameter 210
security risks 210

create object (CO) file layout 584

create object (CO) journal entry
type 144, 272

create object auditing (CRTOBJAUD)
value 71

create object auditing (QCRTOBJAUD)
system value
overview 71

Create Output Queue (CRTOUQ)
command 211, 214

Create User Profile (CRTUSRPRF)
command
description 311
using 118

Create User Profile display 117

Create Validation Lists (CRTVLDL) 243
creating
audit journal 291
audit journal receiver 291
authority holder 153, 309, 314
authorization list 166, 309
command
ALWLMTUSR (allow limited user)
parameter 83
PRDLIB (product library)
parameter 210
security risks 210
library 157
menu
PRDLIB (product library)
parameter 210
security risks 210
object
audit journal (QAUDJRN)
entry 144, 272
output queue 211, 214
program
adopted authority 151
user profile
audit journal (QAUDJRN)
entry 277
command descriptions 311
example 118
methods 117
creating object
object auditing 500
cross system product map (*CSPMAP)
auditing 509
cross system product table (*CSPTBL)
auditing 510

CRTADMDMN command
authorized IBM-supplied user
profiles 330

CRTALRTBL (Create Alert Table)
command
object authority required 352

CRTAUT (create authority) parameter
description 139
displaying 158
risks 140

CRTAUTHLR (Create Authority Holder)
command
authorized IBM-supplied user
profiles 330
considerations 153
description 309, 314
object authority required 354

CRTAUTL (Create Authorization List)
command
description 309
object authority required 354
using 166

CRTBESTMDL (Create Best/1-400 Model)
command
object authority required 457

CRTBNDC (Create Bound C Program)
command
object authority required 424

CRTBNDCBL (Create Bound COBOL
Program) command
object authority required 424

CRTBNDCCL
object authority required 424

CRTBNDCPP (Create Bound CPP
Program) command
object authority required 425

CRTBNDDIR (Create Binding Directory)
command
object authority required 355

CRTBNDRPG (Create Bound RPG
Program) command
object authority required 425

CRTBSCF (Create Bisync File) command
object auditing 522

CRTCAD command
authorized IBM-supplied user
profiles 330
object authority required 358

CRTCBMOD (Create COBOL Module)
command
object authority required 425

CRTCBPLPGM (Create COBOL Program)
command
object authority required 426

CRTCFGL (Create Configuration List)
command
object authority required 364

CRTCKMKSF command
object authority required 367

CRTCLD (Create C Locale Description)
command
object authority required 425

CRTCLMOD
object authority required 425

CRTCLPGM (Create Control Language
Program) command
object authority required 426

CRTCLS (Create Class) command
authorized IBM-supplied user
profiles 330
object authority required 356

CRTCLU
authorized IBM-supplied user
profiles 330

CRTCLU command
object authority required 358

CRTCMD (Create Command) command
ALWLMTUSR (allow limited user)
parameter 83
object authority required 361
PRDLIB (product library)
parameter 210
security risks 210

CRTCMNF (Create Communications File)
command
object auditing 522

CRTCMOD (Create C Module) command
object authority required 426

CRTCOSD (Create Class-of-Service
Description) command
object authority required 356

CRTCPPMOD (Create Bound CPP
Module) command
object authority required 426

CRTCRG
authorized IBM-supplied user
profiles 330

CRTCRQD (Create Change Request
Description) command
object authority required 355

CRTCSI (Create Communications Side
Information) command
object authority required 362

CRTCTLAPPC (Create Controller
Description (APPC)) command
object authority required 365

CRTCTLASC (Create Controller
Description (Async)) command
object authority required 365

CRTCTLBSC (Create Controller
Description (BSC)) command
object authority required 365

CRTCTLFNC (Create Controller
Description (Finance)) command
object authority required 365

CRTCTLHOST (Create Controller
Description (SNA Host)) command
object authority required 366

CRTCTLLWS (Create Controller
Description (Local Workstation))
command
object authority required 366

CRTCTLNET (Create Controller
Description (Network)) command
object authority required 366

CRTCTLRTL (Create Controller
Description (Retail)) command
object authority required 366

CRTCTLRWS (Create Controller
Description (Remote Workstation))
command
object authority required 366

CRTCTLTAP (Create Controller
Description (Tape)) command
object authority required 366

CRTCTLVWS (Create Controller Description (Virtual Workstation)) command
 object authority required 366
 CRTDDMF (Create Distributed Data Management File) command
 object authority required 384
 CRTDEVAPPC (Create Device Description (APPC)) command
 object authority required 369
 CRTDEVASC (Create Device Description (Async)) command
 object authority required 369
 CRTDEVASP (Create Device Description for Auxiliary Storage Pool) command
 object authority required 369
 CRTDEVBSC (Create Device Description (BSC)) command
 object authority required 369
 CRTDEVDSP (Create Device Description (Display)) command
 object authority required 369
 CRTDEVFNC (Create Device Description (Finance)) command
 object authority required 369
 CRTDEVHOST (Create Device Description (SNA Host)) command
 object authority required 369
 CRTDEVINTR (Create Device Description (Intrasystem)) command
 object authority required 369
 CRTDEVMLB command
 object authority required 369
 CRTDEVNET (Create Device Description (Network)) command
 object authority required 369
 CRTDEVNWSH command
 object authority required 369
 CRTDEVOPT (Create Device Description (Optical)) command
 object authority required 369
 CRTDEVOPT (Create Device Description (Optical)) command
 object authority required 452
 CRTDEVPRT (Create Device Description (Printer)) command
 object authority required 369
 CRTDEVRIL (Create Device Description (Retail)) command
 object authority required 369
 CRTDEVSNPT (Create Device Description (SNPT)) command
 object authority required 369
 CRTDEVSNUF (Create Device Description (SNUF)) command
 object authority required 369
 CRTDEVTAP (Create Device Description (Tape)) command
 object authority required 369
 CRTDIR (Create Directory) command
 object auditing 513
 CRTDKTF (Create Diskette File) command
 object authority required 384
 CRTDOC (Create Document) command
 object authority required 375
 CRTDSPF (Create Display File) command
 object auditing 522
 object authority required 384
 CRTDSTL (Create Distribution List) command
 object authority required 374
 CRTDTAARA (Create Data Area) command
 object authority required 367
 CRTDTADCT (Create a Data Dictionary) command
 object authority required 410
 CRTDTAQ (Create Data Queue) command
 object authority required 368
 CRTDUPOBJ (Create Duplicate Object) command
 object auditing 499
 object authority required 344
 CRTEDTD (Create Edit Description) command
 object authority required 380
 CRTFCNARA
 authorized IBM-supplied user profiles 330
 CRTFCNARA (Create Functional Area) command
 object authority required 457
 CRTFCT (Create Forms Control Table) command
 object authority required 472
 CRTFLR (Create Folder) command
 object auditing 517
 object authority required 375
 CRTFNTRSC (Create Font Resources) command
 object authority required 351
 CRTFNNTBL (Create DBCS Font Table) command
 object authority required for commands 351
 CRTFORMDF (Create Form Definition) command
 object authority required 351
 CRTFTR (Create Filter) command
 object authority required 388
 CRTGDF (Create Graphics Data File) command
 object auditing 505
 CRTGPHFMT
 authorized IBM-supplied user profiles 330
 CRTGPHPKG
 authorized IBM-supplied user profiles 330
 CRTGPHPKG (Create Graph Package) command
 object authority required 457
 CRTGSS (Create Graphics Symbol Set) command
 object authority required 390
 CRTHSTDTA
 authorized IBM-supplied user profiles 330
 CRTHSTDTA (Create Historical Data) command
 object authority required 457
 CRTICFF (Create ICF File) command
 object auditing 522
 CRTICFF (Create Intersystem Communications Function File) command
 object authority required 385
 CRTIGCDCT (Create DBCS Conversion Dictionary) command
 object authority required 380
 CRTIMGCLG command
 object authority required 391
 CRTJOB (Create Job Description) command
 authorized IBM-supplied user profiles 330
 object authority required 415
 CRTJOBQ (Create Job Queue) command
 object authority required 416
 CRTJRN (Create Journal) command
 creating audit (QAUDJRN) journal 291
 object authority required 418
 CRTJRNRCV (Create Journal Receiver) command
 creating audit (QAUDJRN) journal receiver 291
 object authority required 421
 CRTLASREP (Create Local Abstract Syntax) command
 authorized IBM-supplied user profiles 330
 CRTLF (Create Logical File) command
 object auditing 522, 559
 object authority required 385
 CRTLIB (Create Library) command 157
 object authority required 431
 CRTLINASC (Create Line Description (Async)) command
 object authority required 436
 CRTLINBSC (Create Line Description (BSC)) command
 object authority required 436
 CRTLINDDI (Create Line Description (DDI Network)) command
 object authority required 436
 CRTLINETH (Create Line Description (Ethernet)) command
 object authority required 436
 CRTLINFAX (Create Line Description (FAX)) command
 object authority required 436
 CRTLINFR (Create Line Description (Frame Relay Network)) command
 object authority required 436
 CRTLINS DLC (Create Line Description (SDLC)) command
 object authority required 436
 CRTLINTDLC (Create Line Description (TDLC)) command
 object authority required 436
 CRTLINTRN (Create Line Description (Token-Ring Network)) command
 object authority required 436
 CRTLINWLS (Create Line Description (Wireless)) command
 object authority required 437

CRTLINX25 (Create Line Description (X.25)) command
 object authority required 437
 CRTLOCALE (Create Locale) command
 object authority required 437
 CRTMNU (Create Menu) command
 object authority required 439
 PRDLIB (product library)
 parameter 210
 security risks 210
 CRTMODD (Create Mode Description) command
 object authority required 442
 CRTMSDF (Create Mixed Device File) command
 object auditing 522
 CRTMSGF (Create Message File) command
 object authority required 441
 CRTMSGFMNU (Create Message File Menu) command
 object authority required 486
 CRTMSGQ (Create Message Queue) command
 object authority required 441
 CRTNODL (Create Node List) command
 object authority required 449
 CRTNTBD (Create NetBIOS Description) command
 object authority required 443
 CRTNWIFR (Create Network Interface Description (Frame Relay Network)) command
 object authority required 446
 CRTNWSALS (Create Network Server Alias) command
 object authority required 447
 CRTNWSCFG command
 authorized IBM-supplied user profiles 330
 object authority required 448
 CRTNWSD (Create Network Server Description) command
 object authority required 448
 CRTNWSSTG (Create Network Server Storage Space) command
 object authority required 446
 CRTOBJAUD (create object auditing) value 71, 288
 CRTOUTQ (Create Output Queue) command
 examples 214
 object authority required 454
 using 211
 CRTOVL (Create Overlay) command
 object authority required 351
 CRTPAGDFN (Create Page Definition) command
 object authority required 351
 CRTPAGSEG (Create Page Segment) command
 object authority required 351
 CRTPDG (Create Print Descriptor Group) command
 object authority required 461
 CRTPEXDTA (Create Performance Explorer Data) command
 authorized IBM-supplied user profiles 330
 CRTPF (Create Physical File) command
 object auditing 522
 object authority required 385
 CRTPFRTDA
 authorized IBM-supplied user profiles 330
 CRTPFRTDA (Create Performance Data) command
 object authority required 458
 CRTPFERSUM
 authorized IBM-supplied user profiles 330
 CRTPFERSUM command
 object authority required 458
 CRTPGM (Create Program) command
 object auditing 504, 535, 543, 554
 CRTPNLGRP (Create Panel Group) command
 object authority required 439
 CRTPRTF (Create Printer File) command
 object auditing 522
 object authority required 385
 CRTPSFCFG (Create Print Services Facility Configuration) command
 object authority required 461
 CRTQMFFORM (Create Query Management Form) command
 object auditing 545
 object authority required 466
 CRTQMORY (Create Query Management Query) command
 object auditing 546
 CRTQSTDB (Create Question and Answer Database) command
 authorized IBM-supplied user profiles 330
 object authority required 468
 CRTQSTLOD (Create Question-and-Answer Load) command
 authorized IBM-supplied user profiles 330
 object authority required 468
 CRTRJEBSCF (Create RJE BSC File) command
 object authority required 472
 CRTRJECFG (Create RJE Configuration) command
 object authority required 472
 CRTRJECMNF (Create RJE Communications File) command
 object authority required 472
 CRTRNDCCFG (RNDC Configuration Utility) command
 object authority required 379
 CRTRPGMOD (Create RPG Module) command
 object authority required 426
 CRTRPGPGM (Create RPG/400 Program) command
 object authority required 427
 CRTRPTPGM (Create Auto Report Program) command
 object authority required 427
 CRTS36CBL (Create System/36 COBOL) command
 object authority required 427
 CRTS36DSPF (Create System/36 Display File) command
 object authority required 385, 486
 CRTS36MNU (Create System/36 Menu) command
 object authority required 439, 487
 CRTS36MSGF (Create System/36 Message File) command
 object authority required 487
 CRTS36RPG (Create System/36 RPG) command
 object authority required 427
 CRTS36RPGR (Create System/36 RPGR) command
 object authority required 427
 CRTS36RPT (Create System/36 Auto Report) command
 object authority required 427
 CRTSAVF (Create Save File) command
 object authority required 385
 CRTSBSD (Create Subsystem Description) command
 authorized IBM-supplied user profiles 330
 object authority required 484
 CRTSCHIDX (Create Search Index) command
 object authority required 411
 CRTSPADCT (Create Spelling Aid Dictionary) command
 object auditing 552
 object authority required 480
 CRTSQLCBL (Create Structured Query Language COBOL) command
 object authority required 428
 CRTSQLCBLI (Create Structured Query Language ILE COBOL Object) command
 object authority required 428
 CRTSQLCI (Create Structured Query Language ILE C Object) command
 object authority required 427
 CRTSQLCPPI (Create SQL ILE C++ Object) command
 object authority required 428
 CRTSQLFTN (Create Structured Query Language FORTRAN) command
 object authority required 428
 CRTSQLPKG (Create Structured Query Language Package) command
 object authority required 455
 CRTSQLPLI (Create Structured Query Language PL/I) command
 object authority required 429
 CRTSQLRPG (Create Structured Query Language RPG) command
 object authority required 429
 CRTSQLRPGI (Create Structured Query Language ILE RPG Object) command
 object authority required 429
 CRTSRCPF (Create Source Physical File) command
 object authority required 385

CRTSRVPGM (Create Service Program) command
 object auditing 504, 536, 554
 object authority required 463
 CRTSSND (Create Session Description) command
 object authority required 472
 CRTTAPF (Create Tape File) command
 object authority required 386
 CRTTBL (Create Table) command
 object authority required 489
 CRTTIMZON command 491
 CRTUDFS
 authorized IBM-supplied user profiles 330
 CRTUDFS (Create User-Defined File System) command
 authorized IBM-supplied user profiles 330
 object authority required 491
 CRTUSRPRF (Create User Profile) command
 description 311
 object authority required 493
 using 118
 CRTVLDL (Create Validation List) command
 authorized IBM-supplied user profiles 330
 object authority required 495
 CRTWSCST (Create Workstation Customizing Object) command
 object authority required 496
 cryptographic configuration (CY) file layout 593
 cryptography
 object authority required for commands 366
 CU (Cluster Operations) file layout 589
 CURLIB (current library) parameter user profile 81
 current library
 changing
 limit capabilities 81
 methods 207
 recommendations 210
 definition 81
 library list 207, 210
 limit capabilities 81
 recommendations 210
 user profile 81
 current library (CURLIB) parameter user profile 81
 customizing
 security values 715
 CV (connection verification) file layout 591
 CVTBASSTR (Convert BASIC Stream Files) command
 authorized IBM-supplied user profiles 330
 object authority required 442
 CVTBASUNF (Convert BASIC Unformatted Files) command
 authorized IBM-supplied user profiles 331
 object authority required 442

CVTBGUDTA (Convert BGU Data) command
 authorized IBM-supplied user profiles 331
 object authority required 442
 CVTCLSRC (Convert CL Source) command
 object authority required 464
 CVTDIR
 authorized IBM-supplied user profiles 331
 CVTDIR (Convert Directory) command
 object authority required 396
 CVTEDU (Convert Education) command
 object authority required 450
 CVTIPSIFC (Convert IP over SNA Interface) command
 object authority required 352
 CVTIPSLOC (Convert IP over SNA Location Entry) command
 object authority required 352
 CVTOPTBKU (Convert Optical Backup) command
 object authority required 452
 CVTPFCOL (Convert Performance Collection) command
 authorized IBM-supplied user profiles 331
 object authority required 458
 CVTPFRDTA
 authorized IBM-supplied user profiles 331
 CVTPFRDTA (Convert Performance Data) command
 object authority required 458
 CVTPFRTHD
 authorized IBM-supplied user profiles 331
 CVTPFRTHD (Convert Performance Thread Data) command
 object authority required 458
 CVTRJEDTA (Convert RJE Data) command
 object authority required 472
 CVTRPGSRC (Convert RPG Source) command
 object authority required 429
 CVTS36FCT (Convert System/36 Forms Control Table) command
 authorized IBM-supplied user profiles 331
 object authority required 442
 CVTS36JOB (Convert System/36 Job) command
 authorized IBM-supplied user profiles 331
 object authority required 442
 CVTS38JOB (Convert System/38 Job) command
 authorized IBM-supplied user profiles 331
 object authority required 442
 CVTSQLCPP (Convert SQL C++ Source) command
 object authority required 429

CVTTCPCPL (Convert TCP/IP CL) command
 object authority required 489
 CVTTCPCPL (Convert TCP/IP Control Language) command
 authorized IBM-supplied user profiles 331
 CVTTOFLR (Convert to Folder) command
 object auditing 517
 CY(cryptographic configuration) file layout 593

D

damaged audit journal 292
 damaged authorization list recovering 254
 data area
 object authority required for commands 367
 data authority
 definition 132
 data queue
 object authority required for commands 368
 database share (QDBSHR) user profile 321
 DB2LDIF command
 object authority required 372
 DCEADM (QDCEADM) user profile 321
 DCPOBJ (Decompress Object) command
 object auditing 501
 object authority required 344
 DDM (distributed data management) security 216
 DDM request access (DDMACC) network attribute 216
 DDMACC (DDM request access) network attribute 216
 DDMACC (distributed data management access) network attribute 262
 debug functions
 adopted authority 150
 dedicated service tools (DST)
 auditing passwords 258
 changing passwords 129
 changing user ID 129
 resetting password
 audit journal (QAUDJRN) entry 277
 command description 311
 Dedicated Service Tools (DST) users 128
 default 321
 *DFT delivery mode
 user profile 102
 job description (QDFTJOB) 96
 object
 auditing 288
 owner (QDFTOWN) user profile
 audit journal (QAUDJRN) entry 276
 default values 321
 description 145
 restoring programs 253

default (*continued*)

- sign-on
 - security level 40 16
 - subsystem description 205
- value
 - IBM-supplied user profile 319
 - user profile 319

delete (*DELETE) audit level 272

delete (*DLT) authority 132, 340

Delete Authority Holder (DLTAUTHLR)

- command 154, 309, 314

Delete Authorization List (DLTAUTL)

- command 169, 309

Delete Journal Receiver (DLTJRNRVCV)

- command 294

Delete Kerberos Credentials Cache File (DLTKRBCCF) command

- object authority required 423

delete operation (DO) file layout 601

delete operation (DO) journal entry type 272

Delete Performance Collection (DLTPFCOL) command

- authorized IBM-supplied user profiles 331
- object authority required 458

Delete User Profile (DLTUSRPRF)

- command
 - description 311
 - example 122
 - object ownership 143

Delete User Profile display 122

Delete Validation Lists (DLTVLDDL) 243

deleting

- audit journal receiver 294
- authority for user 161
- authority holder 154, 309
- authorization list 169, 309
- object
 - audit journal (QAUDJRN) entry 272
- object owner profile 143
- performance collection
 - authorized IBM-supplied user profiles 331
 - object authority required 458
- user profile
 - command description 311
 - directory entry 122
 - distribution lists 122
 - message queue 122
 - owned objects 122
 - primary group 122
 - spooled files 124
 - user's authority 161

deleting object

- object auditing 500

delivery (DLVRY) parameter

- user profile 102

describing

- library security requirements 228
- menu security 230

description (TEXT) parameter

- user profile 84

descriptor

- giving
 - audit journal (QAUDJRN) entry 281

designing

- libraries 225
- security 219

detaching

- audit journal receiver 293, 294
- journal receiver 293

DEV (print device) parameter

- user profile 103

development commands

- Application 353

device

- authority to sign-on 201
- securing 201
- virtual
 - automatic configuration (QAUTOVRT system value) 37
 - definition 37

device description

- authority to use 201
- creating
 - public authority 140
 - QCRTAUT (create authority) system value 140
- definition 201
- object authority required for commands 368
- ownership
 - changing 203
 - default owner 203
 - owned by QPGMR (programmer) profile 203
 - owned by QSECOFR (security officer) user profile 203
- printing security-relevant parameters 711
- securing 201

device description (*DEVVD) auditing 511

device recovery action (QDEVRCYACN)

- system value 38
- value set by CFGSYSSEC command 716

device session

- limiting
 - LMTDEVSSN user profile parameter 93
 - QLMTDEVSSN system value 29

DI (Directory Server) file layout 596

digital ID

- if private authorization is not found. 116

directory

- authority 5
 - new objects 140
- object authority required for commands 357, 371, 390, 392
- security 138
- working with 314

directory (*DIR) auditing 512

directory entry

- adding 314
- changing 314
- deleting user profile 122
- removing 314

directory server

- auditing 514
- object authority required for commands 371

directory server (DI) file layout 596

directory, system distribution

- commands for working with 314

disabled (*DISABLED) user profile status

- description 78
- QSECOFR (security officer) user profile 78

disabling

- audit function 295
- security level 40 19
- security level 50 21
- user profile 78
 - automatically 707

disconnected job time-out interval (QDSCJOBITV) system value 38

- value set by CFGSYSSEC command 716

disk

- limiting use (MAXSTG) parameter 94

diskette

- object authority required for commands 438

Display Activation Schedule (DSPACTSCD) command

- description 707

Display Audit Journal Entries (DSPAUDJRNE) command

- description 315, 711

Display Authority (DSPAUT)

- command 310

Display Authority Holder (DSPAUTHLR)

- command 153, 309

Display Authorization List (DSPAUTL)

- command 309

Display Authorization List display

- displaying detail (*EXPERT user option) 106, 107, 108

Display Authorization List Document Library Objects (DSPAUTLDLO)

- command 313

Display Authorization List Objects (DSPAUTLOBJ) command 168, 309

Display Authorized Users (DSPAUTUSR)

- command
 - auditing 301
 - description 311
 - example 125

Display Authorized Users (DSPAUTUSR)

- display 125, 301

Display Document Library Object Auditing (DSPDLAUD)

- command 313
- using 288

Display Document Library Object Authority (DSPDLAOUT)

- command 313

Display Expiration Schedule (DSPEXPSCD) command

- description 707

Display Job Description (DSPJOBDD)

- command 261

Display Journal (DSPJRN) command
 audit (QAUDJRN) journal
 example 295
 auditing file activity 236, 300
 creating output file 296
 displaying QAUDJRN (audit) journal 263

Display Kerberos Credentials Cache File (DSPKRBCCF) command
 object authority required 423

Display Kerberos Keytab Entries (DSPKRBKTE) command
 object authority required 423

Display Library (DSPLIB) command 303

Display Library Description (DSPLIBD) command
 CRTAUT parameter 158

Display Object Authority (DSPOBJAUT) command 303, 310

Display Object Authority display
 displaying detail (*EXPERT user option) 106, 107, 108
 example 157, 159

Display Object Description (DSPOBJD) command 310
 created by 144
 object domain 15
 program state 15
 using 288
 using output file 302

Display Program (DSPPGM) command
 adopted authority 151
 program state 15

Display Programs That Adopt (DSPPGMADP) command
 auditing 303
 description 312
 using 151, 236

Display Security Auditing (DSPSECAUD) command
 description 709

Display Security Auditing Values (DSPSECAUD) command
 description 315

display service function
 *SERVICE (service) special authority 87

Display Service Program (DSPSRVPGM) command
 adopted authority 151

display sign-on information (QDSPSGNINF) system value
 value set by CFGSYSSEC command 716

Display Spooled File (DSPSPLF) command 211

display station pass-through
 object authority required for commands 372
 target profile change
 audit journal (QAUDJRN) entry 281

Display User Profile (DSPUSRPRF) command
 description 311
 using 125
 using output file 302

displaying
 adopted authority
 command description 312
 critical files 236
 programs that adopt a profile 151
 USRPRF parameter 151

all user profiles 125

audit (QAUDJRN) journal
 entries 263, 295

audit journal entries 315

authority 154, 310

authority holders 153
 command description 309

authorization list
 document library objects (DLO) 313
 users 309

authorization list objects 168, 309

authorized users 301, 311

CRTAUT (create authority) parameter 158

document library object
 authority 313

job description 261

journal
 auditing file activity 236, 300

object
 originator 144
 object auditing 288
 object authority 303, 310
 object description 310
 object domain 15
 path name 164
 program adopt 151
 program state 15
 Display Program (DSPPGM) command 15
 programs that adopt 151, 303

QAUDCTL (audit control) system value 315, 709

QAUDLVL (audit level) system value 315, 709

security auditing 315, 709

sign-on information
 DSPSGNINF user profile parameter 91
 QDSPSGNINF system value 26

recommendations 91

spooled file 211

user profile
 activation schedule 707
 active profile list 707
 command description 311
 expiration schedule 707
 individual 125
 summary list 125

distributed data management access (DDMACC) network attribute 262

distributed systems node executive (QDSNX) user profile 321

distribution
 object authority required for commands 373

distribution directory
 changing
 audit journal (QAUDJRN) entry 275

distribution directory, system
 commands for working with 314

distribution list
 deleting user profile 122
 object authority required for commands 374

DLCOBJ (Deallocate Object) command
 object auditing 501
 object authority required 344

DLO (document library object) authority
 command descriptions 313

DLTADMDMN command
 authorized IBM-supplied user profiles 331

DLTALR (Delete Alert) command
 object authority required 352

DLTALRTBL (Delete Alert Table) command
 object authority required 352

DLTAPARDTA (Delete APAR Data) command
 authorized IBM-supplied user profiles 331
 object authority required 475

DLTAUTHLR (Delete Authority Holder) command
 description 309, 314
 object authority required 354
 using 154

DLTAUTL (Delete Authorization List) command
 description 309
 object authority required 354
 using 169

DLTBESTMDL (Delete BEST/1 Model) command
 authorized IBM-supplied user profiles 331

DLTBESTMDL (Delete Best/1-400 Model) command
 object authority required 458

DLTBNDDIR (Delete Binding Directory) command
 object authority required 355

DLTCAD
 authorized IBM-supplied user profiles 331

DLTCAD command
 object authority required 359

DLTCFGL (Delete Configuration List) command
 object authority required 364

DLTCHTFMT (Delete Chart Format) command
 object authority required 356

DLTCLD (Delete C Locale Description) command
 object authority required 430

DLTCLS (Delete Class) command
 object authority required 356

DLTCLU
 authorized IBM-supplied user profiles 331

DLTCLU command
 object authority required 359

DLTCMD (Delete Command) command
 object authority required 361

DLTCMNTRC (Delete Communications Trace) command
 authorized IBM-supplied user profiles 331
 object authority required 475

DLTCNNL (Delete Connection List) command
 object authority required 364

DLTCOSD (Delete Class-of Service Description) command
 object authority required 356

DLTCRGCLU
 authorized IBM-supplied user profiles 331

DLTCRQD (Delete Change Request Description) command
 object authority required 355

DLTCSI (Delete Communications Side Information) command
 object authority required 362

DLTCTLD (Delete Controller Description) command
 object authority required 366

DLTDEVD (Delete Device Description) command
 object auditing 559
 object authority required 369

DLTDFUPGM (Delete DFU Program) command
 object authority required 464

DLTDLO (Delete Document Library Object) command
 object auditing 517
 object authority required 375

DLTDOCL (Delete Document List) command
 object auditing 517
 object authority required 375

DLTDST (Delete Distribution) command
 object auditing 517
 object authority required 373

DLTDSTL (Delete Distribution List) command
 object authority required 374

DLTDTAARA (Delete Data Area) command
 object authority required 367

DLTDTADCT (Delete Data Dictionary) command
 object authority required 410

DLTDTAQ (Delete Data Queue) command
 object authority required 368

DLTEDTD (Delete Edit Description) command
 object authority required 380

DLTEXPSPLF
 authorized IBM-supplied user profiles 331

DLTF (Delete File) command
 object authority required 386

DLTFCNARA
 authorized IBM-supplied user profiles 331

DLTFCNARA (Delete Functional Area) command
 object authority required 458

DLTFCT (Delete Forms Control Table) command
 object authority required 473

DLTFNTRSC (Delete Font Resources) command
 object authority required 351

DLTFNTTBL (Delete DBCS Font Table) object authority required for commands 351

DLTFORMDF (Delete Form Definition) command
 object authority required 351

DLTFTR (Delete Filter) command
 object authority required 388

DLTGPHFMT
 authorized IBM-supplied user profiles 331

DLTGPHFMT (Delete Graph Format) command
 object authority required 458

DLTGPHPKG
 authorized IBM-supplied user profiles 331

DLTGPHPKG (Delete Graph Package) command
 object authority required 458

DLTGSS (Delete Graphics Symbol Set) command
 object authority required 390

DLTHSTDTA
 authorized IBM-supplied user profiles 331

DLTHSTDTA (Delete Historical Data) command
 object authority required 458

DLTIGCDCT (Delete DBCS Conversion Dictionary) command
 object authority required 380

DLTIGCSRT (Delete IGC Sort) command
 object authority required 380

DLTIGCTBL (Delete DBCS Font Table) command
 object authority required 380

DLTIMGCLG command
 object authority required 391

DLTINTSVR command
 authorized IBM-supplied user profiles 331

DLTIPXD command 411

DLTJOB (Delete Job Description) command
 object authority required 415

DLTJOBQ (Delete Job Queue) command
 object authority required 416

DLTJRN (Delete Journal) command
 object authority required 418

DLTJRNRCV (Delete Journal Receiver) command
 object authority required 421
 stopping auditing function 294

DLTLIB (Delete Library) command
 object authority required 431

DLTLICPGM (Delete Licensed Program) command
 authorized IBM-supplied user profiles 331
 object authority required 435

DLTLIND (Delete Line Description) command
 object authority required 437

DLTLOCALE (Create Locale) command
 object authority required 437

DLTMNU (Delete Menu) command
 object authority required 439

DLTMOD (Delete Module) command
 object authority required 443

DLTMODD (Delete Mode Description) command
 object authority required 442

DLTMSGF (Delete Message File) command
 object authority required 441

DLTMSGQ (Delete Message Queue) command
 object authority required 441

DLTNETF (Delete Network File) command
 object authority required 444

DLTNODL (Delete Node List) command
 object authority required 449

DLTNTBD (Delete NetBIOS Description) command
 object authority required 444

DLTNWID (Delete Network Interface Description) command
 object authority required 446

DLTNWSALS (Delete Network Server Alias) command
 object authority required 447

DLTNWSCFG command
 authorized IBM-supplied user profiles 331
 object authority required 448

DLTNWSD (Delete Network Server Description) command
 object authority required 448

DLTNWSSTG (Delete Network Server Storage Space) command
 object authority required 446

DLTOBJ (Delete Object) command
 object authority required 344

DLTOUTQ (Delete Output Queue) command
 object authority required 454

DLTOVL (Delete Overlay) command
 object authority required 351

DLTPAGDFN (Delete Page Definition) command
 object authority required 351

DLTPAGSEG (Delete Page Segment) command
 object authority required 351

DLTPDG (Delete Print Descriptor Group) command
 object authority required 461

DLTPEXDTA
 authorized IBM-supplied user profiles 331

DLTPEXDTA (Delete Performance Explorer Data) command
 object authority required 458

DLTPFRCOL (Delete Performance Collection) command
 authorized IBM-supplied user profiles 331
 object authority required 458

DLTPFRDTA
 authorized IBM-supplied user profiles 331

DLTPFRDTA (Delete Performance Data) command
 object authority required 458

DLTPGM (Delete Program) command
 object authority required 464

DLTPNLGRP (Delete Panel Group) command
 object authority required 439

DLTPRB (Delete Problem) command
 authorized IBM-supplied user profiles 331
 object authority required 462

DLTPSFCEG (Delete Print Services Facility Configuration) command
 object authority required 461

DLTPTF (Delete PTF) command
 authorized IBM-supplied user profiles 331
 object authority required 476

DLTQMFORM (Delete Query Management Form) command
 object authority required 467

DLTQMQRV (Delete Query Management Query) command
 object authority required 467

DLTQRY (Delete Query) command
 object auditing 547
 object authority required 467

DLTQST (Delete Question) command
 authorized IBM-supplied user profiles 331
 object authority required 468

DLTQSTDB (Delete Question-and-Answer Database) command
 authorized IBM-supplied user profiles 331
 object authority required 468

DLTRJECFG (Delete RJE Configuration) command
 object authority required 473

DLTRMTPTF (Delete Remote PTF) command
 authorized IBM-supplied user profiles 331

DLTSBSD (Delete Subsystem Description) command
 object authority required 484

DLTSCHIDX (Delete Search Index) command
 object authority required 411

DLTSHF (Delete Bookshelf) command
 object auditing 517

DLTSMGOBJ (Delete Systems Management Object) command
 authorized IBM-supplied user profiles 331

DLTSPADCT (Delete Spelling Aid Dictionary) command
 object authority required 480

DLTSPLF (Delete Spooled File) command
 action auditing 553
 object auditing 540
 object authority required 481

DLTSQLPKG (Delete Structured Query Language Package) command
 object authority required 455

DLTSRVPGM (Delete Service Program) command
 object authority required 464

DLTSSND (Delete Session Description) command
 object authority required 473

DLTTBL (Delete Table) command
 object authority required 489

DLTTIMZON command 491

DLTTRC (Delete Trace) command
 object authority required 476

DLTUDFS (Delete User-Defined File System) command
 authorized IBM-supplied user profiles 331
 object authority required 491

DLTUSRIDX (Delete User Index) command
 object authority required 491

DLTUSRPRF (Delete User Profile) command
 description 311
 example 122
 object auditing 560
 object authority required 493
 object ownership 143

DLTUSRQ (Delete User Queue) command
 object authority required 491

DLTUSRSPC (Delete User Space) command
 object authority required 491

DLTUSRTRC (Delete User Trace) command
 object authority required 412

DLTVLDL (Delete Validation List) command
 authorized IBM-supplied user profiles 331
 object authority required 495

DLTWNTSVR command
 authorized IBM-supplied user profiles 331

DLTWSCST (Delete Workstation Customizing Object) command
 object authority required 496

DLVRY (message queue delivery) parameter
 user profile 102

DLYJOB (Delay Job) command
 object authority required 412

DMPCLPGM (Dump CL Program) command
 object auditing 543
 object authority required 464

DMPDLO (Dump Document Library Object) command
 authorized IBM-supplied user profiles 331
 object auditing 516
 object authority required 375

DMPJOB (Dump Job) command
 authorized IBM-supplied user profiles 331
 object authority required 476

DMPJOBINT (Dump Job Internal) command
 authorized IBM-supplied user profiles 332
 object authority required 476

DMPJVM
 authorized IBM-supplied user profiles 332

DMPMEMINF
 authorized IBM-supplied user profiles 332

DMPOBJ (Dump Object) command
 authorized IBM-supplied user profiles 332
 object auditing 499
 object authority required 344

DMPYSOJB (Dump System Object) command
 authorized IBM-supplied user profiles 332
 object auditing 499
 object authority required 344

DMPUSRPRF (Dump User Profile) command
 authorized IBM-supplied user profiles 332
 object auditing 499
 object authority required 344

DMPUSRTRC (Dump User Trace) command
 object authority required 438

DMPTRC (Dump Trace) command
 authorized IBM-supplied user profiles 332
 object authority required 458

DMPUSRPRF (Dump User Profile) command
 authorized IBM-supplied user profiles 332
 object auditing 499
 object authority required 412

DO (delete operation) file layout 601

DO (delete operation) journal entry type 272

DOCPWD (document password) parameter
 user profile 100

document
 library object (DLO) 245
 object authority required for commands 374
 password
 changes when restoring profile 248
 password (DOCPWD user profile parameter) 100
 QDOC profile 321
 restoring 245
 saving 245

document library object
 object auditing 516

document library object (DLO)
 adding authority 313

document library object (DLO)
(continued)
 changing authority 313
 changing owner 313
 changing primary group 313
 commands 313
 displaying authority 313
 displaying authorization list 313
 editing authority 313
 object authority required for
 commands 374
 removing authority 313

document library object auditing
 changing
 command description 313

domain attribute, object
 description 15
 displaying 15

Domain Name System
 object authority required for
 commands 378

double byte-character set dictionary
 (*IGCDCT) object auditing 527

double byte-character set sort (*IGCSRT)
 object auditing 528

double byte-character set table (*IGCTBL)
 object auditing 528

double-byte character set (DBCS)
 object authority required for
 commands 380

DS (DST password reset) journal entry
 type 277

DS (IBM-Supplied Service Tools User ID
 Reset) file layout 603

DSCJOB (Disconnect Job) command
 object authority required 412

DSPACC (Display Access Code)
 command
 object auditing 519
 object authority required 449

DSPACCAUT (Display Access Code
 Authority) command
 object authority required 449

DSPACTPJ (Display Active Prestart Jobs)
 command
 object authority required 413

DSPACTPRFL (Display Active Profile
 List) command
 description 707
 object authority required 493

DSPACTSCD (Display Activation
 Schedule) command
 description 707
 object authority required 494

DSPASPCPYD command
 authorized IBM-supplied user
 profiles 332

DSPASPSSN command
 authorized IBM-supplied user
 profiles 332

DSPASPSTS command
 object authority required 369

DSPAUDJRNE (Display Audit Journal
 Entries) command
 description 315, 711
 object authority required 418

DSPAUT (Display Authority) command
 description 310
 object auditing 514, 551, 557
 object authority required 396

DSPAUTHLR (Display Authority Holder)
 command
 description 309
 object auditing 504
 object authority required 354
 using 153

DSPAUTL (Display Authorization List)
 command
 description 309
 object auditing 503
 object authority required 354

DSPAUTLDLO (Display Authorization
 List Document Library Objects)
 command
 description 313
 object auditing 504
 object authority required 354, 375

DSPAUTLOBJ (Display Authorization List
 Objects) command
 description 309
 object auditing 503
 object authority required 354
 using 168

DSPAUTUSR (Display Authorized Users)
 command
 auditing 301
 description 311
 example 125
 object authority required 494

DSPBCKSTS (Display Backup Status)
 command
 object authority required 450

DSPBCKUP (Display Backup Options)
 command
 object authority required 450

DSPBCKUPL (Display Backup List)
 command
 object authority required 450

DSPBKP (Display Breakpoints) command
 object authority required 464

DSPBNDDIR (Display Binding Directory)
 command
 object authority required 355

DSPBNDDIRE (Display Binding
 Directory) command
 object auditing 504

DSPCDEFNT (Display Coded Font)
 object authority required for
 commands 351

DSPCFGL (Display Configuration List)
 command
 object auditing 505
 object authority required 364

DSPCHT (Display Chart) command
 object auditing 505
 object authority required 356

DSPCKMKSFE command
 object authority required 367

DSPCLS (Display Class) command
 object auditing 507
 object authority required 356

DSPCLUINF command
 authorized IBM-supplied user
 profiles 332

DSPCMD (Display Command) command
 object auditing 507
 object authority required 361

DSPCNNL (Display Connection List)
 command
 object auditing 508
 object authority required 364

DSPCNNSTS (Display Connection Status)
 command
 object authority required 369

DSPCOSD (Display Class-of-Service
 Description) command
 object auditing 509
 object authority required 357

DSPCPCST (Display Check Pending
 Constraint) command
 object authority required 386

DSPCPCST (Display Check Pending
 Constraints) command
 object auditing 525

DSPCRGINF command
 authorized IBM-supplied user
 profiles 332

DSPCSI (Display Communications Side
 Information) command
 object auditing 509
 object authority required 362

DSPCSPOBJ (Display CSP/AE Object)
 command
 object auditing 509, 510, 543

DSPCTLD (Display Controller
 Description) command
 object auditing 510
 object authority required 366

DSPCURDIR (Display Current Directory)
 command
 object auditing 512
 object authority required 396

DSPDBG (Display Debug) command
 object authority required 464

DSPDBGWCH (Display Debug Watches)
 command
 object authority required 464

DSPDBR (Display Database Relations)
 command
 object auditing 525
 object authority required 386

DSPDDMF (Display Distributed Data
 Management File) command
 object authority required 386

DSPDEVD (Display Device Description)
 command
 object auditing 511
 object authority required 369

DSPDIRE (Display Directory Entry)
 command
 object authority required 371

DSPDLOADUD (Display Document
 Library Object Auditing) command
 description 313
 object auditing 516
 object authority required 375
 using 288

DSPDLOAUT (Display Document Library Object Authority) command
description 313
object auditing 516
object authority required 375

DSPDLONAM (Display Document Library Object Name) command
object authority required 375

DSPDOC (Display Document) command
object auditing 516
object authority required 375

DSPDSTL (Display Distribution List) command
object authority required 374

DSPDSTLOG (Display Distribution Log) command
authorized IBM-supplied user profiles 332
object authority required 373

DSPDSTSRV (Display Distribution Services) command
object authority required 373

DSPDTA (Display Data) command
object authority required 386

DSPDTA (display data) parameter 211

DSPDTAARA (Display Data Area) command
object auditing 519
object authority required 367

DSPDTADCT (Display Data Dictionary) command
object authority required 410

DSPEDTD (Display Edit Description) command
object auditing 521
object authority required 380

DSPEWCBCDE (Display Extended Wireless Controller Bar Code Entry) command
object authority required 381

DSPEWCM (Display Extended Wireless Controller Member) command
object authority required 381

DSPEWCPTCE (Display Extended Wireless Controller PTC Entry) command
object authority required 381

DSPEWLM (Display Extended Wireless Line Member) command
object authority required 381

DSPEXPSCD (Display Expiration Schedule) command
description 707
object authority required 494

DSPF (Display File) command 396

DSPFD (Display File Description) command
object auditing 525
object authority required 386

DSPFFD (Display File Field Description) command
object auditing 525
object authority required 386

DSPFLR (Display Folder) command
object authority required 375

DSPFNTRSCA (Display Font Resource Attributes) command
object authority required 351

DSPFNTTBL (Display DBCS Font Table) command
object authority required for commands 351

DSPGDF (Display Graphics Data File) command
object authority required 356

DSPHDWRSC (Display Hardware Resources) command
object authority required 470

DSPHLPDOC (Display Help Document) command
object auditing 516

DSPHSTGPH
authorized IBM-supplied user profiles 332

DSPHSTGPH (Display Historical Graph) command
object authority required 458

DSPIGCDCT (Display DBCS Conversion Dictionary) command
object auditing 527
object authority required 380

DSPIPXD command 411

DSPJOB (Display Job) command
object authority required 413

DSPJOB (Display Job Description) command
object auditing 529
object authority required 415
using 261

DSPJOBLOG (Display Job Log) command
object authority required 413

DSPJRN (Display Journal) command
audit (QAUDJRN) journal example 295
auditing file activity 236, 300
creating output file 296
displaying QAUDJRN (audit) journal 263
object auditing 530, 532
object authority required 419

DSPJRNA (S/38E) Work with Journal Attributes
object auditing 532

DSPJRN (S/38E) Work with Journal
object auditing 532

DSPJRNRCVA (Display Journal Receiver Attributes) command
object auditing 532
object authority required 422

DSPJVMJOB command
object authority required 411

DSPLANADPP (Display LAN Adapter Profile) command
object authority required 437

DSPLANSTS (Display LAN Status) command
object authority required 437

DSPLIB (Display Library) command
object auditing 532
object authority required 431
using 303

DSPLIBD (Display Library Description) command
CRTAUT parameter 158
object authority required 431

DSPLICKEY (Display License Key) command
object authority required 434

DSPLIND (Display Line Description) command
object auditing 533
object authority required 437

DSPLNK
object authority required 397

DSPLNK (Display Links) command
object auditing 512, 550, 555, 558

DSPLOG (Display Log) command
object auditing 537
object authority required 441

DSPMFSINF (Display Mounted File System Information) command
object authority required 445

DSPMGDSYSA (Display Managed System Attributes) command
authorized IBM-supplied user profiles 332

DSPMNUA (Display Menu Attributes) command
object auditing 535
object authority required 439

DSPMOD (Display Module) command
object auditing 536
object authority required 443

DSPMODD (Display Mode Description) command
object auditing 535
object authority required 442

DSPMODSRC (Display Module Source) command
object auditing 522
object authority required 464

DSPMODSTS (Display Mode Status) command
object auditing 511
object authority required 442

DSPMSG (Display Messages) command
object auditing 537
object authority required 440

DSPMSGD (Display Message Descriptions) command
object auditing 536
object authority required 441

DSPNETA (Display Network Attributes) command
object authority required 444

DSPNTBD (Display NetBIOS Description) command
object auditing 539
object authority required 444

DSPNWID (Display Network Interface Description) command
object auditing 539
object authority required 446

DSPNWSA (Display Network Server Attribute) command
object authority required 447

DSPNWSALS (Display Network Server Alias) command
 object authority required 447

DSPNWSCFG command
 authorized IBM-supplied user profiles 332
 object authority required 448

DSPNWSDD (Display Network Server Description) command
 object auditing 540
 object authority required 448

DSPNWSSES (Display Network Server Session) command
 object authority required 447

DSPNWSSTC (Display Network Server Statistics) command
 object authority required 447

DSPNWSSTG (Display Network Server Storage Space) command
 object authority required 447

DSPNWSUSR (Display Network Server User) command
 object authority required 447

DSPNWSUSRA (Display Network Server User Attribute) command
 object authority required 447

DSPOBJAUT (Display Object Authority) command
 description 310
 object auditing 502
 object authority required 344
 using 303

DSPOBJD (Display Object Description) command
 created by 144
 description 310
 object auditing 502
 object authority required 345
 using 288
 using output file 302

DSPOPT (Display Optical) command
 object authority required 452

DSPOPTLCK (Display Optical Lock) command
 object authority required 452

DSPOPTSVR (Display Optical Server) command
 object authority required 452

DSPPDGPRF (Display Print Descriptor Group Profile) command
 object authority required 461

DSPPFM (Display Physical File Member) command
 object auditing 522
 object authority required 386

DSPPFRDTA
 authorized IBM-supplied user profiles 332

DSPPFRDTA (Display Performance Data) command
 object authority required 459

DSPPFRGPH
 authorized IBM-supplied user profiles 332

DSPPFRGPH (Display Performance Graph) command
 object authority required 459

DSPPGM (Display Program) command
 adopted authority 151
 object auditing 543
 object authority required 464
 program state 15

DSPPGMADP (Display Program Adopt) command
 object authority required 494

DSPPGMADP (Display Programs that Adopt) command
 object auditing 560

DSPPGMADP (Display Programs That Adopt) command
 auditing 303
 description 312
 using 151, 236

DSPPGMREF (Display Program References) command
 object auditing 525
 object authority required 464

DSPPGMVAR (Display Program Variable) command
 object authority required 464

DSPPRB (Display Problem) command
 object authority required 462

DSPPTF (Display Program Temporary Fix) command
 authorized IBM-supplied user profiles 332
 object authority required 476

DSPPWRSCD (Display Power On/Off Schedule) command
 object authority required 450

DSPPRYAP (Display Recovery for Access Paths) command
 object auditing 503
 object authority required 350

DSPPRDBDIRE (Display Relational Database Directory Entry) command
 object authority required 469

DSPPRJECFG (Display RJE Configuration) command
 object authority required 473

DSPS36 (Display System/36) command
 object auditing 559
 object authority required 487

DSPSAVF (Display Save File) command
 object authority required 386

DSPSBSD (Display Subsystem Description) command
 object auditing 549
 object authority required 484

DSPSECA (Display Security Attributes) command
 object authority required 474

DSPSECAUD (Display Security Auditing Values) command
 description 315
 object authority required 474

DSPSECAUD (Display Security Auditing) command
 description 709

DSPSFWRSC (Display Software Resources) command
 object authority required 470

DSPSGNINF (display sign-on information) parameter
 user profile 91

DSPSOCSTS (Display Sphere of Control Status) command
 object authority required 480

DSPSPLF (Display Spooled File) command
 action auditing 552
 DSPDTA parameter of output queue 211
 object auditing 541
 object authority required 482

DSPSRVA (Display Service Attributes) command
 object authority required 476

DSPSRVPGM (Display Service Program) command
 adopted authority 151
 object auditing 554
 object authority required 464

DSPSRVSTS (Display Service Status) command
 authorized IBM-supplied user profiles 332
 object authority required 476

DSPSSTUSR (Display service tools user ID) command
 object authority required 476

DSPSSTUSR command
 object authority required 494

DSPSYSSTS (Display System Status) command
 object authority required 485

DSPSYSVAL (Display System Value) command
 object authority required 486

DSPTAP (Display Tape) command
 object authority required 438

DSPTAPCTG (Display Tape Cartridge) command
 object authority required 438

DSPTRC (Display Trace) command
 object authority required 464

DSPTRCDTA (Display Trace Data) command
 object authority required 464

DSPUDFS (Display User-Defined File System) command
 object authority required 491

DSPUSRPMN (Display User Permission) command
 object auditing 519
 object authority required 449

DSPUSRPRF (Display User Profile) command
 description 311
 object auditing 560
 object authority required 494
 using 125
 using output file 302

DSPVTMAP (Display VT100 Keyboard Map) command
 object authority required 490

DST (dedicated service tools)
 auditing passwords 258
 changing passwords 129

DST (dedicated service tools) *(continued)*
 changing user ID 129
 resetting password
 audit journal (QAUDJRN)
 entry 277
 command description 311
 DST password reset (DS) journal entry
 type 277
 dump function
 *SERVICE (service) special
 authority 87
 duplicate password (QPWDRQDDIF)
 system value 51
 DUPOPT (Duplicate Optical) command
 object authority required 452
 DUPTAP (Duplicate Tape) command
 object authority required 438

E

Edit Authorization List (EDTAUTL)
 command 167, 309
 Edit Authorization List display
 displaying detail (*EXPERT user
 option) 106, 107, 108
 edit description
 object authority required for
 commands 380
 Edit Document Library Object Authority
 (EDTDLOAUT) command 313
 Edit Library List (EDTLIBL)
 command 207
 Edit Object Authority (EDTOBJAUT)
 command 159, 310
 Edit Object Authority display
 displaying detail (*EXPERT user
 option) 106, 107, 108
 editing
 authorization list 167, 309
 document library object (DLO)
 authority 313
 library list 207
 object authority 159, 310
 EDTAUTL (Edit Authorization List)
 command
 description 309
 object auditing 503
 object authority required 354
 using 167
 EDTBCKUPL (Edit Backup List)
 command
 object authority required 450
 EDTCPCST (Edit Check Pending
 Constraints) command
 authorized IBM-supplied user
 profiles 332
 object auditing 525
 object authority required 386
 EDTDEVRSR (Edit Device Resources)
 command
 object authority required 470
 EDTDLOAUT (Edit Document Library
 Object Authority) command
 description 313
 object auditing 516, 517
 object authority required 375

EDTDOC (Edit Document) command
 object auditing 517
 object authority required 375
 EDTF (Edit file) command 399
 EDTIGCDCT (Edit DBCS Conversion
 Dictionary) command
 object auditing 527
 object authority required 380
 EDTLIBL (Edit Library List) command
 object authority required 431
 using 207
 EDTOBJAUT (Edit Object Authority)
 command
 description 310
 object auditing 502
 object authority required 345
 using 159
 EDTQST (Edit Questions and Answers)
 command
 authorized IBM-supplied user
 profiles 332
 object authority required 468
 EDTRBDAP (Edit Rebuild Of Access
 Paths) command
 authorized IBM-supplied user
 profiles 332
 EDTRCYAP (Edit Recovery for Access
 Paths) command
 authorized IBM-supplied user
 profiles 332
 object auditing 502
 object authority required 350
 EDTS36PGMA (Edit System/36 Program
 Attributes) command
 object auditing 543
 object authority required 487
 EDTS36PRCA (Edit System/36 Procedure
 Attributes) command
 object auditing 524
 object authority required 487
 EDTS36SRCA (Edit System/36 Source
 Attributes) command
 object auditing 524
 object authority required 487
 EDTWSOAUT (Edit Workstation Object
 Authority) command
 object authority required 389
 eim association (EIMASSOC) parameter
 user profile 110
 EIMASSOC (eim association) parameter
 user profile 110
 EJTEMLOUT (Eject Emulation Output)
 command
 object authority required 370
 EML3270 (Emulate 3270 Display)
 command
 object authority required 371
 EMLPRTKEY (Emulate Printer Key)
 command
 object authority required 370
 emulation
 object authority required for
 commands 370
 enabled (*ENABLED) user profile
 status 78

enabling
 QSECOFR (security officer) user
 profile 78
 user profile
 automatically 707
 sample program 125
 ENCCPHK (Encipher Cipher Key)
 command
 authorized IBM-supplied user
 profiles 332
 ENCFRMMSTK (Encipher from Master
 Key) command
 authorized IBM-supplied user
 profiles 332
 encrypting
 password 76
 ENCTOMSTK (Encipher to Master Key)
 command
 authorized IBM-supplied user
 profiles 332
 End Job (ENDJOB) command
 QINACTMSGQ system value 28
 ENDASPBAL
 authorized IBM-supplied user
 profiles 332
 ENDASPBAL command 370
 ENDASPSSN
 authorized IBM-supplied user
 profiles 332
 ENDCAD
 authorized IBM-supplied user
 profiles 332
 ENDCAD command
 object authority required 359
 ENDCBLDBG (End COBOL Debug)
 command
 object authority required 430, 464
 ENDCHTSVR
 authorized IBM-supplied user
 profiles 332
 ENDCLNUP (End Cleanup) command
 object authority required 450
 ENDCLUNOD
 authorized IBM-supplied user
 profiles 332
 ENDCLUNOD command
 object authority required 359
 ENDCMNTRC
 authorized IBM-supplied user
 profiles 332
 ENDCMNTRC (End Communications
 Trace) command
 object authority required 476
 ENDCMTCTL (End Commitment
 Control) command
 object authority required 362
 ENDCPYSCN (End Copy Screen)
 command
 object authority required 476
 ENDCRG
 authorized IBM-supplied user
 profiles 332
 ENDCTLRCY (End Controller Recovery)
 command
 object auditing 510
 object authority required 366

ENDDBG (End Debug) command
 object authority required 464
 ENDDBGSVR (End Debug Server)
 command
 authorized IBM-supplied user
 profiles 332
 ENDDBMON (End Database Monitor)
 command
 object authority required 461
 ENDDEVRCY (End Device Recovery)
 command
 object auditing 511
 object authority required 370
 ENDDIRSHD (End Directory Shadow
 System) command
 object authority required 371
 ENDDIRSHD (End Directory Shadowing)
 command
 object auditing 515
 ENDDSKRGZ (End Disk Reorganization)
 command
 object authority required 372
 ENDDW command
 authorized IBM-supplied user
 profiles 332
 object authority required 459
 ENDGRPJOB (End Group Job) command
 object authority required 413
 ENDHOSTSVR
 authorized IBM-supplied user
 profiles 332
 ENDHOSTSVR (End Host Server)
 command
 object authority required 390
 ENDIDXMN (End Index Monitor)
 command
 authorized IBM-supplied user
 profiles 332
 ending
 audit function 295
 auditing 66
 connection
 audit journal (QAUDJRN)
 entry 273
 disconnected job 38, 41
 inactive job 27
 ENDIPSIFC (End IP over SNA Interface)
 command
 authorized IBM-supplied user
 profiles 332
 object authority required 352
 ENDJOB (End Job) command
 action auditing 553
 object authority required 413
 QINACTMSGQ system value 28
 ENDJOBABN (End Job Abnormal)
 command
 authorized IBM-supplied user
 profiles 332
 object authority required 413
 ENDJOBTRC
 authorized IBM-supplied user
 profiles 332
 ENDJOBTRC (End Job Trace) command
 object authority required 459
 ENDJRN (End Journal) command
 object authority required 400, 419
 ENDJRN (End Journaling) command
 object auditing 500
 ENDJRNAP (End Journal Access Path)
 command
 object authority required 419
 ENDJRNLIB (End Journaling the Library)
 command
 object authority required 419
 ENDJRNPF (End Journal Physical File
 Changes) command
 object authority required 419
 ENDJRNxxx (End Journaling) command
 object auditing 531
 ENDJW command
 authorized IBM-supplied user
 profiles 333
 object authority required 459
 ENDLINRCY (End Line Recovery)
 command
 object auditing 533
 object authority required 437
 ENDLOGSVR (End Job Log Server)
 command
 object authority required 413
 ENDMGDSYS (End Managed System)
 command
 authorized IBM-supplied user
 profiles 333
 ENDMGRSRV (End Manager Services)
 command
 authorized IBM-supplied user
 profiles 333
 ENDMOD (End Mode) command
 object auditing 535
 object authority required 442
 ENDMSF (End Mail Server Framework)
 command
 authorized IBM-supplied user
 profiles 333
 object authority required 438
 ENDNFSSVR (End Network File System
 Server) command
 authorized IBM-supplied user
 profiles 333
 object authority required 445
 ENDNWIRCY (End Network Interface
 Recovery) command
 object auditing 539
 ENDPASTHR (End Pass-Through)
 command
 object authority required 372
 ENDPEX (End Performance Explorer)
 command
 authorized IBM-supplied user
 profiles 333
 object authority required 459
 ENDPFRMON (End Performance
 Monitor) command
 object authority required 461
 ENDPFRTRC (End Performance Trace)
 command
 authorized IBM-supplied user
 profiles 333
 ENDPJ (End Prestart Jobs) command
 action auditing 553
 object authority required 413
 ENDPRTML (End Printer Emulation)
 command
 object authority required 370
 ENDRDR (End Reader) command
 object authority required 469
 ENDRJESSN (End RJE Session) command
 object authority required 473
 ENDRQS (End Request) command
 object authority required 464
 ENDS36 (End System/36) command
 object auditing 559
 ENDSBS (End Subsystem) command
 object auditing 548
 object authority required 484
 ENDSRVJOB (End Service Job) command
 authorized IBM-supplied user
 profiles 333
 object authority required 476
 ENDSYS (End System) command
 object authority required 485
 ENDSYSMGR (End System Manager)
 command
 authorized IBM-supplied user
 profiles 333
 ENDTCP (End TCP/IP) command
 authorized IBM-supplied user
 profiles 333
 ENDTCPNN (End TCP/IP Connection)
 command
 authorized IBM-supplied user
 profiles 333
 ENDTCP (End TCP/IP) command
 object authority required 490
 ENDTCPIFC (End TCP/IP Interface)
 command
 object authority required 490
 object authority required 490
 ENDTCPIFC
 authorized IBM-supplied user
 profiles 333
 ENDTCPPT (End Point-to-Point
 TCP/IP) command
 object authority required 489
 ENDTCPSRV (End TCP/IP Service)
 command
 object authority required 489
 ENDTCPSRV (End TCP/IP Server)
 command
 authorized IBM-supplied user
 profiles 333
 ENDTRC (End Trace) command
 object authority required 476
 ENDWCH (End Watch) command
 authorized IBM-supplied user
 profiles 333
 ENDWCH command
 object authority required 476
 ENDWTR (End Writer) command
 object authority required 496
 enhanced hardware storage protection
 audit journal (QAUDJRN) entry 276
 security level 40 17
 enrolling
 users 118
 ENTCBLDBG (Enter COBOL Debug)
 command
 object authority required 430, 464

- Entries
 - journal entries
 - auditing 270
 - security 270
- EV (Environment variable) file layout 604
- example
 - adopted authority
 - application design 230, 233
 - authority checking process 189, 192
 - assistance level
 - changing 80
 - authority checking
 - adopted authority 189, 192
 - authorization list 193
 - group authority 187
 - ignoring group authority 191
 - primary group 187
 - public authority 189, 191
 - changing
 - assistance levels 80
 - system portion of library list 227
 - controlling
 - user library list 226
 - describing
 - library security 228
 - menu security 229, 230
 - enabling user profile 125
 - ignoring adopted authority 232
 - JKL Toy Company applications 219
 - library list
 - changing system portion 227
 - controlling user portion 226
 - program 226
 - security risk 208
 - library security
 - describing 228
 - planning 225
 - menu security
 - describing 229, 230
 - password validation exit program 62
 - password validation program 61
 - public authority
 - creating new objects 139
 - restricting save and restore
 - commands 217
 - RSTLICPGM (Restore Licensed Program) command 253
 - securing output queues 214
- exceeding
 - account limit
 - audit journal (QAUDJRN) entry 284
- exclude (*EXCLUDE) authority 133
- execute (*EXECUTE) authority 132, 340
- existence (*OBJEXIST) authority 132, 340
- exit 62
- exit points
 - user profile 128
- expert (*EXPERT) user option 106, 107, 108, 160
- expiration
 - password (QPWDEXPITV system value) 47
 - password (QPWDEXPWRN system value) 48

- expiration (*continued*)
 - user profile
 - displaying schedule 707
 - setting schedule 707
- extended wireless LAN configuration
 - object authority required for commands 381
- EXTPGMINF (Extract Program Information) command
 - object authority required 464

F

- faccessx (Determine file accessibility for a class of users by descriptor) command
 - object auditing 512
- failure
 - sign-on
 - *ALLOBJ (all object) special authority 201
 - *SERVICE (service) special authority 201
 - QSECOFR (security officer) user profile 201
- field authorities 136
- field authority
 - definition 132
- field-level security 236
- FILDOC (File Document) command
 - object auditing 518
 - object authority required 375
- file
 - journaling
 - security tool 236
 - object authority required for commands 381
 - planning security 236
 - program-described
 - holding authority when deleted 153
 - securing
 - critical 236
 - fields 236
 - records 236
 - source
 - securing 242
- file (*FILE) object auditing 522
- file layout 570
- file security
 - SQL 239
- file transfer
 - securing 216
- filter
 - object authority required for commands 388
- filter (*FTR) object auditing 526
- finance
 - object authority required for commands 389
- finance (QFNC) user profile 321
- flowchart
 - authority checking 170
 - determining special environment 90
 - device description authority 202
- FNDSTRPDM (Find String Using PDM) command
 - object authority required 353

- folder
 - security shared 216
- font resource (*FNTRSC) object
 - auditing 526
- force conversion on restore (QFRCCVNRST)
 - system value 43
- force level
 - audit records 67
- form definition (*FORMDF) object
 - auditing 526
- forms control table
 - object authority required for commands 470
- FTP (File Transfer Protocol) command
 - object authority required 489
- full
 - audit (QAUDJRN) journal receiver 293
- full-screen help (*HLPFULL) user option 108

G

- GENCAT (Merge Message Catalog) command
 - object authority required 386
- GENCKMKSFE command
 - object authority required 367
- GENCMDDOC (Generate Command Documentation) command
 - object authority required 361
- GENCPHK (Generate Cipher Key) command
 - authorized IBM-supplied user profiles 333
- GENCRSDMNK (Generate Cross Domain Key) command
 - authorized IBM-supplied user profiles 333
- generic name
 - example 163
- generic record(GR) file layout 605
- GENJVMDMP command
 - object authority required 411
- GENMAC (Generate Message Authentication Code) command
 - authorized IBM-supplied user profiles 333
- GENPIN (Generate Personal Identification Number) command
 - authorized IBM-supplied user profiles 333
- GENS36RPT (Generate System/36 Report) command
 - authorized IBM-supplied user profiles 333
 - object authority required 442
- GENS38RPT (Generate System/38 Report) command
 - authorized IBM-supplied user profiles 333
 - object authority required 442
- gid (group identification number) restoring 249
- give descriptor (GS) file layout 610

- give descriptor (GS) journal entry type 281
- giving
 - descriptor
 - audit journal (QAUDJRN) entry 281
 - socket
 - audit journal (QAUDJRN) entry 281
- GO (Go to Menu) command
 - object authority required 440
- GR (generic record) file layout 605
- Grant Object Authority (GRTOBJAUT) command 159, 310
 - affect on previous authority 162
 - multiple objects 162
- Grant User Authority (GRTUSRAUT) command
 - copying authority 121
 - description 311
 - recommendations 165
 - renaming profile 127
- Grant User Permission (GRTUSRPMN) command 313
- granting
 - authority using referenced object 165
 - object authority 310
 - affect on previous authority 162
 - multiple objects 162
 - user authority
 - command description 311
 - user permission 313
- graphic symbols set (*GSS) object auditing 527
- graphical operations
 - object authority required for commands 389
- graphics symbol set
 - object authority required for commands 390
- group
 - authority
 - displaying 156
 - primary
 - introduction 5
- group (*GROUP) authority 156
- group authority
 - adopted authority 150
 - authority checking example 187, 191
 - description 131
 - GRPAUT user profile parameter 98, 143, 145
 - GRPAUTTYP user profile parameter 98, 145
- group authority type
 - GRPAUTTYP user profile parameter 98
- group identification number (gid) restoring 249
- group job
 - adopted authority 150
- group profile
 - auditing
 - *ALLOBJ special authority 260
 - membership 260
 - password 259

- group profile (*continued*)
 - authorization list
 - comparison 241
 - comparison
 - authorization list 241
 - GRPPRF user profile parameter
 - changes when restoring profile 248
 - description 97
 - introduction 4, 74
 - multiple
 - planning 240
 - naming 76
 - object ownership 143
 - password 76
 - planning 239
 - primary 144
 - planning 240
 - resource security 5, 131
 - supplemental
 - SUPGRPPRF (supplemental groups) parameter 99
 - user profile
 - description 97
 - user profile parameter
 - changes when restoring profile 248
- GRPAUT (group authority) parameter
 - user profile 98, 143, 145
- GRPAUTTYP (group authority type) parameter
 - user profile 98, 145
- GRPPRF (group profile) parameter
 - user profile
 - description 97
 - example 145
- GRTACCAUT (Grant Access Code Authority) command
 - authorized IBM-supplied user profiles 333
 - object auditing 518
 - object authority required 449
- GRTOBJAUT (Grant Object Authority) command 159
 - affect on previous authority 162
 - description 310
 - multiple objects 162
 - object auditing 500
 - object authority required 345
- GRTUSRAUT (Grant User Authority) command
 - copying authority 121
 - description 311
 - object auditing 560
 - object authority required 494
 - recommendations 165
 - renaming profile 127
- GRTUSRPMN (Grant User Permission) command
 - description 313
 - object auditing 518
 - object authority required 449
- GRTWSOAUT (Grant Workstation Object Authority) command
 - object authority required 389
- GS (give descriptor) file layout 610

- GS (give descriptor) journal entry type 281

H

- hardware
 - enhanced storage protection 17
 - object authority required for commands 470
- help full screen (*HLPFULL) user option 108
- help information
 - displaying full screen (*HLPFULL user option) 108
- history (QHST) log
 - using to monitor security 299
- HLDCMNDDEV (Hold Communications Device) command
 - authorized IBM-supplied user profiles 333
 - object auditing 511
 - object authority required 370
- HLDDSTQ (Hold Distribution Queue) command
 - authorized IBM-supplied user profiles 333
 - object authority required 373
- HLDJOB (Hold Job) command
 - object authority required 413
- HLDJOBQ (Hold Job Queue) command
 - object auditing 529
 - object authority required 416
- HLDJOBSCDE (Hold Job Schedule Entry) command
 - object auditing 530
 - object authority required 417
- HLDOUQ (Hold Output Queue) command
 - object auditing 540
 - object authority required 454
- HLDRDR (Hold Reader) command
 - object authority required 469
- HLDSPLF (Hold Spooled File) command
 - action auditing 553
 - object auditing 541
 - object authority required 482
- HLDWTR (Hold Writer) command
 - object authority required 496
- hold (*HOLD) delivery mode
 - user profile 102
- home directory (HOMEDIR) parameter
 - user profile 109
- HOMEDIR (home directory) parameter
 - user profile 109
- host server
 - object authority required for commands 390

I

- IBM-supplied objects
 - securing with authorization list 139
- IBM-Supplied Service Tools User ID Reset (DS) file layout 603
- IBM-supplied user profile
 - ADSM (QADSM) 321

IBM-supplied user profile (*continued*)

- AFDFTUSR (QAFDFTUSR) 321
- AFOWN (QAFOWN) 321
- AFUSR (QAFUSR) 321
- auditing 258
- authority profile (QAUTPROF) 321
- automatic install (QLPAUTO) 321
- basic service (QSRVBAS) 321
- BRM (QBRMS) 321
- BRM user profile (QBRMS) 321
- changing password 129
- database share (QDBSHR) 321
- DCEADM (QDCEADM) 321
- default owner (QDFTOWN)
 - default values 321
 - description 145
- default values table 319
- distributed systems node executive (QDSNX) 321
- document (QDOC) 321
- finance (QFNC) 321
- IBM authority profile (QAUTPROF) 321
- install licensed programs (QLPINSTALL) 321
- mail server framework (QMSF) 321
- NFS user profile (QNFSANON) 321
- programmer (QPGMR) 321
- purpose 128
- QADSM (ADSM) 321
- QAFDFTUSR (AFDFTUSR) 321
- QAFOWN (AFOWN) 321
- QAFUSR (AFUSR) 321
- QAUTPROF (database share) 321
- QAUTPROF (IBM authority profile) 321
- QBRMS (BRM user profile) 321
- QBRMS (BRM) 321
- QDBSHR (database share) 321
- QDCEADM (DCEADM) 321
- QDFTOWN (default owner)
 - default values 321
 - description 145
- QDOC (document) 321
- QDSNX (distributed systems node executive) 321
- QFNC (finance) 321
- QGATE (VM/MVS bridge) 321
- QLPAUTO (licensed program automatic install) 321
- QLPINSTALL (licensed program install) 321
- QMSF (mail server framework) 321
- QNFSANON (NFS user profile) 321
- QPGMR (programmer) 321
- QRJE (remote job entry) 321
- QSECOFR (security officer) 321
- QSNADS (Systems Network Architecture distribution services) 321
- QSPL (spool) 321
- QSPLJOB (spool job) 321
- QSRV (service) 321
- QSRVBAS (service basic) 321
- QSYS (system) 321
- QSYSOPR (system operator) 321
- QTCP (TCP/IP) 321

IBM-supplied user profile (*continued*)

- QTMLPDP (TCP/IP printing support) 321
- QTSTRQS (test request) 321
- QUSER (workstation user) 321
- remote job entry (QRJE) 321
- restoring 249
- restricted commands 327
- security officer (QSECOFR) 321
- service (QSRV) 321
- service basic (QSRVBAS) 321
- SNA distribution services (QSNADS) 321
- spool (QSPL) 321
- spool job (QSPLJOB) 321
- system (QSYS) 321
- system operator (QSYSOPR) 321
- TCP/IP (QTCP) 321
- TCP/IP printing support (QTMLPDP) 321
- test request (QTSTRQS) 321
- VM/MVS bridge (QGATE) 321
- workstation user (QUSER) 321

ignoring

- adopted authority 152

image

- object authority required for commands 390

inactive

- job
 - message queue (QINACTMSGQ) system value 28
 - time-out interval (QINACTITV) system value 27
- user
 - listing 302

inactive job

- message (CPI1126) 28

inactive job message queue (QINACTMSGQ) system value

- value set by CFGSYSSEC command 716

inactive job time-out interval (QINACTITV) system value

- value set by CFGSYSSEC command 716

INCLUDE command

- object authority required 430

incorrect password

- audit journal (QAUDJRN) entry 271

incorrect user ID

- audit journal (QAUDJRN) entry 271

information search index

- object authority required 411

initial library list

- current library 81
- job description (JOBDD) user profile 96
- recommendations 210
- relationship to library list for job 207
- risks 210

initial menu

- *SIGNOFF 82
- changing 82
- preventing display 82
- recommendation 84
- user profile 82

initial menu (INLMNU) parameter

- user profile 82

initial program (INLPGM) parameter

- changing 81
- user profile 81

initial program load (IPL)

- *JOBCTL (job control) special authority 86

INLMNU (initial menu) parameter

- user profile 82

INLPGM (initial program) parameter

- changing 81
- user profile 81

INSINTSVR command

- authorized IBM-supplied user profiles 333

INSPTF (Install Program Temporary Fix) command

- authorized IBM-supplied user profiles 333
- object authority required 476

INSRMTPRD (Install Remote Product) command

- authorized IBM-supplied user profiles 333

install licensed program (QLPINSTALL) user profile

- default values 321
- restoring 249

install licensed program automatic (QLPAUTO) user profile

- restoring 249

installing

- operating system 255

INSWNTSVR command

- authorized IBM-supplied user profiles 333

integrated file system

- object authority required for commands 392

integrity 1

- checking
 - auditing use 262
 - description 304, 311

interactive data definition

- object authority required for commands 410

interactive data definition utility (IDDU)

- object auditing 520

interactive job

- routing
 - SPCENV (special environment) parameter 90
 - security when starting 199

intermediate assistance level 74, 80

internal control block

- preventing modification 20

Internet security management (GS) file layout 617

Internet user

- validation lists 243

interprocess communication actions (IP) file layout 614

interprocess communications

- incorrect
 - audit journal (QAUDJRN) entry 271

interprocess communications (IP) journal entry type 271

INZDSTQ (Initialize Distribution Queue) command

- authorized IBM-supplied user profiles 333
- object authority required 373

INZNWSCFG command

- authorized IBM-supplied user profiles 333
- object authority required 448

INZOPT (Initialize Optical) command

- object authority required 452

INZPFM (Initialize Physical File Member) command

- object auditing 524
- object authority required 386

INZSYS (Initialize System) command

- authorized IBM-supplied user profiles 333
- object authority required 435

INZTAP (Initialize Tape) command

- object authority required 438

IP (change ownership) journal entry type 281

IP (interprocess communication actions) file layout 614

IP (interprocess communications) journal entry type 271

IP rules actions (IR) file layout 615

IPC object

- changing
 - audit journal (QAUDJRN) entry 281

IPL (initial program load)

- *JOBCTL (job control) special authority 86

IR (IP rules actions) file layout 615

IS (Internet security management) file layout 617

iSeries Access

- controlling sign-on 32
- file transfer security 216
- message function security 216
- shared folder security 216
- virtual printer security 216

J

jar files

- class files 243

Java

- object authority required for commands 411

JD (job description change) file layout 619

JD (job description change) journal entry type 281

JKL Toy Company

- diagram of applications 219

job

- *JOBCTL (job control) special authority 86
- automatic cancelation 38, 41
- changing
 - adopted authority 151
- changing (*continued*)
 - audit journal (QAUDJRN) entry 273
- disconnected job interval (QDSCJOBITV) system value 38
- inactive
 - time-out interval (QINACTITV) system value 27
- object authority required for commands 412
- restricting to batch 218
- scheduling 218
- security when starting 199
- verify object on restore (QVFYOJBIRST) system value 41

job accounting

- user profile 100

job action (JOBACN) network attribute 214, 262

job change (*JOBDDTA) audit level 273

job change (JS) file layout 620

job change (JS) journal entry type 273

job control (*JOBCTL) special authority functions allowed 86

- output queue parameters 212
- priority limit (PTYLMT) 95
- risks 86

job description

- changing
 - audit journal (QAUDJRN) entry 281
 - communications entry 206
 - default (QDFTJOBDD) 96
 - displaying 261
 - monitoring 261
 - object authority required for commands 415
 - printing security-relevant parameters 711
 - protecting 16
 - protecting system resources 218
 - QDFTJOBDD (default) 96
 - recommendations 96
 - restoring
 - audit journal (QAUDJRN) entry 276
 - security issues 206
 - security level 40 16
 - USER parameter 206
 - user profile 96
 - workstation entry 206
- description (*JOBDD) object auditing 528
- description (JOBDD) parameter user profile 96
- description change (JD) file layout 619
- description change (JD) journal entry type 281
- description violation
 - audit journal (QAUDJRN) entry 16
- initiation
 - adopted authority 200
 - Attention-key-handling program 200

job queue

- *JOBCTL (job control) special authority 86
- *OPRCTL (operator control) parameter 86
- *SPLCTL (spool control) special authority 86
- object authority required for commands 416
- printing security-relevant parameters 316, 713

job queue (*JOBQ) auditing 529

job schedule

- object authority required for commands 417

job scheduler (*JOBSCD) auditing 530

JOBACN (job action) network attribute 214, 262

JOBDD (job description) parameter user profile 96

journal

- audit (QAUDJRN)
 - introduction 262
 - displaying
 - auditing file activity 236, 300
 - managing 293
 - object authority required for commands 417
 - using to monitor security 300
 - working with 301
- (*JRN) auditing 530
- attributes
 - working with 301
- Journal Entries
 - security auditing 270
- entry
 - sending 292
- receiver
 - changing 294
 - deleting 294
 - detaching 293, 294
 - managing 293
 - maximum storage (MAXSTG) 94
 - object authority required for commands 421
 - storage needed 94
- receiver (*JRNRCV) auditing 532
- receiver, audit
 - creating 291
 - naming 291
 - saving 294
 - storage threshold 293
- audit 291
- working with 294

journaling

- security tool 236

JRNAP (Journal Access Path) command

- object authority required 419

JRNAP (Start Journal Access Path) command

- object auditing 531

JRNPF (Journal Physical File) command

- object authority required 419

JRNPF (Start Journal Physical File) command

- object auditing 531

JS (job change) file layout 620

JS (job change) journal entry type 273

K

Kerberos

object authority required for
commands 422

kerberos authentication (X0) file
layout 691

keyboard buffering

KBDBUF user profile parameter 93

QKDBUF system value 94

keylock security 2

keylock switch

auditing 258

KF (key ring file) file layout 625

L

LANGID (language identifier) parameter

SRTSEQ user profile parameter 105

user profile 105

language identifier

LANGID user profile parameter 105

QLANGID system value 105

SRTSEQ user profile parameter 105

language, programming

object authority required for
commands 424

large profiles

planning applications 226

large user profile 302

LCLPWDMGT (local password
management) parameter 92

LD (link, unlink, search directory) file
layout 628

LDIF2DB command

authorized IBM-supplied user
profiles 333

object authority required 372

length of password 50, 51

level 10

QSECURITY (security level) system
value 12

level 20

QSECURITY (security level) system
value 12

level 30

QSECURITY (security level) system
value 13

level 40

internal control blocks 20

QSECURITY (security level) system
value 14

level 50

internal control blocks 20

message handling 20

QSECURITY (security level) system
value 19

QTEMP (temporary) library 19

validating parameters 17

level of security (QSECURITY) system
value

comparison of levels 9

level 20 12

level 30 13

level of security (QSECURITY) system
value (*continued*)

level 40 14

level 50 19

overview 9

recommendations 11

special authority 11

user class 11

library

authority

definition 5

description 136

new objects 139

AUTOCFG (automatic device

configuration) value 37

automatic device configuration

(AUTOCFG) value 37

create authority (CRTAUT) parameter

description 139

example 145

risks 140

specifying 157

create object auditing (CROBJAUD)

value 71

creating 157

CRTAUT (create authority) parameter

description 139

example 145

risks 140

specifying 157

CROBJAUD (create object auditing)

value 71

current 81

designing 225

listing

all libraries 303

contents 303

object authority required for

commands 430

object ownership 242

planning 225

printing list of subsystem

descriptions 316

public authority

specifying 157

QRETSVRSEC (retain server security)

value 31

QTEMP (temporary)

security level 50 19

restoring 245

retain server security (QRETSVRSEC)

value 31

saving 245

security

adopted authority 136

description 136

designing 225

example 225

guidelines 225

risks 135

library (*LIB) auditing 532

library list

adding entries 207, 210

adopted authority 136

changing 207

current library

description 207

library list (*continued*)

current library (*continued*)

recommendations 210

user profile 81

definition 207

editing 207

job description (JOBDD)

user profile 96

monitoring 261

product library

description 207

recommendations 209

removing entries 207

security risks 207, 208

system portion

changing 227

description 207

recommendations 209

user portion

controlling 226

description 207

recommendations 210

licensed program

automatic install (QLPAUTO) user

profile

description 321

install (QLPINSTALL) user profile

default values 321

object authority required for

commands 435

restoring

recommendations 253

security risks 253

licensed program automatic install

(QLPAUTO) user profile

restoring 249

licensed program install (QLPINSTALL)

user profile

restoring 249

limit capabilities (LMTCPB) parameter

user profile 83

limit characters (QPWDLMTCHR) system

value 52

limit repeated characters

(QPWDLMTREP) system value 53

limit security officer (QLMTSECOFR)

system value

value set by CFGSYSSEC

command 716

limiting

capabilities 83

changing Attention-key-handling

program 104

changing current library 81, 210

changing initial menu 82

changing initial program 81

commands allowed 83

functions allowed 83

listing users 302

LMTCPB user profile

parameter 83

command line use 83

device sessions

auditing 260

LMTDEVSSN user profile

parameter 93

- limiting (*continued*)
 - device sessions (*continued*)
 - recommendations 93
 - device sessions (QLMTDEVSSN)
 - system value sign-on
 - description 29
 - multiple devices 29
 - disk usage (MAXSTG) 94
 - security officer (QLMTSECOFR)
 - changing security levels 13
 - security officer (QLMTSECOFR)
 - system value
 - auditing 258
 - authority to device
 - descriptions 201
 - description 29
 - sign-on process 203
 - sign-on
 - attempts (QMAXSGNACN) system
 - value 30
 - attempts (QMAXSIGN) system
 - value 30
 - sign-on attempts
 - auditing 258, 262
 - use of system resources
 - priority limit (PTYLMT)
 - parameter 95
- line description
 - object authority required for
 - commands 435
- line description (*LIND) auditing 533
- link
 - object authority required for
 - commands 357, 392
- listing
 - all libraries 303
 - authority holders 153
 - library contents 303
 - selected user profiles 302
 - system values 258
 - user profile
 - individual 125
 - summary list 125
- Lists, Create Validation 243
- Lists, Delete Validation 243
- LMTDEVSSN (limit device sessions)
 - parameter
 - user profile 93
- LNKDTADFN (Link Data Definition)
 - command
 - object auditing 520
 - object authority required 410
- local socket (*SOCKET) auditing 550
- locale
 - object authority required for
 - commands 437
- LOCALE (user options) parameter
 - user profile 107
- LODIMGCLG command
 - object authority required 391
- LODIMGCLGE command
 - object authority required 391
- LODOPTFMW
 - authorized IBM-supplied user
 - profiles 333
- LODOPTFMW command
 - object authority required 452

- LODPTF (Load Program Temporary Fix)
 - command
 - authorized IBM-supplied user
 - profiles 333
 - object authority required 476
- LODQSTDB (Load Question-and-Answer Database) command
 - authorized IBM-supplied user
 - profiles 333
 - object authority required 468
- logging off
 - network
 - audit journal (QAUDJRN)
 - entry 273
- logging on
 - network
 - audit journal (QAUDJRN)
 - entry 273
- logical file
 - securing
 - fields 236
 - records 236
- LPR (Line Printer Requester) command
 - object authority required 489

M

- mail
 - handling
 - audit journal (QAUDJRN)
 - entry 275
 - mail actions (ML) file layout 630
 - mail actions (ML) journal entry type 275
 - mail server framework
 - object authority required for
 - commands 438
 - mail server framework (QMSF) user
 - profile 321
 - mail services
 - action auditing 534
 - management (*OBJMGT) authority
 - object 132, 340
 - managing
 - audit journal 292
 - maximum
 - auditing 258
 - length of password (QPWDMAXLEN)
 - system value 51
 - sign-on attempts (QMAXSIGN)
 - system value 258
 - description 30
 - size
 - audit (QAUDJRN) journal
 - receiver 293
 - storage (MAXSTG) parameter
 - authority holder 145
 - group ownership of objects 143
 - journal receiver 94
 - restore operation 94
 - user profile 94
 - maximum sign-on attempts
 - (QMAXSIGN) system value
 - value set by CFGSYSSEC
 - command 716

- maximum storage (MAXSTG) parameter
 - authority holder
 - transferred to QDFTOWN (default
 - owner) 145
 - group ownership of objects 143
 - journal receiver 94
 - restore operation 94
 - user profile 94
- MAXSTG (maximum storage) parameter
 - authority holder
 - transferred to QDFTOWN (default
 - owner) 145
 - group ownership of objects 143
 - journal receiver 94
 - restore operation 94
 - user profile 94
- media
 - object authority required for
 - commands 438
- memory
 - sharing control
 - QSHRMEMCTL (share memory
 - control) system value 34
- menu
 - changing
 - PRDLIB (product library)
 - parameter 210
 - security risks 210
 - creating
 - PRDLIB (product library)
 - parameter 210
 - security risks 210
 - designing for security 228
 - initial 82
 - object authority required for
 - commands 439
 - security tools 707
 - user profile 82
 - menu (*MENU) auditing 535
 - Merge Source (Merge Source) command
 - object authority required 386
 - message
 - inactive timer (CPI1126) 28
 - print notification (*PRTMSG user
 - option) 108
 - printing completion (*PRTMSG user
 - option) 108
 - restricting content 20
 - security
 - monitoring 299
 - status
 - displaying (*STSMMSG user
 - option) 108
 - not displaying (*NOSTSMMSG user
 - option) 108
 - message description
 - object authority required for
 - commands 441
 - message file
 - object authority required for
 - commands 441
 - message file (*MSGF) auditing 536
 - message function (iSeries Access)
 - securing 216
 - message queue
 - *BREAK (break) delivery mode 102
 - *DFT (default) delivery mode 102

message queue (*continued*)

- *HOLD (hold) delivery mode 102
- *NOTIFY (notify) delivery mode 102
- automatic creation 101
- default responses 102
- inactive job (QINACTMSGQ) system value 28
- object authority required for commands 441
- QSYSMSG 299
 - QMAXSGNACN (action when attempts reached) system value 31
 - QMAXSIGN (maximum sign-on attempts) system value 30
- recommendation
 - MSGQ user profile parameter 101
- restricting 207
- severity (SEV) parameter 102
- user profile
 - deleting 122
 - delivery (DLVRY) parameter 102
 - recommendations 101
 - severity (SEV) parameter 102

message queue (*MSGQ) auditing 537

message queue (MSGQ) parameter user profile 101

MGRS36 (Migrate System/36) command

- authorized IBM-supplied user profiles 333

MGRS36APF

- authorized IBM-supplied user profiles 333

MGRS36CBL

- authorized IBM-supplied user profiles 333

MGRS36DFU

- authorized IBM-supplied user profiles 333

MGRS36DSPF

- authorized IBM-supplied user profiles 333

MGRS36ITM (Migrate System/36 Item) command

- authorized IBM-supplied user profiles 333
- object authority required 442

MGRS36LIB

- authorized IBM-supplied user profiles 334

MGRS36MNU

- authorized IBM-supplied user profiles 334

MGRS36MSGF

- authorized IBM-supplied user profiles 334

MGRS36QRY

- authorized IBM-supplied user profiles 334

MGRS36RPG

- authorized IBM-supplied user profiles 334

MGRS36SEC

- authorized IBM-supplied user profiles 334

MGRS38OBJ (Migrate System/38 Objects) command

- authorized IBM-supplied user profiles 334
- object authority required 442

MGRTCPHT (Merge TCP/IP Host Table) command

- object authority required 490

MIGRATE

- authorized IBM-supplied user profiles 334

migrating

- security level (QSECURITY) system value
 - level 10 to level 20 12
 - level 20 to level 30 13
 - level 20 to level 40 18
 - level 20 to level 50 20
 - level 30 to level 20 13
 - level 30 to level 40 18
 - level 30 to level 50 20
 - level 40 to level 20 13

migration

- object authority required for commands 442

minimum length of password (QPWDMINLEN) system value 50

ML (mail actions) file layout 630

ML (mail actions) journal entry type 275

mode description

- object authority required for commands 442

mode description (*MODD) auditing 535

mode of access

- definition 132

module

- binding directory 443
- object authority required for commands 443

module (*MODULE) auditing 535

monitoring

- *ALLOBJ (all object) special authority 260
- adopted authority 261
- authority
 - user profiles 261
- authorization 261
- checklist for 257
- communications 262
- encryption of sensitive data 262
- group profile
 - membership 260
 - password 259
- IBM-supplied user profiles 258
- inactive users 260
- job descriptions 261
- library lists 261
- limit capabilities 260
- message
 - security 299
- methods 299
- network attributes 262
- object authority 303
- object integrity 304
- overview 257
- password controls 259

monitoring (*continued*)

- physical security 258
- program failure 303
- programmer authorities 260
- remote sign-on 262
- security officer 305
- sensitive data
 - authority 261
 - encrypting 262
- sign-on without user ID and password 261
- system values 258
- unauthorized access 262
- unauthorized programs 262
- unsupported interfaces 262
- user profile
 - administration 260
- using
 - journals 300
 - QHST (history) log 299
 - QSYSMSG message queue 262

MOUNT (Add Mounted File System) command

- object authority required 491

MOUNT (Add Mounted File System) command) command

- object authority required 445

MOV

- object authority required 400

MOV (Move) command

- object auditing 513, 555, 556, 558

MOVDOC (Move Document) command

- object auditing 518
- object authority required 375

moving

- object
 - audit journal (QAUDJRN) entry 275
 - spooled file 211

MOVOBJ (Move Object) command

- object auditing 500, 533
- object authority required 345

MRGDOC (Merge Document) command

- object auditing 516, 518
- object authority required 375

MRGFORMD (Merge Form Description) command

- object authority required 353

MRGMSGF (Merge Message File) command

- object auditing 536
- object authority required 441

MSGQ (message queue) parameter user profile 101

multiple group

- example 194
- planning 240

N

NA (network attribute change) file layout 630

NA (network attribute change) journal entry type 281

naming

- audit journal receiver 291
- group profile 75, 76

- naming (*continued*)
 - user profile 75
- national language version (NLV)
 - command security 235
- ND (APPN directory) file layout 631
- NE (APPN end point) file layout 632
- NetBIOS description
 - object authority required for commands 443
- NetBIOS description (*NTBD)
 - auditing 538
- NETSTAT (Network Status) command
 - object authority required 490
- network
 - logging off
 - audit journal (QAUDJRN) entry 273
 - logging on
 - audit journal (QAUDJRN) entry 273
 - password
 - audit journal (QAUDJRN) entry 271
- network attribute
 - *SECADM (security administrator) special authority 85
 - changing
 - audit journal (QAUDJRN) entry 281
 - command 214
 - client request access (PCSACC) 215
 - command for setting 316, 715
 - DDM request access (DDMACC) 216
 - DDMACC (DDM request access) 216
 - DDMACC (distributed data management access) 262
 - distributed data management access (DDMACC) 262
 - job action (JOBACN) 214, 262
 - JOBACN (job action) 214, 262
 - object authority required for commands 444
 - PC Support (PCSACC) 262
 - PCSACC (client request access) 215
 - PCSACC (PC Support access) 262
 - printing security-relevant 711
- network attribute change (NA) file layout 630
- network attribute change (NA) journal entry type 281
- network attributes
 - printing security-communications 316
 - printing security-relevant 316
- network interface (*NWID) auditing 539
- network interface description
 - object authority required for commands 446
- network log on and off (VN) file layout 684
- network log on or off (VN) journal entry type 273
- network password error (VP) file layout 686
- network password error (VP) journal entry type 271

- network profile
 - changing
 - audit journal (QAUDJRN) entry 282
- network profile change (VU) file layout 689
- network profile change (VU) journal entry type 282
- network resource access (VR) file layout 687
- Network Server
 - object authority required for commands 446
- network server configuration
 - object authority required for commands 448
- network server description
 - object authority required for commands 448
- network server description (*NWSD)
 - auditing 540
- network spooled file
 - sending 211
- new object
 - authority
 - CRTAUT (create authority) parameter 139, 157
 - GRPAUT (group authority) parameter 98, 143
 - GRPAUTYP (group authority type) parameter 98
 - authority (QCRTAUT system value) 26
 - authority (QUSEADPAUT system value) 35
 - authority example 145
 - ownership example 145
- NLV (national language version)
 - command security 235
- node group (*NODGRP) auditing 538
- node list
 - object authority required for commands 449
- node list (*NODL) auditing 538
- notification, message
 - DLVRY (message queue delivery) parameter
 - user profile 102
 - no status message (*NOSTSMMSG) user option 108
- notify (*NOTIFY) delivery mode
 - user profile 102
- number required in password 54
- numeric character required in password 54
- numeric password 76
- numeric user ID 75

O

- OBJAUD (object auditing) parameter user profile 112
- object
 - (*Mgt) authority 132
 - (*Ref) authority 132
 - add (*ADD) authority 132, 340

- object (*continued*)
 - altered
 - checking 304
 - assigning authority and ownership 145
 - auditing
 - changing 88
 - default 288
 - authority
 - *ALL (all) 134, 341
 - *CHANGE (change) 134, 341
 - *USE (use) 134, 341
 - changing 159
 - commonly used subsets 133
 - new 140
 - new object 139
 - storing 247
 - system-defined subsets 133
 - using referenced 165
 - authority required for
 - commands 343
 - controlling access 15
 - default owner (QDFTOWN) user profile 145
 - delete (*DLT) authority 132, 340
 - displaying
 - originator 144
 - domain attribute 15
 - execute (*EXECUTE) authority 132, 340
 - existence (*OBJEXIST) authority 132, 340
 - failure of unsupported interface 15
 - management (*OBJMGT)
 - authority 132, 340
 - non-IBM
 - printing list 316
 - operational (*OBJOPR) authority 132, 339
 - ownership
 - introduction 5
 - primary group 122, 144
 - printing
 - adopted authority 711
 - authority source 711
 - non-IBM 711
 - read (*READ) authority 132, 340
 - restoring 245, 249
 - saving 245
 - securing with authorization list 167
 - state attribute 15
 - storing
 - authority 246, 247
 - update (*UPD) authority 132, 340
 - user domain
 - restricting 19
 - security exposure 19
 - working with 310
- object alter (*OBJALTER) authority 132, 340
- object auditing
 - *ALRTBL (alert table) object 503
 - *AUTHLR (authority holder)
 - object 504
 - *AUTL (authorization list) object 503
 - *BNDDIR (binding directory)
 - object 504

object auditing (*continued*)

*CFGL (configuration list) object 505
 *CHTFMT (chart format) object 505
 *CLD (C locale description) object 506
 *CLS (Class) object 507
 *CMD (Command) object 507
 *CNNL (connection list) object 508
 *COSD (class-of-service description) object 509
 *CRQD (change request description) object 506
 *CSI (communications side information) object 509
 *CSPMAP (cross system product map) object 509
 *CSPTBL (cross system product table) object 510
 *CTLD (controller description) object 510
 *DEVD (device description) object 511
 *DIR (directory) object 512
 *DOC (document) object 516
 *DTAARA (data area) object 519
 *DTADCT (data dictionary) object 520
 *DTAQ (data queue) object 520
 *EDTD (edit description) object 521
 *EXITRG (exit registration) object 521
 *FCT (forms control table) object 522
 *FILE (file) object 522
 *FLR (folder) object 516
 *FNTRSC (font resource) object 526
 *FORMDF (form definition) object 526
 *FTR (filter) object 526
 *GSS (graphic symbols set) object 527
 *IGCDCT (double-byte character set dictionary) object 527
 *IGCSRT (double-byte character set sort) object 528
 *IGCTBL (double-byte character set table) object 528
 *JOBBD (job description) object 528
 *JOBQ (job queue) object 529
 *JOBSCD (job scheduler) object 530
 *JRN (journal) object 530
 *JRNRCV (journal receiver) object 532
 *LIB (library) object 532
 *LIND (line description) object 533
 *MENU (menu) object 535
 *MODD (mode description) object 535
 *MODULE (module) object 535
 *MSGF (message file) object 536
 *MSGQ (message queue) object 537
 *NODGRP (node group) object 538
 *NODL (node list) object 538
 *NTBD (NetBIOS description) object 538
 *NWID (network interface) object 539
 *NWSD (network server description) object 540

object auditing (*continued*)

*OUTQ (output queue) object 540
 *OVL (overlay) object 541
 *PAGDFN (page definition) object 542
 *PAGSEG (page segment) object 542
 *PDG (print descriptor group) object 542
 *PGM (program) object 542
 *PNLGRP (panel group) object 544
 *PRDAVL (product availability) object 544
 *PRDDFN (product definition) object 545
 *PRDLOD (product load) object 545
 *QMFORM (query manager form) object 545
 *QMORY (query manager query) object 546
 *QRYDFN (query definition) object 546
 *RCT (reference code table) object 547
 *S36 (S/36 machine description) object 558
 *SBSD (subsystem description) object 548
 *SCHIDX (search index) object 549
 *SOCKET (local socket) object 550
 *SPADCT (spelling aid dictionary) object 552
 *SQLPKG (SQL package) object 554
 *SRVPGM (service program) object 554
 *SSND (session description) object 555
 *STMF (stream file) object 555
 *SVRSTG (server storage space) object 555
 *SYMLNK (symbolic link) object 557
 *TBL (table) object 559
 *USRIDX (user index) object 559
 *USRPRF (user profile) object 560
 *USRQ (user queue) object 561
 *USRSPC (user space) object 561
 *VLDL (validation list) object 562
 alert table (*ALRTBL) object 503
 authority holder (*AUTHLR) object 504
 authorization list (*AUTL) object 503
 binding directory (*BDNDIR) object 504
 C locale description (*CLD) object 506
 change request description (*CRQD) object 506
 changing
 command description 310, 313
 chart format (*CHTFMT) object 505
 Class (*CLS) object 507
 class-of-service description (*COSD) object 509
 Command (*CMD) object 507
 common operations 499
 communications side information (*CSI) object 509
 configuration list (*CFGL) object 505

object auditing (*continued*)

connection list (*CNNL) object 508
 controller description (*CTLD) object 510
 cross system product map (*CSPMAP) object 509
 cross system product table (*CSPTBL) object 510
 data area (*DTAARA) object 519
 data dictionary (*DTADCT) object 520
 data queue (*DTAQ) object 520
 definition 286
 device description (*DEVD) object 511
 directory (*DIR) object 512
 displaying 288
 document (*DOC) object 516
 double byte-character set dictionary (*IGCDCT) object 527
 double byte-character set sort (*IGCSRT) object 528
 double byte-character set table (*IGCTBL) object 528
 edit description (*EDTD) object 521
 exit registration (*EXITRG) object 521
 file (*FILE) object 522
 filter (*FTR) object 526
 folder (*FLR) object 516
 font resource (*FNTRSC) object 526
 form definition (*FORMDF) object 526
 forms control table (*FCT) object 522
 graphic symbols set (*GSS) object 527
 job description (*JOBBD) object 528
 job queue (*JOBQ) object 529
 job scheduler (*JOBSCD) object 530
 journal (*JRN) object 530
 journal receiver (*JRNRCV) object 532
 library (*LIB) object 532
 line description (*LIND) object 533
 local socket (*SOCKET) object 550
 menu (*MENU) object 535
 message file (*MSGF) object 536
 message queue (*MSGQ) object 537
 mode description (*MODD) object 535
 module (*MODULE) object 535
 NetBIOS description (*NTBD) object 538
 network interface (*NWID) object 539
 network server description (*NWSD) object 540
 node group (*NODGRP) object 538
 node list (*NODL) object 538
 output queue (*OUTQ) object 540
 overlay (*OVL) object 541
 page definition (*PAGDFN) object 542
 page segment (*PAGSEG) object 542
 panel group (*PNLGRP) object 544
 planning 286
 print descriptor group (*PDG) object 542

object auditing (*continued*)
 product availability (*PRDAVL)
 object 544
 product definition (*PRDDFN)
 object 545
 product load (*PRDLOD) object 545
 program (*PGM) object 542
 query definition (*QRYDFN)
 object 546
 query manager form (*QMFORM)
 object 545
 query manager query (*QMQRQY)
 object 546
 reference code table (*RCT)
 object 547
 S/36 machine description (*S36)
 object 558
 search index (*SCHIDX) object 549
 server storage space (*SVRSTG)
 object 555
 service program (*SRVPGM)
 object 554
 session description (*SSND)
 object 555
 spelling aid dictionary (*SPADCT)
 object 552
 SQL package (*SQLPCK) object 554
 stream file (*STMF) object 555
 subsystem description (*SBSD)
 object 548
 symbolic link (*SYMLNK) object 557
 table (*TBL) object 559
 user index (*USRIDX) object 559
 user profile (*USRPRF) object 560
 user queue (*USRQ) object 561
 user space (*USRSPC) object 561
 validation list (*VLDL) object 562
 object auditing (OBJAUD) parameter
 user profile 112
 object authority
 *ALLOBJ (all object) special
 authority 85
 *SAVSYS (save system) special
 authority 86
 access code commands 449
 access path recovery 350
 Advanced Function Printing
 commands 351
 AF_INET sockets over SNA 352
 alert commands 352
 alert description commands 352
 alert table commands 352
 analyzing 303
 authority holder commands 354
 authorization list commands 354
 backup commands 450
 binding directory 355
 change request description
 commands 355
 changing
 audit journal (QAUDJRN)
 entry 280
 procedures 159
 chart format commands 356
 class commands 356
 class-of-service description
 commands 356

object authority (*continued*)
 cleanup commands 450
 commands 310
 commitment control commands 362
 common object commands 343
 communications side information
 commands 362
 configuration commands 363
 configuration list commands 364
 connection list commands 364
 controller description commands 365
 cryptography commands 366
 data area commands 367
 data queue commands 368
 definition 132
 detail, displaying (*EXPERT user
 option) 106, 107, 108
 device description commands 368
 directory commands 371
 directory server commands 371
 display station pass-through
 commands 372
 displaying 303, 310
 displaying detail (*EXPERT user
 option) 106, 107, 108
 distribution commands 373
 distribution list commands 374
 DNS commands 378
 document commands 374
 document library object (DLO)
 commands 374
 Domain Name System
 commands 378
 double-byte character set
 commands 380
 edit description commands 380
 editing 159, 310
 emulation commands 370
 extended wireless LAN configuration
 commands 381
 file commands 381
 filter commands 388
 finance commands 389
 format on save media 247
 forms control table commands 470
 granting 310
 affect on previous authority 162
 multiple objects 162
 graphical operations 389
 graphics symbol set commands 390
 hardware commands 470
 host server 390
 information search index
 commands 411
 interactive data definition 410
 job commands 412
 job description commands 415
 job queue commands 416
 job schedule commands 417
 journal commands 417
 journal receiver commands 421
 Kerberos commands 422
 language commands 424
 library commands 430
 licensed program commands 435
 line description commands 435
 locale commands 437

object authority (*continued*)
 mail server framework
 commands 438
 media commands 438
 menu commands 439
 message description commands 441
 message file commands 441
 message queue commands 441
 migration commands 442
 mode description commands 442
 NetBIOS description commands 443
 network attribute commands 444
 network interface description
 commands 446
 Network Server commands 446
 network server configuration
 commands 448
 network server description
 commands 448
 node list commands 449
 online education commands 450
 Operational Assistant commands 450
 optical commands 451
 output queue commands 454
 package commands 455
 panel group commands 439
 performance commands 455
 printer output commands 481
 printer writer commands 496
 problem commands 462
 program commands 463
 program temporary fix (PTF)
 commands 475
 programming language
 commands 424
 PTF (program temporary fix)
 commands 475
 Query Management/400
 commands 466
 question and answer commands 468
 reader commands 469
 relational database directory
 commands 469
 reply list commands 485
 required for *CMD commands 361
 resource commands 470
 revoking 310
 RJE (remote job entry)
 commands 470
 search index commands 411
 security attributes commands 474
 security audit commands 474
 server authentication 475
 service commands 475
 session commands 470
 spelling aid dictionary
 commands 480
 sphere of control commands 480
 spooled file commands 481
 storing 246, 247
 subsystem commands 483
 system commands 485
 system reply list commands 485
 system value commands 486
 System/36 environment
 commands 486
 table commands 489

- object authority (*continued*)
 - TCP/IP (Transmission Control Protocol/Internet Protocol) commands 489
 - text index commands 449
 - token-ring commands 437
 - user index, queue, and space commands 491
 - user permission commands 449
 - user profile commands 491, 492
 - validation list 495
 - workstation customizing object commands 496
 - writer commands 496
- object description
 - displaying 310
- object domain
 - definition 15
 - displaying 15
- object integrity
 - auditing 304
- object management (*OBJMGT) audit level 275
- object management (OM) journal entry type 275
- object ownership
 - adopted authority 151
 - ALWOBJDIF (allow object differences) parameter 250
 - changes when restoring 249
 - changing
 - audit journal (QAUDJRN) entry 281
 - authority required 143
 - command description 310
 - methods 163
 - moving application to production 242
 - deleting
 - owner profile 122, 143
 - description 143
 - flowchart 175
 - group profile 143
 - managing
 - owner profile size 143
 - private authority 131
 - responsibilities 261
 - restoring 245, 249
 - saving 245
 - working with 163, 310
- object reference (*OBJREF)
 - authority 132, 340
- object restore (OR) journal entry type 276
- object signing 3
- objective
 - availability 1
 - confidentiality 1
 - integrity 1
- objects by primary group
 - working with 144
- office services
 - action auditing 534
- office services (*OFCSRVR) audit level 275, 514, 534
- OM (object management) journal entry type 275
- on behalf
 - auditing 534
- online education
 - object authority required for commands 450
- online help information
 - displaying full screen (*HLPFULL user option) 108
- operating system
 - security installation 255
- operational (*OBJOPR) authority 132, 339
- Operational Assistant Attention Program
 - Attention-key-handling program 104
- Operational Assistant commands
 - object authority required for commands 450
- OPNDBF (Open Database File) command
 - object authority required 386
- OPNQRYF (Open Query File) command
 - object authority required 386
- OPRCTL (operator control)
 - parameter 212
- optical
 - object authority required for commands 451
- OR (object restore) journal entry type 276
- output
 - object authority required for commands 481
- output priority 218
- output queue
 - *JOBCTL (job control) special authority 86
 - *OPRCTL (operator control) parameter 86
 - *SPLCTL (spool control) special authority 86
 - AUTCHK (authority to check) parameter 212
 - authority to check (AUTCHK) parameter 212
 - changing 211
 - creating 211, 214
 - display data (DSPDTA) parameter 211
 - DSPDTA (display data) parameter 211
 - object authority required for commands 454
 - operator control (OPRCTL) parameter 212
 - OPRCTL (operator control) parameter 212
 - printing security-relevant parameters 316, 713
 - securing 211, 214
 - user profile 103
 - working with description 211
- output queue (*OUTQ) auditing 540
- output queue (OUTQ) parameter
 - user profile 103
- OUTQ (output queue) parameter
 - user profile 103
- overlay (*OVL) auditing 541
- Override commands 239
- OVRMSGF (Override with Message File)
 - command
 - object auditing 537
- OW (ownership change) file layout 640
- OW (ownership change) journal entry type 281
- owner 145
 - OWNER user profile parameter description 143
- OWNER (owner) parameter
 - user profile 145
- owner authority
 - flowchart 175
- ownership
 - adopted authority 151
 - ALWOBJDIF (allow object differences) parameter 250
 - assigning to new object 145
 - change when restoring
 - audit journal (QAUDJRN) entry 276
 - changes when restoring 249
 - changing
 - audit journal (QAUDJRN) entry 281
 - authority required 143
 - methods 163
 - default (QDFTOWN) user profile 145
 - deleting
 - owner profile 122, 143
 - description 143
 - device description 203
 - flowchart 175
 - group profile 143
 - introduction 5
 - managing
 - owner profile size 143
 - new object 145
 - object
 - managing 242
 - private authority 131
 - OWNER user profile parameter description 97
 - printer output 211
 - restoring 245, 249
 - saving 245
 - spooled file 211
 - working with 163
 - workstation 203
- ownership change (OW) file layout 640
- ownership change (OW) journal entry type 281
- ownership change for restored object (RO) file layout 657
- ownership change for restored object (RO) journal entry type 276
- ownership, object
 - responsibilities 261

P

- PA (program adopt) file layout 645
- PA (program adopt) journal entry type 281
- package
 - object authority required for commands 455

PAGDOC (Paginate Document) command
 object auditing 518
 object authority required 375
 page definition (*PAGDFN) auditing 542
 page down key
 reversing (*ROLLKEY user option) 108
 page segment (*PAGSEG) auditing 542
 page up key
 reversing (*ROLLKEY user option) 108
 panel group
 object authority required for commands 439
 panel group (*PNLGRP) auditing 544
 parameter
 validating 17
 partial (*PARTIAL) limit capabilities 83
 pass-through
 controlling sign-on 32
 target profile change
 audit journal (QAUDJRN) entry 281
 password
 all-numeric 76
 allowing users to change 259
 approval program
 example 61, 62
 QPWDVLDPGM system value 60
 requirements 61
 security risk 61
 auditing
 DST (dedicated service tools) 258
 user 259
 changes when restoring profile 248
 changing
 description 311
 DST (dedicated service tools) 311
 enforcing password system values 47
 setting password equal to profile name 76
 checking 128, 311
 checking for default 707
 commands for working with 311
 communications 51
 document
 DOCPWD user profile parameter 100
 DST (dedicated service tools)
 auditing 258
 changing 129
 encrypting 76
 equal to user profile name 47, 76
 expiration interval
 auditing 259
 PWDEXPITV user profile parameter 91
 QPWDEXPITV system value 47
 expiration interval (QPWDEXPITV) system value
 value set by CFGSYSSEC command 716
 expiration warning
 QPWDEXPWRN system value 48
 expired (PWDEXP) parameter 77
 password (*continued*)
 IBM-supplied user profile
 auditing 258
 changing 129
 immediate expiration 47
 incorrect
 audit journal (QAUDJRN) entry 271
 length
 maximum (QPWDMAXLEN) system value 51
 minimum (QPWDMINLEN) system value 50
 limit repeated characters (QPWDLMTREP) system value
 value set by CFGSYSSEC command 716
 local password management
 LCLPWDMGT user profile parameter 92
 lost 76
 maximum length (QPWDMAXLEN) system value 51
 maximum length (QPWDMAXLEN) system value
 value set by CFGSYSSEC command 716
 minimum length (QPWDMINLEN) system value 50
 minimum length (QPWDMINLEN) system value
 value set by CFGSYSSEC command 716
 network
 audit journal (QAUDJRN) entry 271
 position characters (QPWDPOSDIF) system value 53
 possible values 77
 preventing
 adjacent digits (QPWDLMTAJC) system value 52
 repeated characters 53
 trivial 46, 259
 use of words 52
 PWDEXP (set password to expired) 77
 QPGMR (programmer) user profile 717
 QSRV (service) user profile 717
 QSRVBAS (basic service) user profile 717
 QSYSOPR (system operator) user profile 717
 QUSER (user) user profile 717
 recommendations 77, 78
 require numeric character (QPWDRQDDGT) system value
 value set by CFGSYSSEC command 716
 require position difference (QPWDPOSDIF) system value
 value set by CFGSYSSEC command 716
 password (*continued*)
 required difference (QPWDRQDDIF) system value
 value set by CFGSYSSEC command 716
 requiring
 change (PWDEXPITV parameter) 91
 change (QPWDEXPITV system value) 47
 complete change 53
 different (QPWDRQDDIF system value) 51
 numeric character 54
 resetting
 DST (dedicated service tools) 277
 user 76
 restrict adjacent characters (QPWDLMTAJC) system value
 value set by CFGSYSSEC command 716
 restrict characters (QPWDLMTCHR) system value
 value set by CFGSYSSEC command 716
 restricting
 adjacent digits (QPWDLMTAJC) system value 52
 characters 52
 repeated characters 53
 rules 76
 setting to expired (PWDEXP) 77
 system 131
 system values
 overview 46
 trivial
 preventing 46, 259
 user profile 76
 validation exit program
 example 62
 validation program
 example 61
 QPWDVLDPGM system value 60
 requirements 61
 security risk 61
 validation program (QPWDVLDPGM) system value
 value set by CFGSYSSEC command 716
 password (PW) journal entry type 271
 password characters 49
 password expiration interval (PWDEXPITV)
 recommendations 91
 password expiration interval (QPWDEXPITV) system value
 auditing 259
 Password Level (QPWDLVL) description 48
 Password Level (QPWDLVL) system value
 description 48
 password required difference (QPWDRQDDIF) system value
 value set by CFGSYSSEC command 716

password validation program
(QPWDVLDPGM) system value 60

passwords
password levels 302

Passwords 48

path name
displaying 164

PC (personal computer)
preventing access 215

PC Organizer
allowing for limit capabilities user 83
disconnecting (QINACTMSGQ system
value) 28

PC Support access (PCSACC) network
attribute 262

PC text-assist function (PCTA)
disconnecting (QINACTMSGQ system
value) 28

PCSACC (client request access) network
attribute 215

PCSACC (PC Support access) network
attribute 262

performance
class 217
job description 218
job scheduling 218
object authority required for
commands 455
output priority 218
pool 218
priority limit 218
restricting jobs to batch 218
routing entry 218
run priority 217
storage
pool 218
subsystem description 218
time slice 217

performance tuning
security 217

permission
definition 134

PG (primary group change) file
layout 647

PG (primary group change) journal entry
type 281

physical security 2
auditing 258
planning 258

PING (Verify TCP/IP Connection)
command
object authority required 490

PKGPRDDST (Package Product
Distribution) command
authorized IBM-supplied user
profiles 334

planning
application programmer security 242
audit
system values 288
auditing
actions 263
objects 286
overview 263
checklist for 257
command security 235
file security 236

planning (*continued*)
group profiles 239
library design 225
menu security 228
multiple groups 240
password controls 259
physical security 258
primary group 240
security 1
system programmer security 243

planning password level changes
changing password levels (0 to 1) 222
changing password level from 1 to
0 225
changing password level from 2 to
0 224
changing password level from 2 to
1 224
changing password level from 3 to
0 224
changing password level from 3 to
1 224
changing password level from 3 to
2 224
changing password levels
planning level changes 221, 222
changing password levels (2 to
3) 223
decreasing password levels 224, 225
increasing password level 222
QPWDLVL changes 221, 222

PO (printer output) file layout 650

PO (printer output) journal entry
type 276

pool 218

position characters (QPWDPOSDF)
system value 53

preventing
access
DDM request (DDM) 216
iSeries Access 215
modification of internal control
blocks 20
performance abuses 217
remote job submission 214
sign-on without user ID and
password 261
trivial passwords 46, 259
unauthorized access 262
unauthorized programs 262

preventing large profiles
planning applications 226

primary group
changes when restoring 250
changing 144
audit journal (QAUDJRN)
entry 281
command description 310
changing during restore
audit journal (QAUDJRN)
entry 277
definition 131
deleting
profile 122
description 144
introduction 5
new object 145

primary group (*continued*)
planning 240
restoring 245, 250
saving 245
working with 124, 164
working with objects 310

primary group authority
authority checking example 187

primary group change (PG) file
layout 647

primary group change (PG) journal entry
type 281

primary group change for restored object
(RZ) file layout 662

primary group change for restored object
(RZ) journal entry type 277

Print Adopting Objects (PRTADPOBJ)
command
description 711

Print Communications Security
(PRTCMNSEC) command
description 316, 711

print descriptor group (*PDG)
auditing 542

print device (DEV) parameter
user profile 103

Print Job Description Authority
(PRTJOBDAUT) command 316
description 711

Print Private Authorities (PRTPVTAUT)
command 316
authorization list 711
description 713

Print Publicly Authorized Objects
(PRTPUBAUT) command 316
description 713

Print Queue Authority (PRTQAUT)
command
description 316, 713

Print Subsystem Description
(PRTSBSDAUT) command
description 711

Print Subsystem Description Authority
(PRTSBSDAUT) command
description 316

Print System Security Attributes
(PRTSYSSECA) command
description 316, 711

Print Trigger Programs (PRTTRGPGM)
command
description 316, 711

Print User Objects (PRTUSROBJ)
command
description 316, 711

Print User Profile (PRTUSRPRF)
command
description 711

printed output (*PRTDTA) audit
level 276

printer
user profile 103
virtual
securing 216

printer output
*JOBCTL (job control) special
authority 86

printer output (*continued*)

- *SPLCTL (spool control) special authority 86
- object authority required for commands 481
- owner 211
- securing 211

printer output (PO) file layout 650

printer output (PO) journal entry type 276

printer writer

- object authority required for commands 496

printing 108

- adopted object information 711
- audit journal (QAUDJRN) entry 276
- audit journal entries 711
- authority holder 316
- authorization list information 711
- communications 316
- list of non-IBM objects 316, 711
- list of subsystem descriptions 316
- network attributes 316, 711
- notification (*PRTMSG user option) 108
- publicly authorized objects 713
- security 211
- security-relevant communications settings 711
- security-relevant job queue parameters 316, 713
- security-relevant output queue parameters 316, 713
- security-relevant subsystem description values 711
- sending message (*PRTMSG user option) 108
- system values 258, 316, 711
- trigger programs 316, 711

printing message (*PRTMSG) user option 108

priority 218

priority limit (PTYLMT) parameter

- recommendations 96
- user profile 95

private authorities

- authority cache 197

private authority

- definition 131
- flowchart 174
- object ownership 131
- planning applications 226
- restoring 245, 250
- saving 245

privilege

- definition 131

problem

- object authority required for commands 462

problem analysis

- remote service attribute (QRMTSRVATR) system value 39

processor keylock 258

processor password 131

product availability (*PRDAVL) auditing 544

product definition (*PRDDFN)

- auditing 545

product library

- library list 209
- description 207
- recommendations 209

product load (*PRDLOD) auditing 545

profile

- action auditing (AUDLVL) 113
- analyzing with query 301
- auditing
 - *ALLOBJ special authority 260
 - authority to use 261
- auditing membership 260
- auditing password 259
- AUDLVL (action auditing) 113
- changing 311
- default values table 319
- group 259, 260
 - auditing 260
 - introduction 4, 74
 - naming 76
 - object ownership 143
 - password 76
 - planning 239
 - resource security 5
- handle
 - audit journal (QAUDJRN) entry 281

IBM-supplied

- auditing 258
- authority profile (QAUTPROF) 321
- automatic install (QLPAUTO) 321
- basic service (QSRVBAS) 321
- BRM user profile (QBRMS) 321
- database share (QDBSHR) 321
- default owner (QDFTOWN) 321
- distributed systems node executive (QDSNX) 321
- document (QDOC) 321
- finance (QFNC) 321
- IBM authority profile (QAUTPROF) 321
- install licensed programs (QLPINSTALL) 321
- mail server framework (QMSF) 321
- network file system (QNFS) 321
- programmer (QPGMR) 321
- QAUTPROF (IBM authority profile) 321
- QBRMS (BRM user profile) 321
- QDBSHR (database share) 321
- QDFTOWN (default owner) 321
- QDOC (document) 321
- QDSNX (distributed systems node executive) 321
- QFNC (finance) 321
- QGATE (VM/MVS bridge) 321
- QLPAUTO (licensed program automatic install) 321
- QLPINSTALL (licensed program install) 321
- QMSF (mail server framework) 321

profile (*continued*)

IBM-supplied (*continued*)

- QNFSANON (network file system) 321
- QPGMR (programmer) 321
- QRJE (remote job entry) 321
- QSECOFR (security officer) 321
- QSNADS (Systems Network Architecture distribution services) 321
- QSPL (spool) 321
- QSPLJOB (spool job) 321
- QSRV (service) 321
- QSRVBAS (service basic) 321
- QSYS (system) 321
- QSYSOPR (system operator) 321
- QTCP (TCP/IP) 321
- QTMLPD (TCP/IP printing support) 321
- QTSTRQS (test request) 321
- QUSER (workstation user) 321
- remote job entry (QRJE) 321
- restricted commands 327
- security officer (QSECOFR) 321
- service (QSRV) 321
- service basic (QSRVBAS) 321
- SNA distribution services (QSNADS) 321
- spool (QSPL) 321
- spool job (QSPLJOB) 321
- system (QSYS) 321
- system operator (QSYSOPR) 321
- TCP/IP (QTCP) 321
- TCP/IP printing support (QTMLPD) 321
- test request (QTSTRQS) 321
- VM/MVS bridge (QGATE) 321
- workstation user (QUSER) 321

OBJAUD (object auditing) 112

object auditing (OBJAUD) 112

QDFTOWN (default owner)

- restoring programs 253

swap

- audit journal (QAUDJRN) entry 281

user 112, 113, 301

- accounting code (ACGCDE) 100
- ACGCDE (accounting code) 100
- assistance level (ASTLVL) 80
- ASTLVL (assistance level) 80
- ATNPGM (Attention-key-handling program) 104
- Attention-key-handling program (ATNPGM) 104
- auditing 260
- authority (AUT) 112
- automatic creation 73
- CCSID (coded character set identifier) 106
- changing 122
- CHRIDCTL (user options) 106
- CNTRYID (country or region identifier) 105
- coded character set identifier (CCSID) 106
- country or region identifier (CNTRYID) 105

profile (*continued*)
 user (*continued*)
 CURLIB (current library) 81
 current library (CURLIB) 81
 delivery (DLVRY) 102
 description (TEXT) 84
 DEV (print device) 103
 display sign-on information (DSPSGNINF) 91
 DLVRY (message queue delivery) 102
 DOCPWD (document password) 100
 document password (DOCPWD) 100
 DSPSGNINF (display sign-on information) 91
 eim association (EIMASSOC) 110
 group (GRPPRF) 97
 group authority (GRPAUT) 98, 143
 group authority type (GRPAUTTYP) 98
 group identification number(gid) 109
 GRPAUT (group authority) 98, 143
 GRPAUTTYP (group authority type) 98
 GRPPRF (group) 97
 home directory (HOMEDIR) 109
 IBM-supplied 128
 initial menu (INLMNU) 82
 initial program (INLPGM) 81
 INLMNU (initial menu) 82
 INLPGM (initial program) 81
 introduction 4
 job description (JOBDD) 96
 JOBDD (job description) 96
 KBDBUF (keyboard buffering) 93
 keyboard buffering (KBDBUF) 93
 LANGID (language identifier) 105
 language identifier (LANGID) 105
 large, examining 302
 LCLPDMGT (local password management) 92
 limit capabilities 83, 260
 limit device sessions (LMTDEVSSN) 93
 listing inactive 302
 listing selected 302
 listing users with command capability 302
 listing users with special authorities 302
 LMTCPB (limit capabilities) 83
 LMTDEVSSN (limit device sessions) 93
 local password management (LCLPDMGT) 92
 LOCALE (user options) 107
 maximum storage (MAXSTG) 94
 MAXSTG (maximum storage) 94
 message queue (MSGQ) 101

profile (*continued*)
 user (*continued*)
 message queue delivery (DLVRY) 102
 message queue severity (SEV) 102
 MSGQ (message queue) 101
 name (USRPRF) 75
 naming 75
 output queue (OUTQ) 103
 OUTQ (output queue) 103
 owner of objects created (OWNER) 97, 143
 password 76
 password expiration interval (PWDEXPITV) 91
 print device (DEV) 103
 priority limit (PTYLMT) 95
 PTYLMT (priority limit) 95
 public authority (AUT) 112
 PWDEXP (set password to expired) 77
 PWDEXPITV (password expiration interval) 91
 renaming 126
 retrieving 128
 roles 73
 set password to expired (PWDEXP) 77
 SETJOBATR (user options) 107
 SEV (message queue severity) 102
 severity (SEV) 102
 sort sequence (SRTSEQ) 105
 SPCAUT (special authority) 84
 SPCENV (special environment) 89
 special authority (SPCAUT) 84
 special environment (SPCENV) 89
 SRTSEQ (sort sequence) 105
 status (STATUS) 78
 SUPGRPPRF (supplemental groups) 99
 supplemental groups (SUPGRPPRF) 99
 System/36 environment 89
 text (TEXT) 84
 user class (USRCLS) 79
 user expiration date (USREXPDATE) 111
 user expiration interval (USREXPITV) 111
 user identification number 108
 user options (CHRIDCTL) 106
 user options (LOCALE) 107
 user options (SETJOBATR) 107
 user options (USROPT) 106, 107, 108
 USRCLS (user class) 79
 USREXPDATE (user expiration date) 111
 USREXPITV (user expiration interval) 111
 USROPT (user options) 106, 107, 108
 USRPRF (name) 75

profile swap (PS) file layout 651
 profile swap (PS) journal entry type 281
 program
 adopt authority function auditing 303
 adopted authority
 audit journal (QAUDJRN) entry 281
 auditing 261
 creating 151
 displaying 151
 ignoring 152
 purpose 149
 restoring 253
 transferring 150
 bound
 adopted authority 151
 changing
 specifying USEADPAUT parameter 152
 creating
 adopted authority 151
 displaying
 adopted authority 151
 ignoring
 adopted authority 152
 object authority required for commands 463
 password validation example 61
 QPWDVLDPGM system value 60
 requirements 61
 password validation exit example 62
 preventing
 unauthorized 262
 program failure
 audit journal (QAUDJRN) entry 281
 restoring
 adopted authority 253
 risks 252
 validation value 17
 service
 adopted authority 151
 transferring
 adopted authority 150
 translation 17
 trigger
 listing all 316
 unauthorized 262
 working with user profiles 128
 program (*PGM) auditing 542
 program adopt (PA) file layout 645
 program adopt (PA) journal entry type 281
 program adopt function 261
 program failure
 auditing 303
 restoring programs
 audit journal (QAUDJRN) entry 276
 program failure (*PGMFAIL) audit level 276
 program state
 definition 15
 displaying 15

program temporary fix (PTF)
 object authority required for
 commands 475

program validation
 definition 17

program-described file
 holding authority when deleted 153

programmer
 application
 planning security 242
 auditing access to production
 libraries 260
 system
 planning security 243

programmer (QPGMR) user profile
 default values 321
 device description owner 203

programming language
 object authority required for
 commands 424

programs that adopt
 displaying 303

protecting
 backup media 258

protection
 enhanced hardware storage 17

PRTACTRPT
 authorized IBM-supplied user
 profiles 334

PRTACTRPT (Print Activity Report)
 command
 object authority required 459

PRTADPOBJ (Print Adopted Object)
 command
 object authority required 345

PRTADPOBJ (Print Adopting Objects)
 command
 description 711

PRTCADMRE command
 object authority required 359

PRTCMDUSG (Print Command Usage)
 command
 object auditing 507, 543
 object authority required 464

PRTCMNSEC (Print Communication
 Security) command
 object authority required 366

PRTCMNSEC (Print Communications
 Security) command
 description 316, 711
 object authority required 370, 437

PRTCMNTRC (Print Communications
 Trace) command
 authorized IBM-supplied user
 profiles 334
 object authority required 476

PRTCPTTRPT
 authorized IBM-supplied user
 profiles 334

PRTCPTTRPT (Print Component Report)
 command
 object authority required 459

PRTCSPAPP (Print CSP/AE Application)
 command
 object auditing 544

PRTDEVADR (Print Device Addresses)
 command
 object auditing 510
 object authority required 363

PRTDOC (Print Document) command
 object auditing 516

PRTDSKINF
 authorized IBM-supplied user
 profiles 334

PRTDSKINF (Print Disk Activity
 Information) command
 object authority required 450

PRTERRLOG
 authorized IBM-supplied user
 profiles 334

PRTERRLOG (Print Error Log) command
 object authority required 476

PRTINTDTA
 authorized IBM-supplied user
 profiles 334

PRTINTDTA (Print Internal Data)
 command
 object authority required 476

PRTIPSCFG (Print IP over SNA
 Configuration) command
 object authority required 352

PRTJOBDAUT (Print Job Description
 Authority) command
 description 316, 711
 object authority required 415

PRTJOBTRPT
 authorized IBM-supplied user
 profiles 334

PRTJOBTRPT (Print Job Report) command
 object authority required 459

PRTJOBTRC
 authorized IBM-supplied user
 profiles 334

PRTJOBTRC (Print Job Trace) command
 object authority required 459

PRTJVMJOB command
 object authority required 412

PRTLCKRPT
 authorized IBM-supplied user
 profiles 334

PRTLCKRPT (Print Lock Report)
 command
 object authority required 459

PRTPEXRPT (Print Performance Explorer
 Report) command
 object authority required 459

PRTPOLRPT
 authorized IBM-supplied user
 profiles 334

PRTPOLRPT (Print Pool Report)
 command
 object authority required 459

PRTPRFINT (Print Profile Internals)
 command
 authorized IBM-supplied user
 profiles 334

PRTPUBAUT (Print Public Authorities)
 command
 object authority required 345

PRTPUBAUT (Print Publicly Authorized
 Objects) command
 description 316, 711

PRTPVTAUT (Print Private Authorities)
 command
 authorization list 711
 description 316, 713
 object authority required 345

PRTQAUT (Print Queue Authorities)
 command
 object authority required 416, 454

PRTQAUT (Print Queue Authority)
 command
 description 316, 713

PRTRSCRPT
 authorized IBM-supplied user
 profiles 334

PRTRSCRPT (Print Resource Report)
 command
 object authority required 459

PRTSBSDAUT (Print Subsystem
 Description Authority) command
 description 316
 object authority required 484

PRTSBSDAUT (Print Subsystem
 Description) command
 description 711

PRTSQLINF (Print SQL Information)
 command
 object auditing 544, 554

PRTSQLINF (Print Structured Query
 Language Information) command
 object authority required 455

PRTSYSRPT
 authorized IBM-supplied user
 profiles 334

PRTSYSRPT (Print System Report)
 command
 object authority required 460

PRTSYSSECA (Print System Security
 Attribute) command
 object authority required 474

PRTSYSSECA (Print System Security
 Attributes) command
 description 316, 711

PRTTNSRPT
 authorized IBM-supplied user
 profiles 334

PRTTNSRPT (Print Transaction Report)
 command
 object authority required 460

PRTTRC (Print Trace) command
 object authority required 476

PRTTRCRPT
 authorized IBM-supplied user
 profiles 334

PRTTRGPGM (Print Trigger Program)
 command
 object authority required 386

PRTTRGPGM (Print Trigger Programs)
 command
 description 316, 711

PRTUSROBJ (Print User Object)
 command
 object authority required 345

PRTUSROBJ (Print User Objects)
 command
 description 316, 711

PRTUSRPRF (Print User Profile)
 command
 description 711
 object authority required 494
 PS (profile swap) file layout 651
 PS (profile swap) journal entry type 281
 PTF (program temporary fix)
 object authority required for
 commands 475
 PTYLMT (priority limit) parameter
 recommendations 96
 user profile 95
 public authority
 authority checking example 189, 191
 definition 131
 flowchart 181
 library 157
 new objects
 description 139
 specifying 157
 printing 713
 restoring 245, 250
 revoking 316, 715
 revoking with RVKPUBAUT
 command 718
 saving 245
 user profile
 recommendation 112
 PW (password) journal entry type 271
 PWDEXP (set password to expired)
 parameter 77
 PWDEXPITV (password expiration
 interval) parameter 91
 PWRDWN SYS (Power Down System)
 command
 authorized IBM-supplied user
 profiles 334
 object authority required 485

Q

QADSM (ADSM) user profile 321
 QAFDFTUSR (AFDFTUSR) user
 profile 321
 QAFOWN (AFOWN) user profile 321
 QAFUSR (AFUSR) user profile 321
 QALWOBJRST (allow object restore
 option) system value 45
 QALWOBJRST (allow object restore)
 system value
 value set by CFGSYSSEC
 command 716
 QALWUSRDMN (allow user objects)
 system value 19, 25
 QASYADJE (auditing change) file
 layout 570
 QASYAFJE (authority failure) file
 layout 573
 QASYAPJE (adopted authority) file
 layout 579
 QASYAUJ5 (attribute change) file
 layout 579
 QASYCAJE (authority change) file
 layout 580
 QASYCDJE (command string) file
 layout 583
 QASYCOJE (create object) file
 layout 584
 QASYCPJE (user profile change) file
 layout 586
 QASYCQJE (*CRQD change) file
 layout 589
 QASYCUJ4 (Cluster Operations) file
 layout 589
 QASYCVJ4 (connection verification) file
 layout 591
 QASYCYJ4 (cryptographic configuration)
 file layout 593
 QASYCYJ4 (Directory Server) file
 layout 596
 QASYDOJE (delete operation) file
 layout 601
 QASYDSJE (IBM-Supplied Service Tools
 User ID Reset) file layout 603
 QASYEVJE (EV) file layout 604
 QASYGRJ4 (generic record) file
 layout 605
 QASYGSJE (give descriptor) file
 layout 610
 QASYGSJE (Internet security
 management) file layout 617
 QASYGSJE (interprocess communication
 actions) file layout 614
 QASYIRJ4 (IP rules actions) file
 layout 615
 QASYJDJE (job description change) file
 layout 619
 QASYJSJE (job change) file layout 620
 QASYKFJ4 (key ring file) file layout 625
 QASYLDJE (link, unlink, search
 directory) file layout 628
 QASYMLJE (mail actions) file
 layout 630
 QASYNAJE (network attribute change)
 file layout 630
 QASYNDJE (APPN directory) file
 layout 631
 QASYNEJE (APPN end point) file
 layout 632
 QASYO1JE (optical access) file
 layout 642, 643
 QASYO3JE (optical access) file
 layout 644
 QASYOMJE (object management) file
 layout 632
 QASYORJE (object restore) file
 layout 636
 QASYOWJE (ownership change) file
 layout 640
 QASYPAJE (program adopt) file
 layout 645
 QASYPGJE (primary group change) file
 layout 647
 QASYPOJE (printer output) file
 layout 650
 QASYPSJE (profile swap) file layout 651
 QASYPWJE (password) file layout 653
 QASYRAJE (authority change for restored
 object) file layout 654
 QASYRJE (restoring job description) file
 layout 656
 QASYROJE (ownership change for object
 program) file layout 657
 QASYRPJE (restoring programs that
 adopt authority) file layout 659
 QASYRQJE (restoring *CRQD that adopts
 authority) file layout 661
 QASYRUJE (restore authority for user
 profile) file layout 661
 QASYRZJE (primary group change for
 restored object) file layout 662
 QASYSDJE (change system distribution
 directory) file layout 664
 QASYSEJE (change of subsystem routing
 entry) file layout 665
 QASYSFJE (action to spooled file) file
 layout 666
 QASYSGJ4() file layout 670, 671
 QASYSMJE (systems management
 change) file layout 673
 QASYSOJ4 (server security user
 information actions) file layout 674
 QASYSTJE (service tools action) file
 layout 675
 QASYSVJE (action to system value) file
 layout 680
 QASYVAJE (changing access control list)
 file layout 681
 QASYVCJE (connection start and end)
 file layout 681
 QASYVFJE (close of server files) file
 layout 682
 QASYVLJE (account limit exceeded) file
 layout 683
 QASYVNJE (network log on and off) file
 layout 684
 QASYVOJ4 (validation list) file
 layout 685
 QASYVPE (network password error) file
 layout 686
 QASYVRJE (network resource access) file
 layout 687
 QASYVSJE (server session) file
 layout 688
 QASYVUJE (network profile change) file
 layout 689
 QASYVVJE (service status change) file
 layout 690
 QASYX0JE (kerberos authentication) file
 layout 691
 QASYXCJE (change to DLO object) file
 layout 698
 QASYXRJE (read of DLO object) file
 layout 699
 QASYZCJE (change to object) file
 layout 700
 QASYZRJE (read of object) file
 layout 703
 QATNPGM (Attention-key-handling
 program) system value 104
 QAUDCTL (audit control) system value
 changing 315, 709
 displaying 315, 709
 QAUDCTL (auditing control) system
 value
 overview 66
 QAUDENDACN (auditing end action)
 system value 66, 289
 QAUDFRCLVL (auditing force level)
 system value 67, 288

- QAUDJRN (audit) journal 281, 284, 499
- AD (auditing change) entry type 280
 - AD (auditing change) file layout 570
 - AF (authority failure) entry type 276
 - default sign-on violation 16
 - description 270
 - hardware protection violation 17
 - job description violation 16
 - program validation 18
 - restricted instruction 18
 - unsupported interface 16, 18
 - AF (authority failure) file layout 573
 - analyzing
 - with query 296
 - AP (adopted authority) entry type 275
 - AP (adopted authority) file layout 579
 - AU (attribute change) file layout 579
 - auditing level (QAUDLVL) system value 67
 - auditing level extension (QAUDLVL2) system value 69
 - automatic cleanup 293
 - CA (authority change) entry type 280
 - CA (authority change) file layout 580
 - CD (command string) entry type 272
 - CD (command string) file layout 583
 - changing receiver 294
 - CO (create object) entry type 144, 272
 - CO (create object) file layout 584
 - CP (user profile change) entry type 277
 - CP (user profile change) file layout 586
 - CQ (*CRQD change) file layout 589
 - CQ (change *CRQD object) entry type 277
 - creating 291
 - CU(Cluster Operations) file layout 589
 - CV(connection verification) file layout 591
 - CY(cryptographic configuration) file layout 593
 - damaged 292
 - detaching receiver 293, 294
 - DI(Directory Server) file layout 596
 - displaying entries 263, 295
 - DO (delete operation) entry type 272
 - DO (delete operation) file layout 601
 - DS (DST password reset) entry type 277
 - DS (IBM-Supplied Service Tools User ID Reset) file layout 603
 - error conditions 66
 - EV (Environment variable) file layout 604
 - force level 67
 - GR(generic record) file layout 605
 - GS (give descriptor) file layout 610
 - introduction 262
 - IP (Interprocess Communication actions) file layout 614
 - IP (interprocess communications) entry type 271
- QAUDJRN (audit) journal (*continued*)
- IR(IP rules actions) file layout 615
 - IS (Internet security management) file layout 617
 - JD (job description change) entry type 281
 - JD (job description change) file layout 619
 - JS (job change) entry type 273
 - JS (job change) file layout 620
 - KF (key ring file) file layout 625
 - LD (link, unlink, search directory) file layout 628
 - managing 292
 - methods for analyzing 295
 - ML (mail actions) entry type 275
 - ML (mail actions) file layout 630
 - NA (network attribute change) entry type 281
 - NA (network attribute change) file layout 630
 - ND (APPN directory) file layout 631
 - NE (APPN end point) file layout 632
 - O1 (optical access) file layout 642, 643
 - O3 (optical access) file layout 644
 - OM (object management) entry type 275
 - OM (object management) file layout 632
 - OR (object restore) entry type 276
 - OR (object restore) file layout 636
 - OW (ownership change) entry type 281
 - OW (ownership change) file layout 640
 - PA (program adopt) entry type 281
 - PA (program adopt) file layout 645
 - PG (primary group change) entry type 281
 - PG (primary group change) file layout 647
 - PO (printer output) entry type 276
 - PO (printer output) file layout 650
 - PS (profile swap) entry type 281
 - PS (profile swap) file layout 651
 - PW (password) entry type 271
 - PW (password) file layout 653
 - RA (authority change for restored object) entry type 276
 - RA (authority change for restored object) file layout 654
 - receiver storage threshold 293
 - RJ (restoring job description) entry type 276
 - RJ (restoring job description) file layout 656
 - RO (ownership change for restored object) entry type 276
 - RO (ownership change for restored object) file layout 657
 - RP (restoring programs that adopt authority) entry type 276
 - RP (restoring programs that adopt authority) file layout 659
 - RQ (restoring *CRQD object that adopts authority) file layout 661
- QAUDJRN (audit) journal (*continued*)
- RQ (restoring *CRQD object) entry type 277
 - RU (restore authority for user profile) entry type 277
 - RU (restore authority for user profile) file layout 661
 - RZ (primary group change for restored object) entry type 277
 - RZ (primary group change for restored object) file layout 662
 - SD (change system distribution directory) entry type 275
 - SD (change system distribution directory) file layout 664
 - SE (change of subsystem routing entry) entry type 282
 - SE (change of subsystem routing entry) file layout 665
 - SF (action to spooled file) file layout 666
 - SF (change to spooled file) entry type 284
 - SG file layout 670, 671
 - SM (systems management change) entry type 284
 - SM (systems management change) file layout 673
 - SO (server security user information actions) file layout 674
 - ST (service tools action) entry type 283
 - ST (service tools action) file layout 675
 - stopping 295
 - SV (action to system value) entry type 282
 - SV (action to system value) file layout 680
 - system entries 292
 - VA (access control list change) entry type 282
 - VA (changing access control list) file layout 681
 - VC (connection start and end) file layout 681
 - VC (connection start or end) entry type 273
 - VF (close of server files) file layout 682
 - VL (account limit exceeded) file layout 683
 - VN (network log on and off) file layout 684
 - VN (network log on or off) entry type 273
 - VO (validation list) file layout 685
 - VP (network password error) entry type 271
 - VP (network password error) file layout 686
 - VR (network resource access) file layout 687
 - VS (server session) entry type 273
 - VS (server session) file layout 688
 - VU (network profile change) entry type 282

QAUDJRN (audit) journal (*continued*)
 VU (network profile change) file layout 689
 VV (service status change) entry type 283
 VV (service status change) file layout 690
 X0 (kerberos authentication) file layout 691
 YC (change to DLO object) file layout 698
 YR (read of DLO object) file layout 699
 ZC (change to object) file layout 700
 ZR (read of object) file layout 703
 QAUDLVL (audit level) system value
 *AUTFAIL value 270
 *CREATE (create) value 272
 *DELETE (delete) value 272
 *JOBDTA (job change) value 273
 *OBJMGT (object management) value 275
 *OFCSRVR (office services) value 275
 *PGMADP (adopted authority) value 275
 *PGMFAIL (program failure) value 276
 *PRTDATA (printer output) value 276
 *SAVRST (save/restore) value 276
 *SECURITY (security) value 280
 *SERVICE (service tools) value 283
 *SPLFDATA (spooled file changes) value 284
 *SYSMGT (systems management) value 284
 changing 292, 315, 709
 displaying 315, 709
 purpose 263
 user profile 113
 QAUDLVL (auditing level) system value overview 67
 QAUDLVL2 (auditing level extension) system value overview 69
 QAUTOCFG (automatic configuration) system value
 value set by CFGSYSSEC command 716
 QAUTOCFG (automatic device configuration) system value 37
 QAUTOVRT (automatic configuration of virtual devices) system value 37
 QAUTOVRT (automatic virtual-device configuration) system value
 value set by CFGSYSSEC command 716
 QAUTPROF (authority profile) user profile 321
 QBRMS (BRM) user profile 321
 QCCSID (coded character set identifier) system value 106
 QCL program 137
 QCMD command processor
 Attention-key-handling program 104
 special environment (SPCENV) 89
 QCNTYID (country or region identifier) system value 106
 QCONSOLE (console) system value 203
 QCRTAUT (create authority) system value
 description 26
 risk of changing 26
 using 139
 QCRTOBJAUD (create object auditing) system value 71
 QDBSHRDO (database share) user profile 321
 QDCEADM (DCEADM) user profile 321
 QDEVRCYACN (device recovery action) system value 38
 value set by CFGSYSSEC command 716
 QDFTJOBDD (default) job description 96
 QDFTOWN (default owner) user profile
 audit journal (QAUDJRN) entry 276
 default values 321
 description 145
 restoring programs 253
 QDOC (document) user profile 321
 QDSCJOBITV (disconnected job time-out interval) system value 38
 value set by CFGSYSSEC command 716
 QDSNX (distributed systems node executive) user profile 321
 QDSPSGNINF (display sign-on information) system value 26, 91
 value set by CFGSYSSEC command 716
 QEZMAIN program 104
 QFNC (finance) user profile 321
 QGATE (VM/MVS bridge) user profile 321
 QHST (history) log
 using to monitor security 299
 QINACITV (inactive job time-out interval) system value 27
 value set by CFGSYSSEC command 716
 QINACTMSGQ (inactive job message queue) system value 28
 value set by CFGSYSSEC command 716
 QjoAddRemoteJournal (Add Remote Journal) API
 object auditing 531
 QjoChangeJournal State(Change Journal State) API
 object auditing 531
 QjoEndJournal (End journaling) API
 object auditing 500
 QjoEndJournal (End Journaling) API
 object auditing 531
 QJORDJE2 record format 564
 QjoRemoveRemoteJournal (Remove Remote Journal) API
 object auditing 531
 QjoRetrieveJournalEntries (Retrieve Journal Entries) API
 object auditing 531
 QjoRetrieveJournalInformation (Retrieve Journal Information) API
 object auditing 532
 QJORJIDI (Retrieve Journal Identifier (JID) Information) API
 object auditing 531
 QjoSJRNE (Send Journal Entry) API
 object auditing 531
 QjoStartJournal (Start Journaling) API
 object auditing 501, 531
 QKBDBUF (keyboard buffering) system value 94
 QLANGID (language identifier) system value 105
 QlgAccess command (Determine File Accessibility)
 object auditing 512
 QlgAccessx command (Determine File Accessibility)
 object auditing 512
 QLMTDEVSSN (limit device sessions) system value
 auditing 260
 description 29
 LMTDEVSSN user profile parameter 93
 QLMTSECOFR (limit security officer) system value
 auditing 258
 authority to device descriptions 201
 changing security levels 13
 description 29
 sign-on process 203
 value set by CFGSYSSEC command 716
 QLPAUTO (licensed program automatic install) user profile
 default values 321
 restoring 249
 QLPINSTALL (licensed program install) user profile
 default values 321
 restoring 249
 QMAXSGNACN (action when sign-on attempts reached) system value
 description 30
 user profile status 78
 value set by CFGSYSSEC command 716
 QMAXSIGN (maximum sign-on attempts) system value
 auditing 258, 262
 description 30
 user profile status 78
 value set by CFGSYSSEC command 716
 QMSF (mail server framework) user profile 321
 QPGMR (programmer) user profile
 default values 321
 device description owner 203
 password set by CFGSYSSEC command 717
 QPRTDEV (print device) system value 103
 QPWDCHGBLK (block password change) system value
 description 47

QPWDEXPITV (password expiration interval) system value
 auditing 259
 description 47
 PWDEXPITV user profile parameter 91
 value set by CFGSYSSEC command 716

QPWDEXPWRN (password expiration warning) system value
 description 48

QPWDLMTAJC (password limit adjacent) system value 52

QPWDLMTAJC (password restrict adjacent characters) system value
 value set by CFGSYSSEC command 716

QPWDLMTCHR (limit characters) system value 52

QPWDLMTCHR (password restrict characters) system value
 value set by CFGSYSSEC command 716

QPWDLMTCHR command 77

QPWDLMTREP (limit repeated characters) system value 53

QPWDLVL
 case sensitive passwords 53, 76
 Password levels (maximum length) 51
 Password levels (minimum length) 50
 Password levels (QPWDLVL) 50, 51, 52

QPWDLVL (case sensitive)
 case sensitive passwords
 QPWDLVL case sensitive 53
 Password levels (case sensitive) 53

QPWDLVL (current or pending value) and program name 60

QPWDMAXLEN (password maximum length) system value 51
 value set by CFGSYSSEC command 716

QPWDMINLEN (password minimum length) system value 50
 value set by CFGSYSSEC command 716

QPWDPOSDIF (password require position difference) system value
 value set by CFGSYSSEC command 716

QPWDPOSDIF (position characters) system value 53

QPWDRQDDGT (password require numeric character) system value
 value set by CFGSYSSEC command 716

QPWDRQDDGT (required password digits) system value 54

QPWDRQDDIF (duplicate password) system value 51

QPWDRQDDIF (password required difference) system value
 value set by CFGSYSSEC command 716

QPWDVLDPGM (password validation program) system value 60
 value set by CFGSYSSEC command 716

QRCL (reclaim storage) library
 setting QALWUSRDMN (allow user objects) system value 26

QRCLAUTL (reclaim storage) authorization list 255

QRETSVRSEC (retain server security) system value 31

QRETSVRSEC (retain server security) value 31

QRJE (remote job entry) user profile 321

QRMTSIGN (allow remote sign-on) system value
 value set by CFGSYSSEC command 716

QRMTSIGN (remote sign-on) system value 32, 262

QRMTSRVATR (remote service attribute) system value 2, 39

QRYDOCLIB (Query Document Library) command
 object auditing 518
 object authority required 376

QRYDST (Query Distribution) command
 object authority required 373

QRYPRBSTS (Query Problem Status) command
 object authority required 462

QSCANFS (Scan File Systems) system value 33

QSCANFCTL (Scan File Systems Control) system value 33

QSECOFR (security officer) user profile
 authority to console 203
 default values 321
 device description owner 203
 disabled status 78
 enabling 78
 restoring 249

QSECURITY (security level) system value
 auditing 258
 automatic user profile creation 73
 changing, 20 from higher level 13
 changing, level 10 to level 20 12
 changing, level 20 to 30 13
 changing, to level 40 18
 changing, to level 50 20
 comparison of levels 9
 disabling level 40 19
 disabling level 50 21
 enforcing QLMTSECOFR system value 203
 internal control blocks 20
 introduction 2
 level 10 12
 level 20 12
 level 30 13
 level 40 14
 level 50 19
 message handling 20
 validating parameters 17
 overview 9
 recommendations 11
 special authority 11

QSECURITY (security level) system value
 value (*continued*)
 user class 11
 value set by CFGSYSSEC command 716

QSH (Start QSH) command
 alias for STRQSH 466

QSHRMEMCTL (share memory control) system value
 description 34
 possible values 35

QSNADS (Systems Network Architecture distribution services) user profile 321

QSPCENV (special environment) system value 89

QSPL (spool) user profile 321

QSPLJOB (spool job) user profile 321

QSPRJOBQ (Retrieve job queue information) API
 object auditing 529

QsrRestore
 object auditing 501

QSRRSTO (Restore Object) API
 object auditing 501

QsrSave
 object auditing 499

QSRSAVO
 object auditing 499

QSRTSEQ (sort sequence) system value 105

QSRV (service) user profile
 authority to console 203
 default values 321
 password set by CFGSYSSEC command 717

QSRVBAS (basic service) user profile
 authority to console 203
 default values 321
 password set by CFGSYSSEC command 717

QSSLCSL (SSL cipher specification list) system value 39

QSSLCSLCTL (SSL cipher control) system value 40

QSSLPCL (SSL protocols) system value 40

QSYS (system) library
 authorization lists 139

QSYS (system) user profile
 default values 321
 restoring 249

QSYSLIBL (system library list) system value 207

QSYSMSG message queue
 auditing 262, 299
 QMAXSGNACN (action when attempts reached) system value 31
 QMAXSIGN (maximum sign-on attempts) system value 30

QSYSOPR (system operator) message queue
 restricting 207

QSYSOPR (system operator) user profile 321
 password set by CFGSYSSEC command 717

QTCP (TCP/IP) user profile 321

QTEMP (temporary) library
 security level 50 19

QTMLPD (TCP/IP printing support)
 user profile 321

QTSTRQS (test request) user profile 321

query
 analyzing audit journal entries 296

query definition (*QRYDFN)
 auditing 546

Query Management/400
 object authority required for
 commands 466

query manager form (*QMFORM)
 auditing 545

query manager query (*QMQRV)
 auditing 546

question and answer
 object authority required for
 commands 468

QUSEADPAUT (use adopted authority)
 system value
 description 35
 risk of changing 36

QUSER (user) user profile
 password set by CFGSYSSEC
 command 717

QUSER (workstation user) user
 profile 321

QUSER38 library 137

QVfyOjRST (verify object on restore)
 system value 41

QVfyOjRST (Verify Object Restore)
 system value 3

QWCLSCDE (List job schedule entry) API
 object auditing 530

R

RA (authority change for restored object)
 journal entry type 276

RCLACTGRP (Reclaim Activation Group)
 command
 object authority required 485

RCLDBXREF command
 authorized IBM-supplied user
 profiles 334
 object authority required 345

RCLDLO (Reclaim Document Library
 Object) command
 object auditing 519
 object authority required 376

RCLLNK (Reclaim Object Links)
 command
 object authority required 401

RCLOBJOWN (Reclaim Objects by
 Owner) command
 authorized IBM-supplied user
 profiles 334
 object authority required 345

RCLOPT (Reclaim Optical) command
 authorized IBM-supplied user
 profiles 334
 object authority required 453

RCLRSC (Reclaim Resources) command
 object authority required 485

RCLSPLSTG (Reclaim Spool Storage)
 command
 authorized IBM-supplied user
 profiles 334
 object authority required 482

RCLSTG (Reclaim Storage) command
 authorized IBM-supplied user
 profiles 334
 damaged authorization list 255
 object auditing 501
 object authority required 345

QDFTOWN (default owner)
 profile 145
 security level 50 19
 setting QALWUSRDMN (allow user
 objects) system value 26

RCLTMPSTG (Reclaim Temporary
 Storage) command
 authorized IBM-supplied user
 profiles 334
 object auditing 502
 object authority required 345

RCVDST (Receive Distribution) command
 object auditing 518
 object authority required 373

RCVJRNE (Receive Journal Entry)
 command
 object auditing 531
 object authority required 420

RCVMGRDTA (Receive Migration Data)
 command
 object authority required 442

RCVMSG (Receive Message) command
 object auditing 537
 object authority required 440

RCVNETF (Receive Network File)
 command
 object authority required 444

read (*READ) authority 132, 340

read of DLO object (YR) file layout 699

read of object (ZR) file layout 703

reader
 object authority required for
 commands 469

receiver
 changing 294
 deleting 294
 detaching 293, 294
 saving 294

reclaim storage (QRCL) library
 setting QALWUSRDMN (allow user
 objects) system value 26

reclaim storage (QRCLAUTL)
 authorization list 255

Reclaim Storage (RCLSTG)
 command 19, 145, 255
 setting QALWUSRDMN (allow user
 objects) system value 26

reclaiming
 storage 19, 145, 255
 setting QALWUSRDMN (allow
 user objects) system value 26

recommendation
 adopted authority 152
 application design 226
 display sign-on information
 (DSPSGNINF) 91

recommendation (*continued*)
 initial library list 96
 initial menu (INLMNU) 84
 initial program (INLPGM) 84
 job descriptions 96
 library design 225
 library list
 current library 210
 product library portion 209
 system portion 209
 user portion 210

limit capabilities (LMTCPB) 84

limiting
 device sessions 93

message queue 101

naming
 group profile 76
 user profiles 75

password expiration interval
 (PWDEXPITV) 91

passwords 77

priority limit (PTYLMT)
 parameter 96

public authority
 user profiles 112

QUSRLIBL system value 96

RSTLICPGM (Restore Licensed
 Program) command 253

security design 220

security level (QSECURITY) system
 value 11

set password to expired
 (PWDEXP) 78

special authority (SPCAUT) 88

special environment (SPCENV) 89

summary 220

user class (USRCLS) 79

record-level security 236

recovering
 authority holder 245
 authorization list 245
 damaged audit journal 292
 damaged authorization list 254
 object ownership 245
 private authority 245
 public authority 245
 security information 245
 user profiles 245

reference code table (*RCT) auditing 547

referenced object 165

rejecting
 access
 DDM request (DDM) 216
 iSeries Access access 215
 remote job submission 214

relational database directory
 object authority required for
 commands 469

remote job entry (QRJE) user profile 321

remote job entry (RJE)
 object authority required for
 commands 470

remote job submission
 securing 214

remote service attribute (QRMTSRVATR)
 system value 39

- remote sign-on
 - QRMTSIGN system value 32
- remote sign-on (QRMTSIGN) system value 32, 262
- Remove Authorization List Entry (RMVAUTLE) command 167, 309
- Remove Directory Entry (RMVDIRE) command 314
- Remove Document Library Object Authority (RMVDLOAUT) command 313
- Remove Kerberos Keytab Entry (RMVKRBKTE) command
 - object authority required 424
- Remove Library List Entry (RMVLIBLE) command 207
- Remove User display 123
- removing
 - authority for user 161
 - authorization list
 - object 169
 - user authority 167, 309
 - directory entry 314
 - document library object
 - authority 313
 - employees who no longer need
 - access 260
 - library list entry 207
 - security level 40 19
 - security level 50 21
 - server authentication entry 314
 - user authority
 - authorization list 167
 - object 161
 - user profile
 - automatically 707
 - directory entry 122
 - distribution lists 122
 - message queue 122
 - owned objects 122
 - primary group 122
- renaming
 - object
 - audit journal (QAUDJRN) entry 275
 - user profile 126
- repeated characters (QPWDLMTREP) system value 53
- repeating passwords 51
- reply list
 - action auditing 548
 - object authority required for commands 485
- required password digits (QPWDRQDDGT) system value 54
- resetting
 - DST (dedicated service tools) password
 - audit journal (QAUDJRN) entry 277
- RESMGRNAM (Resolve Duplicate and Incorrect Office Object Names) command
 - authorized IBM-supplied user profiles 334
 - object authority required 442
- resource
 - object authority required for commands 470
- resource security
 - definition 131
 - introduction 5
 - limit access 244
- restore
 - security risks 216
- Restore Authority (RSTAUT) command
 - audit journal (QAUDJRN) entry 277
 - description 312
 - procedure 252
 - role in restoring security 245
 - using 251
- restore authority for user profile (RU) file layout 661
- restore authority for user profile (RU) journal entry type 277
- Restore Document Library Object (RSTDLO) command 245
- Restore Library (RSTLIB) command 245
- Restore Licensed Program (RSTLICPGM) command
 - recommendations 253
 - security risks 253
- Restore Object (RSTOBJ) command
 - using 245
- restore operation
 - maximum storage (MAXSTG) 94
 - storage needed 94
- Restore Performance Collection (RSTPFRCOL) command
 - authorized IBM-supplied user profiles 335
 - object authority required 460
- restore system value
 - security-related
 - overview 41
- Restore User Profiles (RSTUSRPRF) command 245, 312
- restoring
 - *ALLOBJ (all object) special authority
 - all object (*ALLOBJ) special authority 249
 - *CRQD object
 - audit journal (QAUDJRN) entry 277
 - *CRQD object that adopts authority (RQ) file layout 661
 - adopted authority
 - changes to ownership and authority 253
 - allow object differences (ALWOBJDIF) parameter 250
 - ALWOBJDIF (allow object differences) parameter 250
 - authority
 - audit journal (QAUDJRN) entry 277
 - command description 312
 - description of process 252
 - overview of commands 245
 - procedure 251
 - authority changed by system
 - audit journal (QAUDJRN) entry 276
- restoring (*continued*)
 - authority holder 245
 - authorization list
 - association with object 250
 - description of process 254
 - overview of commands 245
 - document library object (DLO) 245
 - gid (group identification number) 249
 - job description
 - audit journal (QAUDJRN) entry 276
 - library 245
 - licensed program
 - recommendations 253
 - security risks 253
 - maximum storage (MAXSTG) 94
 - object
 - audit journal (QAUDJRN) entry 276
 - commands 245
 - ownership 245, 249
 - security issues 249
 - operating system 255
 - ownership change
 - audit journal (QAUDJRN) entry 276
 - performance collection
 - authorized IBM-supplied user profiles 335
 - object authority required 460
 - primary group 245, 250
 - private authority 245, 250
 - program failure
 - audit journal (QAUDJRN) entry 276
 - program validation 17
 - programs 252
 - public authority 245, 250
 - QDFTOWN (default) owner
 - audit journal (QAUDJRN) entry 276
 - restricting 216, 217
 - security information 245
 - storage needed 94
 - uid (user identification number) 249
 - user profile
 - audit journal (QAUDJRN) entry 277
 - command description 312
 - procedures 245, 248
- restoring *CRQD (RQ) file layout 662
- restoring *CRQD object (RQ) journal entry type 277
- restoring job description (RJ) file layout 656
- restoring job description (RJ) journal entry type 276
- restoring programs that adopt authority (RP) file layout 659
- restoring programs that adopt authority (RP) journal entry type 276
- restricted instruction
 - audit journal (QAUDJRN) entry 276
- restricting
 - access
 - console 258

restricting (*continued*)
 access (*continued*)
 workstations 258
 adjacent digits in passwords
 (QPWDLMTAJC system value) 52
 capabilities 83
 characters in passwords 52
 command line use 83
 commands (ALWLMTUSR) 83
 consecutive digits in passwords
 (QPWDLMTAJC system value) 52
 messages 20
 QSYSOPR (system operator) message
 queue 207
 repeated characters in passwords 53
 restore operations 216
 save operations 216
 security officer (QLMTSECOFR
 system value) 258
 retain server security (QRETSVRSEC)
 system value
 overview 31
 retain server security (QRETSVRSEC)
 value 31
 Retrieve Authorization List Entry
 (RTVAUTLE) command 309
 Retrieve Journal Receiver Information
 API
 object auditing 532
 Retrieve User Profile (RTVUSRPRF)
 command 128, 311
 retrieving
 authorization list entry 309
 user profile 128, 311
 RETURN (Return) command
 object authority required 485
 reversing
 page down (*ROLLKEY user
 option) 108
 page up (*ROLLKEY user
 option) 108
 Revoke Object Authority (RVKOBJAUT)
 command 159, 169, 310
 Revoke Public Authority (RVKPUBAUT)
 command
 description 316, 715
 details 718
 Revoke User Permission (RVKUSRPMN)
 command 313
 revoking
 object authority 310
 public authority 316, 715
 user permission 313
 RGZDLO (Reorganize Document Library
 Object) command
 object auditing 518
 object authority required 376
 RGZPFM (Reorganize Physical File
 Member) command
 object auditing 524
 object authority required 387
 risk
 *ALLOBJ (all object) special
 authority 85
 *AUDIT (audit) special authority 88
 *IOSYSCFG (system configuration)
 special authority 88
 risk (*continued*)
 *JOBCTL (job control) special
 authority 86
 *SAVSYS (save system) special
 authority 86
 *SERVICE (service) special
 authority 87
 *SPLCTL (spool control) special
 authority 86
 adopted authority 152
 authority holder 154
 create authority (CRTAUT)
 parameter 140
 library list 208
 password validation program 61
 restore commands 216
 restoring programs that adopt
 authority 253
 restoring programs with restricted
 instructions 252
 RSTLICPGM (Restore Licensed
 Program) command 253
 save commands 216
 special authorities 85
 RJ (restoring job description) file
 layout 656
 RJ (restoring job description) journal
 entry type 276
 RJE (remote job entry)
 object authority required for
 commands 470
 RLSCMNDEV (Release Communications
 Device) command
 authorized IBM-supplied user
 profiles 334
 object auditing 511, 533
 object authority required 370
 RLSDSTQ (Release Distribution Queue)
 command
 authorized IBM-supplied user
 profiles 334
 object authority required 373
 RLSIFSLCK (Release IFS Lock) command
 authorized IBM-supplied user
 profiles 334
 RLSIFSLCK (Release IFS Lock) command)
 command
 object authority required 445
 RLSJOB (Release Job) command
 object authority required 413
 RLSJOBQ (Release Job Queue) command
 object auditing 529
 object authority required 416
 RLSJOBSCDE (Release Job Schedule
 Entry) command
 object auditing 530
 object authority required 417
 RLSOUTQ (Release Output Queue)
 command
 object auditing 541
 object authority required 454
 RLSRDR (Release Reader) command
 object authority required 469
 RLSRMTPHS (Release Remote Phase)
 command
 authorized IBM-supplied user
 profiles 334
 RLSSPLF (Release Spooled File)
 command
 object auditing 541
 object authority required 482
 RLSWTR (Release Writer) command
 object authority required 496
 RMVACC (Remove Access Code)
 command
 authorized IBM-supplied user
 profiles 334
 object auditing 518
 object authority required 449
 RMVAJE (Remove Autostart Job Entry)
 command
 object auditing 549
 object authority required 484
 RMVALRD (Remove Alert Description)
 command
 object auditing 503
 object authority required 352
 RMVASPCPYD
 authorized IBM-supplied user
 profiles 334
 RMVAUTLE (Remove Authorization List
 Entry) command
 description 309
 object auditing 503
 object authority required 354
 using 167
 RMVBKP (Remove Breakpoint) command
 object authority required 464
 RMVBNDIRE (Remove Binding
 Directory Entry) command
 object auditing 504
 object authority required 355
 RMVCADMRE
 authorized IBM-supplied user
 profiles 334
 RMVCADMRE command
 object authority required 360
 RMVCADNODE
 authorized IBM-supplied user
 profiles 334
 RMVCADNODE command
 object authority required 360
 RMVCFGLE (Remove Configuration List
 Entries) command
 object authority required 364
 RMVCFGLE (Remove Configuration List
 Entry) command
 object auditing 505
 RMVCLUMON
 authorized IBM-supplied user
 profiles 335
 RMVCLUMON command
 object authority required 360
 RMVCLUNODE
 authorized IBM-supplied user
 profiles 335
 RMVCLUNODE command
 object authority required 360
 RMVCMNE (Remove Communications
 Entry) command
 object auditing 549
 object authority required 484

RMVCNNLE (Remove Connection List Entry) command
 object auditing 508
 RMVCOMSNMP (Remove Community for SNMP) command
 object authority required 490
 RMVCRGDEVE
 authorized IBM-supplied user profiles 335
 RMVCRGNODE
 authorized IBM-supplied user profiles 335
 RMVCRQD (Remove Change Request Description Activity) command
 object auditing 507
 RMVCRQDA (Remove Change Request Description Activity) command
 object authority required 356
 RMVCRSDMNK (Remove Cross Domain Key) command
 authorized IBM-supplied user profiles 335
 RMVDEVDMNE command
 authorized IBM-supplied user profiles 335
 object authority required 360
 RMVDFRID (Remove Defer ID) command
 object auditing 502
 RMVDFRID command
 authorized IBM-supplied user profiles 335
 object authority required 345
 RMVDIR (Remove Directory) command
 object auditing 513
 object authority required 401
 RMVDIRE (Remove Directory Entry) command
 description 314
 object authority required 371
 RMVDIRSHD (Remove Directory Shadow System) command
 object authority required 371
 RMVDLOAUT (Remove Document Library Object Authority) command
 description 313
 object auditing 518
 object authority required 376
 RMVDSTLE (Remove Distribution List Entry) command
 object authority required 374
 RMVDSTQ (Remove Distribution Queue) command
 authorized IBM-supplied user profiles 335
 object authority required 374
 RMVDSTRTE (Remove Distribution Route) command
 authorized IBM-supplied user profiles 335
 object authority required 374
 RMVDSTSYSN (Remove Distribution Secondary System Name) command
 authorized IBM-supplied user profiles 335
 object authority required 374
 RMVDWDFN command 335
 RMVEMLCFGE (Remove Emulation Configuration Entry) command
 object authority required 371
 RMVENVVAR (Remove Environment Variable) command
 object authority required 380
 RMVEWCBCDE (Remove Extended Wireless Controller Bar Code Entry) command
 object authority required 381
 RMVEWCPTCE (Remove Extended Wireless Controller PTC Entry) command
 object authority required 381
 RMVEXITPGM (Add Exit Program) command
 object auditing 522
 RMVEXITPGM (Remove Exit Program) command
 authorized IBM-supplied user profiles 335
 object authority required 469
 RMVFCTE (Remove Forms Control Table Entry) command
 object authority required 473
 RMVFNTTBLE (Remove DBCS Font Table Entry)
 object authority required for commands 351
 RMVFTRACNE (Remove Filter Action Entry) command
 object auditing 527
 object authority required 388
 RMVFTRSLTE (Remove Filter Selection Entry) command
 object auditing 527
 object authority required 388
 RMVICFDEVE (Remove Intersystem Communications Function Program Device Entry) command
 object authority required 387
 RMVIMGCLGE command
 object authority required 391
 RMVIPSIFC (Remove IP over SNA Interface) command
 object authority required 352
 RMVIPSLOC (Remove IP over SNA Location Entry) command
 object authority required 352
 RMVIPS RTE (Remove IP over SNA Route) command
 object authority required 352
 RMVJOBQE (Remove Job Queue Entry) command
 object auditing 529, 549
 object authority required 484
 RMVJOBSCDE (Remove Job Schedule Entry) command
 object auditing 530
 object authority required 417
 RMVJRNCHG (Remove Journalized Changes) command
 authorized IBM-supplied user profiles 335
 object auditing 501, 531
 object authority required 420
 RMVJWDFN command 335
 RMVLANADP (Remove LAN Adapter) command
 authorized IBM-supplied user profiles 335
 RMVLANADPI (Remove LAN Adapter Information) command
 object authority required 437
 RMVLANADPT (Remove LAN Adapter) command
 object authority required 437
 RMVLIBLE (Remove Library List Entry) command
 using 207
 RMVLICKEY (Remove License Key) command
 object authority required 434
 RMVLNK (Remove Link) command
 object auditing 551, 556, 558
 object authority required 402
 RMVVM (Remove Member) command
 object auditing 524
 object authority required 387
 RMVMFS (Remove Mounted File System) object authority required 491
 RMVMFS (Remove Mounted File System) command
 authorized IBM-supplied user profiles 335
 object authority required 445
 RMVMSG (Remove Message) command
 object auditing 537
 object authority required 440
 RMVMSGD (Remove Message Description) command
 object auditing 537
 object authority required 441
 RMVNETJOB (Remove Network Job Entry) command
 authorized IBM-supplied user profiles 335
 object authority required 444
 RMVNETTBLE (Remove Network Table Entry) command
 object authority required 490
 RMVNODLE (Remove Node List Entry) command
 object auditing 538
 object authority required 449
 RMVNWSSTGL (Remove Network Server Storage Link) command
 object authority required 447
 RMVOPTCTG (Remove Optical Cartridge) command
 authorized IBM-supplied user profiles 335
 object authority required 453
 RMVOPTSVR (Remove Optical Server) command
 authorized IBM-supplied user profiles 335
 object authority required 453
 RMVPEXDFN (Remove Performance Explorer Definition) command
 authorized IBM-supplied user profiles 335
 object authority required 460

RMVPEXFTR command
 authorized IBM-supplied user profiles 335

RMVPPFCST (Remove Physical File Constraint) command
 object auditing 525
 object authority required 387

RMVPPFTGR (Remove Physical File Trigger) command
 object auditing 525

RMVPPFTRG (Remove Physical File Trigger) command
 object authority required 387

RMVPPGM (Remove Program) command
 object authority required 464

RMVPPJE (Remove Prestart Job Entry) command
 object auditing 549
 object authority required 484

RMVPPTF (Remove Program Temporary Fix) command
 authorized IBM-supplied user profiles 335
 object authority required 476

RMVRRDBDIRE (Remove Relational Database Directory Entry) command
 object authority required 470

RMVRRJECMNE (Remove RJE Communications Entry) command
 object authority required 473

RMVRRJERDRE (Remove RJE Reader Entry) command
 object authority required 473

RMVRRJEWTR (Remove RJE Writer Entry) command
 object authority required 473

RMVRRMTJRN (Remove Remote Journal) command
 object auditing 531

RMVRRMTPTF (Remove Remote Program Temporary Fix) command
 authorized IBM-supplied user profiles 335

RMVRRPYLE (Remove Reply List Entry) command
 authorized IBM-supplied user profiles 335
 object auditing 548
 object authority required 486

RMVRRTGE (Remove Routing Entry) command
 object auditing 549
 object authority required 484

RMVRSCHIDX (Remove Search Index Entry) command
 object auditing 550
 object authority required 411

RMVRSOCE (Remove Sphere of Control Entry) command
 object authority required 480

RMVRSVRAUTE (Remove Server Authentication Entry) command
 object authority required 475

RMVRTAPCTG (Remove Tape Cartridge) command
 object authority required 438

RMVTCPHTE (Remove TCP/IP Host Table Entry) command
 object authority required 490

RMVTCPIFC (Remove TCP/IP Interface) command
 object authority required 490

RMVTCPPORT (Remove TCP/IP Port Entry) command
 object authority required 490

RMVTCPRSI (Remove TCP/IP Remote System Information) command
 object authority required 490

RMVTCPRTE (Remove TCP/IP Route) command
 object authority required 490

RMVTRC (Remove Trace) command
 object authority required 464

RMVTRCFTR
 authorized IBM-supplied user profiles 335

RMVWSE (Remove Workstation Entry) command
 object auditing 549
 object authority required 484

RNM (Rename) command
 object auditing 513, 551, 556, 558
 object authority required 402

RNMCNNLE (Rename Connection List Entry) command
 object auditing 508

RNMDIRE (Rename Directory Entry) command
 object authority required 371

RNMDLO (Rename Document Library Object) command
 object auditing 518
 object authority required 376

RNMDSTL (Rename Distribution List) command
 object authority required 374

RNMM (Rename Member) command
 object auditing 525
 object authority required 387

RNMOBJ (Rename Object) command
 object auditing 501, 533, 559
 object authority required 345

RNMTCPHTE (Rename TCP/IP Host Table Entry) command
 object authority required 490

RO (ownership change for restored object) file layout 657

RO (ownership change for restored object) journal entry type 276

roll key (*ROLLKEY) user option 108

ROLLBACK (Rollback) command
 object authority required 362

routing entry
 authority to program 200
 changing
 audit journal (QAUDJRN) entry 282
 performance 218

RP (restoring programs that adopt authority) file layout 659

RP (restoring programs that adopt authority) journal entry type 276

RPLDOC (Replace Document) command
 object auditing 518
 object authority required 376

RQ (restoring *CRQD object that adopts authority) file layout 661

RQ (restoring *CRQD object) journal entry type 277

RRTJOB (Reroute Job) command
 object authority required 413

RSMBKP (Resume Breakpoint) command
 object authority required 464

RSMCTLR (Resume Controller Recovery) command
 object auditing 510
 object authority required 366

RSMDEVRCY (Resume Device Recovery) command
 object auditing 511
 object authority required 370

RSMLINRCY (Resume Line Recovery) command
 object auditing 534
 object authority required 437

RSMNWIRCY (Resume Network Interface Recovery) command
 object auditing 539

RST (Restore) command
 authorized IBM-supplied user profiles 335
 object auditing 501, 513, 551, 556, 558
 object authority required 403

RSTAUT (Restore Authority) command
 audit journal (QAUDJRN) entry 277
 authorized IBM-supplied user profiles 335
 description 312
 object authority required 494
 procedure 252
 role in restoring security 245
 using 251

RSTCFG (Restore Configuration) command
 authorized IBM-supplied user profiles 335
 object auditing 501
 object authority required 363

RSTDFROBJ (Restore Deferred Object) command
 object auditing 502

RSTDFROBJ command
 authorized IBM-supplied user profiles 335
 object authority required 346

RSTDLO (Restore Document Library Object) command 245
 authorized IBM-supplied user profiles 335
 object auditing 518
 object authority required 376

RSTLIB (Restore Library) command 245
 authorized IBM-supplied user profiles 335
 object auditing 501
 object authority required 432

RSTLICPGM (Restore Licensed Program) command
 authorized IBM-supplied user profiles 335
 object auditing 501
 object authority required 435
 recommendations 253
 security risks 253

RSTOBJ (Restore Object) command
 authorized IBM-supplied user profiles 335
 object auditing 501
 object authority required 346
 using 245

RSTPFRCOL (Restore Performance Collection) command
 authorized IBM-supplied user profiles 335
 object authority required 460

RSTPFRDTA command 335

RSTS36F (Restore System/36 File) command
 authorized IBM-supplied user profiles 335
 object authority required 387, 488

RSTS36FLR (Restore System/36 Folder) command
 authorized IBM-supplied user profiles 335
 object authority required 376, 488

RSTS36LIBM (Restore System/36 Library Members) command
 authorized IBM-supplied user profiles 335
 object authority required 432, 488

RSTS38AUT (Restore System/38 Authority) command
 authorized IBM-supplied user profiles 335
 object authority required 442

RSTSHF (Restore Bookshelf) command
 object auditing 518

RSTSYSINF
 object authority required 346

RSTUSRPRF (Restore User Profiles) command
 authorized IBM-supplied user profiles 335
 description 245, 312
 object auditing 560
 object authority required 494

RTVAUTLE (Retrieve Authorization List Entry) command
 description 309
 object auditing 504
 object authority required 354

RTVBCKUP (Retrieve Backup Options) command
 object authority required 450

RTVBNDSRC (Retrieve Binder Source) command
 *SRVPGM, retrieving exports from 443
 object auditing 504, 536, 554
 object authority required 443

RTVCFGSRC (Retrieve Configuration Source) command
 object auditing 508, 509, 510, 511, 534, 539, 540
 object authority required 363

RTVCFGSTS (Retrieve Configuration Status) command
 object auditing 510, 512, 534, 539, 540
 object authority required 363

RTVCLDSRC (Retrieve C Locale Source) command
 object auditing 506

RTVCLNUP (Retrieve Cleanup) command
 object authority required 450

RTVCLSRC (Retrieve CL Source) command
 object auditing 536, 543, 554
 object authority required 465

RTVCLSRC command
 object authority required 430

RTVCURDIR (Retrieve Current Directory) command
 object auditing 512
 object authority required 404

RTVDLONAM (Retrieve Document Library Object Name) command
 object authority required 376

RTVDOC (Retrieve Document) command
 object auditing 516, 518
 object authority required 376

RTVDSKINF (Retrieve Disk Activity Information) command
 authorized IBM-supplied user profiles 336
 object authority required 450

RTVDTAARA (Retrieve Data Area) command
 object auditing 519
 object authority required 367

RTVGRPA (Retrieve Group Attributes) command
 object authority required 485

RTVIMGCLG command
 object authority required 391

RTVJOBA (Retrieve Job Attributes) command
 object authority required 413

RTVJRNE (Retrieve Journal Entry) command
 object auditing 531
 object authority required 420

RTVLIBD (Retrieve Library Description) command
 object authority required 432

RTVMBRD (Retrieve Member Description) command
 object auditing 525
 object authority required 387

RTVMSG (Retrieve Message) command
 object auditing 536

RTVNETA (Retrieve Network Attributes) command
 object authority required 444

RTVOBJD (Retrieve Object Description) command
 object auditing 502
 object authority required 347

RTVPDGPFR (Retrieve Print Descriptor Group Profile) command
 object authority required 461

RTVPRD (Retrieve Product) command
 authorized IBM-supplied user profiles 336

RTVPTF (Retrieve PTF) command
 authorized IBM-supplied user profiles 336

RTVPWRSCDE (Retrieve Power On/Off Schedule Entry) command
 object authority required 450

RTVQMFOM (Retrieve Query Management Form) command
 object auditing 547
 object authority required 467

RTVQMQR (Retrieve Query Management Query) command
 object auditing 546, 547
 object authority required 467

RTVS36A (Retrieve System/36 Attributes) command
 object auditing 559
 object authority required 488

RTVSMGOBJ (Retrieve Systems Management Object) command
 authorized IBM-supplied user profiles 336

RTVSYSVAL (Retrieve System Value) command
 object authority required 486

RTVUSRPRF (Retrieve User Profile) command
 description 311
 object auditing 561
 object authority required 494
 using 128

RTVWSCST (Retrieve Workstation Customizing Object) command
 object auditing 562
 object authority required 496

RU (restore authority for user profile) file layout 661
 RU (restore authority for user profile) journal entry type 277
 run priority 217, 218

RUNBCKUP (Run Backup) command
 object authority required 450

RUNDNSUPD command
 object authority required 379

RUNLPDA (Run LPDA-2) command
 authorized IBM-supplied user profiles 336
 object auditing 533
 object authority required 476

RUNQRY (Run Query) command
 object auditing 547
 object authority required 467

RUNRNDCCMD command
 object authority required 379

RUNSMGCM (Run Systems Management Command) command
 authorized IBM-supplied user profiles 336

RUNSMGOBJ (Run Systems Management Object) command
 authorized IBM-supplied user profiles 336

RUNSQLSTM (Run Structured Query Language Statement) command
 object authority required 430

RVKACCAUT (Revoke Access Code Authority) command
 object auditing 518
 object authority required 449

RVKOBJAUT (Revoke Object Authority) command 159
 description 310
 object auditing 501
 object authority required 347
 using 169

RVKPUBAUT (Revoke Public Authority) command
 authorized IBM-supplied user profiles 336
 description 316, 715
 details 718
 object authority required 346

RVKUSRPMN (Revoke User Permission) command
 description 313
 object auditing 518
 object authority required 449

RVKWSOAUT (Revoke Workstation Object Authority) command
 object authority required 389

RZ (primary group change for restored object) file layout 662

RZ (primary group change for restored object) journal entry type 277

S

S/36 machine description (*S36)
 auditing 558

SAV (Save) command
 object auditing 499, 512, 555, 558
 object authority required 404

SAVAPAR (Save APAR Data) command
 authorized IBM-supplied user profiles 336
 object authority required 477

SAVCFG (Save Configuration) command
 object auditing 510, 511, 533, 539, 540
 object authority required 363

SAVCHGOBJ (Save Changed Object) command
 object auditing 499
 object authority required 347

SAVDLO (Save Document Library Object) command
 object auditing 499, 516
 object authority required 377
 using 245

Save Document Library Object (SAVDLO) command 245

Save Library (SAVLIB) command 245

Save Object (SAVOBJ) command 245, 294

Save Performance Collection (SAVPFCOL) command
 authorized IBM-supplied user profiles 336
 object authority required 460

Save Security Data (SAVSECDA) command 245, 312

save system (*SAVSYS) special authority
 *OBJEXIST authority 132, 340
 description 256
 functions allowed 86
 removed by system
 changing security levels 13
 risks 86

Save System (SAVSYS) command 245, 312

save/restore (*SAVRST) audit level 276

saving
 audit journal receiver 294
 auditing 256
 authority holder 245
 authorization list 245
 document library object (DLO) 245
 library 245
 object 245
 object ownership 245
 performance collection
 authorized IBM-supplied user profiles 336
 object authority required 460
 primary group 245
 private authority 245
 public authority 245
 restricting 216, 217
 security data 245, 312
 security information 245
 security risks 216
 system 245, 312
 user profile
 commands 245

SAVLIB (Save Library) command
 object auditing 499
 object authority required 433
 using 245

SAVLICPGM (Save Licensed Program) command
 authorized IBM-supplied user profiles 336
 object auditing 499
 object authority required 435

SAVOBJ (Save Object) command
 object auditing 499
 object authority required 347
 saving audit journal receiver 294
 using 245

SAVPFCOL (Save Performance Collection) command
 authorized IBM-supplied user profiles 336
 object authority required 460

SAVPRD (Save Performance Report Data) command 336

SAVRSOBJ (Save Restore Object) command
 object authority required 348

SAVRSTCFG (Save Restore Configuration) command
 object authority required 363

SAVRSTCHG
 authorized IBM-supplied user profiles 336

SAVRSTCHG (Save Restore Change) command
 object authority required 348

SAVRSTDLO (Save Restore Document Library Object) command
 object authority required 377

SAVRSTLIB
 authorized IBM-supplied user profiles 336

SAVRSTLIB (Save Restore Library) command
 object authority required 433

SAVRSTOBJ
 authorized IBM-supplied user profiles 336

SAVS36F (Save System/36 File) command
 object authority required 387, 488

SAVS36LIB (Save System/36 Library Members) command
 object authority required 387, 433

SAVSAV (Save Save File Data) command
 object auditing 499
 object authority required 387

SAVSECDA (Save Security Data) command
 description 312
 object authority required 494
 using 245

SAVSHF (Save Bookshelf) command
 object auditing 500, 516

SAVSTG (Save Storage) command
 object auditing 502
 object authority required 348

SAVSYS (Save System) command
 description 312
 object authority required 348
 using 245

SAVSYSINF
 object authority required 348

SBMCRQ (Submit Change Request) command
 object auditing 506

SBMDBJOB (Submit Database Jobs) command
 object authority required 413

SBMDKTJOB (Submit Diskette Jobs) command
 object authority required 413

SBMFNCJOB (Submit Finance Job) command
 authorized IBM-supplied user profiles 336
 object authority required 389

SBMJOB (Submit Job) command
 authority checking 200
 object authority required 413
 SECBATCH menu 710

SBMNETJOB (Submit Network Job) command
 object authority required 413

SBMNWSCMD (Submit Network Server Command) command
 authorized IBM-supplied user profiles 336
 object authority required 447

SBMRJEJOB (Submit RJE Job) command
 object authority required 473

SBMRMTCMD (Submit Remote Command) command
 object authority required 361

scan
 object alterations 262, 304, 311
 scan file systems (QSCANFS) system value 33
 scan file systems control (QSCANFSCCTL) system value 33

scheduling
 security reports 710
 user profile
 activation 707
 expiration 707

scheduling priority
 limiting 95

scrolling
 reversing (*ROLLKEY user option) 108

SD (change system distribution directory)
 file layout 664

SD (change system distribution directory)
 journal entry type 275

SE (change of subsystem routing entry)
 file layout 665

SE (change of subsystem routing entry)
 journal entry type 282

search index
 object authority required 411
 search index (*SCHIDX) auditing 549

SECBATCH (Submit Batch Reports) menu
 scheduling reports 710
 submitting reports 709

SECTOOLS (Security Tools) menu 707

Secure Sockets Layer (SSL) cipher control (QSSLCSLCTL) system value 40

Secure Sockets Layer (SSL) cipher specification list (QSSLCSL) system value 39

Secure Sockets Layer (SSL) protocols (QSSLPCL) system value 40

security
 Common Criteria
 description 6
 critical files 236
 designing 219
 job description 206
 keylock 2
 library lists 207
 objective
 availability 1
 confidentiality 1
 integrity 1
 output queue 211
 overall recommendations 220
 physical 2
 planning 1
 printer output 211
 source files 242
 spooled file 211

security (*continued*)
 starting
 batch job 200
 interactive job 199
 jobs 199
 subsystem description 205
 system values 3
 tools 315
 why needed 1

security (*SECURITY) audit level 280

security administrator (*SECADM)
 special authority
 functions allowed 85

security attribute
 object authority required for commands 474

security audit
 object authority required for commands 474

security audit journal
 displaying entries 315
 printing entries 711

security auditing
 displaying 315, 709
 setting up 315, 709

security auditing function
 activating 290
 CHGSECAUD 290
 stopping 295

Security Auditing Journal Entries 270

security command list 309

security data
 saving 245, 312

security information
 backup 245
 format on save media 247
 format on system 246
 recovery 245
 restoring 245
 saving 245
 stored on save media 247
 stored on system 246

security level (QSECURITY) system value
 auditing 258
 automatic user profile creation 73
 changing
 level 10 to level 20 12
 level 20 to level 30 13
 level 20 to level 40 18
 level 20 to level 50 20
 level 30 to 20 13
 level 30 to level 40 18
 level 30 to level 50 20
 level 40 to 20 13
 level 40 to level 30 19
 level 50 to level 30 or 40 21
 comparison of levels 9
 disabling level 40 19
 disabling level 50 21
 enforcing QLMTSECOFR system value 203
 internal control blocks 20
 introduction 2
 level 10 12
 level 20 12
 level 30 13

security level (QSECURITY) system value (*continued*)
 level 40 14
 level 50
 message handling 20
 overview 19
 QTEMP (temporary) library 19
 validating parameters 17
 overview 9
 recommendations 11
 special authority 11
 user class 11
 value set by CFGSYSSEC command 716

security officer
 limiting workstation access 29
 monitoring actions 305
 restricting to certain workstations 258

security officer (QSECOFR) user profile
 authority to console 203
 default values 321
 device description owner 203
 disabled status 78
 enabling 78
 restoring 249

security tools
 commands 315, 707
 contents 315, 707
 menus 707

Security Tools (SECTOOLS) menu 707

security value
 setting 715

Send Journal Entry (SNDJRNE)
 command 292

Send Network Spooled File (SNDNETSPLF) command 211

sending
 journal entry 292
 network spooled file 211

sensitive data
 encrypting 262
 protecting 261

server authentication
 object authority required for commands 475

server authentication entry
 adding 314
 changing 314
 removing 314

server security user information actions (SO) file layout 674

server session
 audit journal (QAUDJRN) entry 273

server session (VS) file layout 688

server session VS) journal entry type 273

server storage space (*SVRSTG)
 object 555

service
 object authority required for commands 475

service (*SERVICE) special authority
 failed sign-on 201
 functions allowed 87
 risks 87

service (QSRV) user profile
 authority to console 203
 default values 321
 service basic (QSRVBAS) user
 profile 321
 service program
 adopted authority 151
 service program (*SRVPGM)
 auditing 554
 service status change (VV) file
 layout 690
 service status change (VV) journal entry
 type 283
 service tools (*SERVICE) audit level 283
 service tools action (ST) file layout 675
 service tools action (ST) journal entry
 type 283
 session
 object authority required for
 commands 470
 session description (*SSND)
 auditing 555
 Set Attention Program (SETATNPGM)
 command 104
 set password to expired (PWDEXP)
 parameter 77
 SETATNPGM (Set Attention Program)
 command
 job initiation 104
 object authority required 465
 SETCSTDTA (Set Customization Data)
 command
 object authority required 389
 SETJOBATR (user options) parameter
 user profile 107
 SETMSTK (Set Master Key) command
 authorized IBM-supplied user
 profiles 336
 SETMSTKEY command
 authorized IBM-supplied user
 profiles 336
 object authority required 367
 SETOBJACC (Set Object Access)
 command
 object authority required 348
 SETPGMINF (Set Program Information)
 command
 object authority required 465
 SETTAPCGY (Set Tape Category)
 command
 object authority required 438
 setting
 Attention-key-handling program
 (ATNPGM) 104
 network attributes 316, 715
 security values 715
 system values 316, 715
 setting up
 auditing function 290
 security auditing 315, 709
 SETVTMAP (Set VT100 Keyboard Map)
 command
 object authority required 490
 STRTCP (Start TCP/IP) command
 object authority required 490
 SETVTMAP (Set VT100 Keyboard Map)
 command (*continued*)
 STRTCPIFC (Start TCP/IP Interface)
 command
 object authority required 490
 SETVTTBL (Set VT Translation Tables)
 command
 object authority required 489
 SEV (message queue severity) parameter
 user profile 102
 severity (SEV) parameter
 user profile 102
 SF (action to spooled file) file layout 666
 SF (change to spooled file) journal entry
 type 284
 share memory control (QSHRMEMCTL)
 system value
 description 34
 possible values 35
 shared folder
 securing 216
 sign-on
 action when attempts reached
 (QMAXSGNACN system value) 30
 authorities required 199
 authority failures 199
 console 203
 incorrect password
 audit journal (QAUDJRN)
 entry 271
 incorrect user ID
 audit journal (QAUDJRN)
 entry 271
 limiting attempts 30
 preventing default 261
 remote (QRMTSIGN system
 value) 32
 restricting security officer 201
 security checking 199
 security officer fails 201
 service user fails 201
 user with *ALLOBJ special authority
 fails 201
 user with *SERVICE special authority
 fails 201
 without user ID 205
 without user ID and password 16
 workstation authority needed 201
 sign-on information
 displaying
 DSPSGNINF user profile
 parameter 91
 QDSPSGNINF system value 26
 Sign-on Information display
 DSPSGNINF user profile
 parameter 90
 example 27
 expiration warning message 48
 expired password message 47, 78
 signing
 integrity 3
 object 3
 SIGNOFF (Sign Off) command
 object authority required 485
 Signon screen
 changing 204
 displaying source for 204
 Signon screen display file 204
 size of password 50, 51
 SLTCMD (Select Command) command
 object authority required 361
 SM (systems management change) file
 layout 673
 SM (systems management change)
 journal entry type 284
 SNA distribution services (QSNADS) user
 profile 321
 SNADS (Systems Network Architecture
 distribution services)
 QSNADS user profile 321
 SNDBRKMSG (Send Break Message)
 command
 object authority required 440
 SNDDOC (Send Document) command
 object auditing 516
 SNDDST (Send Distribution) command
 object auditing 517
 object authority required 374
 SNDDSTQ (Send Distribution Queue)
 command
 authorized IBM-supplied user
 profiles 336
 object authority required 374
 SNDDTAARA (Send Data Area)
 command
 object auditing 519
 SNDEMLIGC (Send DBCS 3270PC
 Emulation Code) command
 object authority required 371
 SNDFNCIMG (Send Finance Diskette
 Image) command
 object authority required 389
 SNDJRNE (Send Journal Entry)
 command 292
 object auditing 531
 object authority required 420
 SNDMGRDTA (Send Migration Data)
 command
 object authority required 442
 SNDMSG (Send Message) command
 object authority required 440
 SNDNETF (Send Network File) command
 object authority required 444
 SNDNETMSG (Send Network Message)
 command
 object authority required 444
 SNDNETSPLF (Send Network Spooled
 File) command
 action auditing 552
 object auditing 541
 object authority required 482
 output queue parameters 211
 SNDNWSMSG (Send Network Server
 Message) command
 object authority required 447
 SNDPGMMSG (Send Program Message)
 command
 object authority required 440
 SNDPRD (Send Product) command
 authorized IBM-supplied user
 profiles 336
 SNDPTF (Send PTF) command
 authorized IBM-supplied user
 profiles 336

SNDPTFORD (Send Program Temporary Fix Order) command
 authorized IBM-supplied user profiles 336
 object authority required 477

SNDRJECMD (Send RJE Command) command
 object authority required 473

SNDRJECMD (Send RJE) command
 object authority required 473

SNDRPY (Send Reply) command
 object auditing 538
 object authority required 440

SNDSMGOBJ (Send Systems Management Object) command
 authorized IBM-supplied user profiles 336

SNDSRVRQS (Send Service Request) command
 authorized IBM-supplied user profiles 336
 object authority required 477

SNDTCPSPLF (Send TCP Spooled File) command
 object authority required 482

SNDTCPSPLF (Send TCP/IP Spooled File) command
 action auditing 552
 object auditing 562
 object authority required 489

SNDUSRMSG (Send User Message) command
 object authority required 440

SO (server security user information actions) file layout 674

socket
 giving
 audit journal (QAUDJRN) entry 281

sockets
 object authority required for commands 352

sort sequence
 QSRTSEQ system value 105
 shared weight 105
 unique weight 105
 user profile 105

source file
 securing 242

SPCAUT (special authority) parameter
 recommendations 88
 user profile 84

SPCENV (special environment) parameter
 recommendations 89
 routing interactive job 90

Special Authorities
 authorities, special 240

Special Authorities, Accumulating 240

special authority
 *ALLOBJ (all object)
 auditing 260
 automatically added 13
 automatically removed 13
 failed sign-on 201
 functions allowed 85
 risks 85

special authority (*continued*)
 *AUDIT (audit)
 functions allowed 88
 risks 88

 *IOSYSCFG (system configuration)
 functions allowed 88
 risks 88

 *JOBCTL (job control)
 functions allowed 86
 output queue parameters 212
 priority limit (PTYLMT) parameter 95
 risks 86

 *SAVSYS (save system)
 *OBJEXIST authority 132, 340
 automatically removed 13
 description 256
 functions allowed 86
 risks 86

 *SECADM (security administrator)
 functions allowed 85

 *SERVICE (service)
 failed sign-on 201
 functions allowed 87
 risks 87

 *SPLCTL (spool control)
 functions allowed 86
 output queue parameters 213
 risks 86

 added by system
 changing security level 13

 adopted authority 150

 analyzing assignment 711

 changing security level 13

 definition 84

 listing users 302

 recommendations 88

 removed by system
 automatically removed 249
 changing security level 13

 user profile 84

special authority (SPCAUT) parameter
 recommendations 88
 user profile 84

special environment (QSPCENV) system value 89

special environment (SPCENV) parameter
 recommendations 89
 routing interactive job 90

Special Files (*CHRSE) auditing 505

spelling aid dictionary
 object authority required for commands 480

spelling aid dictionary (*SPADCT) auditing 552

sphere of control
 object authority required for commands 480

spool (QSPL) user profile 321

spool control (*SPLCTL) special authority
 functions allowed 86
 output queue parameters 213
 risks 86

spool job (QSPLJOB) user profile 321

spooled file
 *JOBCTL (job control) special authority 86

spooled file (*continued*)
 *SPLCTL (spool control) special authority 86
 action auditing 552
 changing
 audit journal (QAUDJRN) entry 284
 copying 211
 deleting user profile 124
 displaying 211
 moving 211
 object authority required for commands 481
 owner 211
 securing 211
 working with 211

spooled file changes (*SPLFDTA) audit level 284, 552

SQL
 file security 239

SQL catalog 239

SQL package (*SQLPKG) auditing 554

SRC (system reference code)
 B900 3D10 (auditing error) 66

SRTSEQ (sort sequence) parameter
 user profile 105

ST (service tools action) file layout 675

ST (service tools action) journal entry type 283

Start QSH (STRQSH) command
 object authority required
 alias, QSH 466

Start System/36 (STRS36) command
 user profile
 special environment 89

starting
 auditing function 290
 connection
 audit journal (QAUDJRN) entry 273

state
 program 15

state attribute
 object 15

state attribute, program
 displaying 15

STATFS (Display Mounted File System Information) command
 object authority required 445

status (STATUS) parameter
 user profile 78

status message
 displaying (*STSMMSG user option) 108
 not displaying (*NOSTSMMSG user option) 108

stopping
 audit function 295
 auditing 66

storage
 enhanced hardware protection 17
 maximum (MAXSTG) parameter 94
 reclaiming 19, 145, 255
 setting QALWUSRDMN (allow user objects) system value 26

storage (*continued*)
 threshold
 audit (QAUDJRN) journal receiver 293
 user profile 94
 storage pool 218
 STRAPF (Start Advanced Printer Function) command
 object authority required 353, 387
 STRASPBAL
 authorized IBM-supplied user profiles 336
 STRASPBAL command 370
 STRASPSSN
 authorized IBM-supplied user profiles 336
 STRBEST (Start Best/1-400 Capacity Planner) command
 object authority required 460
 STRBEST (Start BEST/1) command
 authorized IBM-supplied user profiles 336
 STRBGU (Start Business Graphics Utility) command
 object authority required 353
 STRCAD
 authorized IBM-supplied user profiles 336
 STRCAD command
 object authority required 360
 STRCBLDBG (Start COBOL Debug) command
 object authority required 430, 465
 STRCGU (Start CGU) command
 object authority required 380
 STRCHTSVR (Start Clustered Hash Table Server)
 authorized IBM-supplied user profiles 336
 STRCLNUP (Start Cleanup) command
 object authority required 451
 STRCLUNOD
 authorized IBM-supplied user profiles 336
 STRCLUNOD command
 object authority required 360
 STRCMNTRC (Start Communications Trace) command
 authorized IBM-supplied user profiles 336
 object authority required 477
 STRCMTCTL (Start Commitment Control) command
 object authority required 362
 STRCPYSCN (Start Copy Screen) command
 object authority required 477
 STRCRG
 authorized IBM-supplied user profiles 336
 STRCSP (Start CSP/AE Utilities) command
 object auditing 544
 STRDBG (Start Debug) command
 authorized IBM-supplied user profiles 336
 object auditing 523, 543
 STRDBG (Start Debug) command (*continued*)
 object authority required 465
 STRDBGSVR (Start Debug Server) command
 authorized IBM-supplied user profiles 336
 STRDBMON (Start Database Monitor) command
 object authority required 460
 STRDBRDR (Start Database Reader) command
 object authority required 469
 STRDFU (Start DFU) command
 object authority required 353, 387
 STRDIGQRY (Start DIG Query) command
 object authority required 379
 STRDIRSHD (Start Directory Shadow System) command
 object authority required 371
 STRDIRSHD (Start Directory Shadowing) command
 object auditing 515
 STRDKTRDR (Start Diskette Reader) command
 object authority required 469
 STRDKTWTR (Start Diskette Writer) command
 object authority required 497
 STRDSKRGZ (Start Disk Reorganization) command
 object authority required 372
 STRDW (Start Disk Watcher) command
 authorized IBM-supplied user profiles 336
 object authority required 460
 stream file (*STMF) auditing 555
 STREDU (Start Education) command
 object authority required 450
 STREML3270 (Start 3270 Display Emulation) command
 object authority required 371
 STRFMA (Start Font Management Aid) command
 object auditing 528
 object authority required 380
 STRHOSTQRY (Start HOST Query) command
 object authority required 379
 STRHOSTSVR
 authorized IBM-supplied user profiles 336
 STRHOSTSVR (Start Host Server) command
 object authority required 390
 STRIDD (Start Interactive Data Definition Utility) command
 object authority required 410
 STRIDXMON (Start Index Monitor) command
 authorized IBM-supplied user profiles 336
 STRIPSIFC (Start IP over SNA Interface) command
 authorized IBM-supplied user profiles 336
 object authority required 352
 STRJOBTRC (Start Job Trace) command
 authorized IBM-supplied user profiles 337
 object authority required 460
 STRJRN (Start Journal) command
 object authority required 405, 420
 STRJRN (Start Journaling) command
 object auditing 501
 STRJRNAP (Start Journal Access Path) command
 object authority required 420
 STRJRNLIB (Start Journaling the Llibrary) command
 object authority required 421
 STRJRNOBJ (Start Journal Object) command
 object authority required 421
 STRJRNPF (Start Journal Physical File) command
 object authority required 421
 STRJRNxxx (Start Journaling) command
 object auditing 531
 STRJW command
 authorized IBM-supplied user profiles 336
 object authority required 460
 STRLOGSVR (Start Job Log Server) command
 object authority required 413
 STRMGDSYS (Start Managed System) command
 authorized IBM-supplied user profiles 337
 STRMGRSRV (Start Manager Services) command
 authorized IBM-supplied user profiles 337
 STRMOD (Start Mode) command
 object auditing 535
 object authority required 442
 STRMSF (Start Mail Server Framework) command
 authorized IBM-supplied user profiles 337
 object authority required 438
 STRNETINS (Start Network Install) command
 authorized IBM-supplied user profiles 337
 STRNETINS (Start Network Install) command
 object authority required 453
 STRNETINS command
 object authority required 391
 STRNFSSVR (Start Network File System Server) command
 authorized IBM-supplied user profiles 337
 STRNFSSVR (Start Network File System Server) command
 object authority required 445
 STROBJCVN
 authorized IBM-supplied user profiles 337
 STROBJCVN command 348

STRPASTHR (Start Pass-Through) command
 object auditing 511
 object authority required 373

STRPDM (Start Programming Development Manager) command
 object authority required 353

STRPEX (Start Performance Explorer) command
 authorized IBM-supplied user profiles 337
 object authority required 460

STRPFRG
 authorized IBM-supplied user profiles 337

STRPFRG (Start Performance Graphics) command
 object authority required 460

STRPFRT
 authorized IBM-supplied user profiles 337

STRPFRT (Start Performance Tools) command
 object authority required 460

STRPFRTRC (Start Performance Trace) command
 authorized IBM-supplied user profiles 337
 object authority required 461

STRPJ (Start Prestart Jobs) command
 object authority required 413

STRPRTEML (Start Printer Emulation) command
 object authority required 371

STRPRTWTR (Start Printer Writer) command
 object auditing 540, 562
 object authority required 497

STRQMQR (Start Query Management Query) command
 object auditing 545, 546, 547
 object authority required 467

STRQRY (Start Query) command
 object authority required 467

STRQSH (Start QSH) command
 object authority required
 alias, QSH 466

STRQST (Start Question and Answer) command
 object authority required 468

STRREXPRC (Start REXX Procedure) command
 object authority required 430

STRRGZIDX (Start Reorganization of Index) command
 authorized IBM-supplied user profiles 337

STRRJECSL (Start RJE Console) command
 object authority required 473

STRRJERDR (Start RJE Reader) command
 object authority required 473

STRRJESSN (Start RJE Session) command
 object authority required 473

STRRJEWTR (Start RJE Writer) command
 object authority required 474

STRRLU (Start Report Layout Utility) command
 object authority required 353

STRRMTWTR (Start Remote Writer) command
 action auditing 552, 562
 object auditing 540
 object authority required 497

STRS36 (Start System/36) command
 object auditing 559
 user profile
 special environment 89

STRS36MGR (Start System/36 Migration) command
 authorized IBM-supplied user profiles 337
 object authority required 442

STRS38MGR (Start System/38 Migration) command
 authorized IBM-supplied user profiles 337
 object authority required 442

STRSAVSYNC (Set Object Access) command
 object authority required 348

STRSBS (Start Subsystem) command
 object auditing 548
 object authority required 484

STRSCHIDX (Start Search Index) command
 object auditing 549
 object authority required 411

STRSDA (Start SDA) command
 object authority required 353

STRSEU (Start SEU) command
 object authority required 353

STRSPLRCL command
 authorized IBM-supplied user profiles 337
 object authority required 482

STRSQL (Start Structured Query Language) command
 object authority required 430, 455

STRSRVJOB (Start Service Job) command
 authorized IBM-supplied user profiles 337
 object authority required 477

STRSST (Start System Service Tools) command
 authorized IBM-supplied user profiles 337
 object authority required 477

STRSSYSMGR (Start System Manager) command
 authorized IBM-supplied user profiles 337

STRTCP (Start TCP/IP) command
 authorized IBM-supplied user profiles 337

STRTCPFTP (Start TCP/IP File Transfer Protocol) command
 object authority required 489

STRTCPIFC (Start TCP/IP Interface) command
 authorized IBM-supplied user profiles 337

STRTCPPTP (Start Point-to-Point TCP/IP) command
 object authority required 489

STRTCPSPVR (Start TCP/IP Server) command
 authorized IBM-supplied user profiles 337
 object authority required 489

STRTCPTELN (Start TCP/IP TELNET) command
 object authority required 490

STRTRC (Start Trace) command
 object authority required 477

STRUPDIDX (Start Update of Index) command
 authorized IBM-supplied user profiles 337

STRWCH (Start Watch) command
 authorized IBM-supplied user profiles 337

STRWCH command
 object authority required 477

Submit Job (SBMJOB) command 200

SECBATCH menu 710

submitting
 security reports 709

subset
 authority 133

subsystem
 *JOBCTL (job control) special authority 86
 object authority required for commands 483
 sign on without user ID and password 16

subsystem description
 authority 316
 communications entry 206
 default user 316
 entry 316
 performance 218
 printing list of descriptions 316
 printing security-relevant parameters 711
 routing entry change
 audit journal (QAUDJRN) entry 282
 security 205

subsystem description (*SBSD)
 auditing 548

SUPGRPPRF (supplemental groups) parameter
 user profile 99

supplemental group
 planning 240

supplemental groups
 SUPGRPPRF user profile parameter 99

SV (action to system value) file
 layout 680

SV (action to system value) journal entry
 type 282

symbolic link (*SYMLNK) auditing 557

system
 object authority required for commands 485
 saving 245, 312

- system (*SYSTEM) domain 15
- system (*SYSTEM) state 15
- system (QSYS) library
 - authorization lists 139
- system (QSYS) user profile
 - default values 321
 - restoring 249
- system change-journal management
 - support 293
- system configuration
 - *IOSYSCFG (system configuration)
 - special authority 88
- system configuration (*IOSYSCFG)
 - special authority
 - functions allowed 88
 - risks 88
- system console 203
 - QCONSOLE system value 203
- system directory
 - changing
 - audit journal (QAUDJRN)
 - entry 275
- system distribution directory
 - *SECADM (security administrator)
 - special authority 85
 - commands for working with 314
 - deleting user profile 122
- system library list
 - changing 207, 227
 - QSYSLIBL system value 207
- system operations
 - special authority (SPCAUT)
 - parameter 84
- system operator (QSYSOPR) user
 - profile 321
- system password 131
- system portion
 - library list
 - changing 227
 - description 207
 - recommendations 209
- system program
 - calling directly 15
- system reference code (SRC)
 - B900 3D10 (auditing error) 66
- system reply list
 - object authority required for
 - commands 485
- system request function
 - adopted authority 150
- System request menu
 - options and commands 234
 - using 234
- System Request menu
 - limit device sessions
 - (LMTDEVSSN) 93
- system resources
 - limiting use
 - priority limit (PTYLMT)
 - parameter 95
 - preventing abuse 217
- system signing 3
- system status
 - working with 218
- system value
 - action when sign-on attempts reached
 - (QMAXSGNACN)
 - description 30
 - user profile status 78
 - allow object restore option
 - (QALWOBJRST) 45
 - allow user objects
 - (QALWUSRDMN) 19, 25
 - Attention-key-handling program
 - (QATNPGM) 104
 - audit
 - planning 288
 - audit control (QAUDCTL)
 - changing 315
 - displaying 315
 - audit level (QAUDLVL)
 - *AUTFAIL (authority failure)
 - description 270
 - *CREATE (create) value 272
 - *DELETE (delete) value 272
 - *JOBDDTA (job change) value 273
 - *OBJMGT (object management)
 - value 275
 - *OFCSRV (office services)
 - value 275
 - *PGMADP (adopted authority)
 - value 275
 - *PGMFAIL (program failure)
 - value 276
 - *PRTDDTA (printer output)
 - value 276
 - *SAVRST (save/restore) value 276
 - *SECURITY (security) value 280
 - *SERVICE (service tools)
 - value 283
 - *SPLFDDTA (spooled file changes)
 - value 284
 - *SYSMGT (systems management)
 - value 284
 - changing 292, 315
 - displaying 315
 - purpose 263
 - user profile 113
 - auditing 258
 - overview 65
 - auditing control (QAUDCTL)
 - overview 66
 - auditing end action
 - (QAUDENDACN) 66, 289
 - auditing force level
 - (QAUDFRCLVL) 67, 288
 - auditing level (QAUDLVL)
 - overview 67
 - auditing level extension (QAUDLVL2)
 - overview 69
 - automatic configuration of virtual
 - devices (QAUTOVRT) 37
 - automatic device configuration
 - (QAUTOCFG) 37
 - block password change
 - (QPWDCCHGBLK) 47
 - changing
 - *SECADM (security administrator)
 - special authority 85
 - audit journal (QAUDJRN)
 - entry 282
- system value (*continued*)
 - coded character set identifier
 - (QCCSID) 106
 - command for setting 316, 715
 - console (QCONSOLE) 203
 - country or region identifier
 - (QCNTYID) 106
 - create authority (QCRTAUT)
 - description 26
 - risk of changing 26
 - using 139
 - create object auditing
 - (QCRTOBJAUD) 71
 - disconnected job time-out interval
 - (QDSCJOBITV) 38
 - display sign-on information
 - (QDSPSGNINF) 26, 91
 - file systems
 - scan (QSCANFS) 33
 - file systems control
 - scan (QSCANFCTL) 33
 - inactive job
 - message queue
 - (QINACTMSGQ) 28
 - time-out interval
 - (QINACTITV) 27
 - integrated file systems
 - scan (QSCANFS) 33
 - integrated file systems control
 - scan (QSCANFCTL) 33
 - keyboard buffering (QKBDBUF) 94
 - language identifier (QLANGID) 105
 - limit device sessions (QLMTDEVSSN)
 - auditing 260
 - description 29
 - LMTDEVSSN user profile
 - parameter 93
 - QLMTDEVSSN (limit device
 - sessions) 29
 - limit security officer (QLMTSECOFR)
 - authority to device
 - descriptions 201
 - changing security levels 13
 - description 29
 - sign-on process 203
 - listing 258
 - maximum sign-on attempts
 - (QMAXSIGN)
 - auditing 258, 262
 - description 30
 - user profile status 78
 - object authority required for
 - commands 486
 - password
 - approval program
 - (QPWDVLDPGM) 60
 - auditing expiration 259
 - duplicate (QPWDRQDDIF) 51
 - expiration interval
 - (QPWDEXPITV) 47, 91
 - expiration warning
 - (QPWDEXPWRN) 48
 - limit adjacent
 - (QPWDLMTAJC) 52
 - limit characters
 - (QPWDLMTCHR) 52

system value (*continued*)

- password (*continued*)
 - limit repeated characters (QPWDLMTREP) 53
 - maximum length (QPWDMAXLEN) 51
 - minimum length (QPWDMINLEN) 50
 - overview 46
 - position characters (QPWDPOSDIF) 53
 - preventing trivial 259
 - required password digits (QPWDRQDDGT) 54
 - restriction of consecutive digits (QPWDLMTAJC) 52
 - validation program (QPWDLDPGM) 60
- password expiration interval (QPWDEXPITV)
 - PWDEXPITV user profile parameter 91
- print device (QPRTDEV) 103
- printing 258
- printing security-communications 316
- printing security-relevant 316, 711
- QALWOBJRST (allow object restore option) 45
- QALWOBJRST (allow object restore)
 - value set by CFGSYSSEC command 716
- QALWUSRDMN (allow user objects) 19, 25
- QATNPGM (Attention-key-handling program) 104
- QAUDCTL (audit control)
 - changing 315, 709
 - displaying 315, 709
- QAUDCTL (auditing control)
 - overview 66
- QAUDENDACN (auditing end action) 66, 289
- QAUDFRCLVL (auditing force level) 67, 288
- QAUDLVL (audit level)
 - *AUTFAIL (authority failure) description 270
 - *CREATE (create) value 272
 - *DELETE (delete) value 272
 - *JOBDDTA (job change) value 273
 - *OBJMGT (object management) value 275
 - *OFCSRV (office services) value 275
 - *PGMADP (adopted authority) value 275
 - *PGMFAIL (program failure) value 276
 - *PRTDATA (printed output) value 276
 - *SAVRST (save/restore) value 276
 - *SECURITY (security) value 280
 - *SERVICE (service tools) value 283
 - *SPLFDDTA (spooled file changes) value 284

system value (*continued*)

- QAUDLVL (audit level) (*continued*)
 - *SYSMGT (systems management) value 284
 - changing 292, 315, 709
 - displaying 315, 709
 - purpose 263
 - user profile 113
- QAUDLVL (auditing level)
 - overview 67
- QAUDLVL2 (auditing level extension)
 - overview 69
- QAUTOCFG (automatic configuration)
 - value set by CFGSYSSEC command 716
- QAUTOCFG (automatic device configuration) 37
- QAUTOVRT (automatic configuration of virtual devices) 37
- QAUTOVRT (automatic virtual-device configuration)
 - value set by CFGSYSSEC command 716
- QCCSID (coded character set identifier) 106
- QCNTYID (country or region identifier) 106
- QCONSOLE (console) 203
- QCRTAUT (create authority)
 - description 26
 - risk of changing 26
 - using 139
- QCRTOBJAUD (create object auditing) 71
- QDEVRCYACN (device recovery action)
 - value set by CFGSYSSEC command 716
- QDSCJOBITV (disconnected job time-out interval) 38
 - value set by CFGSYSSEC command 716
- QDPSGNINF (display sign-on information) 26, 91
 - value set by CFGSYSSEC command 716
- QFRCCVNRST (force conversion on restore) 43
- QINACTITV (inactive job time-out interval) 27
 - value set by CFGSYSSEC command 716
- QINACTMSGQ (inactive job message queue) 28
 - value set by CFGSYSSEC command 716
- QKBDBUF (keyboard buffering) 94
- QLANGID (language identifier) 105
- QLMTDEVSSN (limit device sessions)
 - auditing 260
 - LMTDEVSSN user profile parameter 93
- QLMTSECOFR (limit security officer)
 - auditing 258
 - authority to device descriptions 201
 - changing security levels 13

system value (*continued*)

- QLMTSECOFR (limit security officer) (*continued*)
 - description 29
 - sign-on process 203
 - value set by CFGSYSSEC command 716
- QMAXSGNACN (action when sign-on attempts reached)
 - description 30
 - user profile status 78
 - value set by CFGSYSSEC command 716
- QMAXSIGN (maximum sign-on attempts)
 - auditing 258, 262
 - description 30
 - user profile status 78
 - value set by CFGSYSSEC command 716
- QPRTDEV (print device) 103
- QPWDCCHGBLK (block password change)
 - description 47
- QPWDEXPITV (password expiration interval)
 - auditing 259
 - description 47
 - PWDEXPITV user profile parameter 91
 - value set by CFGSYSSEC command 716
- QPWDEXPWRN (password expiration warning)
 - description 48
- QPWDLMTAJC (password limit adjacent) 52
- QPWDLMTAJC (password restrict adjacent characters)
 - value set by CFGSYSSEC command 716
- QPWDLMTCHR (limit characters) 52
- QPWDLMTCHR (password restrict characters)
 - value set by CFGSYSSEC command 716
- QPWDLMTREP (limit repeated characters) 53
- QPWDLMTREP (password limit repeated characters)
 - value set by CFGSYSSEC command 716
- QPWDLMTREP (password require position difference)
 - value set by CFGSYSSEC command 716
- QPWDMAXLEN (password maximum length) 51
 - value set by CFGSYSSEC command 716
- QPWDMINLEN (password minimum length) 50
 - value set by CFGSYSSEC command 716
- QPWDPOSDIF (position characters) 53

- system value (*continued*)
 - QPWDRQDDGT (password require numeric character)
 - value set by CFGSYSSEC command 716
 - QPWDRQDDGT (required password digits) 54
 - QPWDRQDDIF (duplicate password) 51
 - QPWDRQDDIF (password required difference)
 - value set by CFGSYSSEC command 716
 - QPWDVLDPGM (password validation program) 60
 - value set by CFGSYSSEC command 716
 - QRETSVRSEC (retain server security) 31
 - QRMTSIGN (allow remote sign-on)
 - value set by CFGSYSSEC command 716
 - QRMTSIGN (remote sign-on) 32, 262
 - QRMTSRVATR (remote service attribute) 39
 - QSCANFS (scan file systems) 33
 - QSCANFCTL (scan file systems control) 33
 - QSECURITY (security level)
 - auditing 258
 - automatic user profile creation 73
 - changing, 20 from higher level 13
 - changing, level 10 to level 20 12
 - changing, level 20 to 30 13
 - changing, to level 40 18
 - changing, to level 50 20
 - comparison of levels 9
 - disabling level 40 19
 - disabling level 50 21
 - enforcing QLMTSECOFR system value 203
 - internal control blocks 20
 - introduction 2
 - level 10 12
 - level 20 12
 - level 30 13
 - level 40 14
 - level 50 19
 - message handling 20
 - overview 9
 - recommendations 11
 - special authority 11
 - user class 11
 - validating parameters 17
 - value set by CFGSYSSEC command 716
 - QSHRMEMCTL (share memory control)
 - description 34
 - possible values 35
 - QSPCENV (special environment) 89
 - QSRTSEQ (sort sequence) 105
 - QSSLCSL (SSL cipher specification list) 39
 - QSSLCSLCTL (SSL cipher control) 40
 - QSSLPCL (SSL protocols) 40
 - QSYSLIBL (system library list) 207
 - system value (*continued*)
 - QUSEADPAUT (use adopted authority)
 - description 35
 - risk of changing 36
 - QUSRLIBL (user library list) 96
 - QVFYOBRJST (verify object on restore) 41
 - remote service attribute (QRMTSRVATR) 39
 - remote sign-on (QRMTSIGN) 32, 262
 - retain server security (QRETSVRSEC) 31
 - Scan File Systems (QSCANFS) 33
 - Scan File Systems (QSCANFCTL) 33
 - Secure Sockets Layer (SSL) cipher control (QSSLCSLCTL) 40
 - Secure Sockets Layer (SSL) cipher specification list (QSSLCSL) 39
 - Secure Sockets Layer (SSL) protocols (QSSLPCL) 40
 - security
 - introduction 3
 - overview 24
 - setting 715
 - security level (QSECURITY)
 - auditing 258
 - automatic user profile creation 73
 - changing, 20 from higher level 13
 - changing, level 10 to level 20 12
 - changing, level 20 to 30 13
 - changing, to level 40 18
 - changing, to level 50 20
 - comparison of levels 9
 - disabling level 40 19
 - disabling level 50 21
 - enforcing QLMTSECOFR system value 203
 - introduction 2
 - level 10 12
 - level 20 12
 - level 30 13
 - level 40 14
 - level 50 19
 - overview 9
 - recommendations 11
 - special authority 11
 - user class 11
 - security-related
 - overview 36
 - share memory control (QSHRMEMCTL)
 - description 34
 - possible values 35
 - sign-on 48
 - action when attempts reached (QMAXSGNACN) 30, 78
 - maximum attempts (QMAXSIGN) 30, 78, 258, 262
 - remote (QRMTSIGN) 32, 262
 - sort sequence (QSRTSEQ) 105
 - special environment (QSPCENV) 89
 - system library list (QSYSLIBL) 207
 - use adopted authority (QUSEADPAUT)
 - description 35
 - system value (*continued*)
 - use adopted authority (QUSEADPAUT) (*continued*)
 - risk of changing 36
 - user library list (QUSRLIBL) 96
 - verify object on restore (QVFYOBRJST) 41
 - working with 258
 - system-defined authority 133
 - System/36
 - authority for deleted files 153
 - migration
 - authority holders 154
 - System/36 environment
 - object authority required for commands 486
 - user profile 89
 - System/38
 - command security 235
 - System/38 environment 89
 - System/38 Environment 137
 - systems management
 - changing
 - audit journal (QAUDJRN) entry 284
 - systems management (*SYSMGT) audit level 284
 - systems management change (SM) file layout 673
 - systems management change (SM) journal entry type 284
 - Systems Network Architecture (SNA)
 - distribution services (QSNADS) user profile 321
 - Systems Network Architecture
 - distribution services (SNADS) QSNADS user profile 321
- ## T
- table
 - object authority required for commands 489
 - table (*TBL) auditing 559
 - tape
 - object authority required for commands 438
 - protecting 258
 - tape cartridge
 - object authority required for commands 438
 - TCP/IP (QTCP) user profile 321
 - TCP/IP (Transmission Control Protocol/Internet Protocol)
 - object authority required for commands 489
 - TCP/IP printing support (QTMLPLPD)
 - user profile 321
 - TELNET (Start TCP/IP TELNET)
 - command
 - object authority required 490
 - temporary (QTEMP) library
 - security level 50 19
 - test request (QTSTRQS) user profile 321
 - text (TEXT) parameter
 - user profile 84

text index
 object authority required for
 commands 449

TFRBCHJOB (Transfer Batch Job)
 command
 object auditing 529
 object authority required 414

TFRCTL (Transfer Control) command
 object authority required 465
 transferring adopted authority 150

TFRGRPJOB (Transfer to Group Job)
 command
 adopted authority 150
 object authority required 414

TFRJOB (Transfer Job) command
 object auditing 529
 object authority required 414

TFRPASTHR (Transfer Pass-Through)
 command
 object authority required 373

TFRSECJOB (Transfer Secondary Job)
 command
 object authority required 414

time slice 217

time zone description commands 491

time-out interval
 inactive jobs (QINACTITV) system
 value 27
 message queue (QINACTMSGQ)
 system value 28

token-ring
 object authority required for
 commands 437

total change of password 53

Transfer Control (TFRCTL) command
 transferring adopted authority 150

Transfer to Group Job (TFRGRPJOB)
 command
 adopted authority 150

transferring
 adopted authority 150
 to group job 150

translation of programs 17

Transmission Control Protocol/Internet
 Protocol (TCP/IP)
 object authority required for
 commands 489

TRCASPBAL
 authorized IBM-supplied user
 profiles 337

TRCASPBAL command 370

TRCCNN (Trace Connection) command
 object authority required 477

TRCCPIC (Trace CPI Communications)
 command
 authorized IBM-supplied user
 profiles 337
 object authority required 477

TRCCSP (Trace CSP/AE Application)
 command
 object auditing 544

TRCICF (Trace ICF) command
 authorized IBM-supplied user
 profiles 337
 object authority required 477

TRCINT (Trace Internal) command
 authorized IBM-supplied user
 profiles 337
 object authority required 477

TRCJOB (Trace Job) command
 authorized IBM-supplied user
 profiles 337
 object authority required 477

TRCTCPAPP
 authorized IBM-supplied user
 profiles 337

TRCTCPAPP command
 object authority required 478

trigger program
 listing all 316, 711

trivial password
 preventing 46, 259

TRMPRTEML (Terminate Printer
 Emulation) command
 object authority required 371

TRNCKMKSF command
 object authority required 367

TRNPIN (Translate Personal Identification
 Number) command
 authorized IBM-supplied user
 profiles 337

type-ahead (*TYPEAHEAD) keyboard
 buffering 94

U

uid (user identification number)
 restoring 249

unauthorized
 programs 262

UNMOUNT (Remove Mounted File
 System)
 object authority required 491

UNMOUNT (Remove Mounted File
 System) command
 object authority required 445

unsupported interface
 audit journal (QAUDJRN) entry 16,
 276

update (*UPD) authority 132, 340

UPDDTA (Update Data) command
 object authority required 387

UPDPGM (Update Program) command
 object auditing 504, 536, 543
 object authority required 465

UPDPTFINF (Update PTF Information)
 command
 authorized IBM-supplied user
 profiles 337

UPDSRVPGM (Create Service Program)
 command
 object auditing 536

UPDSRVPGM (Update Service Program)
 command
 object auditing 504, 554
 object authority required 465

use (*USE) authority 134, 341

use adopted authority (QUSEADPAUT)
 system value
 description 35
 risk of changing 36

use adopted authority (USEADPAUT)
 parameter 152

USEADPAUT (use adopted authority)
 parameter 152

user
 adding 118
 auditing
 changing 88
 working with 127
 enrolling 118
 user (*USER) domain 15
 user (*USER) state 15
 user auditing
 changing
 command description 313
 command descriptions 311

user authority
 adding 161
 copying
 command description 311
 example 121
 recommendations 165
 renaming profile 127

user class
 analyzing assignment 711

user class (USRCLS) parameter
 description 79
 recommendations 79

USER DEF (user-defined) authority 160

user domain object
 restricting 19
 security exposure 19

user expiration date (USREXPDATE)
 parameter
 user profile 111

user expiration interval (USREXPITV)
 parameter
 user profile 111

user ID
 DST (dedicated service tools)
 changing 129
 incorrect
 audit journal (QAUDJRN)
 entry 271

user identification number (uid)
 restoring 249

user identification number parameter
 user profile 108

user index (*USRIDX) auditing 559

user index (*USRIDX) object 19

user option (CHRIDCTL) parameter
 user profile 106

user option (LOCALE) parameter
 user profile 107

user option (SETJOBATR) parameter
 user profile 107

user option (USROPT) parameter
 *CLKWD (CL keyword) 106, 107, 108
 *EXPERT (expert) 106, 107, 108, 160
 *HLPFULL (help full screen) 108
 *NOSTSMG (no status
 message) 108
 *PRTMSG (printing message) 108
 *ROLLKEY (roll key) 108
 *STSMG (status message) 108
 user profile 106, 107, 108

USER parameter on job description 206

- user permission
 - granting 313
 - object authority required for commands 449
 - revoking 313
- user portion
 - library list
 - controlling 226
 - description 207
 - recommendations 210
- user profile
 - (gid) group identification number 109
 - *ALLOBJ (all object) special authority 85
 - *AUDIT (audit) special authority 88
 - *IOSYSCFG (system configuration) special authority 88
 - *JOBCTL (job control) special authority 86
 - *SAVSYS (save system) special authority 86
 - *SECADM (security administrator) special authority 85
 - *SERVICE (service) special authority 87
 - *SPLCTL (spool control) special authority 86
 - accounting code (ACGCDE) 100
 - ACGCDE (accounting code) 100
 - action auditing (AUDLVL) 113
 - all numeric user ID 75
 - all object (*ALLOBJ) special authority 85
 - analyzing
 - by special authorities 711
 - by user class 711
 - analyzing with query 301
 - assistance level (ASTLVL) 80
 - ASTLVL (assistance level) 80
 - ATNPGM (Attention-key-handling program) 104
 - Attention-key-handling program (ATNPGM) 104
 - audit (*AUDIT) special authority 88
 - audit level (AUDLVL)
 - *CMD (command string) value 272
 - auditing
 - *ALLOBJ special authority 260
 - authority to use 261
 - authorized users 301
 - AUDLVL (action auditing) 113
 - AUDLVL (audit level)
 - *CMD (command string) value 272
 - AUT (authority) 112
 - authority
 - storing 247
 - authority (AUT) 112
 - automatic creation 73
 - CCSID (coded character set identifier) 106
 - changes when restoring 248
 - changing
 - audit journal (QAUDJRN) entry 277

- user profile (*continued*)
 - changing (*continued*)
 - command descriptions 311
 - methods 122
 - password 311
 - password composition system values 47
 - setting password equal to profile name 76
 - checking for default password 707
 - CNTYRID (country or region identifier) 105
 - coded character set identifier (CCSID) 106
 - commands for working with 311
 - copying 119
 - countryor region identifier (CNTYRID) 105
 - creating
 - audit journal (QAUDJRN) entry 277
 - command descriptions 311
 - example description 118
 - methods 117
 - CURLIB (current library) 81
 - current library (CURLIB) 81
 - default values table 319
 - deleting
 - command description 311
 - directory entry 122
 - distribution lists 122
 - message queue 122
 - spooled files 124
 - delivery (DLVRY) 102
 - description (TEXT) 84
 - DEV (print device) 103
 - displaying
 - command description 311
 - individual 125
 - programs that adopt 151
 - sign-on information (DSPSGNINF) 91
 - DLVRY (message queue delivery) 102
 - DOCPWD (document password) 100
 - document password (DOCPWD) 100
 - DSPSGNINF (display sign-on information) 91
 - eim association (EIMASSOC) 110
 - EIMASSOC (eim association) 110
 - enabling
 - sample program 125
 - exit points 128
 - expiration date (USREXPDATE) 111
 - expiration interval (USREXPITV) 111
 - group authority (GRPAUT) 98, 143, 145
 - group authority type (GRPAUTTYP) 98, 145
 - group identification number (gid) 109
 - group profile (GRPPRF) 145
 - changes when restoring profile 248
 - description 97
 - GRPAUT (group authority) 98, 143, 145

- user profile (*continued*)
 - GRPAUTTYP (group authority type) 98, 145
 - GRPPRF (group profile) 145
 - changes when restoring profile 248
 - description 97
 - home directory (HOMEDIR) 109
 - HOMEDIR (home directory) 109
 - IBM-supplied
 - auditing 258
 - default values table 319
 - purpose 128
 - initial menu (INLMNU) 82
 - initial program (INLPGM) 81
 - INLMNU (initial menu) 82
 - INLPGM (initial program) 81
 - introduction 4
 - job control (*JOBCTL) special authority 86
 - job description (JOBDD) 96
 - JOBDD (job description) 96
 - KBDBUF (keyboard buffering) 93
 - keyboard buffering (KBDBUF) 93
 - LANGID (language identifier) 105
 - language identifier (LANGID) 105
 - large, examining 302
 - LCLPWDMGT (local password management) 92
 - limit capabilities
 - auditing 260
 - description 83
 - library list 210
 - limit device sessions (LMTDEVSSN) 93
 - list of permanently active
 - changing 707
 - listing
 - all users 125
 - inactive 302
 - selected 302
 - users with command capability 302
 - users with special authorities 302
 - listing all 125
 - LMTCPB (limit capabilities) 83, 210
 - LMTDEVSSN (limit device sessions) 93
 - local password management (LCLPWDMGT) 92
 - LOCALE (locale) 107
 - LOCALE (user options) 107
 - maximum storage (MAXSTG)
 - description 94
 - group ownership of objects 143
 - MAXSTG (maximum storage)
 - description 94
 - group ownership of objects 143
 - message queue (MSGQ) 101
 - message queue delivery (DLVRY) 102
 - message queue severity (SEV) 102
 - MSGQ (message queue) 101
 - name (USRPRF) 75
 - naming 75
 - OBJAUD (object auditing) 112
 - object auditing (OBJAUD) 112

- user profile (*continued*)
 - object authority required for
 - commands 491, 492
 - object owner
 - deleting 143
 - output queue (OUTQ) 103
 - OUTQ (output queue) 103
 - owned object information 115
 - OWNER (owner of objects
 - created) 97, 143
 - owner (OWNER) 145
 - OWNER (owner) 145
 - owner of objects created
 - (OWNER) 97, 143
 - password 76
 - password expiration interval
 - (PWDEXPITV) 91
 - performance
 - save and restore 115
 - primary group 124
 - print device (DEV) 103
 - printing 302
 - priority limit (PTYLMT) 95
 - private authorities 115
 - PTYLMT (priority limit) 95
 - public authority (AUT) 112
 - PWDEXP (set password to
 - expired) 77
 - PWDEXPITV (password expiration
 - interval) 91
 - related commands for working
 - with 312
 - renaming 126
 - restoring
 - audit journal (QAUDJRN)
 - entry 277
 - command description 312
 - commands 245
 - procedures 248
 - restoring authority
 - audit journal (QAUDJRN)
 - entry 277
 - retrieving 128, 311
 - roles 73
 - save system (*SAVSYS) special
 - authority 86
 - saving 245
 - security administrator (*SECADM)
 - special authority 85
 - service (*SERVICE) special
 - authority 87
 - set job attribute (user options) 106, 107
 - set password to expired
 - (PWDEXP) 77
 - SEV (message queue severity) 102
 - severity (SEV) 102
 - sort sequence (SRTSEQ) 105
 - SPCAUT (special authority) 84
 - SPCENV (special environment) 89
 - special authority (SPCAUT) 84
 - special environment (SPCENV) 89
 - spool control (*SPLCTL) special
 - authority 86
 - SRTSEQ (sort sequence) 105
 - status (STATUS) 78

- user profile (*continued*)
 - storing
 - authority 246, 247
 - SUPGRPPRF (supplemental
 - groups) 99
 - supplemental groups
 - (SUPGRPPRF) 99
 - system configuration (*IOSYSCFG)
 - special authority 88
 - System/36 environment 89
 - text (TEXT) 84
 - types of displays 126
 - types of reports 126
 - used in job description 16
 - user class (USRCLS) 79
 - user identification number 108
 - user options (CHRIDCTL) 106
 - user options (LOCALE) 107
 - user options (SETJOBATR) 107
 - user options (USROPT) 106, 107, 108
 - USRCLS (user class) 79
 - USREXPDATE (user expiration
 - date) 111
 - USREXPITV (user expiration
 - interval) 111
 - USROPT (user options) 106, 107, 108
 - USRPRF (name) 75
 - working with 117, 311
 - user profile (*USRPRF) auditing 560
 - user profile change (CP) file layout 586
 - user profile change (CP) journal entry
 - type 277
 - user profile parameter
 - group identification number(gid) 109
 - user queue (*USRQ) auditing 561
 - user queue (*USRQ) object 19
 - user space (*USRSPC) auditing 561
 - user space (*USRSPC) object 19
 - user-defined (USER DEF) authority 160
 - USRCLS (user class) parameter
 - description 79
 - recommendations 79
 - USREXPDATE (user expiration date)
 - parameter
 - user profile 111
 - USREXPITV (user expiration interval)
 - parameter
 - user profile 111
 - USROPT (user option) parameter
 - *CLKWD (CL keyword) 106, 107, 108
 - *EXPERT (expert) 106, 107, 108, 160
 - *HLPFULL (help full screen) 108
 - *NOSTSMMSG (no status
 - message) 108
 - *PRTMSG (printing message) 108
 - *ROLLKEY (roll key) 108
 - *STSMSG (status message) 108
 - USROPT (user options) parameter
 - user profile 106, 107, 108
 - USRPRF (name) parameter 75

V

- VA (access control list change) journal
 - entry type 282
- VA (changing access control list) file
 - layout 681

- validating
 - restored programs 17
- validating parameters 17
- validating password 60
- validation list
 - object authority required for
 - commands 495
- validation list (*VLDDL) auditing 562
- validation list (VO) file layout 685
- validation lists
 - Internet user 243
- Validation Lists, Create 243
- Validation Lists, Delete 243
- validation program, password 61, 62
- validation value
 - audit journal (QAUDJRN) entry 276
 - definition 17
- VC (connection start and end) file
 - layout 681
- VC (connection start or end) journal entry
 - type 273
- verify object on restore (QVfyOBRST)
 - system value 41
- VF (close of server files) file layout 682
- VFYCMN (Verify Communications)
 - command
 - authorized IBM-supplied user
 - profiles 337
 - object auditing 510, 511, 533
 - object authority required 462, 478
- VFYIMGCLG command
 - object authority required 391
- VFYLNKLPDA (Verify Link supporting
 - LPDA-2) command
 - authorized IBM-supplied user
 - profiles 337
 - object authority required 478
- VFYLNKLPDA (Verify Link Supporting
 - LPDA-2) command
 - object auditing 533
- VFYMSTK (Verify Master Key) command
 - authorized IBM-supplied user
 - profiles 337
- VFYPIN (Verify Personal Identification
 - Number) command
 - authorized IBM-supplied user
 - profiles 337
- VFYPR (Verify Printer) command
 - authorized IBM-supplied user
 - profiles 337
 - object authority required 462, 478
- VFYTAP (Verify Tape) command
 - authorized IBM-supplied user
 - profiles 337
 - object authority required 462, 478
- VFYTCPCNN (Verify TCP/IP
 - Connection) command
 - object authority required 490
- viewing
 - audit journal entries 295
- virtual device
 - automatic configuration (QAUTOVRT
 - system value) 37
 - definition 37
- virtual printer
 - securing 216

- virus
 - detecting 262, 304, 311
 - scanning 304
- VL (account limit exceeded) file layout 683
- VL (account limit exceeded) journal entry type 284
- VM/MVS bridge (QGATE) user profile 321
- VN (network log on and off) file layout 684
- VN (network log on or off) journal entry type 273
- VO (validation list) file layout 685
- VP (network password error) file layout 686
- VP (network password error) journal entry type 271
- VR (network resource access) file layout 687
- VRYCFG (Vary Configuration) command
 - object auditing 510, 511, 533, 539, 540
 - object authority required 363
- VS (server session) file layout 688
- VS (server session) journal entry type 273
- VU (network profile change) file layout 689
- VU (network profile change) journal entry type 282
- VV (service status change) file layout 690
- VV (service status change) journal entry type 283

W

- wireless LAN configuration
 - object authority required for commands 381
- Work with Authority (WRKAUT) command 159, 310
- Work with Authorization Lists (WRKAUTL) command 309
- Work with Database Files Using IDDU (WRKDBFIDD) command
 - object authority required 410
- Work with Directory (WRKDIRE) command 314
- Work with Journal (WRKJRN) command 294, 301
- Work with Journal Attributes (WRKJRNA) command 294, 301
- Work with Objects (WRKOBJ) command 310
- Work with Objects by Owner (WRKOBJOWN) command
 - auditing 261
 - description 310
 - using 163
- Work with Objects by Owner display 123, 163
- Work with Objects by Primary Group (WRKOBJPGP) command 144, 164
 - description 310
- Work with Output Queue Description (WRKOUTQD) command 211
- Work with Spooled Files (WRKSPLF) command 211
- Work with System Status (WRKSYSSTS) command 218
- Work with System Values (WRKSYSVAL) command 258
- Work with User Enrollment display 118
- Work with User Profiles (WRKUSRPRF) command 117, 311
- Work with User Profiles display 117
- working on behalf auditing 534
- working with
 - authority 310
 - authority holders 309, 314
 - authorization lists 309
 - directory 314
 - document library objects (DLO) 313
 - journal 301
 - journal attributes 294, 301
 - object authority 310
 - object ownership 163
 - objects 310
 - objects by owner 310
 - objects by primary group 144, 310
 - output queue description 211
 - password 311
 - primary group 164
 - spooled files 211
 - system directory 314
 - system status 218
 - user auditing 127
 - user profiles 117, 311, 312
- workstation
 - authority to sign-on 201
 - limiting user to one at a time 29
 - restricting access 258
 - securing 201
 - security officer access 29
- workstation customizing object
 - object authority required for commands 496
- workstation entry
 - job description 206
 - sign on without user ID and password 16
- workstation user (QUSER) user profile 321
- writer
 - *JOBCTL (job control) special authority 86
 - object authority required for commands 496
- WRKACTJOB (Work with Active Jobs) command
 - object authority required 414
- WRKALR (Work with Alerts) command
 - object authority required 352
- WRKALRD (Work with Alert Description) command
 - object auditing 503
- WRKALRD (Work with Alert Descriptions) command
 - object authority required 352
- WRKALRTBL (Work with Alert Table) command
 - object auditing 503
- WRKALRTBL (Work with Alert Tables) command
 - object authority required 352
- WRKARMJOB command
 - object authority required 414
- WRKASPCPYD
 - authorized IBM-supplied user profiles 337
- WRKASPJOB command
 - object authority required 414
- WRKAUT (Work with Authority Directory) command
 - object authority required 405
- WRKAUT (Work with Authority) command 159
 - description 310
 - object auditing 513, 551, 556
- WRKAUTL (Work with Authorization List) command
 - object auditing 504
- WRKAUTL (Work with Authorization Lists) command
 - description 309
 - object authority required 354
- WRKBNDDIR (Work with Binding Directory) command
 - object auditing 504
 - object authority required 355
- WRKBNDDIRE (Work with Binding Directory Entry) command
 - object auditing 505
 - object authority required 355
- WRKCFGL (Work with Configuration List) command
 - object auditing 505
- WRKCFGL (Work with Configuration Lists) command
 - object authority required 364
- WRKCFGSTS (Work with Configuration Status) command
 - object auditing 512, 534, 539
 - object authority required 363
- WRKCHTFMT (Work with Chart Formats) command
 - object authority required 356
- WRKCLS (Work with Class) command
 - object auditing 507
- WRKCLS (Work with Classes) command
 - object authority required 356
- WRKCMD (Work with Command) command
 - object auditing 508
- WRKCMD (Work with Commands) command
 - object authority required 361
- WRKCMTDFN (Work with Commitment Definition) command
 - object authority required 362
- WRKCNNL (Work with Connection Lists) command
 - object auditing 508
 - object authority required 364
- WRKCNNLE (Work with Connection List Entries) command
 - object auditing 508

WRKCNTINF (Work with Contact Information) command
 authorized IBM-supplied user profiles 337
 object authority required 468, 478

WRKCODS (Work with Class-of-Service Descriptions) command
 object auditing 509
 object authority required 357

WRKCRQD (Work with Change Request Description) command
 object authority required 356

WRKCRQD (Work with Change Request Descriptions) command
 object auditing 507

WRKCSI (Work with Communications Side Information) command
 object auditing 509
 object authority required 362

WRKCTLD (Work with Controller Descriptions) command
 object auditing 510
 object authority required 366

WRKDBFIDD (Work with Database Files Using IDDU) command
 object authority required 410

WRKDDMF (Work with Distributed Data Management Files) command
 object authority required 388

WRKDEVD (Work with Device Descriptions) command
 object auditing 512
 object authority required 370

WRKDEVTBL (Work with Device Tables) command
 authorized IBM-supplied user profiles 338
 object authority required 389

WRKDIRE (Work with Directory Entry) command
 object authority required 371

WRKDIRE (Work with Directory) command
 description 314

WRKDIRLOC (Work with Directory Locations) command
 object authority required 371

WRKDIRSHD (Work with Directory Shadow Systems) command
 object authority required 371

WRKDOC (Work with Documents) command
 object auditing 517
 object authority required 377

WRKDOCLIB (Work with Document Libraries) command
 object auditing 519
 object authority required 449

WRKDOCPRITQ (Work with Document Print Queue) command
 object auditing 519
 object authority required 449

WRKDPCQ (Work with DSNX/PC Distribution Queues) command
 authorized IBM-supplied user profiles 338
 object authority required 374

WRKDSKSTS (Work with Disk Status) command
 object authority required 372

WRKDSTL (Work with Distribution Lists) command
 object authority required 374

WRKDSTQ (Work with Distribution Queue) command
 authorized IBM-supplied user profiles 338
 object authority required 374

WRKDTAARA (Work with Data Areas) command
 object auditing 520
 object authority required 367

WRKDTADCT (Work with Data Dictionaries) command
 object authority required 410

WRKDTADFN (Work with Data Definitions) command
 object authority required 410

WRKDTAQ (Work with Data Queues) command
 object auditing 520
 object authority required 368

WRKEDTD (Work with Edit Descriptions) command
 object auditing 521
 object authority required 380

WRKENVVAR (Work with Environment Variable) command
 object authority required 380

WRKF (Work with Files) command
 object auditing 525
 object authority required 388

WRKFNCNARA
 authorized IBM-supplied user profiles 338

WRKFNCNARA (Work with Functional Areas) command
 object authority required 460

WRKFCT (Work with Forms Control Table) command
 object authority required 474

WRKFLR (Work with Folders) command
 object authority required 377

WRKFNTRSC (Work with Font Resources) command
 object auditing 526
 object authority required 351

WRKFORMDF (Work with Form Definitions) command
 object auditing 526
 object authority required 351

WRKFSTAF (Work with FFST Alert Feature) command
 object authority required 478

WRKFSTPCT (Work with FFST Probe Control Table) command
 object authority required 478

WRKFTR (Work with Filters) command
 object auditing 527
 object authority required 389

WRKFTRACNE (Work with Filter Action Entries) command
 object auditing 527
 object authority required 389

WRKFTRSLTE (Work with Filter Selection Entries) command
 object auditing 527
 object authority required 389

WRKGGSS (Work with Graphics Symbol Sets) command
 object auditing 527
 object authority required 390

WRKHWRSC (Work with Hardware Resources) command
 object authority required 470

WRKHLDOPTF (Work with Help Optical Files) command
 object authority required 453

WRKIMGCLG command
 object authority required 391

WRKIMGCLGE command
 object authority required 391

WRKIPXD command 411

WRKJOB (Work with Job) command
 object authority required 414

WRKJOBBD (Work with Job Descriptions) command
 object auditing 529
 object authority required 415

WRKJOBLOG (Work with Job Logs) command
 object authority required 414

WRKJOBQ (Work with Job Queue) command
 object auditing 530
 object authority required 416

WRKJOBQD (Work with Job Queue Description) command
 object authority required 416

WRKJOBSCDE (Work with Job Schedule Entries) command
 object auditing 530
 object authority required 417

WRKJRN (Work with Journal) command
 authorized IBM-supplied user profiles 338
 object auditing 532
 object authority required 421
 using 294, 301

WRKJRNA (Work with Journal Attributes) command
 object auditing 532
 object authority required 421
 using 294, 301

WRKJRNRCV (Work with Journal Receivers) command
 object auditing 532
 object authority required 422

WRKJVMJOB command
 object authority required 412

WRKLANADPT (Work with LAN Adapters) command
 object authority required 437

WRKLIB (Work with Libraries) command
 object authority required 433

WRKLIBPDM (Work with Libraries Using PDM) command
 object authority required 353

WRKLCINF (Work with License Information) command
 authorized IBM-supplied user profiles 338

WRKLIND (Work with Line Descriptions) command
 object auditing 534
 object authority required 437

WRKLNK (Work with Links) command
 object auditing 512, 513, 550, 551, 555, 556, 558
 object authority required 406

WRKMBRPDM (Work with Members Using PDM) command
 object authority required 353

WRKMNU (Work with Menus) command
 object auditing 535
 object authority required 440

WRKMOD (Work with Module) command
 object authority required 443

WRKMOD (Work with Modules) command
 object auditing 536

WRKMODD (Work with Mode Descriptions) command
 object auditing 535
 object authority required 442

WRKMSG (Work with Messages) command
 object auditing 538
 object authority required 440

WRKMSGD (Work with Message Descriptions) command
 object auditing 536
 object authority required 441

WRKMSGF (Work with Message Files) command
 object auditing 537
 object authority required 441

WRKMSGQ (Work with Message Queues) command
 object auditing 538
 object authority required 441

WRKNAMSMTP (Work with Names for SMTP) command
 object authority required 490

WRKNETF (Work with Network Files) command
 object authority required 444

WRKNETJOBE (Work with Network Job Entries) command
 object authority required 444

WRKNETTBL (Work with Network Table Entries) command
 object authority required 490

WRKNODL (Work with Node List) command
 object auditing 538
 object authority required 449

WRKNODLE (Work with Node List Entries) command
 object auditing 538
 object authority required 449

WRKNNTBD (Work with NetBIOS Description) command
 object auditing 539

WRKNNTBD (Work with NetBIOS Description) command *(continued)*
 object authority required 444

WRKNWID (Work with Network Interface Description Command) command
 object authority required 446

WRKNWID (Work with Network Interface Description) command
 object auditing 539

WRKNWSALS (Work with Network Server Alias) command
 object authority required 447

WRKNWSCFG command
 authorized IBM-supplied user profiles 338
 object authority required 448

WRKNWSD (Work with Network Server Description) command
 object auditing 540
 object authority required 448

WRKNWSENR (Work with Network Server User Enrollment) command
 object authority required 447

WRKNWSSSN (Work with Network Server Session) command
 object authority required 447

WRKNWSSTG (Work with Network Server Storage Space) command
 object authority required 447

WRKNWSSTS (Work with Network Server Status) command
 object authority required 447

WRKOBJ (Work with Objects) command
 description 310
 object authority required 348

WRKOBJCSP (Work with Objects for CSP/AE) command
 object auditing 510, 544

WRKOBJLCK (Work with Object Lock) command
 object auditing 502

WRKOBJLCK (Work with Object Locks) command
 object authority required 348

WRKOBJOWN (Work with Objects by Owner) command
 auditing 261
 description 310
 object auditing 502, 561
 object authority required 348
 using 163

WRKOBJPDM (Work with Objects Using PDM) command
 object authority required 353

WRKOBJPGP (Work with Objects by Primary Group) command 144, 164
 object authority required 348

WRKOBJPGP (Work with Objects by Primary) command
 description 310

WRKOPTDIR (Work with Optical Directories) command
 object authority required 453

WRKOPTF (Work with Optical Files) command
 object authority required 453

WRKOPTVOL (Work with Optical Volumes) command
 object authority required 453

WRKOUTQ (Work with Output Queue) command
 object auditing 541
 object authority required 454

WRKOUTQD (Work with Output Queue Description) command
 object auditing 541
 object authority required 454
 security parameters 211

WRKOV (Work with Overlays) command
 object auditing 541
 object authority required 351

WRKPAGDFN (Work with Page Definitions) command
 object auditing 542
 object authority required 351

WRKPAGSEG (Work with Page Segments) command
 object auditing 542
 object authority required 352

WRKPCLTBL (Work with Protocol Table Entries) command
 object authority required 490

WRKPDG (Work with Print Descriptor Group) command
 object auditing 542

WRKPEXDFN command
 authorized IBM-supplied user profiles 338

WRKPEXFTR command
 authorized IBM-supplied user profiles 338

WRKPPFCST (Work with Physical File Constraints) command
 object auditing 525
 object authority required 388

WRKPGM (Work with Programs) command
 object auditing 544
 object authority required 465

WRKPGMTBL (Work with Program Tables) command
 authorized IBM-supplied user profiles 338
 object authority required 389

WRKPNLGRP (Work with Panel Groups) command
 object auditing 544
 object authority required 440

WRKPRB (Work with Problem) command
 authorized IBM-supplied user profiles 338
 object authority required 462, 478

WRKPTFGRP (Work with Program Temporary Fix Groups) 338

WRKPTFGRP (Work with PTF Group) command
 object authority required 478

WRKPTFORD 338

WRKQMF (Work with Query Management Form) command
 object auditing 546
 object authority required 467

WRKQMORY (Work with Query Management Query) command
 object authority required 467
 WRKQRY (Work with Query) command
 object authority required 467
 WRKQST (Work with Questions) command
 object authority required 468
 WRKRDBDIRE (Work with Relational Database Directory Entries) command
 object authority required 470
 WRKREGINF (Work with Registration Information) command
 object auditing 522
 WRKREGINF (Work with Registration) command
 object authority required 469
 WRKRJESSN (Work with RJE Session) command
 object authority required 474
 WRKRYPYLE (Work with System Reply List Entries) command
 object auditing 548
 object authority required 486
 WRKS36PGMA (Work with System/36 Program Attributes) command
 object auditing 543
 object authority required 488
 WRKS36PRCA (Work with System/36 Procedure Attributes) command
 object auditing 525
 object authority required 488
 WRKS36SRCA (Work with System/36 Source Attributes) command
 object auditing 525
 object authority required 488
 WRKSBMJOB (Work with Submitted Jobs) command
 object authority required 414
 WRKSBS (Work with Subsystems) command
 object auditing 549
 object authority required 484
 WRKSBSD (Work with Subsystem Descriptions) command
 object auditing 549
 object authority required 484
 WRKSBSJOB (Work with Subsystem Jobs) command
 object auditing 549
 object authority required 414
 WRKSCHIDX (Work with Search Indexes) command
 object auditing 550
 object authority required 411
 WRKSCHIDX (Work with Search Index Entries) command
 object auditing 549
 object authority required 411
 WRKSHRPOOL (Work with Shared Storage Pools) command
 object authority required 485
 WRKSOC (Work with Sphere of Control) command
 object authority required 480
 WRKSPADCT (Work with Spelling Aid Dictionaries) command
 object authority required 480
 WRKSPLF (Work with Spooled Files) command 211
 object auditing 541
 object authority required 482
 WRKSPLFA (Work with Spooled File Attributes) command
 object auditing 541
 WRKSPTPRD (Work with Supported Products) command
 object auditing 544, 545
 WRKSRVPGM (Work with Service Programs) command
 object auditing 555
 object authority required 465
 WRKSRVPVD (Work with Service Providers) command
 authorized IBM-supplied user profiles 338
 object authority required 478
 WRKSRVTBLE (Work with Service Table Entries) command
 object authority required 490
 WRKSSND (Work with Session Description) command
 object authority required 474
 WRKSYSACT
 authorized IBM-supplied user profiles 338
 WRKSYSACT (Work with System Activity) command
 object authority required 460
 WRKSYSSTS (Work with System Status) command 218
 object authority required 485
 WRKSYSVAL (Work with System Values) command
 object authority required 486
 using 258
 WRKTAPCTG (Work with Tape Cartridge) command
 object authority required 438
 WRKTBL (Work with Tables) command
 object auditing 559
 object authority required 489
 WRKTCPPSTS (Work with TCP/IP Network Status) command
 object authority required 490
 WRKTIMZON command 491
 WRKTRC command
 authorized IBM-supplied user profiles 338
 WRKTXIDX (Work with Text Index) command
 authorized IBM-supplied user profiles 338
 WRKUSRJOB (Work with User Jobs) command
 object authority required 414
 WRKUSRPRF (Work with User Profiles) command
 description 311
 object auditing 561
 object authority required 494
 using 117
 WRKUSRTBL (Work with User Tables) command
 authorized IBM-supplied user profiles 338
 object authority required 389
 WRKWCH command
 authorized IBM-supplied user profiles 338
 WRKWTR (Work with Writers) command
 object authority required 497

X

X0 (kerberos authentication) file layout 691

Y

YC (change to DLO object) file layout 698
 YR (read of DLO object) file layout 699

Z

ZC (change to object) file layout 700
 ZR (read of object) file layout 703



Printed in USA

SC41-5302-11

