



IBM Systems - iSeries Security Reference

Version 5 Release 4

SC41-5302-09





# @server

IBM Systems - iSeries Security Reference

Version 5 Release 4

SC41-5302-09

# Note Before using this information and the product it supports, read the information in Appendix I, "Notices," on page 637.

## **Tenth Edition (February 2006)**

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

This edition replaces SC41-5302-08.

© Copyright International Business Machines Corporation 1996, 2006. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

Figures ix	Chapter 3. Security System Values	19
	General Security System Values	
Tables xi		21
Tubles I I I I I I I I I I I I I I I	Authority for New Objects (QCRTAUT)	22
About Committe Defended (CC44 F200)	Display Sign-On Information (QDSPSGNINF)	
About Security Reference (SC41-5302) xv	Inactive Job Time-Out Interval (QINACTITV)	
Who Should Read This Book xv	Inactive Job Time-Out Message Queue	~`
Conventions and Terminology Used in This Book xvi	(QINACTMSGQ)	2.4
Prerequisite and Related Information xvi	Limit Device Sessions (QLMTDEVSSN)	24
How to Send Your Comments xvi	Limit Security Officer (QLMTSECOFR)	
	Maximum Sign-On Attempts (QMAXSIGN)	
What's New for V5R4 xix	Action When Sign-On Attempts Reached (QMAXSGNACN)	
Chapter 1. Introduction to iSeries	Retain Server Security (QRETSVRSEC)	
Security	Remote Sign-On Control (QRMTSIGN)	
Physical Security	Scan File Systems (QSCANFS)	
	Scan File Systems Control (QSCANFSCTL)	
Keylock Security	Share Memory Control (QSHRMEMCTL)	
Security Level	Use Adopted Authority (QUSEADPAUT)	
System Values	Security-Related System Values	
Signing		31
Single Signon Enablement	Automatic Configuration of Virtual Devices	•
User Profiles	(QAUTOVRT)	31
Group Profiles	Device Recovery Action (QDEVRCYACN)	
Resource Security	Disconnected Job Time-Out Interval	0.
Security Audit Journal	(QDSCJOBITV)	33
Common Criteria (CC) Security	Remote Service Attribute (QRMTSRVATR)	
Independent Disk Pool 6	Security-Related Restore System Values	
	Verify Object on Restore (QVFYOBJRST)	
Chapter 2. Using System Security	Force Conversion on Restore (QFRCCVNRST).	
(QSecurity) System Value 7	Allow Restoring of Security-Sensitive Objects	00
Security Level 10	(QALWOBJRST)	33
Security Level 20	System Values That Apply to Passwords	39
Changing to Level 20 from Level 10 10	Password Expiration Interval (QPWDEXPITV).	
Changing to Level 20 from a Higher Level 10	Password Level (QPWDLVL)	
Security Level 30	Minimum Length of Passwords	10
Changing to Level 30 from a Lower Level 10	(QPWDMINLEN)	11
Security Level 40	Maximum Length of Passwords	1
Preventing the Use of Unsupported Interfaces 12	(QPWDMAXLEN)	15
Protecting Job Descriptions	Required Difference in Passwords	44
Signing On without a User ID and Password 13		42
Enhanced Hardware Storage Protection 14	Restricted Characters for Passwords	44
Protecting a Program's Associated Space 14	(QPWDLMTCHR)	45
Protecting a Job's Address Space 14	Restriction of Consecutive Digits for Passwords	4.
Validating Parameters		45
Validation of Programs Being Restored 14	(QPWDLMTAJC)	4.
Changing to Security Level 40		45
Disabling Security Level 40	(QPWDLMTREP)	4.
Security Level 50	(QPWDPOSDIF)	4
Restricting User Domain Objects 16		44
Restricting Message Handling 16	Requirement for Numeric Character in	4
Preventing Modification of Internal Control	Passwords (QPWDRQDDGT)	
Blocks	Password Approval Program (QPWDVLDPGM)	
Changing to Security Level 50	System Values That Control Auditing	
Disabling Security Level 50	Auditing Control (QAUDCTL)	
Disability Develop	Auditing End Action (QAUDENDACN)	5(
	Auditing Force Level (QAUDFRCLVL)	5

Auditing Level (QAUDLVL)	. 51	Owned Object Information	. 96
Auditing Level Extension (QAUDLVL2)	. 53	Digital ID Authentication	. 96
Auditing for New Objects (QCRTOBJAUD)	. 54	Working with User Profiles	
		Creating User Profiles	
Chapter 4. User Profiles	. 57	Copying User Profiles	. 99
Roles of the User Profile		Changing User Profiles	. 101
Group Profiles		Deleting User Profiles	
User-Profile Parameter Fields	. 58	Working with Objects by Private Authorities	103
User Profile Name		Working with Objects by Primary Group	. 104
Password		Enabling a User Profile	. 104
Set Password to Expired	. 61	Listing User Profiles	. 104
Status		Renaming a User Profile	
User Class		Working with User Auditing	
Assistance Level		Working with Profiles in CL Programs	
Current Library		User Profile Exit Points	. 107
Initial Program		IBM-Supplied User Profiles	. 108
Initial Menu			
Limit Capabilities		Chapter 5. Resource Security	111
Text		Defining Who Can Access Information	
Special Authority		Defining How Information Can Be Accessed	
Special Environment	72	Commonly Used Authorities	
Display Sign-On Information		Defining What Information Can Be Accessed	
Password Expiration Interval	74	Library Security	114
Local Password Management	75	Field Authorities	
Limit Device Sessions	. 75	Security and the System/38 Environment	
Keyboard Buffering.		Directory Security	
Maximum Storage	76	Authorization List Security	117
Priority Limit.		Authority for New Objects in a Library	
Job Description		Create Authority (CRTAUT) Risks	
Group Profile		Authority for New Objects in a Directory	
Owner		Object Ownership	
Group Authority		Group Ownership of Objects	
Group Authority Type	. 81	Primary Group for an Object	
Supplemental Groups	81	Default Owner (QDFTOWN) User Profile	
Accounting Code		Assigning Authority and Ownership to New	. 1~1
Document Password		Objects	. 124
Message Queue		Objects That Adopt the Owner's Authority	
Delivery		Adopted Authority Risks and Recommendations	
Severity	. 84	Programs That Ignore Adopted Authority	
Print Device		Authority Holders	
Output Queue		Authority Holders and System/36 Migration	
Attention-Key-Handling Program		Authority Holder Risks	
Sort Sequence		Working with Authority	
Language Identifier		Authority Displays	. 133
Country or Region Identifier		Authority Reports	
Coded Character Set Identifier		Working with Libraries	
Character Identifier Control		Creating Objects	
Job Attributes		Working with Individual Object Authority	
Locale		Working with Authority for Multiple Objects	141
User Options		Working with Object Ownership	
User Identification Number		Working with Primary Group Authority	
Group Identification Number		Using a Referenced Object	
Home Directory	. 91	Copying Authority from a User	
EIM Association		Working with Authorization Lists	
Authority		How the System Checks Authority	
Object Auditing		Authority Checking Flowcharts	
Action Auditing		Authority Checking Examples	
Additional Information Associated with a User		Authority Cache	
Profile	. 95		
Private Authorities		Chapter 6. Work Management Security	175
Primary Group Authorities	. 96	Onapior of Hork management decurity	.,,

Job Initiation	Planning Authorization Lists 213
Starting an Interactive Job 175	Advantages of Using an Authorization List 213
Starting a Batch Job	Planning Group Profiles
Adopted Authority and Batch Jobs 176	Planning Primary Groups for Objects 215
Workstations	Planning Multiple Group Profiles 215
Ownership of Device Descriptions 179	Using an Individual Profile as a Group Profile 215
Signon Screen Display File	Comparison of Group Profiles and Authorization
Changing the Signon Screen Display 180	Lists
Subsystem Descriptions	Planning Security for Programmers
Controlling How Jobs Enter the System 181	Managing Source Files
Job Descriptions	Protecting Java Class Files and Jar Files in the
System Operator Message Queue	Integrated File System
Library Lists	Planning Security for System Programmers or
Security Risks of Library Lists	Managers
Recommendations for System Portion of Library	Planning the Use of Validation List Objects 218
List	Limit Access to Program Function
Recommendations for Product Library 184	Limit Access to Frogram Punction
Recommendations for the Current Library 185	Observan O. Dooleyn and Doocyany of
Recommendations for the User Portion of the	Chapter 8. Backup and Recovery of
	Security Information
Library List	How Security Information is Stored
Printing	Saving Security Information
Securing Spooled Files	Recovering Security Information
Output Queue and Parameter Authorities	Restoring User Profiles
Required for Printing	Restoring Objects
Examples: Output Queue	Restoring Authority
Network Attributes	Restoring Programs
Job Action (JOBACN) Network Attribute 189	Restoring Licensed Programs
Client Request Access (PCSACC) Network	Restoring Authorization Lists 228
Attribute	Restoring the Operating System
DDM Request Access (DDMACC) Network	*SAVSYS Special Authority
Attribute	Auditing Save and Restore Operations
Save and Restore Operations	
Restricting Save and Restore Operations 191	Chapter 9. Auditing Security on the
Example: Restricting Save and Restore	
Commands	iSeries System 231
Performance Tuning	Checklist for Security Officers and Auditors 231
Restricting Jobs to Batch	Physical Security
	System Values
Chapter 7. Designing Security 195	IBM-Supplied User Profiles 232
Overall Recommendations	Password Control
Planning Password Level Changes 196	User and Group Profiles
Considerations for Changing QPWDLVL from 0	Authorization Control
to 1	Unauthorized Access
Considerations for Changing QPWDLVL from 0	Unauthorized Programs
or 1 to 2	Communications
Considerations for Changing QPWDLVL from 2	Using the Security Audit Journal
to 3	Planning Security Auditing 236
Changing to a Lower Password Level 199	Using CHGSECAUD to Set up Security
Planning Libraries	Auditing
Planning Applications to Prevent Large Profiles 201	Setting up Security Auditing 258
Library Lists	Managing the Audit Journal and Journal
Describing Library Security	Receivers
Planning Menus	Stopping the Audit Function 261
Using Adopted Authority in Menu Design 204	Analyzing Audit Journal Entries 262
	Relationship of Object Change Date/time to Audit
Describing Menu Security	Records
System Request Menu	Other Techniques for Monitoring Security 266
Planning Command Security	Monitoring Security Messages 266
Planning File Security	Using the History Log 266
Securing Logical Files	Using Journals to Monitor Object Activity 267
Overriding Files	Analyzing User Profiles 268
tine aechiny and aval. (15	v 0

Analyzing Object Authorities 269	Document Library Object Commands	333
Analyzing Programs That Adopt Authority 270	Double-byte Character Set Commands	
Checking for Objects That Have Been Altered 270	Edit Description Commands	338
Checking the Operating System 271	Environment Variable Commands	
Auditing the Security Officer's Actions 271	Extended Wireless LAN Configuration Commands	
	File Commands	
Appendix A. Security Commands 273	Filter Commands	
,	Finance Commands	
Appendix B. IBM-Supplied User	i5/OS Graphical Operations	
Profiles 281	Graphics Symbol Set Commands	
Fioliles	Host Server Commands	
	Image Catalog Commands	
Appendix C. Commands Shipped with	Integrated File System Commands	
Public Authority *EXCLUDE 289	Interactive Data Definition Commands	
	Internetwork Packet Exchange (IPX) Commands	
Appendix D. Authority Required for	Information Search Index Commands	
Objects Used by Commands 301	IPL Attribute Commands	
Referenced Object	Java Commands	
Authority Required for Object	Job Commands	
Authority Required for Library	Job Description Commands	
Command Usage Assumptions	Job Queue Commands	372
General Rules for Object Authorities on Commands 303	Job Schedule Commands	
Common Commands for Most Objects	Journal Commands	
Access Path Recovery Commands: Authorities	Journal Receiver Commands	377
Required	Language Commands	378
Advanced Function Presentation (AFP) Commands:	Library Commands	
Authorities Required	License Key Commands	
AF_INET Sockets over SNA Commands:	Licensed Program Commands	
Authorities Required	Line Description Commands	
Alerts: Authorities Required	Local Area Network (LAN) Commands	
Application Development Commands: Authorities	Locale Commands	
Required	Mail Server Framework Commands	
Authority Holder Commands: Authorities	Media Commands	
Required	Menu and Panel Group Commands	
Authorization List Commands: Authorities	Message Commands	
Required	Message Description Commands	394
Binding Directory Commands: Authorities	Message File Commands	395
Required	Message Queue Commands	
Change Request Description Commands 317	Migration Commands	395
Chart Commands	Mode Description Commands	
Class Commands	Module Commands	396
Class-of-Service Commands	NetBIOS Description Commands	
Cluster Commands	Network Commands	
Command (*CMD) Commands	Network File System Commands	
Commitment Control Commands	Network Interface Description Commands	399
Communications Side Information Commands 322	Network Server Commands	
Configuration Commands	Network Server Configuration Commands	
Configuration List Commands	Network Server Description Commands	
Connection List Commands	Node List Commands	
Controller Description Commands	Office Services Commands	
Cryptography Commands	Online Education Commands	
Data Area Commands	Operational Assistant Commands	
Data Queue Commands	Optical Commands	
Device Description Commands	Output Queue Commands	
Device Emulation Commands	Package Commands	
Directory and Directory Shadowing Commands 331	Performance Commands	
Disk Commands	Print Descriptor Group Commands	
Display Station Pass-through Commands	Print Services Facility Configuration Commands	414
Distribution Commands	Problem Commands	
Distribution List Commands	Program Commands	
Distribution List Communities	OSH Shall Interpreter Commands	/119

Query Commands	Options on the Security Tools Menu 619
Question and Answer Commands 420	How to Use the Security Batch Menu 622
Reader Commands	Options on the Security Batch Menu 623
Registration Facility Commands	Commands for Customizing Security 627
Relational Database Commands	Values That Are Set by the Configure System
Resource Commands	Security Command 628
Remote Job Entry (RJE) Commands 422	Changing the Program 629
Security Attributes Commands	What the Revoke Public Authority Command Does 630
Server Authentication Entry Commands 427	Changing the Program 630
Service Commands	
Spelling Aid Dictionary Commands 431	Appendix H. Related Information for
Sphere of Control Commands	iSeries Security Reference 633
Spooled File Commands	Advanced Security
Subsystem Description Commands 434	Backup and Recovery
System Commands	Basic Security Information and Physical Security 633
System Reply List Commands	iSeries Access for Windows Licensed Program 633
System Value Commands	Communications and Networking 633
System/36 Environment Commands 437	Cryptography
Table Commands	General System Operations
TCP/IP Commands	IBM-Supplied Program Installation and System
Time Zone Description Commands 441	Configuration
Upgrade Order Information Data Commands 442	Integrated File System
User Index, User Queue, and User Space	The Internet
Commands	IBM Lotus Domino
User-defined File System Commands 442	Optical Support
User Profile Commands	
Validation List Commands 446	Printing
Workstation Customization Commands 446	Programming
Writer Commands	Utilities
	Appendix I. Notices 637
Appendix E. Object Operations and	Programming Interface Information 638
Auditing 449	Trademarks
•	Terms and Conditions
Appendix F. Layout of Audit Journal	terms and conditions
• •	Indov C44
Entries 507	Index 641
Appendix G. Commands and Menus	
for Security Commands 619	
ioi occurry commanus	

# **Figures**

1.	Password Expiration Message 62	17.	Flowchart 5: Fast Path for User Authority	155
2.	Description of Special Environment 73	18.	Flowchart 6: Group Authority Checking	158
3.	Sign-On Information Display	19.	Flowchart 7: Check Public Authority	160
4.	Display Object Authority display showing	20.	Flowchart 8A: Checking Adopted Authority	
	F16=Display field authorities. This function		User *ALLOBJ and Owner	. 161
	key will be displayed when a database file	21.	Flowchart 8B: Checking Adopted Authority	
	has field authorities		Using Private Authorities	. 163
5.	Display Field Authority display. When	22.	Authority for the PRICES File	
	"F17=Position to" is pressed, the Position List	23.	Authority for the CREDIT File	. 165
	prompt will be displayed. If F16 is pressed,	24.	Display Object Authority	. 169
	the previous position to operation will be	25.	Authority for the ARWRK01 File	
	repeated	26.	Authority for the ARLST1 Authorization List	170
6.	New Object Example: Public Authority from	27.	Authority for the CRLIM File	. 171
	Library, Group Given Private Authority 125	28.	Authority for CRLIMWRK File	. 172
7.	New Object Example: Public Authority from	29.	Authority for the CRLST1 Authorization List	172
	System Value, Group Given Private Authority 126	30.	Authority Checking for Workstations	178
8.	New Object Example: Public Authority from	31.	Library List-Expected Environment	. 183
	Library, Group Given Primary Group	32.	Library List-Actual Environment	. 184
	Authority	33.	Example Applications	. 195
9.	New Object Example: Public Authority	34.	Program to Replace and Restore Library List	202
	Specified, Group Owns Object 128	35.	Format for Describing Library Security	203
10.	Adopted Authority and the CALL Command 129	36.	Sample Inquiry Menu	. 204
11.	Adopted Authority and the TFRCTL	37.	Sample Initial Menu	. 204
	Command	38.	Sample Initial Application Program	. 205
12.	Display Object Authority Display 134	39.	Sample Program for Query with Adopted	
13.	Flowchart 1: Main Authority Checking		Authority	. 205
	Process	40.	Sample Application Menu with Query	207
14.	Flowchart 2: Fast Path for Object Authority 151	41.	Format for Menu Security Requirements	208
15.	Flowchart 3: Check User Authority 152	42.	Using a Logical File for Security	. 211
16	Flowchart A: Owner Authority Checking 154			

# **Tables**

	Security Levels: Function Comparison	. 7	31.	Possible Values for the QPWDMINLEN System	
2.	Default Special Authorities for User Classes by				41
	Security Level	. 9	32.	Possible Values for the QPWDMAXLEN	
3.	Comparison of Security Levels 30, 40, and 50	11			42
4.	Domain and State Access	13	33.	Possible Values for the QPWDRQDDIF System	
5.	System values that can be locked	19			42
	Possible Values for the QALWUSRDMN		34.	Possible Values for the QPWDLMTCHR	
		21		· · · · · · · · · · · · · · · · · · ·	43
7.	Possible Values for the QCRTAUT System		35.	Possible Values for the QPWDLMTAJC System	
		22			43
R	Possible Values for the QDSPSGNINF System	~~	36	Possible Values for the QPWDLMTREP System	10
0.		23	50.		43
a	Possible Values for the QINACTITV System	20	37	Passwords with Repeating Characters with	40
9.		99	37.		4.4
10	Value:	23	20		44
10.	Possible Values for QINACTMSGQ System	0.4	38.	Passwords with Repeating Characters with	
	Value:	24	00	V	44
11.	Possible Values for the QLMTDEVSSN System		39.	Possible Values for the QPWDPOSDIF System	
	Value:	25			44
12.	Possible Values for the QLMTSECOFR System		40.	Possible Values for the QPWDRQDDGT	
	Value:	25		J	44
13.	Possible Values for the QMAXSIGN System		41.	Possible Values for the QPWDVLDPGM	
	Value:	26		System Value:	45
14.	Possible Values for the QMAXSGNACN		42.	Parameters for Password Approval Program	45
	_	26		Possible Values for the QAUDCTL System	
15.	Possible Values for the QRETSVRSEC System				50
	Value:	27	44.	Possible Values for the QAUDENDACN	
16	Possible Values for the QRMTSIGN System	~ .		System Value:	51
10.	Value:	27	45	Possible Values for the QAUDFRCLVL System	01
17	Possible Values for the QSCANFS System	ω1	10.	Value:	51
11.	Value:	90	10		J 1
10		۵0	40.	Possible Values for the QAUDLVL System	E 6
10.	Possible Values for the QSCANFSCTL System	00	47		52
10		28	47.	Possible Values for the QAUDLVL2 System	~ 0
19.	Possible Values for the QSHRMEMCTL System	00	40		53
	Value:	29	48.	Possible Values for the QCRTOBJAUD System	
20.	Possible Values for the QUSEADPAUT System				55
		30			61
21.	Possible Values for the QAUTOCFG System				62
	Value:	31			62
22.	Possible Values for the QAUTOVRT System		52.	Default Special Authorities by User Class	63
	Value:	32	53.	How Assistance Levels Are Stored and	
23.	Possible Values for the QDEVRCYACN System			Changed	64
	Value:	32	54.	Possible Values for ASTLVL:	
24.	Possible Values for the QDSCJOBITV System				65
	Value:	33			65
25	Possible Values for the QRMTSRVATR System			Possible Values for INLPGM Library:	
ωυ.	Value:	33			66
26	Possible Values for the QVFYOBJRST System	33		Possible Values for MENU Library:	
۵0.	•	25			UU
07	Value:	აა იუ	00.	Functions Allowed for Limit Capabilities	0.0
	QFRCCVNRST Values		01	Values	
۷ŏ.	Possible Values for the QALWOBJRST System			Possible Values for text:	
	Value:	38		Possible Values for SPCAUT:	
29.	Possible Values for the QPWDEXPITV System		63.		
	Value:			Possible Values for SPCENV:	
30.	Possible Values for the QPWDLVL System			Possible Values for DSPSGNINF:	
	Value:			Possible Values for PWDEXPITV:	
			67.	Possible Values for LCLPWDMGT:	75

68.	Possible Values for LMTDEVSSN:	76	125.	Action Auditing Values	237
	Possible Values for KBDBUF:			Security Auditing Journal Entries	
70.	Possible Values for MAXSTG:	77		How Object and User Auditing Work	
71.	Possible Values for PTYLMT:	78		Together	254
	Possible Values for JOBD:		128.	Commands for Working with Authority	
	Possible Values for JOBD Library:			Holders	273
	Possible Values for GRPPRF:		129.	Commands for Working with Authorization	
	Possible Values for OWNER:			Lists	273
	Possible Values for GRPAUT:		130	Commands for Working with Object	2.0
77	Possible Values for GRPAUTTYP: 1	81	100.	Authority and Auditing	274
78	Possible Values for SUPGRPPRF	82	131	Commands for Working with Passwords	275
	Possible Values for ACGCDE:			Commands for Working with User Profiles	276
	Possible Values for DOCPWD:			Related User Profile Commands	277
	Possible Values for MSGQ:			Commands for Working with Auditing	277
	Possible Values for MSGQ Library:			Commands for Working with Auditing  Commands for Working with Document	211
	Possible Values for DLVRY:		133.	Library Objects	277
	Possible Values for SEV:		196	Commands for Working with Server	211
	Possible Values for PRTDEV:		130.	Authentication Entries	270
			107		210
	Possible Values for OUTQ:		137.	Commands for Working with the System	070
	Possible Values for OUTQ library:		100	Distribution Directory	
	Possible Values for ATNPGM:			Commands for Working with Validation Lists	279
	Possible Values for ATNPGM Library:		139.	Commands for Working with Function Usage	070
	Possible Values for SRTSEQ:		1.40	Information	
	Possible Values for SRTSEQ Library:			Security Tools for Working with Auditing	279
	Possible Values for LANGID:			Security Tools for Working with Authorities	279
	Possible Values for CNTRYID:		142.	Security Tools for Working with System	
	Possible Values for CCSID:			Security	
	Possible Values for CHRIDCTL:			Default Values for User Profiles	
	Possible Values for SETJOBATR:			IBM-Supplied User Profiles	283
	Possible Values for LOCALE:		145.	Authorities of IBM-Supplied User Profiles to	
98.	Possible Values for USROPT:	90		Restricted Commands	
	Possible Values for UID:			Description of Authority Types	
	Possible Values for GID:			System-Defined Authority	
	Possible Values for HOMEDIR:	91		System-Defined Authority	
	Possible Values for EIMASSOC, Single Values:	92		Common commands for most objects	305
	Possible Values for EIMASSOC, Element 1:	92	150.	Standard Heading Fields for Audit Journal	
	Possible Values for EIMASSOC, Element 2:	92			507
	Possible Values for EIMASSOC, Element 3:	92	151.	Standard Heading Fields for Audit Journal	
06.	Possible Values for EIMASSOC, Element 4:	93		Entries	509
07.	Possible Values for AUT:	93	152.	Standard Heading Fields for Audit Journal	
08.	Possible Values for OBJAUD:	94		Entries	510
09.	Auditing Performed for Object Access	94	153.	Audit Journal (QAUDJRN) Entry Types.	510
10.	Possible Values for AUDLVL:	95	154.	AD (Auditing Change) Journal Entries	512
11.	Description of Authority Types	112	155.	AF (Authority Failure) Journal Entries	514
12.	System-Defined Authority	113	156.	AP (Adopted Authority) Journal Entries	519
13.	System-Defined Authority	113	157.	AU (Attribute Changes) Journal Entries	520
	LAN Server Permissions			CA (Authority Changes) Journal Entries	520
	Public versus Private Authority			CD (Command String) Journal Entries	523
	Accumulated Group Authority			CO (Create Object) Journal Entries	524
		183		CP (User Profile Changes) Journal Entries	525
	Authority Required to Perform Printing			CQ (*CRQD Changes) Journal Entries	527
		187		CU (Cluster Operations) Journal Entries	528
19.	User Profiles for Menu System			CV (Connection Verification) Journal Entries	529
	Objects Used by Menu System			CY (Cryptographic Configuration) Journal	020
	Options and Commands for the System			Entries	531
		209	166.	DI (Directory Server) Journal Entries	532
22	Physical File Example: CUSTMAST File	211		DO (Delete Operation) Journal Entries	536
	Authorization List and Group Profile	~11		DS (IBM-Supplied Service Tools User ID	550
~ 0.		216	100.	Reset) Journal Entries	538
24	How Security Information Is Saved and	~10	169	EV (Environment Variable) Journal Entries	539
. ~ £,	· · · · · · · · · · · · · · · · · · ·	991		CR (Caparic Record) Journal Entries	540

171.	GS (Give Descriptor) Journal Entries 5	544	203.	SE (Change of Subsystem Routing Entry)	
	<u> •</u>	544			586
173.	IP (Interprocess Communication) Journal		204.	SF (Action to Spooled File) Journal Entries	587
	Entries	546	205.	SG (Asychronous Signals) Journal Entries	590
174.	IR (IP Rules Actions) Journal Entries 5	547	206.	SK (Secure Sockets Connections) Journal	
175.	IS (Internet Security Management) Journal			Entries	591
	Entries	548	207.	SM (Systems Management Change) Journal	
176.		550			592
	JS (Job Change) Journal Entries	550	208.	SO (Server Security User Information Actions)	
	KF (Key Ring File) Journal Entries 5			Journal Entries	593
	LD (Link, Unlink, Search Directory) Journal		209.	ST (Service Tools Action) Journal Entries	594
	Entries	557		SV (Action to System Value) Journal Entries	597
180.	ML (Mail Actions) Journal Entries			VA (Change of Access Control List) Journal	
		559			598
	ND (APPN Directory Search Filter) Journal		212.	VC (Connection Start and End) Journal	
	Entries	559		Entries	598
183.		560	213.	VF (Close of Server Files) Journal Entries	599
	OM (Object Management Change) Journal			VL (Account Limit Exceeded) Journal Entries	599
	Entries	560		VN (Network Log On and Off) Journal	
185.	OR (Object Restore) Journal Entries			Entries	600
		566	216.	VO (Validation List) Journal Entries	
	O1 (Optical Access) Journal Entries 5			VP (Network Password Error) Journal Entries	
	O2 (Optical Access) Journal Entries 5			VR (Network Resource Access) Journal	
	O3 (Optical Access) Journal Entries 5				603
	PA (Program Adopt) Journal Entries 5		219.	VS (Server Session) Journal Entries	
		572		VU (Network Profile Change) Journal Entries	
	PO (Printer Output) Journal Entries 5	575		VV (Service Status Change) Journal Entries	605
	PS (Profile Swap) Journal Entries			X0 (Network Authentication) Journal Entries	605
	PW (Password) Journal Entries			X1 (Identity Token) Journal Entries	609
	RA (Authority Change for Restored Object)			YC (Change to DLO Object) Journal Entries	610
	Journal Entries	578		YR (Read of DLO Object) Journal Entries	611
196.	RJ (Restoring Job Description) Journal Entries			ZC (Change to Object) Journal Entries	611
	RO (Ownership Change for Restored Object)			ZR (Read of Object) Journal Entries	
	Journal Entries	580			616
198.	RP (Restoring Programs that Adopt			Tool Commands for User Profiles	
	Authority) Journal Entries	581		Tool Commands for Security Auditing	621
199.	RQ (Restoring Change Request Descriptor			Commands for Security Reports	
	Object) Journal Entries	583		Commands for Customizing Your System	627
200.	RU (Restore Authority for User Profile)			Values Set by the CFGSYSSEC Command	628
	Journal Entries	583		Commands Whose Public Authority Is Set by	
201	RZ (Primary Group Change for Restored				630
	Object) Journal Entries	583	235.	Programs Whose Public Authority Is Set by	
202	SD (Change System Distribution Directory)			the RVKPUBAUT Command	630
	Journal Entries	585			

# **About Security Reference (SC41-5302)**

This book provides information about planning, setting up, managing, and auditing security on your iSeries  $^{\text{\tiny TM}}$  system. It describes all the features of security on the system and discusses how security features relate to other aspects of the system, such as work management, backup and recovery, and application design.

This book does not provide complete operational instructions for setting up security on your system. For a step-by-step example of setting up security, consult the iSeries Information Center (see "Prerequisite and Related Information" on page xvi) and the *Tips and Tools for Securing Your iSeries*, SC41-5300-07 book. Information about planning and setting up Basic System Security and Planning can also be found in the Information Center (see "Prerequisite and Related Information" on page xvi).

This book does not provide complete information about planning for IBM® Lotus® Domino® users. For Lotus Domino users, see the URL http://www.lotus.com/ldd/doc. This Web site provides information about IBM Lotus Notes®, Lotus Domino, and IBM Lotus Domino for iSeries. 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.

This book does not contain complete information about the application programming interfaces (APIs) that are available to access security information. This topic does not contain information about the Internet. For information about considerations when you connect your system to the Internet see the IBM SecureWay®: iSeries and the Internet in the information center (see "Prerequisite and Related Information" on page xvi).

For a list of related publications, see the Appendix H, "Related Information for iSeries Security Reference," on page 633.

## Who Should Read This Book

The primary audience for this book is the security administrator.

Chapter 9, "Auditing Security on the iSeries System," on page 231 is intended for anyone who wants to perform a security audit of the system.

This book assumes you are familiar with entering commands on the system. To use some of the examples in this book, you need to know how to:

- Edit and create a control language (CL) program.
- Use a query tool, such as the Query/400 licensed program.

The information in the following chapters can help the application programmer and systems programmers understand the relationship between security and application and system design:

Chapter 5, "Resource Security," on page 111

Chapter 6, "Work Management Security," on page 175

Chapter 7, "Designing Security," on page 195

Chapter 8, "Backup and Recovery of Security Information," on page 221

## Conventions and Terminology Used in This Book

The iSeries displays in this book can be shown as they are presented through iSeries Navigator, which is part of iSeries Access for Windows® on the personal computer. The example displays in this book can also be shown without iSeries Navigator available.

For more information about using iSeries Navigator, refer to the iSeries Information Center (see "Prerequisite and Related Information").

## **Prerequisite and Related Information**

Use the iSeries Information Center as your starting point for iSeries technical information.

You can access the information center in two ways:

- From the following Web site: http://www.ibm.com/eserver/iseries/infocenter
- From the iSeries Information Center, SK3T-4091-04 CD-ROM. This CD-ROM is included with your new iSeries hardware or IBM i5/OS software upgrade order. You can also order the CD-ROM from the IBM **Publications Center:**

http://www.ibm.com/shop/publications/order

The iSeries Information Center contains new and updated iSeries information such as software and hardware installation, Linux<sup>™</sup>, WebSphere<sup>®</sup>, Java<sup>™</sup>, high availability, database, logical partitions, CL commands, and system application programming interfaces (APIs). In addition, it provides advisors and finders to assist in planning, troubleshooting, and configuring your iSeries hardware and software.

With every new hardware order, you receive the iSeries Setup and Operations CD-ROM, SK3T-4098-02. This CD-ROM contains IBM eServer iSeries Access for Windows and the EZ-Setup wizard. iSeries Access Family offers a powerful set of client and server capabilities for connecting PCs to iSeries servers. The EZ-Setup wizard automates many of the iSeries setup tasks.

For other related information, see the Appendix H, "Related Information for iSeries Security Reference," on page 633.

## **How to Send Your Comments**

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other iSeries documentation, fill out the readers' comment form at the back of this book.

- If you prefer to send comments by mail, use the readers' comment form with the address that is printed on the back. If you are mailing a readers' comment form from a country or region other than the United States, you can give the form to the local IBM branch office or IBM representative for postage-paid mailing.
- If you prefer to send comments by FAX, use either of the following numbers:
  - United States, Canada, and Puerto Rico: 1-800-937-3430
  - Other countries or regions: 1-507-253-5192
- If you prefer to send comments electronically, use one of these e-mail addresses:
  - Comments on books:

RCHCLERK@us.ibm.com

- Comments on the iSeries information center:

RCHINFOC@us.ibm.com

Be sure to include the following information:

- The name of the book or iSeries information center topic.
- The publication number of a book.
- The page number or topic of a book to which your comment applies.

## What's New for V5R4

The iSeries Security Reference book has changed significantly in V5R4. This section provides a brief summary of the main changes.

- From Chapter 1 to Chapter 9, many sections were changed, such as:
  - The "Common Criteria (CC) Security" section was changed in Chapter 1.
- A new section called "Work with Objects by Private Authorities" was added in Chapter 4.
- A new section called "Protecting Java class files and jar files in the integrated file system" was added in Chapter 7.
- The section of "Relationship of Object Change Date/time to Audit Records" in Chapter 9 was added.
- In Appendix A, two tables called "Commands for Working with Object Authority and Auditing" and "Security Tools for Working with Auditing" were updated.
- In Appendix C, 26 new commands were added.
- Appendix D contains the following additions and changes:
  - A new table called the "Network Server Configuration Commands" is added.
  - Many tables were changed, such as the "Image Catalog Commands" table, the "Integrated File System Commands" table, and the "Cluster Commands" table.
- In Appendix E, the following tables were updated: "Operations Common to All Object Types", "Operations for Library (\*LIB)", "Operations for Spooled Files", "Operations for Query Manager Form (\*QMFORM)", and "Operations for User Profile (\*USRPRF)".
- Appendix F contains the following conditions and changes:
  - A new table called the "IM (Intrusion Monitor) Journal Entries" was added.
  - Many tables were changed, such as "AF (Authority Failure) Journal Entries", "CA (Authority Changes) Journal Entries", and "CO (Create Object) Journal Entries".
- In Appendix H, Notices information was updated.
- Appendix G contains the following conditions and changes:
  - The tables updated include "Tool Commands for Security Auditing", "Commands for Security Reports", and "Values Set by the CFGSYSSEC Command".
- The sections updated include "Options on the Security Tools Menu", "Changing the program" in the "What the Revoke Public Authority Command Does", and "Values That Are Set by the Configure System Security Command".

## **Chapter 1. Introduction to iSeries Security**

The @server family of systems covers a wide range of users. 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.

Security on the iSeries system is flexible enough to meet the requirements of this wide range of users and situations. You need to understand the features and options available so that you can adapt them to your own security requirements. This chapter provides an overview of the security features on the system.

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 book 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.

Physical security is described in the Information Center (see "Prerequisite and Related Information" on page xvi for details).

## **Keylock Security**

The keylock on the 940x control panel controls access to various system control panel functions. The keylock position can be retrieved and changed under program control by using either of the following methods:

- Retrieve IPL Attributes (QWCRIPLA) API
- · Change IPL Attributes (CHGIPLA) command

This 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 i5/OS or Dedicated Service Tools (DST).

The  $i5/OS^{\text{TM}}$  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.

## **Security Level**

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

#### Level 10:

Level 10 is no longer supported. See Chapter 2, "Using System Security (QSecurity) System Value," on page 7 for information about security levels (10, 20, 30, 40, and 50).

#### 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 iSeries systems with high security requirements, and it is designed to meet CC security requirements.

The system security levels are described in Chapter 2, "Using System Security (QSecurity) System Value," on page 7.

## **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. For example, you can specify:

- · 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.

The system values that relate to security are described in Chapter 3, "Security System Values," on page 19.

## **Signing**

A key component of security is integrity: being able to trust that objects on the system have not been tampered with or altered. Your operating system software is protected by digital signatures, and now you can reinforce integrity by signing software objects which you rely on. (For more information about using signing to protect your system, see *Tips and Tools for Securing Your iSeries*.) This 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 (QVFYOBJRST) 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 iSeries are signed). DCM is described in the Information Center (see "Prerequisite and Related Information" on page xvi for details).

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.

## Single Signon Enablement

In today's heterogeneous networks with partitioned servers and multiple platforms, administrators must cope with the complexities of managing identification and authentication for network users. IBM's new infrastructure and exploitation of iSeries helps administrators, users, and application programmers to easily manage these identification and authentication issues.

To enable a single signon environment, IBM provides two technologies that work together to allow users to sign in with their Windows username and password and be authenticated to iSeries systems in the network. Network authentication service and Enterprise Identity Mapping (EIM) are the two technologies that an administrator must configure to enable a single signon environment. Windows 2000, XP, AIX®, and zSeries® use Kerberos protocol to authenticate users to the network. A secure, centralized server, called a key distribution center, authenticates principals (Kerberos users) to the network.

While network authentication service allows an iSeries system to participate in that 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 i5/OS username, can also be associated with this EIM identifier. When a user signs on to the network and accesses an iSeries system, that user is not prompted for a userid and password. If the Kerberos authentication is successful, applications can look up the association to the EIM identifier to find the i5/OS username. The user no longer needs a password to iSeries applications and functions 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 signon by configuring network authentication service and Enterprise Identity Mapping (EIM) on your iSeries system. To review a

scenario that shows how to set up a single signon environment, see the information center topic, Scenario: Enable single signon. (Security—>Network authentication service—>Network authentication service scenarios—>Scenario: Enable single signon). See "Prerequisite and Related Information" on page xvi for more information about accessing the information center.

## **User Profiles**

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

The user profile is a powerful and flexible tool. It controls what the user can do and customizes the way the system appears to the user. Following are descriptions of a few 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.

User profiles are discussed in Chapter 4, "User Profiles," on page 57.

## **Group Profiles**

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

"Planning Group Profiles" on page 214 discusses using group authority. "Group Ownership of Objects" on page 122 discusses what objects should be owned by group profiles. "Primary Group for an Object" on page 123 discusses using primary group and primary group authority for an object. "Copying User Profiles" on page 99 describes how to copy a group profile to create an individual user profile.

## **Resource Security**

Resource security on the system allows you to define who can use objects and how those objects can be used. The ability to access an object is called **authority**. 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. Following are descriptions of 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 on 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/ $36^{\text{TM}}$ , 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.

Resource security is described in Chapter 5, "Resource Security," on page 111

## **Security Audit Journal**

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

Chapter 9, "Auditing Security on the iSeries System," on page 231 provides information about auditing security.

## Common Criteria (CC) Security

On August 10, 2005, IBM received Common Criteria certification of i5/OS 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 Scheme Web site:

http://niap.nist.gov/cc-scheme/vpl/vpl\_type.html

## **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 (ASP) 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. For 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 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. In i5/OS V5R1, you can use independent disk pools only with user-defined file systems. However, several objects are not allowed on independent disk pools. For a complete list of supported and unsupported objects, see Supported and unsupported i5/OS object types topic in the information center. (Systems management—>Independent disk pools—>Concepts—>Restrictions and considerations—>Supported and unsupported i5/OS object types)

## Chapter 2. Using System Security (QSecurity) System Value

This chapter discusses the security level (QSECURITY) system value and the issues associated with it.

#### 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:**

\*ALLOBI and \*SECADM

#### **Journal Entry:**

SV

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

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 11.

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 <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>	$Yes^1$
Limit capabilities support active.	Yes	Yes	Yes	Yes
Resource security active.	No	Yes	Yes	Yes
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

Table 1. Security Levels: Function Comparison (continued)

Function	Level 20	Level 30	Level 40	Level 50
Programs that use unsupported interfaces fail at run time.	No	No	Yes	Yes
Enhanced hardware storage protection supported.	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 <sup>2</sup>

When LMTCPB(\*YES) is specified in the user profile.

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 Chapter 3: "Security System Values".

At level 50, more protection of internal control blocks is enforced than at level 40. See "Preventing Modification of Internal Control Blocks" on page 17.

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 63 and "Special Authority" on page 68 provide more information about user classes and special authorities.

#### **Recommendations:**

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.

Also, at security level 30 (or below), users are able to call system interfaces that swap 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 may notice some performance effect because of the additional checking 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 your applications again.

## **Security Level 10**

At security level 10, you have no security protection; therefore, security level 10 is **not recommended** by IBM. 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 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**

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.

All profiles are created with \*ALLOBJ special authority at security level 20 by default. Therefore, security level 20 is **not recommended** by IBM.

## 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.

Following is a recommended list of 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 Table 143 in Appendix B 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. Refer to Table 2 on page 9 to see how special authorities differ between level 20 and higher security levels.

**Attention:** 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.

## **Security Level 30**

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 the next time you perform an 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 9 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. Following is a recommended list of activities:

- For each application, set the appropriate authorities for application objects.
- Test each application using either actual user profiles or special test user profiles:
  - Remove \*ALLOBJ special authority from the user profiles 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 test profiles, grant the appropriate authorities for application objects to all production user profiles.
- 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. 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.

**Note:** See the topic "Defining How Information Can Be Accessed" on page 112 for more information about object authorities.

## **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. These functions are explained in more detail in the sections that follow.

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 <sup>1</sup> ; operation fails.	AF journal entry <sup>1</sup> ; operation fails.
A program attempts to use a restricted instruction.	AF journal entry <sup>1</sup>	AF journal entry <sup>1</sup> ; operation fails.	AF journal entry <sup>1</sup> ; operation fails.
The user submitting a job does not have *USE authority to the user profile specified in the job description.	AF journal entry <sup>1</sup>	AF journal entry <sup>1</sup> ; job does not run.	AF journal entry <sup>1</sup> ; job does not run.
A user attempts default sign-on without a user ID and a password.	AF journal entry <sup>1</sup>	AF journal entry <sup>1</sup> ; sign-on is not successful.	AF journal entry <sup>1</sup> ; 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; <sup>1, 2</sup> operation fails. <sup>2</sup>	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>

Table 3. Comparison of Security Levels 30, 40, and 50 (continued)

Scenario Description	Level 30	Level 40	Level 50
An attempt is made to restore a program that does not have a validation value. <sup>3</sup>	No validation is performed. Program must be retranslated before it can be used.	No validation is performed. Program must be retranslated before it can be used.	No validation is performed. Program must be retranslated before it can be used.
An attempt is made to restore a program	Program validation is	Program validation is	Program validation is
that has a validation value.	performed.	performed.	performed.
An attempt is made to change a program's associated space.	Attempt is successful.	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>
An attempt is made to change a job's address space.	Attempt is successful.	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>
A user state program attempts to call or transfer control to a system domain program.	Attempt is successful.	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>	AF journal entry; <sup>1, 2</sup> operation fails. <sup>2</sup>
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 program 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.
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; <sup>1</sup> . <sup>2</sup> , <sup>4</sup> operation fails. <sup>2</sup> , <sup>4</sup>	AF journal entry; <sup>1, 2, 4</sup> operation fails. <sup>2, 4</sup>
An authority failure (AF) type entry active. See Chapter 9 for more inform			e auditing function is
<sup>2</sup> If the processor supports enhanced h	ardware storage protect	ion.	

- Programs created before Version 1 Release 3 do not have a validation value.
- 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 11, 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 and higher, the system prevents attempts to directly call system programs 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. Objects that are \*SYSTEM domain can be accessed 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 using the Display Program (DSPPGM) command. You can display the state of a service program using the Display Service Program (DSPSRVPGM) command.

Table 4 shows the domain and state access rules:

Table 4. Domain and State Access

	Object Domain		
Program State	*USER	*SYSTEM	
*USER	YES	NO <sup>1</sup>	
*SYSTEM	YES	YES	

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:**

If the auditing function is active and the QAUDLVL system value includes \*PGMFAIL, an authority failure (AF) entry, violation type D or R, is written to the QAUDJRN journal when 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 be run with attributes taken from that user profile. An unauthorized user might use a job description to violate security by submitting a job to run under the user profile specified in the job description.

At security level 40 and higher, the user submitting the job must have \*USE authority to both the job description and the user profile specified in the job description, or the job fails. At security level 30, the job runs if the submitter has \*USE authority to the job description.

#### **Journal Entry:**

If the auditing function is active and the QAUDLVL system value includes \*AUTFAIL, an AF entry, violation type J, is written to the QAUDJRN journal when a user submits a job and is not authorized to the user profile in a job description.

## 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. See the topic "Subsystem Descriptions" on page 181 for more information about security issues associated with subsystem descriptions.

## **Journal Entry:**

If the auditing function is active and the QAUDLVL system value includes \*AUTFAIL, an AF entry, violation type S is written to the QAUDJRN journal when a user attempts to sign on without entering a user ID and password and the subsystem description allows it. (The attempt fails at security level 40 and higher.)

## **Enhanced Hardware Storage Protection**

Enhanced hardware storage protection allows blocks of system information located on disk 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. This support is not available at security levels less than 40.

Enhanced hardware storage protection is supported on all iSeries models, except the following models:

- · All B models
- · All C models
- D models: 9402 D04, 9402 D06, 9404 D10, and 9404 D20.

#### **Journal Entry:**

If the auditing function is active and the QAUDLVL system value includes \*PGMFAIL. an AF entry. violation type R, is written to the QAUDJRN journal when a program attempts to write to an area of disk protected by the enhanced hardware storage protection feature.

## **Protecting a Program's Associated Space**

At security level 40 and higher, a user state program cannot directly change the associated space of a program object.

## 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 operating system are system state programs in user domain. In other words, they are programs that can be called directly by a user. 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 may notice some performance effect because of this additional checking.

## Validation of Programs Being Restored

When a program is created, the iSeries 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 actions taken by the system are controlled by the QFRCCVNRST and QALWOBJRST system values.

In addition to a validation value, a program may optionally have a digital signature that can be verified on restore. Any system actions related to digital signatures are controlled by the QVFYOBJRST and QFRCCVNRST system values. The three system values, Verify Object on Restore (QVFYOBJRST), Force Conversion on Restore (QFRCCVNRST) and Allow Object Restore (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.

The first filter is QVFYOBJRST 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, QFRCCVNRST system value. This system value allows you to 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, QALWOBJRST system value. This system value controls whether objects with security sensitive attributes can be restored.

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

Each of these system values are described in the Chapter 3, "Security System Values" in the section, entitled Security-Related Restore System Values.

## **Changing to Security Level 40**

Make sure that all your applications run successfully at security level 30 before migrating to level 40. Security level 30 gives you the opportunity to test resource security for all your applications. Use the following procedure 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 258 gives complete instructions for setting up the auditing function.
- 2. Make sure 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 your applications at security level 30. Pay particular attention to the following reason codes in AF type entries:
  - **B** Restriction (blocked) instruction violation
  - 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 14 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**

After changing to security level 40, you may find you need to move back to level 30 temporarily. For example, you may need to test new applications for integrity errors. Or, you may 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 9.) 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. It provides enhanced integrity protection in addition to what is provided by security level 40.

These security functions are included for security level 50. They 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 21 for
  more information.

# **Restricting Message Handling**

Messages sent between programs provide the potential for integrity exposures. 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 program 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 and higher, 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

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 15 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 setting the QALWUSRDMN system value. Controlling user domain objects is important to system integrity. See "Restricting User Domain Objects" on page 16.
- · 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<sup>®</sup> or System/38<sup>™</sup> 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.

## **Disabling Security Level 50**

After changing to security level 50, you may find you need to move back to security level 30 or 40 temporarily. For example, you may need to test new applications for integrity errors. Or, you may 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. (See Table 2 on page 9.)

# **Chapter 3. Security System Values**

This chapter describes the system values that control security on your system. 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 IPL.

The following system values can be restricted by using the lock option:

Table 5. System values that can be locked

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

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.

The following sections discuss specific security system values. For information about the security-related system values that you can lock, see their corresponding sections:

- · General security system values
- · Security-related system values
- · Security-related restore system values
- · System values that apply to passwords
- · System values that control auditing

# **General Security System Values**

#### **Overview:**

### **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:**

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

Following are the general system values that control security on your system:

#### **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

### **QSCANFSCTL**

Scan file systems control

### **QSECURITY**

Security level

### **QSHRMEMCTL**

Shared memory control

### **QUSEADPAUT**

**Use Adopted Authority** 

## **QVFYOBJRST**

Verify object on restore

Descriptions of these system values follow. The possible choices are shown. The choices that are underlined are the system-supplied defaults. For most system values, a recommended choice is listed.

# Allow User Domain Objects (QALWUSRDMN)

The QALWUSRDMN system value specifies which libraries are allowed to contain user domain objects of type \*USRSPC, \*USRIDX, and \*USRQ. The restriction does not apply to user domain objects of type \*PGM, \*SRVPGM, and \*SQLPKG. 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.

**Note:** This system value is a restricted value. See Chapter 3: "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.

\*DIR User domain objects are allowed in all directories on the system.

library- name 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 must 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. At security level 50, the QTEMP library is a temporary object and cannot be used to pass confidential data between users.

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 may use MI interface, that cannot be audited, to read or change the data in user domain objects in these libraries.

Note: If you run the Reclaim Storage (RCLSTG) command, user domain objects may need to be moved in and out of the QRCL (reclaim storage) library. To run the RCLSTG command successfully, you may 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 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 Chapter 3: "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 may encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than \*CHANGE, you should ensure 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 (QDSPSGNINF)**

The QDSPSGNINF 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 sign-on attempts that were not valid
- The number of days until the password expires (if the password is due to expire in 7 days or less)

**Note:** This system value is a restricted value. See Chapter 3: "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:

 $\frac{\mathbf{0}}{\mathbf{1}}$  Display is not shown. Display is shown.

**Recommended Value:** 1 (Display is shown) is recommended so 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 (QINACTITY)**

The QINACTITV 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 iSeries 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. Before Version 4, Release 2, telnet jobs were also excluded. To control the time-out of FTP connections, change the INACTTIMO parameter on the Change FTP Attribute (CHGFTPA) command. To control the time-out of telnet sessions before V4R2, use the Change Telnet Attribute (CHGTELNA) command.

Following are examples of 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 iSeries Access job may appear inactive to the system if the user is performing PC functions such as editing a document without interacting with the iSeries 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 QINACTITV system value. For example, if the system is started at 9:46 in the morning and the QINACTITV 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.

interval-in-minutes 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 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 Chapter 3: "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:

Inactive jobs are ended. If the inactive job is a group job, 1 all jobs associated with \*ENDJOB

the group are also ended. If the job is part of a secondary job, 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<sup>1</sup> 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 33 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.

Message CPI1126 is sent to the specified message queue when the inactive job message-queue-name

time-out interval is reached. This message states: Job &3/&2/&1; has not been

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.

Recommended Value: \*DSCJOB unless your users run iSeries Access jobs. Using \*DSCJOB when some iSeries 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 iSeries Access licensed program. The CL Programming book 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 iSeries 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 QLMTDEVSSN system value specifies whether a user is allowed to be signed on to more than one device at a time. 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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

The Work Management book describes group jobs and secondary jobs.

Table 11. Possible Values for the QLMTDEVSSN System Value:

The system allows an unlimited number of sign-on sessions.

1 Users are limited to one device session.

**Recommended Value:** 1 (Yes) 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 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 177 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 Chapter 3: "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:

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.

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 QMAXSIGN system value controls the number of consecutive sign-on attempts that are not correct by local and remote users. Incorrect sign-on 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 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 Chapter 3: "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:

A user can try to sign on a maximum of 3 times.

\*NOMAX The system allows an unlimited number of incorrect sign-on attempts. This gives

a potential intruder unlimited opportunities to guess a valid user ID and

password combination.

Specify a value from 1 through 25. The recommended number of sign-on limit

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 QMAXSGNACN system value determines what the system does when the maximum number of sign-on attempts is reached at a workstation.

Note: This system value is a restricted value. See Chapter 3: "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:

Disable both the user profile and device.

ī 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 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 25 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)

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 iSeries 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 CLRSVRSEC (Clear Server Security Data) command. If you have a large number of user profiles or validation lists on your system the CLRSVRSEC command may 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 from, it is not affected by the QRETSVRSEC system value.

Note: This system value is a restricted value. See Chapter 3: "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:

Server security data is not retained. Server security data is retained.

Recommended Value: 0.

\*VERIFY

# Remote Sign-On Control (QRMTSIGN)

The 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 iSeries Access licensed program, and TELNET access.

Note: This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 16. 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 may 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.

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.

program-name library-name The program specified runs at the start and end of every pass-through session.

Recommended Value: \*REJECT if you do not want to allow any pass-through or iSeries Access access. If you do allow pass-through or iSeries Access access, use \*FRCSIGNON or \*SAMEPRF.

The *Remote Work Station 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 17. 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.

For related information, see the "Scan File Systems Control (QSCANFSCTL)" topic.

# 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.

Table 18. Possible Values for the QSCANFSCTL System Value:

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

points.

\*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.

\*FSVRONLY 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.

Table 18. Possible Values for the QSCANFSCTL System Value: (continued)

\*NOPOSTRST

\*NOWRTUPG

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.

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.

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.

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 failures from the scan exit programs would 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.

For related information, see the "Scan File Systems (QSCANFS)" on page 28 topic.

# **Share Memory Control (QSHRMEMCTL)**

The QSHRMEMCTL system value defines which users are allowed to use shared memory or mapped memory that has write capability. 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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 19. Possible Values for the QSHRMEMCTL System Value:

Users cannot use shared memory, or use mapped memory that has write capability.

This value means that users cannot use shared-memory APIs (for example, shmat() — Shared Memory Attach API), and cannot use mapped memory objects that have write capability (for example, mmap() — Memory Map a File API provides this function).

Use this value in environments with higher security requirements.

**29** 

Table 19. Possible Values for the QSHRMEMCTL System Value: (continued)

1

Users can use shared memory or mapped memory that has write capability.

This value means that users can use shared-memory APIs (for example, shmat() — Shared Memory Attach API), and can use mapped memory objects that have write capability (for example, mmap() — Memory Map a File API provides this function).

Recommended Value: 1.

# **Use Adopted Authority (QUSEADPAUT)**

The 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 Chapter 3: "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 QUSEADPAUT System Value:

authorization list name

A diagnostic message is signaled to indicate that the program is created with USEADPAUT(\*NO) if all of the following are true:

- The user does not have authority to the specified authorization list.
- There are no other errors when the program or service program is created. All users can create or change programs and service programs to use adopted authority if the users have the necessary authority to the program or service program.

\*NONE

**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**

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.

Following 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

## **QDSCJOBITV**

Disconnected job time-out interval

**Note:** This system value is also discussed in the information center (see "Prerequisite and Related Information" on page xvi for details).

### **QRMTSRVATR**

Remote service attribute

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

# **Automatic Device Configuration (QAUTOCFG)**

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 Chapter 3: "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 QAUTOCFG System Value:

<u>O</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 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 Chapter 3: "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 QAUTOVRT System Value:

No virtual devices are created automatically.

Specify a value 1 through 9999. If fewer than the specified number of devices are number-of- virtual- devices

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

The Remote Work Station Support book has more information about using display station pass-through. The TCP/IP Configuration and Reference book has more information about using TELNET.

## **Device Recovery Action (QDEVRCYACN)**

QDEVRCYACN 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 Chapter 3: "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 QDEVRCYACN System Value:

Disconnects the job. When signing on again, an error message is sent to the \*DSCMSG

user's application program.

\*MSG Signals the I/O error message to the user's application program. The application

program performs error recovery.

Disconnects the job. When signing on again, a cancel request function is \*DSCENDRQS

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 next I/O operation is performed by the job. In an LAN/WAN environment, this may allow one device to disconnect and another to connect, using the same address, before the next I/O operation for the job occurs. The job may recover from the I/O error message and continue running to the second device. To avoid this, a device recovery action of \*DSCENDRQS, \*ENDJOB, or \*ENDJOBNOLIST should be specified. 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.

Before Version 3, Release 6, the default value was \*MSG. To leave as \*MSG presents a potential security exposure.

# Disconnected Job Time-Out Interval (QDSCJOBITV)

The QDSCJOBITV 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 QDSCJOBITV 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 Chapter 3: "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 QDSCJOBITV System Value:

240 The system ends a disconnected job after 240 minutes.
\*NONE The system does not automatically end a disconnected job.

time-in-minutes Specify a value between 5 and 1440.

**Recommended Value: 120** 

# Remote Service Attribute (QRMTSRVATR)

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 Chapter 3: "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 25. Possible Values for the QRMTSRVATR System Value:

 $rac{0}{1}$  Remote service attribute is off. Remote service attribute is on.

### Recommended Value: 0

For information about remote access and the QRMTSRVATR system value, see "Keylock Security" on page 2.

# **Security-Related Restore System Values**

#### 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.

Following 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 18 on page 28 for more information about the QSCANFSCTL \*NOPOSTRST system value.

#### **QVFYOBJRST**

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.

# **Verify Object on Restore (QVFYOBJRST)**

The QVFYOBJRST 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 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.

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 QVFYOBJRST system value during a restore operation.

A change to this system value takes effect immediately.

Note: This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

#### Attention

When your system is shipped, the QVFYOBJRST system value is set to 3. If you change the value of QVFYOBJRST, it is important to set the QVFYOBJRST value to 3 or lower before installing a new release of the i5/OS operating system.

Table 26. Possible Values for the QVFYOBJRST System Value:

2

3

5

Do not verify signatures on restore. Restore all objects regardless of their signature.

This value should not be used unless you have signed objects to restore which will fail their signature verification for some acceptable reason.

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.

This value should be used only if there are specific objects with signatures that are not valid which you want to restore. In general, it is dangerous to restore objects with signatures that are not valid on your system.

Verify signatures on restore. Restore unsigned commands and user-state objects. Restore signed commands and user-state objects only if the signatures are valid.

This value may be used 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.

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.

This value should be used only if there are specific objects with signatures that are not valid which you want to restore, but you do not want the possibility of unsigned objects being restored. In general, it is dangerous to restore objects with signatures that are not valid on your system.

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.

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

Objects which have the system-state attribute and objects which have the inherit-state attribute are required to have valid signatures from a system trusted source. The only value which will allow a system-state or inherit-state object to restore without a valid signature is 1. Allowing such a command or program represents an integrity risk to your system. If you change the QVFYOBJRST system value to 1 to allow such an object to restore on your system, be sure to change the QVFYOBJRST system value back to its previous value after the object has been restored.

Some commands use a signature that does not cover 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 wish, 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)

This system value allows you to specify whether to convert the following object types during a restore:

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

It can also prevent some objects from being restored. 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.

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 Chapter 3: "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 27. QFRCCVNRST Values

0	Do not convert anything. Do not prevent anything from being restored.
1	Objects with validation errors will be converted.
$\frac{1}{2}$	Objects will be converted if their conversion is required for the current operating system 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 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) which have validation errors are suspected of having been tampered with, or require conversion to be used on the current version of the operating system 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 which have validation errors, are suspected of having been tampered with, or require conversion to be used on the current version of the operating system 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 QALWOBJRST system value determines whether objects that are security-sensitive may be restored to your system. You can use it to prevent anyone from restoring a system state object or an object that adopts authority.

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.

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 i5/OS 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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

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

Table 28. Possible Values for the QALWOBJRST System Value:

Any object may be restored to your system by a user with the correct authority. \*ALL \*NONE Security-sensitive objects, such as system state programs or programs that adopt

authority, may not be restored to the system.

\*ALWSYSSTT System and inherit state objects may be restored to the system. Objects that adopt authority may be restored to the system. \*ALWPGMADP

System and inherit state objects, objects that adopt authority, objects that have \*ALWPTF

> 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. Allow restore of files that have the S\_ISGID (set-group-ID) attribute enabled. \*ALWSETGID \*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 may need to set the QALWOBJRST system value to \*ALWPGMADP.

# System Values That Apply to Passwords

#### Overview:

**Purpose:** 

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

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.

Following are the system values that control 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:

#### QPWDEXPITV 1

**Expiration interval** 

#### **QPWDLVL**

Password level

## QPWDMINLEN 1

Minimum length

## QPWDMAXLEN 1

Maximum length

## QPWDRQDDIF 1

Required difference

## **QPWDLMTCHR**

Restricted characters

### **QPWDLMTAJC**

Restrict adjacent characters

### **QPWDLMTREP**

Restrict repeating characters

## **QPWDPOSDIF**

Character position difference

### **QPWDRQDDGT**

Require numeric character

### **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.

If the Password Minimum Length (QPWDMINLEN) system value has a value other than 1 or the Password Maximum Length (QPWDMAXLEN) system value has a value other than 10 or you change any of the other password-control system values from the defaults, 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.

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.

# **Password Expiration Interval (QPWDEXPITV)**

The 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.

<sup>1.</sup> These system values are also discussed in the Information Center (see "Prerequisite and Related Information" on page xvi for details).

Sign-on Information

System:

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

request.

Previous sign-on . . . . . . . . . . . . . . . . . . 10/30/91 14:15:00

**Note:** This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 29. 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 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" on page 196.

**Note:** This system value is a restricted value. See Chapter 3: "Security System Values" 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 QPWDLVL System Value:

0

The system supports user profile passwords with a length of 1-10 characters. The allowable characters are A-Z, 0-9 and characters \$\$, @, # and underscore. QPWDLVL 0 should be used if your system communicates with other iSeries systems 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 Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) product and your system communicates with other systems using passwords from 1-10 characters. 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.

Table 30. Possible Values for the QPWDLVL System Value: (continued)

QPWDLVL 1 is the equivalent support of QPWDLVL 0 with the following exception: iSeries NetServer passwords for Windows 95/98/ME clients will be removed from the system. If you use the client support for the iSeries NetServer product you cannot use QPWDLVL value 1. QPWDLVL 1 improves the security of the iSeries system by removing all iSeries NetServer passwords from the system.

2

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. QPWDLVL 2 can be used if your system communicates with the Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) product as long as your password is 1-14 characters in length. QPWDLVL 2 cannot be used if your system communicates with other iSeries systems 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. No encrypted passwords are removed from the system when QPWDLVL is changed to 2.

3

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 3 cannot be used if your system communicates with other iSeries systems 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 Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) product. 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.

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 CL command DSPSECA (Display Security Attributes).

# Minimum Length of Passwords (QPWDMINLEN)

The QPWDMINLEN system value controls the minimum number of characters in a password.

Note: This system value is a restricted value. See Chapter 3: "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 QPWDMINLEN System Value:

A minimum of six characters are required for passwords.

minimum-number-of-characters 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, to prevent users from assigning passwords that are easily guessed, such as initials or a single character.

# Maximum Length of Passwords (QPWDMAXLEN)

The 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.

Note: This system value is a restricted value. See Chapter 3: "Security System Values" 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 QPWDMAXLEN System Value:

A maximum of eight characters for a password are allowed.

Specify a value of 1 through 10 when the password level (QPWDLVL) system maximum-number-of-characters

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 QPWDRQDDIF system value controls whether the password must be different from previous passwords. This value provides additional security by preventing users from specifying passwords 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.

Note: This system value is a restricted value. See Chapter 3: "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 QPWDRQDDIF System Value:

Table co. I coolbie values it	or the at the table eyetem value.
Value	Number of Previous Passwords Checked for Duplicates
0	0 Duplicate passwords are allowed.
$\overline{1}$	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 QPWDRQDDIF system value and the QPWDEXPITV (password expiration interval) 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 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.

**Note:** This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 34. Possible Values for the QPWDLMTCHR System Value:

\*NONE There are no restricted characters for passwords.

restricted-characters Specify up to 10 restricted characters. The valid characters are A through Z, 0

through 9, and special characters pound (#), dollar (\$), at (@), and underscore

(\_).

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

# Restriction of Consecutive Digits for Passwords (QPWDLMTAJC)

The 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.

**Note:** This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 35. Possible Values for the QPWDLMTAJC System Value:

Numeric characters are allowed next to each other in passwords.

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

# **Restriction of Repeated Characters for Passwords (QPWDLMTREP)**

The 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'.

**Note:** This system value is a restricted value. See Chapter 3: "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 QPWDLMTREP System Value:

The same characters can be used more than once in a password.

The same character cannot be used more than once in a password.

The same character cannot be used consecutively in a password.

Table 37 on page 44 shows examples of what passwords are allowed based on the QPWDLMTREP system value.

Table 37. Passwords with Repeating Characters with QPWDLVL 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 38. Passwords with Repeating Characters with QPWDLVL 2 or 3

Password Example	QPWDLMTREP Value of 0	QPWDLMTREP Value of 1	QPWDLMTREP Value of 2
j222222	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 QPWDPOSDIF system value controls each position in a new password. This 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'.

Note: This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 39. Possible Values for the QPWDPOSDIF System Value:

0	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 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.

Note: This system value is a restricted value. See Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 40. Possible Values for the QPWDRQDDGT System Value:

Numeric characters are not required in new passwords. 1 One or more numeric characters are required in new passwords.

Recommended Value: 1.

# Password Approval Program (QPWDVLDPGM)

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.

The topic "Using a Password Approval Program" discusses the requirements of the password approval program and shows an example.

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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 41. Possible Values for the QPWDVLDPGM System Value:

*NONE	No user-written program is used. This includes any password approval programs registered in the exit registration facility.
*REGFAC	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.
program-name	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.
library-name	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 entered by the user has passed all the other tests you 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 42. Parameters for Password Approval Program

Position	1	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 for the password to 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:

```
/* 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)
                    TYPE(*CHAR) LEN(10)
  DCL VAR(&OLD)
  DCL VAR(&RTNCD)
                    TYPE(*CHAR) LEN(1)
  DCL VAR(&USER)
                    TYPE(*CHAR) LEN(10)
                    TYPE(*CHAR) LEN(6)
  DCL VAR(&JOBDATE)
  DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
                    TYPE(*CHAR) LEN(4)
  DCL VAR(&PWDEXP)
/* 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:

```
/* 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
           *DEC 5 0
DCL &UNLEN
DCL &XLTCHR2
           *CHAR 2 VALUE(X'0000')
DCL &XLTCHR
           *DEC 5 0
DCL &XLATEU
           *CHAR 255 VALUE('..... +
                       !"#$%&''()*+,-./0123456789:;<=>?+
                       @ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^ +
                       `ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~.+
                       +
                       *CHAR 255 VALUE('....+
DCL &XLATEC
                       .....+
                       .....+
                       .ABCDEFGHI.....+
                       ..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 */
/st Get new password length, offset and value. Also get user name st/
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)
    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
    ENDD0
   CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEU &XLTCHR 1))
    CHGVAR &INDX2 VALUE(&INDX2 + 2)
    CHGVAR &INDX3 VALUE(&INDX3 + 1)
    IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
   GOTO CVT1
   ECVT1:
    CHGVAR &NPLEN VALUE(&INDX3 - 1)
   CHGVAR %SST(&EXINPUT 65 4) VALUE(X'00000025')
 ENDD0
 /* 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)
   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
   ENDD0
   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 > &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)
L00P2:
           /* 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)
   G0T0 L00P2
 ENDDO
EL00P2:
 CHGVAR &UNLEN VALUE (&UNLEN - 1)
/* CHECK FOR USER NAME IN NEW PASSWORD
IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
CHGVAR &INDX VALUE(1)
L00P3:
  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
EL00P3:
/* New Password is valid
                                                */
GOTO DONE
ERROR1: /* NEW PASSWORD ENDS IN NUMERIC CHARACTER */
CHGVAR &RTN VALUE('3') /* reject */
 SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
 GOTO DONE
ERROR2: /* NEW PASSWORD CONTAINS USER NAME */
 CHGVAR &RTN VALUE('3') /* reject */
 SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
 GOTO DONE
DONE:
ENDPGM
```

# **System Values That Control Auditing**

#### 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

Descriptions of these system values follow. The possible choices are shown. The choices that are underlined are the system-supplied defaults. For most system values, a recommended choice is listed.

# **Auditing Control (QAUDCTL)**

The QAUDCTL system value determines whether auditing is performed. It 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 Chapter 3: "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 43. Possible Values for the QAUDCTL System Value:

\*NONE No auditing is performed for user actions and objects.

\*NOTAVL Indicates 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 the iSeries System," on page 231 for more details. You must specify this value with either \*OBJAUD or \*AUDLVL.

See "Planning Security Auditing" on page 236 for a complete description of the

process for controlling auditing on your system.

# **Auditing End Action (QAUDENDACN)**

The 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 Chapter 3: "Security System Values" 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 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.

\*PWRDWNSYS 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 \*PWRDWNSYS.

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 \*PWRDWNSYS, 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 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 Chapter 3: "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 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.

number-of- records 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 may impair performance.

# **Auditing Level (QAUDLVL)**

The 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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 46. 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.

\*JOBDTA Actions that affect a job are logged.

\*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 allow 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.

\*OFCSRV 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.

\*SECSCKD Socket descriptors are audited.

Table 46. Possible Values for the QAUDLVL System Value: (continued)

\*SECURITY Security-related functions are logged.

\*SECURITY is composed of several values to allow you to better customize your

auditing. The following values make up \*SECURITY:

\*SECCFG \*SECDIRSRV \*SECIPC \*SECNAS \*SECRUN \*SECSCKD \*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.

See "Planning the Auditing of Actions" on page 236 for a complete description of the journal entry types and the possible values for QAUDLVL.

# **Auditing Level Extension (QAUDLVL2)**

The 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 Chapter 3: "Security System Values" for details on how to restrict changes to security system values and a complete list of the restricted system values.

Table 47. 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.

\*JOBDTA Actions that affect a job are logged.

\*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 allow 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.

Table 47. Possible Values for the QAUDLVL2 System Value: (continued)

\*OBJMGT Object move and rename operations are logged.

\*OFCSRV 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. Network authentication service actions are audited. \*SECNAS

\*SECRUN Security run time functions are audited.

Socket descriptors are audited. \*SECSCKD \*SECURITY Security-related functions are logged.

\*SECURITY is composed of several values to allow you to better customize your

auditing. The following values make up \*SECURITY:

\*SECCFG \*SECDIRSRV \*SECIPC \*SECNAS \*SECRUN \*SECSCKD \*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.

See "Planning the Auditing of Actions" on page 236 for a complete description of the journal entry types and the possible values for QAUDLVL2.

# Auditing for New Objects (QCRTOBJAUD)

The QCRTOBJAUD system value is used to determine the auditing value for a new object or directory, if the 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 Chapter 3: "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 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. The section "Planning the Auditing of Object Access" on page 254 provides more information about methods for setting up object auditing on your system. You may 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 may 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**

This chapter describes user profiles: their purpose, their features, and how to design them. 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

### Roles of the User Profile

The 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. Table 143 in Appendix B 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. It 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 may 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 214 shows an example of setting up a group profile.

### **User-Profile Parameter Fields**

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

Following are explanations of each field in the user profile. The fields are described in the order they appear on the Create User Profile command prompt.

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. This is the format used:

#### Field Title

The title of the section shows how the field name appears on the Create User Profile command prompt, which is shown 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 parameter associated with the field.

### **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 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**

Add User prompt:

User

**CL** parameter:

**USRPRF** 

Length:

10

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.

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 (\$), underscore (\_), at (@).

Note: The Add User display allows only an eight-character user name.

The user profile name cannot begin with a number.

**Note:** 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* book.

**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 you use to manage user profiles show them in alphabetical order by user profile name.
- Avoid using special characters in user profile names. Special characters may cause problems with keyboard mapping for certain workstations or with national language versions of the i5/OS licensed program.

One technique for assigning user profile names is to use the first seven characters of the last 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:** If you want to be able to easily identify group profiles on lists and displays, follow the naming convention. Begin all group profile names with the same characters, such as GRP (for group) or DPT (for department).

### **Password**

Add User prompt:

Password

**CL** parameter:

**PASSWORD** 

Length:

128

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).

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 signon 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 signon via the system signon 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. If the password minimum length (QPWDMINLEN) system value is not 1 or the password maximum length (QPWDMAXLEN) system value is not 10 or any of the other password composition system values have been changed from the default values, a user cannot set the password equal to the user profile name using the CHGPWD command, the ASSIST menu, or the QSYCHGPW API.

See the topic "System Values That Apply to Passwords" on page 38 for information about setting the password composition system values.

Table 49. 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.

user- password 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 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**

Add User prompt:

Not shown

**CL** parameter:

**PWDEXP** 

Length:

4

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. 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 Figure 1). 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.

Sign-on Information

System:

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

Previous sign-on . . . . . . . . . . . . :

10/30/91 14:15:00

Figure 1. Password Expiration Message

Table 50. Possible Values for PWDEXP:

\*NO:

\*YES:

The password is not set to expired.

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**

Add User prompt:

Not shown

**CL** parameter:

**STATUS** 

Length:

10

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.

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. The topic "Enabling a User Profile" on page 104 shows an example of an adopted authority program to allow a system operator to enable a profile.

The system may disable a profile after a certain number of incorrect sign-on 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 51. 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**

Add User prompt:

Type of User

**CL** parameter:

**USRCLS** 

Length:

10

User class is used to control what menu options are shown to the user on i5/OS menus. 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 52 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 52. Default Special Authorities by User Class

<b>Special Authority</b>	*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**

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.

The Assistance level field in the user profile is used to specify the default assistance level for the user when the profile is created. 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 53 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 53. How Assistance Levels Are Stored and Changed

Version of Display Shown	Version of Display Stored
Work with User Enrollment display	No change (basic assistance level)
Work with User Profiles display	Changed to intermediate assistance level
Work with User Profiles display	No change (intermediate)
Work with User Profiles display	No change (intermediate)
	Changed to basic assistance level
Work with User Enrollment display	No change (basic)
Work with User Profiles display	No change (basic)
	Work with User Enrollment display Work with User Profiles display

**Note:** The *User option* field in the user profile also affects how system displays are shown. This field is described on page 90.

Table 54. 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.

\*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**

Add User prompt:

Default library

**CL** parameter:

**CURLIB** 

Length:

10

Authority

\*USE

The current library is searched before the libraries in the user portion of the library list for any objects specified as \*LIBL. If the user creates objects and specifies \*CURLIB, the objects are put in the current library.

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 183 provides more information about using library lists and the current library.

Table 55. 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.

current-library-name 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**

### Add User prompt:

Sign on program

#### **CL** parameter:

**INLPGM** 

### Length:

10 (program name) 10 (library name)

#### **Authority:**

\*USE for program \*EXECUTE for library

You can specify the name of a program to call when a user signs on. This program runs before the initial menu, if any, is displayed. 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 175 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 56. 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.

program-name The name of the program that is called when the user signs on.

Table 57. 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.

library-name The library where the program is located.

### **Initial Menu**

#### Add User prompt:

First menu

### **CL** parameter:

**INLMNU** 

### Length:

10 (menu name) 10 (library name)

#### **Authority**

\*USE for menu \*EXECUTE for library

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.

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 58. Possible Values for MENU:

MAIN The iSeries system 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.

menu-name The name of the menu that is called when the user signs on.

Table 59. 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.

library-name The library where the menu is located.

# **Limit Capabilities**

### Add User prompt:

Restrict command line use

### **CL** parameter:

**LMTCPB** 

#### Length:

10

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 one tool for preventing users from experimenting on the system.

A user with LMTCPB(\*YES) can only run commands that are defined as allow limited user (ALWLMTUSR) \*YES. These 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 do the following:

- Running commands in CL programs that are running a command as a result of taking an option from a menu
- · Running 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 60 shows the possible values for *Limit capabilities* and what functions are allowed for each value.

Table 60. Functions Allowed for Limit Capabilities Values

Function	*YES	*PARTIAL	*NO
Change Initial Program	No	No	Yes
Change Initial Menu	No	Yes	Yes
Change Current Library	No	No	Yes
Change Attention Program	No	No	Yes
Enter Commands	A few <sup>1</sup>	Yes	Yes

These commands are allowed: SIGNOFF, SNDMSG, 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. See the topic "Planning Menus" on page 203 for more information about this type of environment.

### **Text**

Add User prompt:

User description

**CL** parameter:

**TEXT** 

### Length:

50

The text in the user profile is used to describe the user profile or what it is used for. 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 61. Possible Values for text:

\*BLANK: No text is specified.

description 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

### Add User prompt:

Not shown

#### **CL** parameter:

**SPCAUT** 

### Length:

100 (10 characters per special authority)

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

Table 62. 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 52 on page 63 shows the default special authorities for each user class.

\*NONE No special authority is granted to this user.

Specify one or more special authorities for the user. The special authorities are special-authority-name

described in the sections that follow.

# \*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

Job control (\*JOBCTL) special authority allows the user to:

- 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 186.

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 with \*JOBCTL special authority can 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). 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, 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 iSeries 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. It also allows the user to debug a program with only \*USE authority to the program and perform the display and alter service functions. The dump function can be performed without \*SERVICE authority. It also allows the user to perform various trace functions.

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 needing to give the user \*SERVICE special authority. In this way, only specific users will 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 the operating system through Application Administration in iSeries 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:

Table 63.

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" on page 71)
TRCINT	Trace Internal
STRTRC	Start Job Trace
ENDTRC	End Job Trace
PRTTRC	Print Job Trace
DLTTRC	Delete Job Trace
TRCTCPAPP	Trace TCP/IP Application
WRKTRC	Work with Traces

**Note:** You need \*ALLOBJ to be able 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. Following the steps below will let you limit who can access these trace commands without having \*SERVICE authority:

- 1. In iSeries 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. The user can:

- · 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.
- Execute some of the security tool commands (for example, 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.

| If it is important that auditing information not be viewable by general users, take additional actions to restrict general users from viewing 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. For example, adding or removing communications configuration information, working with

TCP/IP servers, and configuring the internet connection server (ICS). Most commands for configuring communications require \*IOSYSCFG special authority. Appendix D shows what special authorities are required for specific commands.

**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**

Add User prompt:

Not shown

**CL** parameter:

**SPCENV** 

Length:

10

Special environment determines the environment the user operates in after signing on. The user can operate in the iSeries, 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. See Figure 2 on page 73.

Table 64. 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 iSeries 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 iSeries 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 iSeries applications.

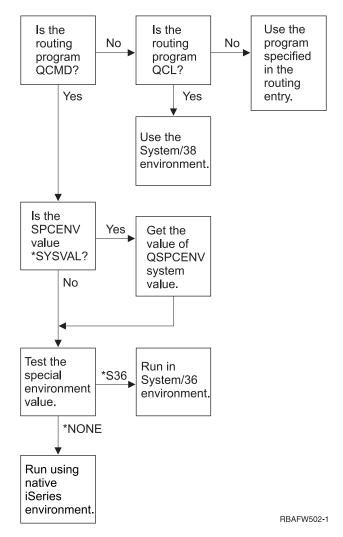


Figure 2. Description of Special Environment

### **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 native iSeries environment.

# **Display Sign-On Information**

Add User prompt:

Not shown

**CL** parameter:

**DSPSGNINF** 

### Length:

The Display sign-on information field specifies whether the Sign-on Information display is shown when the user signs on. Figure 3 shows the display. Password expiration information is only shown if the password expires within seven days.

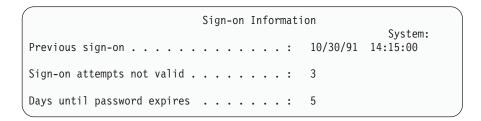


Figure 3. Sign-On Information Display

Table 65. 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:** The Sign-on Information display is a tool for users to monitor their profiles and to detect attempted misuse. 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**

### Add User prompt:

Not shown

#### **CL** parameter:

**PWDEXPITV** 

### Length:

5.0

Requiring users to change their passwords after a specified length of time reduces the risk of an unauthorized person accessing the system. The password expiration interval controls the number of days that a valid password can be used before it must be changed.

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. Figure 1 on page 62 shows an example of the password expiration message.

Recommendations: Use the user profile password expiration interval to require profiles with \*SERVICE, \*SAVSYS, \*SECADM, or \*ALLOBJ special authorities to change passwords more frequently than other users.

Table 66. Possible Values for PWDFXPITV:

\*SYSVAL The QPWDEXPITV system value is used.

\*NOMAX The system does not require the user to change the password.

password- expiration- interval 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 for individual users who should change their passwords more frequently, such as security administrators.

# **Local Password Management**

Add User prompt:

Not shown

**CL** parameter:

LCLPWDMGT

Length:

10

The Local password management specifies whether the user profile password should be managed locally. 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.

If the password is not being managed locally, then the local i5/OS 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 iSeries Integration for Windows Server. The user will not be able to change his password using the Change Password (CHGPWD) command. In addition, he 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 Integration for Windows Server. See your product documentation for details

This parameter should not be set to \*NO unless the user only needs to access the system through some other platform, such as Windows.

Table 67. Possible Values for LCLPWDMGT:

\*YES The password is managed locally.
\*NO The password is not managed locally.

### **Limit Device Sessions**

Add User prompt:

Not shown

**CL** parameter:

**LMTDEVSSN** 

Length:

7

The *Limit device sessions* field controls whether a user can be signed on at more than one workstation at a time. The value does not restrict the use of the System Request menu or a second sign-on from the same device.

Table 68. Possible Values for LMTDFVSSN:

\*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.

**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**

### Add User prompt:

Not shown

#### **CL** parameter:

KBDBUF

### Length:

10

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.

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 69. 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

\*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**

### Add User prompt:

Not shown

#### **CL** parameter:

**MAXSTG** 

#### Length:

11,0

You can specify the maximum amount of auxiliary storage that is used to store permanent objects that are owned by a user profile, including objects placed in the temporary library (QTEMP) during a job. Maximum storage is specified in kilobytes (1024 bytes).

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 owner of a library is assigned the storage for the descriptions of the objects that are placed in a library, even when the objects are owned by another user profile. Examples of such descriptions are text and program references.
- Storage is assigned to the user profile for temporary objects that are used during the processing of a job. Examples of such objects are commitment control blocks, file editing spaces, and documents.

Table 70. Possible Values for MAXSTG:

\*NOMAX

As much storage as required can be assigned to this profile.

maximum- KB

Specify the maximum amount of storage in kilobytes (1 kilobyte equals 1024 bytes) that can be assigned to this user profile.

# **Priority Limit**

### 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 on the job queue. Job priority can be set by the job description or on the submit command.

### **Output priority:**

Determines the scheduling priority for any output created by the job on the output queue. Output priority can be set by the job description or on the submit command.

The priority limit in the user profile determines the maximum scheduling priorities (job priority and output priority) allowed for any jobs the user submits. It controls priority when the job is submitted, as well as any changes made to priority while the job is running or waiting in a queue.

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 71. Possible Values for PTYLMT:

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.

priority- limit 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

### Add User prompt:

Not shown

### **CL** parameter:

**JOBD** 

### 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.

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.

See the Work Management book for more information about job descriptions and their uses.

Table 72. Possible Values for JOBD:

QDFTJOBD The system-supplied job description found in library QGPL is used. You can use

the Display Job Description (DSPJOBD) command to see the attributes contained

in this job description.

job- description- name Specify the name of the job description, 10 characters or less.

Table 73. Possible Values for JOBD 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.

library- name 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 system value.

# **Group Profile**

### 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 128.

Specifying a group profile name makes the user a member of the 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.

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 214 for more information about using group profiles.

Table 74. Possible Values for GRPPRF:

\*NONE No group profile is used with this user profile.

*user- profile- name* Specify the name of a group profile of which this user profile is a member.

### **Owner**

### Add User prompt:

Not shown

### **CL** parameter:

**OWNER** 

### Length:

10

If the user is a member of a group, you 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 the *Group profile* field.

When the OWNER value is changed, the change will take 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 75. Possible Values for OWNER:

\*USRPRF \*GRPPRF This user profile is the OWNER of any new objects it creates.

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.

#### **Notes:**

- 1. If you give ownership to the group, all members of the group can change, replace, and delete the object.
- 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**

### Add User prompt:

Not shown

### **CL** parameter:

**GRPAUT** 

### Length:

10

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.

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 will take 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 76. 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.

See "Defining How Information Can Be Accessed" on page 112 for a complete explanation of the authorities that can be granted.

# **Group Authority Type**

Add User prompt:

Not shown

**CL** parameter:

**GRPAUTTYP** 

Length:

10

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. The GRPAUTTYP parameter works with the OWNER, GRPPRF, and GRPAUT parameters to determine the group's authority to a new object.

When the GRPAUTTYP value is changed, the change will take 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 77. Possible Values for GRPAUTTYP: 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.

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 123 explains how primary group authority works.

**Recommendations:** Specifying \*PGP is a method for beginning to use primary group authority. Consider using GRPAUTTYP(\*PGP) for users who frequently create new objects that must be accessed by members of the group profile.

# **Supplemental Groups**

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 128.

You may 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. The user cannot have supplemental group profiles if the GRPPRF parameter is \*NONE.

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 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 SUPGRPPRF value is changed, the change will take 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 214 for more information about using group profiles.

Table 78. Possible Values for SUPGRPPRF

\*NONE No supplemental groups are used with this user profile.

group- profile- name 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**

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.

See the Work Management book for more information about job accounting.

Table 79. Possible Values for ACGCDE:

\*BLANK An accounting code of 15 blanks is assigned to this user profile.

accounting- code Specify a 15-character accounting code. If less than 15 characters are specified,

the string is padded with blanks on the right.

### **Document Password**

### Add User prompt:

Not shown

### **CL** parameter:

**DOCPWD** 

You can specify a document password for the user to protect the distribution of personal mail from being viewed by people working on behalf of the user. The document password is supported by some Document Interchange Architecture (DIA) products, such as the Displaywriter.

Table 80. Possible Values for DOCPWD:

\*NONE No document password is used by this user.

document- password 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**

### 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.

You can specify the name of a message queue for a user. 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. 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 81. 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.

message- queue-name 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 82. 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.

library- name Specify the library where the message queue is located. If the message queue

does not exist, it is created in this library.

**Recommendations:** When a user signs on, the message queue in the user profile is allocated to that user's job. If the message queue is already allocated to another job, the user receives a warning message during sign-on. To avoid this, give each user profile a unique message queue, preferably with the same name as the user profile.

# **Delivery**

Add User prompt:

Not shown

**CL** parameter:

**DLVRY** 

Length:

10

The delivery mode of a message queue determines whether the user is interrupted when a new message arrives on the queue. 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 affect 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 83. Possible Values for DLVRY:

\*NOTIFY The job that the message queue is assigned to is notified when a message arrives

at the message queue. For interactive jobs at a workstation, the audible alarm is sounded and the message-waiting light is turned 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 is sounded (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

Add User prompt:

Not shown

**CL** parameter:

**SEV** 

Length:

2,0

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.

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 84. Possible Values for SFV:

<u>0</u>: 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.

severity- code 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**

Add User prompt:

Default printer

**CL** parameter:

**PRTDEV** 

Length:

10

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).

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 *Printer Device Programming* book.

Table 85. Possible Values for PRTDEV:

\*WRKSTN

\*SYSVAL

The printer assigned to the user's workstation (in the device description) is used.

The default system printer specified in the QPRTDEV system value is used.

Print- device- name

Specify the name of the printer that is used to print the output for this user.

# **Output Queue**

### Add User prompt:

Not shown

**CL** parameter:

**OUTQ** 

Length:

10 (output queue name) 10 (library name)

**Authority:** 

\*USE for output queue \*EXECUTE for library

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. 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 *Printer Device Programming* book.

Table 86. 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.

output- queue- name 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 87. Possible Values for OUTQ library:

\*LIBL The library list is used to locate the output queue.

\*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.

library- name Specify the library where the output queue is located.

# **Attention-Key-Handling Program**

### Add User prompt:

Not shown

### **CL** parameter:

**ATNPGM** 

### Length:

10 (program name) 10 (library name)

### **Authority:**

\*USE for program

\*EXECUTE for library

The **Attention-key-handling program** (ATNPGM) is the program that is called when the user presses the Attention (ATTN) key during an interactive job.

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 175 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 88. 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.

program- name Specify the name of the Attention-key-handling program. If a program name is

specified, a library must be specified.

Table 89. Possible Values for ATNPGM Library:

\*LIBL The library list is used to locate the Attention-key-handling program.

\*CURLIB The library list is used to locate the Attention-key-handling

program. If no current library entry exists in the library list, QGPL is used.

library- name: Specify the library where the Attention-key-handling program is located.

## **Sort Sequence**

**Add User prompt:** 

Not shown

**CL** parameter:

**SRTSEQ** 

Length:

10 (value or table name) 10 (library name)

**Authority:** 

\*USE for table \*EXECUTE for library

You can specify what sort sequence is used for this user's output. You can use system-provided sort tables or create your own. A sort table may be associated with a particular language identifier on the system.

Table 90. 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.

table-name Specify the name of the sort sequence table for this user.

Table 91. 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.

library- name Specify the library where the sort sequence table is located.

# Language Identifier

Add User prompt:

Not shown

**CL** parameter:

**LANGID** 

Length:

10

You can specify the language identifier to be used by the system for the user. 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 92. Possible Values for LANGID:

\*SYSVAL: The system value QLANGID is used to determine the language identifier.

language- identifier Specify the language identifier for this user.

## **Country or Region Identifier**

### Add User prompt:

Not shown

### **CL** parameter:

**CNTRYID** 

#### Length:

10

You can specify the country or region identifier to be used by the system for the user. 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 93. Possible Values for CNTRYID:

\*SYSVAL The system value QCNTRYID is used to determine the country or region

identifier.

country or region identifier Specify the country or region identifier for this user.

## **Coded Character Set Identifier**

#### Add User prompt:

Not shown

#### **CL** parameter:

**CCSID** 

#### Length:

5,0

You can specify the coded character set identifier to be used by the system for the user. 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 94. Possible Values for CCSID:

\*SYSVAL The QCCSID system value is used to determine the coded character set

identifier.

coded-character- set-identifier Specify the coded character set identifier for this user.

### **Character Identifier Control**

### Add User prompt:

Not shown

#### **CL** parameter:

**CHRIDCTL** 

#### Length:

10

The *CHRIDCTL* attribute controls the type of coded character set conversion that occurs for display files, printer files and panel groups. 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 95. 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.

\*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**

Add User prompt:

Not shown

**CL** parameter:

**SETJOBATR** 

Length:

160

The *SETJOBATR* field specifies which job attributes are to be taken at job initiation from the locale specified in the LOCALE parameter.

Table 96. 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.

Any combination of the following values may be specified:

\*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.

#### Locale

#### Add User prompt:

Not shown

#### **CL** parameter:

LOCALE

The *Locale* field specifies the path name of the locale that is assigned to the LANG environment variable for this user.

Table 97. 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.

locale path name

The path name of the locale to be assigned to this user.

## **User Options**

## **Add User prompt:**

Not shown

#### **CL** parameter:

**USROPT** 

#### Length:

240 (10 characters each)

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.

Table 98. 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 133 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.

\*NOSTSMSG Status messages typically shown at the bottom of the display are not shown to

the user.

\*STSMSG Status messages are displayed when sent to the user.

### **User Identification Number**

### Add User prompt:

Not shown

#### **CL** parameter:

**UID** 

#### Length:

10,0

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.

Table 99. Possible Values for UID:

\*GEN The system generates a unique uid for this user. The generated uid will be

greater than 100.

uid 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**

Add User prompt:

Not shown

**CL** parameter:

**GID** 

Length:

10.0

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.

Table 100. Possible Values for GID:

\*NONE This profile does not have a gid.

\*GEN The system generates a unique gid for this profile. The generated gid will be

greater than 100.

gid 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 may 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**

Add User prompt:

Not shown

**CL** parameter:

**HOMEDIR** 

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. 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 101. Possible Values for HOMEDIR:

\*USRPRF The home directory assigned to the user is /home/xxxxx, where xxxxx is the

user's profile name.

home-directory The name of the home directory to assign to this user.

### **EIM Association**

#### Add User prompt:

Not shown

#### **CL** parameter:

**EIMASSOC** 

The EIM association specifies whether an EIM (Enterprise Identity Mapping) 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.

#### Note:

- 1. This 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 102. Possible Values for EIMASSOC, Single Values:

**Single Values** 

\*NOCHG EIM association will not be added.

Table 103. 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.

character-value Specifies the name of the EIM identifier.

Table 104. 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 i5/OS user.

Target associations are primarily used to secure existing data. They are found as the result of a mapping lookup operation (for example, eimGetTargetFromSource()), 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 105. 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 106. 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.

## **Authority**

### Add User prompt:

Not shown

#### **CL** parameter:

**AUT** 

The *Authority* field specifies the public authority to the user profile. The authority to a profile controls many functions associated with the profile, such as:

Changing it

Displaying it

Deleting it

Submitting a job using it

Specifying it in a job description

Transferring object ownership to it

Adding members, if it is a group profile

Table 107. 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 112 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**

Add User prompt:

Not shown

**CL** parameter:

**OBJAUD** 

Length:

10

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. Object auditing for a user profile cannot be specified on any user profile displays. Use the CHGUSRAUD command to specify object auditing for a user. Only a user with \*AUDIT special authority can use the CHGUSRAUD command.

Table 108. 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 indicates 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 109 shows how the OBJAUD values for the user and the object work together:

Table 109. Auditing Performed for Object Access

	OBJAUD Value for User					
OBJAUD Value for Object	*NONE	*CHANGE	*ALL			
*ALL	Change and Use	Change and Use	Change and Use			
*CHANGE	Change	Change	Change			
*NONE	None	None	None			
*NOTVAL	None	None	None			
*USRPRF	None	Change	Change and Use			

<sup>&</sup>quot;Planning the Auditing of Object Access" on page 254 provides information about how to use system values and the object auditing values for users and objects to meet your security auditing needs.

## **Action Auditing**

#### Add User prompt:

Not shown

### **CL** parameter:

**AUDLVL** 

### Length:

640

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 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 110. Possible Values for AUDI VI:

The QAUDLVL system value controls action auditing for this user. No additional \*NONE

auditing is done.

\*NOTAVL This value indicates 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.

\*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.

\*JOBDTA Job changes are logged.

Object move and rename operations are logged. \*OBJMGT

\*OFCSRV Changes to the system distribution directory and office mail actions are logged. \*PGMADP

Obtaining authority to an object through a program that adopts authority is

logged.

\*SAVRST Save and restore operations are logged. Security-related functions are logged. \*SECURITY

Using service tools is logged. \*SERVICE

\*SPLFDTA Actions performed on spooled files are logged. \*SYSMGT Use of systems management functions is logged.

"Planning the Auditing of Actions" on page 236 provides information about how to use system values and the action auditing for users to meet your security auditing needs.

### Additional Information Associated with a User Profile

The previous sections described the fields you specify when you create and change user profiles. Other information is associated with a user profile on the system and saved with it:

- · Private authorities
- Owned object information
- · Primary group object information

The amount of this information affects the time it takes to save and restore profiles and to build authority displays. "How Security Information is Stored" on page 222 provides more information about how user profiles are stored and saved.

### **Private Authorities**

All the private authorities a user has to objects are stored with the user profile. When a user needs authority to an object, the user's private authorities may be searched. "Flowchart 3: How User Authority to an Object Is Checked" on page 152 provides more information about authority checking.

You can display a user's private authorities to library-based objects using the Display User Profile command: DSPUSRPRF user-profile-name TYPE(\*0BJAUT). 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 the private authorities from one user profile to another using the Grant User Authority (GRTUSRAUT) command. See "Copying Authority from a User" on page 145 for more information.

## **Primary Group Authorities**

The names of all 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(\*0BJPGP). You can also use the Work with Objects by Primary Group (WRKOBJPGP) command.

## **Owned Object Information**

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. 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.

## **Digital ID Authentication**

The iSeries security infrastructure allows x.509 digital certificates to be used for identification. The digital certificates allow users to secure communications and ensure message integrity.

The digital ID APIs create, distribute, and manage digital certificates associated with user profiles. See the API topic in the information center (see "Prerequisite and Related Information" on page xvi) 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 part of the chapter describes the commands and displays you use to create, change, and delete user profiles. All the fields, options, and function keys are not described. Use online information for details.

You must have \*SECADM special authority to create, change, or delete user profiles.

## **Creating User Profiles**

You can create user profiles in several ways:

- 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.
- Using the iSeries Navigator display from the iSeries Access folder.

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: 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.

### Using the Work with User Profiles Command

You can enter a specific profile name, a generic profile set, or \*ALL on the 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
User password . . . . . . . .
                                NEWUSER1
Set password to expired . . . .
                                 *YES
*ENABLED
User class . . . . . . . . . .
                                 *USER
Assistance level . . . . . . .
                                 *SYSVAL
Current library . . . . . . .
                                 *CRTDFT
Initial program to call . . . .
                                 *NONE
Library . . . . . . . . . . . .
                                MATN
Initial menu . . . . . . . . .
                                 QSYS
Library . . . . . . . . . . . .
Limit capabilities . . . . . .
                                 *N0
Text 'description' . . . . . .
```

The Create User Profile display shows all 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 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**

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 . . . . . . . . . . . . .
                          NEWLISER
User description . . . .
Password . . . . . . .
                          NEWUSER
Type of user ....
                          *USER
User group .....
                          *NONF
Restrict command line use
Default library . . . .
Default printer . . . . .
                          *WRKSTN
                          *NONE
Sign on program . . . . .
Library . . . . . . . .
First menu . . . . . .
Library . . . . . . .
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.

The main menu also includes user Options 51—59. These additional options (Options 51--59) are processed similar to Option 50, except the default values for the following fields are blank:

- Text for menu options
- User program
- Library

## **Copying User Profiles**

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

## Copying 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 . . . . . . . . .
                                             Name
User password . . . . . . . > *USRPRF
                                             Name
                                             *NO, *YES
Set password to expired . . . > *NO
Status . . . . . . . . . . > *ENABLED
                                             *ENABLED,
User class . . . . . . . . . > *USER
                                             *USER,
Assistance level . . . . . . > *SYSVAL
                                             *SYSVAL,
Current library . . . . . . > DPTWH
                                             Name,
Initial program to call . . . . > *NONE
                                             Name,
Library . . . . . . . . . . . .
                                             Name,
Initial menu . . . . . . > ICMAIN
                                             Name,
         . . . . . . . . . . > ICPGMLIB
                                             Name,
Limit capabilities . . . . . > *N0
Text 'description' . . . . . > 'Warehouse Department'
```

All the values from the copy-from user profile are shown on the Create User Profile display, except the following fields:

```
Home directory
*USRPRF
```

#### Locale job attributes

Locale job attributes

Locale Locale

### User profile

Blank. Must be filled in.

#### **Password**

\*USRPRF

#### Message queue

\*USRPRF

#### **Document password**

\*NONE

#### **User Identification Number**

\*GEN

#### **Group Identification Number**

\*NONE

#### **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 will not be copied.

## **Copying 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 . . . . . . . . . . . . .
                          Warehouse Department
User description . . . .
Password . . . . . .
Type of user .....
                          USER
User group . . . . . .
Restrict command line use
                          DPTWH
Default library . . . . .
Default printer . . . . .
                          PRT04
Sign on program . . . .
                          *NONE
 Library . . . . . . .
```

All 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 can be useful in some situations, but 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.

The topic "Copying Authority from a User" on page 145 has more information about using this 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. You must delete any objects owned by the profile or transfer ownership of those objects to another profile. Both basic assistance level and intermediate assistance level allow you to handle owned objects when you delete a 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

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 . . . . .
                                              *NODLT, *DLT, *CHGOWN
 User profile name if *CHGOWN
                                WILLISR
Primary group option:
                                 *NOCHG
                                              *NOCHG, *PGP
 Primary group value . . . .
 New primary group . . . . .
 New primary group authority .
```

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
                                                       ASP
Opt Object
                  Library
                               Type
                                         Attribute
                                                       Device
4
    HOGANR
                  QUSRSYS
                               *MSGQ
                                                       *SYSBAS
9
                               *PGM
    QUERY1
                  DPTWH
                                                       *SYSBAS
    OUERY2
                  DPTWH
                               *PGM
                                                       *SYSBAS
```

## Using the Remove User Option

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
                               HOGANR
User description . . . . :
                               Hogan, Richard - Warehouse DPT
                                                Name, F4 for list
New owner . . . . . . . . . . . .
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
    HOGANR
                   QUSRSYS
                                 HOGANR message queue
2
    QUERY1
                   DPTWH
                                 Inventory Query, on-hand report
    OUERY2
                   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 it's primary group to \*NONE.

```
Work with Objects by Primary Group
Primary group . . . . . :
Type options, press Enter.
                   4=Delete 5=Display authority
 2=Edit authority
 8=Display description 9=Change primary group
                           Type Attribute
                                             Device
0pt
      Ob.iect
                Library
      CUSTMAST CUSTLIB
                           *FILE
                                             *SYSBAS
      CUSTWRK
                           *FILE
                CUSTLIB
                                             *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 sign-on attempts, you may want someone like a system operator to enable the profile by changing the status to \*ENABLED. However, to enable a user profile, you must have \*SECADM special authority and \*OBJMGT 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 and \*OBJMGT 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**

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.

		Displa	y Authoriz	ed Users
		Password		
Group	User	Last	No	
Profile	Profile	Changed	Password	Text
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
QSEC0FR	•			,
,	JONESS	09/20/0x		Jones, Sharon
	HARRISON	08/29/0x		Harrison, Ken
*NO GROUP				
	DPTSM	09/05/0x	Χ	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	lUsers	
		Password	Password	Password	Password
User	Group	Last	for level	for level	for
Profile	Profile	Changed	0 or 1	2 or 3	NetServer
ANGELA		04/21/0x	*YES	*N0	*YES
ARTHUR		07/07/0x	*YES	*YES	*YES
CAROL1		05/15/0x	*YES	*YES	*YES
CAROL2		05/15/0x	*N0	*N0	*N0
CHUCKE		05/18/0x	*YES	*N0	*YES
DENNISS		04/20/0x	*YES	*N0	*YES
DPORTER		03/30/0x	*YES	*N0	*YES
GARRY		08/04/0x	*YES	*YES	*YES
JANNY		03/16/0x	*YES	*N0	*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. Consult online information for details about the available types.
- · 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. The topic "Analyzing User Profiles" on page 268 gives suggestions for reports.

#### Types of User Profile Reports

The following commands provide user profile reports.

- Print User Profile (PRTUSRPRF)
  - This command allows you to print a report containing information for the user profiles on the system. Four different reports 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 allows you to print a report of all the user profiles on the system that have a default password and 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 may 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 iSeries user profile to rename a user does not rename any application profiles the user may 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. 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

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
                                   JONESS
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 you specify on this command replace the current AUDLVL values for the users. The values you specify are not added to the current AUDLVL values for the users.

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 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 chapter 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 45 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**

Exit points are provided to create, change, delete, or restore user profiles. 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.

For more information about the Security exit programs, see the API topic in the Information Center (see "Prerequisite and Related Information" on page xvi for details).

## **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.

IBM-supplied user profiles, except QSECOFR, are shipped with a password of \*NONE and are not intended for sign on. With the exception of QSECOFR, do not sign on with the 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 281 contains a complete list of all the IBM-supplied user profiles and the field values for each profile.

Note: IBM-supplied profiles are provided, but they are used by the IBM i5/OS. Therefore, signing on with these profiles or using the profiles to own user (non-IBM supplied ) objects is not recommended.

## 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 system operator (QSYSOPR) password . . . . . .
New user (QUSER) 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 . . . . . . .
```

### 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.

For information about how to work with Service tools, see the information center topic, Service tools (Security—>Service tools). See "Prerequisite and Related Information" on page xvi for more information about accessing the information center.

## **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**

Resource security defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects.

This chapter 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.

Chapter 7 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 148 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.

## **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** 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**

**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 111 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 provides information about the authority that is required to perform a specific function.

Table 111. Description of Authority Types

Authority	Name	Functions Allowed
Object Authorities:		
*OBJOPR	Object Operational	Look at the description of an object. Use the object as determined by the user's data authorities.
*OBJMGT	Object Management	Specify the security for the object. Move or rename the object. All functions defined for *OBJALTER and *OBJREF.
*OBJEXIST	Object Existence	Delete the object. Free storage of the object. Perform save and restore operations for the object <sup>1</sup> . 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 <sup>2</sup> .
Data Authorities:	_	
*READ	Read	Display the contents of the object, such as viewing records in a file.
*ADD	Add	Add entries to an object, such as adding messages to a message queue or adding records to a file.
*UPD	Update	Change the entries in an object, such as changing records in a file.
*DLT	Delete	Remove entries from an object, such as removing messages from a message queue or deleting records from a file.

Table 111. Description of Authority Types (continued)

Authority	Name	Functions Allowed
*EXECUTE	Execute	Run a program, service program, or SQL package. Locate an object in a library or a directory.
Field Authorities:		
*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.

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

## **Commonly Used 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 112 shows the system-defined authorities available using the object authority commands and displays.

Table 112. System-Defined Authority

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

Table 113 shows additional system-defined authorities that are available using the WRKAUT and CHGAUT commands:

Table 113. System-Defined Authority

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

See the topic "Authorization List Management" on page 118 for more information.

Table 113. System-Defined Authority (continued)

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

The LAN Server licensed program uses access control lists to manage authority. A user's authorities are called **permissions**. Table 114 shows how the LAN Server permissions map to object and data authorities:

Table 114. LAN Server Permissions

uthority	LAN Server Permissions	
XCLUDE	None	
eject Authorities		
BJOPR	See note 1	
BJMGT	Permission	
JEXIST	Create, Delete	
JALTER	Attribute	
REF	No equivalent	
Authorities		
D	Read	
D	Create	
)	Write	
	Delete	
ECUTE	Execute	

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**

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 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

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.

### **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 is requested to an object 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. See "Library Lists" on page 183 for more information.

## **Field Authorities**

Field authorities are supported for database files. Authorities supported are Reference 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
                 RLN
                           Primary group . . . :
                                                 DPTAR
 Library. . . . :
Object type. . . : *FILE
                           ASP Device . . . :
                                                 *SYSBAS
Object secured by authorization list .... *NONE
                    Object
                            -----Data-----
User
          Group
                    Authority Read Add Update Delete Execute
*PUBLIC
                    *CHANGE
                              X \qquad X \qquad X \qquad X
                                                    Χ
                    *ALL
                              X X X
PGMR1
                                                      Χ
                            X
X
USER1
                    *USE
                                                      Χ
USER2
                    USER DEF
                                       Χ
                                                      Χ
USER3
                    USER DEF
                                                      Χ
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 . . . . . :
                                                            PGMR1
 Library . . . . :
                        RIN
                                     Primary group . . . :
                                                            *NONE
                      *FILE
Object type . . . :
                       Object
                                ----Field Authorities-----
Field
                     Authority Mgt Alter Ref Read Add Update
           User
                                X X X X
Field3
           PGMR1
                     *ALL
           USER1
                     *Use
                                               Χ
                     USER DEF
                                                           Χ
           USER2
                                               Χ
           USER3
                     USER DEF
                                         Χ
                                               Χ
           *PUBLIC
                     *CHANGE
                                               Χ
                                                           χ
Field4
           PGMR1
                                       Χ
                                               Χ
                     *ALL
                                                           Χ
           USFR1
                      *Use
                                               Χ
           USER2
                     USER DEF
                                               Χ
           USER3
                     USER DEF
                                               Χ
           *PUBLIC
                      *CHANGE
                                                     Χ
                                                           Χ
                                                        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.

Support for 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

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.

See the System/38 Environment Programming manual for more information about the System/38 Environment.

### Recommendation for 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
- 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**

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 authority 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 on 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 "Planning Authorization Lists" on page 213 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 might choose to use an authorization list 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

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, 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 124 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 (MOVOBJ), 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

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

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 desired 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 in 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 using the CRTDIR command in the "root" (/) file system and specify \*PUBLIC authority.

#### Starting conditions: Authorities on parent directory:

```
Display Authority
Object . . . . . . . . . . . . :
                                 /sanders/mytest
SANDERS
                                SANDERSGP3
Primary group . . . . . . . :
Authorization list . . . . . . :
                                 *NONE
           Data
                    ----Object Authorities----
          Authority Exist Mgt Alter
User
                                         Ref
*PUBLIC
          *RWX
                            Χ
                                  Χ
                                          Χ
                    Χ
SANDERS
           *RW
SANDERSGP3
          *RX
QPGMR
          *RWX
          *RWX
                     Χ
                            Χ
                                  Χ
                                          Χ
QTCM
```

User SANDERS issues the following command:

CRTDIR DIR('/sanders/mytest/deletemepub') DTAAUT(\*R) OBJAUT(\*NONE)

#### **Results: Authorities on created directory:**

```
Display Authority
                                     /sanders/mytest/deletemepub
                                     SANDERS
                                     SANDERSGP3
Primary group
Authorization list . . . . . . :
                                     *NONF
                     ----Object Authorities----
User
            Authority Exist Mgt
                                      Alter
*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 with the CRTDIR command in the "root" (/) file system.

#### **Starting conditions: Authorities on parent directory:**

```
Display Authority
                                     /sanders/mytest
Object . . . . . . . . . . . :
                                     SANDERS
Primary group . . . . . . . :
                                     SANDERSGP3
Authorization list . . . . . . :
                                     *NONE
                       ----Object Authorities----
             Data
User
            Authority Exist
                               Mgt
                                      Alter
                                               Ref
*PUBLIC
            *RWX
                                Χ
                                       Χ
                                                Χ
                       Χ
SANDERS
            *RW
SANDERSGP3
            *RX
QPGMR
            *RWX
            *RWX
                        Χ
                                Χ
                                       Χ
                                                Χ
QTCM
```

User SANDERSUSR issues the following command: CRTDIR DIR('/sanders/mytest/deletemepub')

#### Results: Authorities on created directory:

```
Display Authority
                                       /sanders/mytest/deletemepub
                                       SANDERSUSR
                                       SANDERSGP3
Primary group
Authorization list . . . . . . :
                                       *NONE
                        ----Object Authorities----
              Data
User
             Authority Exist
                                 Mgt
                                        Alter
*PUBLIC
             *RWX
                                  Χ
                                         χ
                        Χ
                                                  Χ
SANDERSUSR
             *RWX
SANDERSGP3
             *RX
             *RWX
QPGMR
QTCM
             *RWX
                         Χ
                                  Χ
                                         Χ
                                                  Χ
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**

Each object is assigned 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 124 shows examples of how the system assigns ownership to new objects.

The owner of an object always has all the authority for the object unless any or all authority is removed specifically. As an object owner, you might choose to remove some specific authority as a precautionary measure. 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 "Tools and Tips for Your iSeries" to see whether the rules for object authorities applies 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. A user with \*ALLOBJ authority can transfer ownership, as can any user who has the following authorities:

- Object existence authority for the object (except for an authorization list)
- · Ownership of the object, 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 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 iSeries system. 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 76 for more information.

# **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.

The group authority type (GRPAUTTYP) 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 124 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.

# **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 (GRPAUTTYP) 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 124 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.

### **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 14 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

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 through Figure 9 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
GRPAUTTYP:
       *PRIVATE
Command Used to Create Object:
CRTDTAARA DTAARA(CUSTLIB/DTA1)
       TYPE(*CHAR) AUT(*LIBCRTAUT)
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:
GRPAUTTYP:
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**

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 Information Center concerning security considerations and adopted authority when using SQL packages (see "Prerequisite and Related Information" on page xvi for details).

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 program stack. For example, assume that PGMA uses adopted authority:
  - If PGMA starts PGMB using the CALL command, these are the program stacks before and after the CALL command:

Program Stack before CALL Command:	Program Stack after CALL Command:
QCMD	QCMD
PGMA	PGMA
	PGMB

Figure 10. Adopted Authority and the CALL Command

Because PGMA remains in the program 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 131 for more information about the USEADPAUT parameter.)

 If PGMA starts PGMB using the Transfer Control (TFRCTL) command, the program stacks look like this:

Program Stack before TFRCTL Command:	rogram Stack after TFRCTL Command:	
QCMD	QCMD	
PGMA	PGMB	

Figure 11. Adopted Authority and the TFRCTL Command

PGMB does not use the adopted authority of PGMA, because PGMA is no longer in the program 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 program 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 changed since the last time the command was run.

"Flowchart 8: How Adopted Authority Is Checked" on page 160 provides more information about adopted authority. The topic "Using Adopted Authority in Menu Design" on page 204 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**

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 might not want some programs to use the adopted authority of previous programs in the program 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 206 shows an example of how to use this parameter in menu design. See "Use Adopted Authority (QUSEADPAUT)" on page 30 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.

## **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. Its primary use 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**

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 part of the chapter describes commonly-used methods for setting up, maintaining, and displaying authority information about your system. Appendix A, "Security Commands," on page 273 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**

Four displays show object authorities:
Display Object Authority display
Edit Object Authority display
Display Authority display
Work with Authority display

This section describes some characteristics of these displays. Figure 12 on page 134 shows the basic version of the Display Object Authority display:

```
Display Object Authority
Object . . . . :
                     CUSTN0
                               Owner . . . . . :
                                                       PGMR1
                               Primary group . . . :
                                                       DPTAR
                     CUSTLIB
 Library. . . . :
Object type . . .:
                     *DTAARA
                               ASP device
                                                       *SYSBAS
Object secured by authorization list . . . . . . :
                                                       *NONE
                       Object
User
                       Authority
           Group
*PUBLIC
                       *EXCLUDE
PGMR1
                       *ALL
DPTAR
                       *CHANGE
DPTSM
                       *USE
F3=Exit F11=Display detail object authorities F12=Cancel F17=Top
```

Figure 12. 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
                    CUSTNO
                                                       PGMR1
                                   Owner . . . . :
                     CUSTLIB
                                 Primary group . . . :
                                                       DPTAR
 Library. . . . :
Object type. . . :
                    *DTAARA
                                   ASP device . . . :
                                                       *SYSBAS
Object secured by authorization list ....:
                                                       *NONE
                               -----Object-----
                     Object
User
          Group
                     Authority Opr Mgt Exist Alter Ref
*PUBLIC
                      *EXCLUDE
                                Χ
PGMR1
                      *ALL
                                Χ
                                     Χ
                                          Χ
                                                 Χ
                                                      Χ
DPTAR
                      *CHANGE
                                Χ
DPTSM
                      *USE
F3=Exit F11=Display data authorities F12=Cancel F17=Top F18=Bottom
```

The other shows data authorities:

```
Display Object Authority
Object . . . . :
                    CUSTNO
                              Owner . . . . . . :
                                                    PGMR1
                              Primary group . . . :
                    CUSTLIB
                                                    DPTAR
 Library. . . . :
                    *DTAARA
                              ASP device ...:
                                                    *SYSBAS
Object type. . . :
Object secured by authorization list. . . . . . . . :
                     Object
                              -----Data-----
          Group
                     Authority Read Add Update Delete Execute
User
*PUBLIC
                     *EXCLUDE
PGMR1
                     *ALL
DPTAR
                     *CHANGE
                               Χ
                                                 Χ
                                                        Χ
DPTSM
                     *USE
                               Χ
                                                        Χ
```

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
                      *DTAARA
                                 ASP device
                                                          *SYSBAS
Object type. . . :
                                             . . . . :
Object secured by authorization list. . . . . . . . :
                                                          *NONE
                       Ob.ject
User
           Group
                       Authority
*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
                                  Primary group . . . :
 Library
                      CUSTLIB
                                                         DPTAR
Object type. . . :
                                 ASP device
                                                         *SYSBAS
                     *DTAARA
Object secured by authorization list . . . . . . . :
                                                         *NONE
                      Object
User
           Group
                      Authority
*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
                     CUSTNO
                                                          PGMR1
Object . . . . :
                                  Owner . . . . . :
 Library. . . . :
                     CUSTLIB
                                  Primary group . . . :
                                                         DPTAR
Object type. . . :
                     *DTAARA
                                  ASP device
                                                         *SYSBAS
Object secured by authorization list . . . . . . . . :
                                                         *NONE
                      Object
                                 -----0b.ject-----
User
          Group
                     Authority
                                Opr Mgt Exist Alter Ref
*ADOPTED
                     USER DEF
                                     Χ
                                           Χ
                                                  Χ
                                                       Χ
*PUBLIC
                     *EXCLUDEPGMR1
                     *ALL
                                Χ
                                      Χ
                                           Χ
                                                  Χ
                                                        Χ
*GROUP
          DPTAR
                     *CHANGE
                                 χ
DPTSM
                     *USE
                                 Χ
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
                                Primary group . . . :
                                                        DPTAR
 Library. . . . :
                     CUSTLIB
Object type. . . :
                     *DTAARA
                                ASP device . . . . ::
                                                        *SYSBAS
Object secured by authorization list . . . . . . . :
                                                        *NONE
                          ----Object----
                                             -----Data-----
                OBJECT
User
       Group
                Authority
                           0 M E
                                      Α
                                          R
                                                  A U
*ADOPTED
                USER DEF
                               Χ
                                  Χ
                                      Χ
*PUBLIC
                *EXCLUDE
PGMR1
                *ALL
                                      Χ
                                          Χ
                                              Χ
                                                          Χ
                                                             Χ
                                              χ
                                                  Χ
                                                      Χ
                                                             Χ
*GROUP DPTAR
                *CHANGE
                           Χ
                                                         Χ
                           Χ
                                              Χ
                                                             Χ
DPTSM
                *USE
```

# **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)

For more information about security tools, see the Tips and Tools for Securing Your iSeries.

# Working with 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
                     TESTLIB
                                  Owner . . . . . :
                                                         PGMR1
Object . . . . :
                                                         *NONE
 Library. . . . :
                     QSYS
                                  Primary group . . . :
                                  ASP device . . . :
Object type. . . :
                     *LIB
                                                         *SYSBAS
Object secured by authorization list. . . . . . . . :
                       Object
                       Authority
llser
          Group
*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
                                          CUSTLIB
ASP number . . . . . . . . . . .
ASP device . . . . . . . . . . . . . . . . . . :
                                          *SYSBAS
Create authority . . . . . . . . . . . :
                                          *0B.11 ST
Create object auditing . . . . . . . . . :
                                          *SYSVAL
                                          Customer Rec
Text description . . . . . . . . . . . . . . . . .
```

## **Creating Objects**

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
                     DTA1
                                                         PGMR1
Object . . . . . :
                                 Owner . . . . . :
                                 Primary group . . . :
 Library. . . . :
                     TESTLIB
                                                         *NONE
                                 ASP device . . . . :
Object type. . . :
                     *DTAARA
                                                         *SYSBAS
Object secured by authorization list. . . . . . . . :
                                                         OBJLST
                      Object
User
           Group
                      Authority
*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
                     *DTAARA
                               ASP device . . . . :
Object type. . . :
                                                       *SYSBAS
Object secured by authorization list . . . . . . . :
                      Object
User
           Group
                      Authority
*PUBLIC
                      *CHANGE
PGMR1
                      *ALL
```

# **Working with Individual Object Authority**

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 . . . :
                                                     *NONF
                              ASP device . . . . :
                                                     *SYSBAS
Object type...: *DTAARA
Type changes to current authorities, press Enter.
 Object secured by authorization list . . . . . . :
                                                     OBJLST
                      0b.iect
User
          Group
                      Authority
*PUBLIC
                      *AUTL
PGMR1
                      *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**

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
                     Object 0
                                   -----Object-----
                     Authority Opr Mgt Exist Alter Ref
User
          Group
*PUBLIC
                     *AUTL
PGMR1
                     USER DEF
                               χ
                                   Χ
                                               Χ
                                                    χ
```

You can press F11 (Display data authorities) to view or change the data authorities:

```
Edit Object Authority
Object . . . . . :
                     CONTRACTS Owner . . . . . :
                                                     PGMR1
                    TESTLIB
 Library . . . . :
                               Primary group . . . :
                                                     *NONE
Object type. . . :
                     *FIL
                               ASP device . . . . :
                                                     *SYSBAS
Type changes to current authorities, press Enter.
Object secured by authorization list. . . . . . . . LIST2
                              -----Data-----
                     Ob.ject
User
                     Authority Read Add Update Delete Execute
          Group
*PUBLIC
                     *AUTL
PGMR1
                     USER DEF
                               Χ
                                    Χ
                                          Χ
                                                 Χ
                                                         Χ
```

### **Giving 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.
           0bject
User
           Authority
USER1
           *USE
USER2
           *CHANGE
PGMR2
           *ALL
```

#### Removing a User's Authority

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 overriden 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. . . . . . :
                                                   *NONF
                              -----0b.ject-----
                    Object 0
User
              Authority Opr Mgt Exist Alter Ref
               USER DEF
USERB
                              Χ
                                 Χ
                                                 Χ
```

```
Display Object Authority
                            Owner . . . . . :
                                                  PGMR1
Object . . . . : FILEB
 Library. . . . : LIBB
                            Primary group . . . : *NONE
                            ASP device . . . :
Object type . . . : *FILE
Object secured by authorization list . . . . . . . . . . . .
                             -----Data-----
                    Object
User
                    Authority Read Add Update Delete Execute
          Group
USERB
                    USER DEF
```

# Working with Authority for Multiple Objects

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 . . . . . . . . . . . . . . . .
TESTLIB
*ALL
ASP device . . . . . . . . . . . .
                        *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.
Library . . . . . . . . . . . .
                          TESTLIB
Object type . . . . . . . . .
                          *FILE
ASP device . . . . . . . . . *
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 . . . . . . . . . . . . . . . .
 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.
TESTLIB
 Library . . . . . . . . . . .
Object type .......
ASP device . . . . . . . . . *
                           *PUBLIC
           + for more values
Authority . . . . . . . . . . .
                            *AUTL
```

## **Working with Object Ownership**

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 . . . . . :
                             OI DOWNER
Type options, press Enter.
 2=Edit authority 4=Delete 5=Display author
 8=Display description 9=Change owner
                                                          ASP
Opt Object
                               Type
                                         Attribute
                                                          Device
                 Library
    COPGMMSG
                 COPGMLIB
                               *MSGQ
                                                          *SYSBAS
    CUSTMAS
                 CUSTLIB
                               *FILE
                                                          *SYSBAS
    CUSTMSGQ
                 CUSTLIB
                               *MSGQ
                                                          *SYSBAS
    ITEMMSGQ
                 ITEMLIB
                               *MSGQ
                                                          *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 101 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 entire path name, place your cursor anywhere on the path name and press the F22 key.

# Working with Primary Group Authority

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 "Planning Authorization Lists" on page 213 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 106 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.

# **Working with Authorization Lists**

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.

#### **Creating 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 . . . . . .
                                cust1st1
Text 'description' . . . . . . Files cleared at month-end
                         Additional Parameters
Authority . . . . . . . . *use
```

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

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 118 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
                      CUSTLST1
                                     Owner . . . . . :
 Library . . . . :
                        QSYS
                                    Primary group . . . :
                                                            *NONE
Type changes to current authorities, press Enter.
          Object List
User
          Authority Mgt
*PUBLIC
          *USE
PGMR1
          *AII
                     Χ
```

To give new users authority to the authorization list, press F6 (Add new users):

```
Add New Users
                                  Owner . . . PGMR1
                      CUSTLST1
Object . . . . . :
 Library . . . . :
                      QSYS
Type new users, press Enter.
          Object List
User
          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, the CHGAUT command, or the GRTOBJAUT command to secure an object with an authorization list:

```
Edit Object Authority
                     ARWRK1
Object . . . . :
                                                          PGMR1
                                  Owner . . . . . :
 Library . . . :
                     TESTLIB
                                  Primary group. . . :
                                                          *NONE
                                  ASP device . . . . :
Object type . . . : *FILE
                                                          *SYSBAS
Type changes to current authorities, press Enter.
 Object secured by authorization list . . . . . . . . . . . .
                                                           ARLST1
           0b.ject
           Authority
User
*PUBLIC
           *AUTL
PGMR1
           *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 library-based objects secured by the list:

```
Display Authorization List Objects
Authorization list . . . . . . :
                                 CUSTLST1
 Library . . . . . . . . . . . :
                                 CUSTL TB
                                 OWNAR
Primary group . . . . . . . :
                                 DPTAR
                                       Primary
                    Type
                             0wner
                                                 Text
Object
          Library
                                       group
CUSTMAS
          CUSTLIB
                    *FILE
                             OWNAR
CUSTADDR
          CUSTLIB
                    *FILE
                             OWNAR
```

This is an information list only. You cannot add or remove objects from the list. You can also use the Display Authorization List Objects (DSPAUTLOBJ) command to view or print a list of all library based objects secured by the list.

#### **Deleting an Authorization List**

You cannot delete an authorization list if it is used to secure any objects. Use the DSPAUTLOBJ command to list all the library based 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 128 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**

Following are charts, 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 Flowchart 3 on page 152

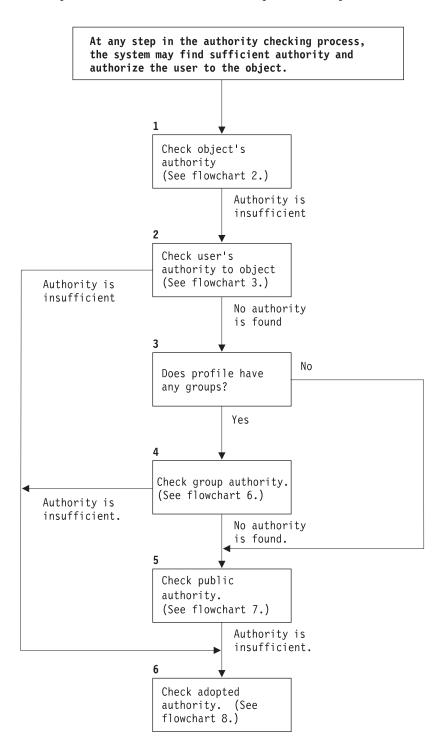
Step 6 in Flowchart 6 on page 158

Step 2 in Flowchart 8B on page 163

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.



- If the user is not authorized, one or more of the following happens:
- 1) A message is sent to the user or program; 2) The program fails;
- 3) An AF entry is written to the audit journal.

RBAFW508-0

Figure 13. Flowchart 1: Main Authority Checking Process

#### **Description of Flowchart 1: Main Authority Checking Process**

**Note:** At any step in the authority checking process, the system might find sufficient authority and authorize the user to the 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 the group does not have authority to the object, it proceeds to Step 5. If the system determines that the group does not have sufficient authority to the object, 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.)

If the user is not authorized, one or more of the following situations take place:

- · A message is sent to the user or program
- The program fails
- · An AF entry is written to the audit journal

### 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.

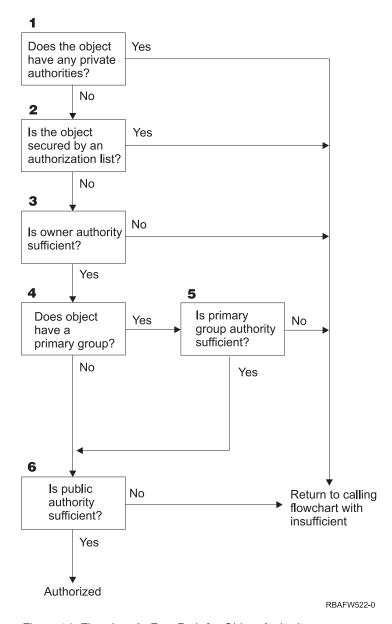


Figure 14. Flowchart 2: Fast Path for Object Authority

#### 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.

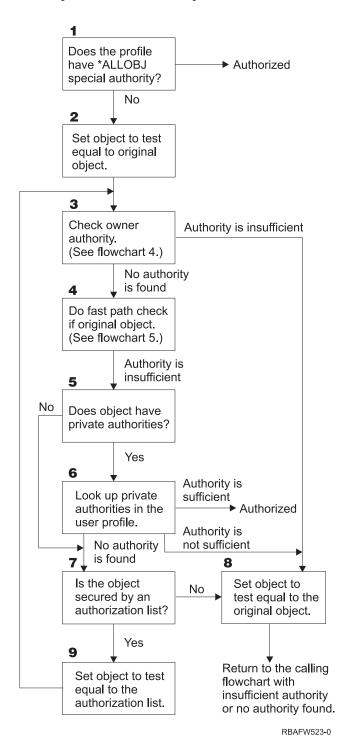


Figure 15. Flowchart 3: Check User Authority

#### **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 the equal the original object. The authority checking proceeds to Step 3.
- 3. The system check the owner authority. If the authority is unsufficient, 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 check 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

Figure 16 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.

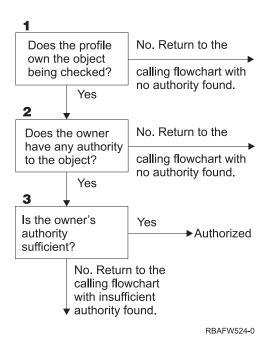


Figure 16. Flowchart 4: Owner Authority Checking

#### **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 he or she is the owner, 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

Figure 17 on page 155 shows the fast path for testing user authority without searching private authorities.

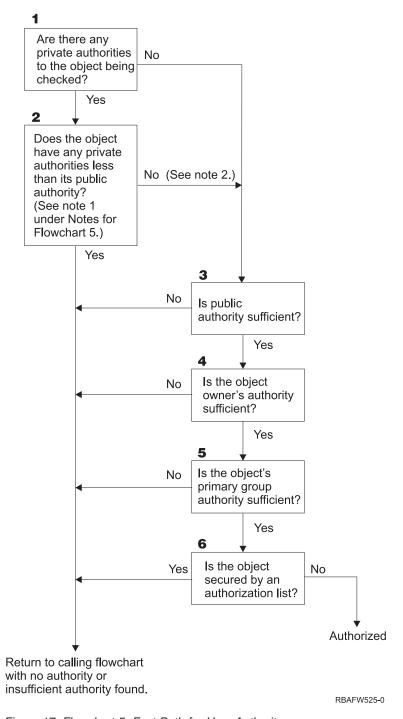


Figure 17. Flowchart 5: Fast Path for User Authority

#### 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 115, 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 115. Public versus Private Authority

Authority	Users			
	OWNAR	DPTMG	WILSONJ	*PUBLIC
Object Authorities:				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
Data Authorities				
*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 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 116 shows the authorities for the CRLIM file:

Table 116. Accumulated Group Authority

Authority	Users			
	OWNAR	DPT506	DPT702	*PUBLIC
Object Authorities:				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Data Authorities				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	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 158 shows the steps in checking group authority.

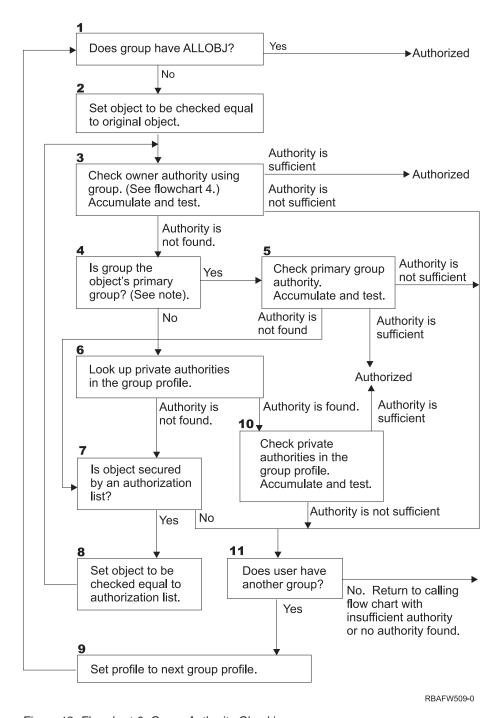


Figure 18. Flowchart 6: Group Authority Checking

**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. If the group does not have ALLOBJ authority, 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 7. If the authority is not found, then the authority check proceeds to Step 4.
- 4. If the owner authority is not found, then 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. If the group is the object's primary group, then 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 insufficient or is not found, then the authority check goes to Step 7.
- 6. If the group is not the object's primary group, then 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. If no authority is found for the private authorities for the group profile, then 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. If the object is secured by an authorization list, then the system set the object to be checked equal to the authorization list and authority check returns to Step 3.
- 9. If the user does belong to another group profile, then the system sets this profile to the next group profile and returns to Step 1 to start the authority checking process over again.
- 10. If authority is found for private authorities within the group profile, then 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 7.
- 11. If an object is not secured by an authorization list, then 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:

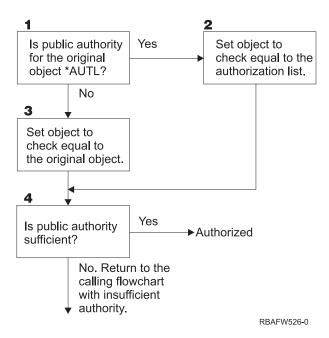


Figure 19. Flowchart 7: Check Public Authority

#### **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 program 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 20 on page 161 and Figure 21 on page 163 show the process for checking adopted authority.

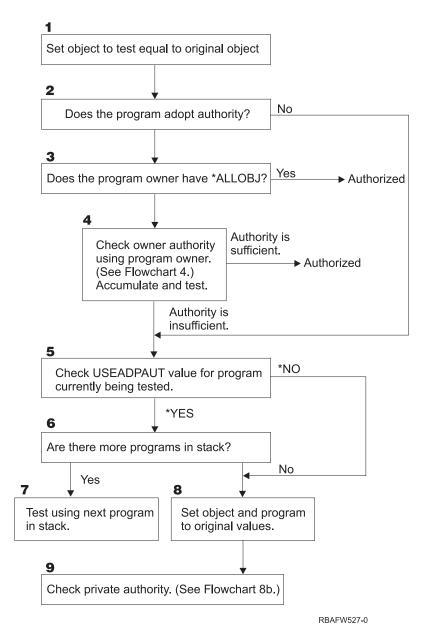


Figure 20. Flowchart 8A: Checking Adopted Authority User \*ALLOBJ and Owner

#### 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. If there are more programs in the stack, the system test the next program in the stack.
- 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 check private authority. This is described in Flowchart 8B: Checking Adopted Authority Using Private Authorities.

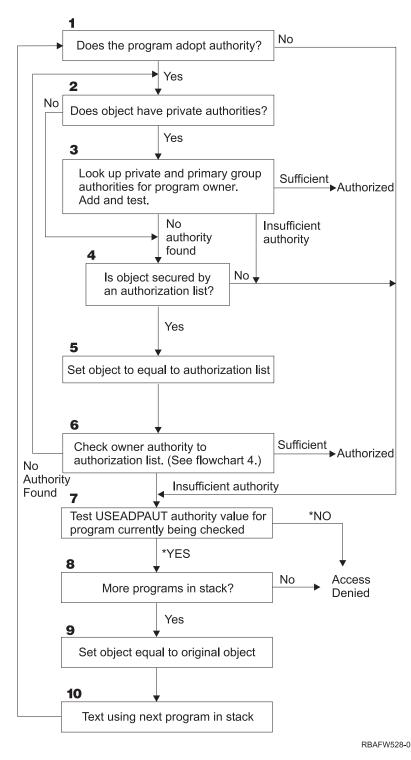


Figure 21. Flowchart 8B: Checking Adopted Authority Using Private Authorities

#### 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. Text using next program in stack and start back at Step 1.

# **Authority Checking Examples**

Following are 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 22 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.

```
Display Object Authority
Object . . . . . :
                       PRICES
                                     Owner . . . . . :
                                                             OWNCP
 Library . . . . :
                                     Primary group . . . :
                       CONTRACTS
                                                             *NONE
Object type
                       *FILE
                                     ASP device . . . . :
                                                             *SYSBAS
Object secured by authorization list ....:
                                                             *NONF
                      Ob.ject
User
           Group
                      Authority
OWNCP
                      *ALL
DPTSM
                      *CHANGE
                      *CHANGE
DPTMG
WILSONJ
                      *USE
*PUBLIC
                      *USE
```

Figure 22. Authority for the PRICES File

## **Case 1: Using 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**

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 23 shows the authorities for the CREDIT file.

```
Display Object Authority
                                                           OWNAR
Object . . . . . :
                                    Owner . . . . . :
 Library . . . . : ACCTSRCV
                                    Primary group . . . :
                                                          DPTAR
Object type
            . . . : *FILE
                                    ASP device . . . . :
                                                           *SYSBAS
Object secured by authorization list .....:
                                                           *NONE
                     Object
User
          Group
                     Authority
OWNAR
                     *ALL
DPTAR
                     *CHANGE
*PUBLIC
                     *USE
```

Figure 23. 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.

### **Case 3: 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:

- 1. Flowchart 1. step 1.
  - a. Flowchart 2, step 1. The CREDIT file has no private authorities. DPTAR's authority is primary group authority, not private authority.
  - b. Flowchart 2, steps 2 and 3. Owner's authority (OWNAR) is sufficient.
  - c. Flowchart 2, steps 4 and 5. Primary group authority (DPTAR) is sufficient.
  - d. 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

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**

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 164.

• 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**

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: This example demonstrates that a user can be denied access to an object even though the user's group has sufficient authority.

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

The authority information for the ITEM file looks like this:

```
Display Object Authority
Object . . . . . :
                       ITEM
                                      Owner . . . . . :
                                                             OWNIC
                                      Primary group . . . :
                                                             *NONE
 Library . . . . :
                       ITEMLIB
Object type ...:
                       *FILE
                                      ASP device
                                                             *SYSBAS
Object secured by authorization list . . . . . . . .
                                                             *NONE
                      Object
                      Authority
User
           Group
OWNIC
                      *ALL
*PUBLIC
                      *USE
```

Figure 24. 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:

- 1. Flowchart 1, step 1.
  - a. Flowchart 2, steps 1, 2, and 3. OWNIC's authority is sufficient.
  - b. Flowchart 2, step 4. The ITEM file does not have a primary group.
  - c. 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

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

The ARWKR01 file in library CUSTLIB is secured by the ARLST1 authorization list. Figure 25 and Figure 26 show the authorities:

```
Display Object Authority
Object . . . . . : ARWRK01
                                  Owner . . . . . : OWNAR
 Library . . . . : CUSTLIB
                                  Primary group . . . :
                                                        *NONE
                                  ASP device . . . . :
Object type . . . : *FILE
                                                         *SYSBAS
Object secured by authorization list. . . . . . . . . . . . .
                                                        ARLST1
                     0b.ject
User
          Group
                     Authority
OWNCP
                     *ALL
*PUBLIC
                     *USE
```

Figure 25. Authority for the ARWRK01 File

```
Display Authorization List
Object . . . . . :
                                  Owner . . . . . :
                       ARLST1
                                                          OWNAR
                       QSYS
                                  Primary group . . . : *NONE
 Library . . . . :
                      Object 0
                                List
User
           Group
                      Authority Mgt
OWNCP
                      *ALL
                      *CHANGE
AMESJ
*PUBLIC
                      *USE
```

Figure 26. 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 172.

### Case 10: 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 27 shows the authorities for the CRLIM file:

```
Display Object Authority
Object . . . . . :
                      CRLIM
                                     Owner . . . . . :
                      CUSTLIB
                                     Primary group . . . :
                                                            DPTAR
 Library . . . . :
Object type
                      *FILE
                                     ASP device . . . . :
                                                            *SYSBAS
Object secured by authorization list ....:
                                                             *NONF
                     Ob.iect
          Group
User
                     Authority
OWNAR
                     *ALL
                     *CHANGE
DPTAR
                     *USE
DPTSM
*PUBLIC
                     *EXCLUDE
```

Figure 27. 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**

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 28 shows the authority for the CRLIMWRK file.

```
Display Object Authority
Object . . . . . :
                       CRLIMWRK
                                       Owner . . . . . :
 Library . . . . :
                       CUSTLIB
                                      Primary group . . . :
                                                               *NONE
                                      ASP device . . . . :
Object type . . . : *FILE
                                                               *SYSBAS
Object secured by authorization list . . . . . . . . . . . . . . . .
                                                               CRLST1
                      0b.ject
User
           Group
                      Authority
OWNAR
                       *ALL
DPTSM
                       *USE
WILSONJ
                       *EXCLUDE
*PUBLIC
                       *USF
```

Figure 28. Authority for CRLIMWRK File

The CRLIMWRK file is secured by the CRLST1 authorization list. Figure 29 shows the authority for the CRLST1 authorization list.

```
Display Authorization List
Object . . . . . :
                       CRLST1
                                    Owner . . . . . :
                                                            OWNAR
 Library . . . . :
                         QSYS
                                    Primary Group . . . : DPTAR
                      Object
                               List
User
           Group
                      Authority Mgt
OWNAR
                      *AII
DPTAR
                      *ALL
*PUBLIC
                      *EXCLUDE
```

Figure 29. 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
- 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
  - I. 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 CRLIST1 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	Туре	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**

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 users'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 chapter discusses security issues associated with work management on the system:

Job initiation

Workstations

Subsystem descriptions

Job descriptions

Library lists

Printing

Network attributes

Performance tuning

For complete information about work management topics, see the Work Management book.

### **Job Initiation**

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 and to other objects 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

Here 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 177 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

Following is 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 SBMJOB command, this checking is performed before the job is added to the job

- 1. If you specify a user profile on the SBMJOB command, you must have \*USE authority to the user profile.
- 2. Authority is checked for objects specified as parameters on the SBMJOB 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 and the SBMJOB command specifies USER(\*JOBD), 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**

When a new job is started, a new program stack is created for the job. Adopted authority cannot take effect until the first program is added to the program 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 SBMJOB request.

You can change characteristics of a batch job when it is waiting to run, using the Change Job (CHGJOB) command. See 369 for the authority that is required to change parameters for a job.

## **Workstations**

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 30 on page 178 shows the logic for determining whether a user is allowed to sign on at a device:

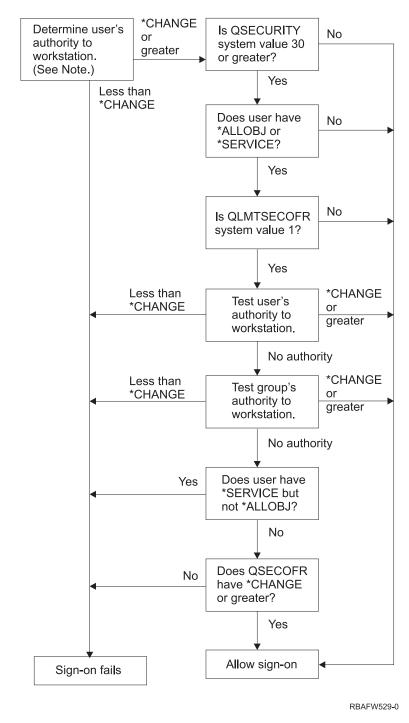


Figure 30. Authority Checking for Workstations

**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 program 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 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 does have \*SERVICE but not \*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**

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. But 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

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

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

To change the format of the Signon display:

- 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.
  - All fields must be input/output fields (type B in DDS source) or hidden fields (type H in DDS
- 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:

- 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**

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.

# Controlling 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 13 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 189 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 181 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 PRJOBD specifies USER(USERB). Public authority for PRJOBD is \*USE.

At security level 30 or lower, USERA can list the payroll file by submitting a batch job: SBMJOB RQSDTA("Call PRLIST") JOBD(PRJOBD) + USER(\*JOBD)

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**

The iSeries 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 394.) 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 117 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 117. 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 ADDLIBLE, RMVLIBLE, CHGLIBL, and EDTLIBL commands.

# **Security Risks of Library Lists**

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 115 provides some general information about the issues associated with library lists. This topic gives more specific examples of the possible exposures and how to avoid them.

Here are two examples of how changes to a library list might break security requirements:

## Change in Function

Figure 31 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.

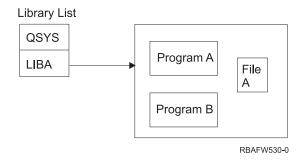


Figure 31. Library List-Expected Environment

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:

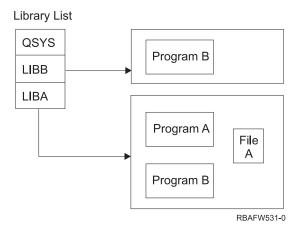


Figure 32. Library List-Actual Environment

#### **Unauthorized Access to Information**

Assume Program A in Figure 31 on page 183 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 simply calls the command processor. The user will have a command line and complete access to File A.

# Recommendations for System Portion of 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 202.

# **Recommendations for 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:

CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)

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**

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 201 to set the current library during application processing.

# Recommendations for 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 203 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 desired 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 desired for the application. When the application ends, return the library list to its original setting. See "Controlling the User Library List" on page 201 for an example of this technique.

## **Printing**

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 Printer Device Programming book provides examples of how to direct output to a particular output queue.

# Securing Spooled Files

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

The DSPDTA parameter is designed to protect the contents of a spooled file. It 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)

#### Possible Values for DSPDTA

<u>*NO</u>	A user cannot display, send, or copy spooled files owned by other users, unless the user has one of the following authorities:
	<ul> <li>*JOBCTL special authority if the OPRCTL parameter is *YES.</li> </ul>
	<ul> <li>*READ, *ADD, and *DLT authority to the output queue if the *AUTCHK parameter is *DTAAUT.</li> </ul>
	<ul> <li>Ownership of the output queue if the *AUTCHK parameter is *OWNER.</li> </ul>
*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

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.

Possible Values f	or AUTCHK
-------------------	-----------

*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 OPRCTL parameter determines whether a user with \*JOBCTL special authority can control the output queue.

#### Possible Values for OPRCTL

*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**

Table 118 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 447.

The authority and output queue parameters for all commands associated with spooled files are listed on "Spooled File Commands" on page 432. Output queue commands are listed on "Output Queue Commands" on page 407.

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 118. Authority Required to Perform Printing Functions

	Output Queue Parameters			Output	
<b>Printing Function</b>	DSPDTA	AUTCHK	OPRCTL	<sup>–</sup> Queue Authority	Special Authority
Add spooled files to queue <sup>1</sup>				*READ	None
			*YES		*JOBCTL

Table 118. Authority Required to Perform Printing Functions (continued)

	Output Queue Parameters			Output	
<b>Printing Function</b>	DSPDTA	AUTCHK	OPRCTL	<sup>—</sup> Queue Authority	Special Authority
View list of spooled files				*READ	None
(WRKOUTQ command <sup>2</sup> )			*YES		*JOBCTL
Display, copy, or send spooled files	*YES			*READ	None
	*NO	*DTAAUT		*READ,	None
(DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP <sup>2</sup> )				*ADD, *DLT	
	*NO	*OWNER		Owner <sup>3</sup>	None
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
Change, delete, hold, and release spooled file (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF <sup>2</sup> )		*DTAAUT		*READ, *ADD, *DLT	None
		*OWNER		Owner <sup>3</sup>	None
			*YES		*JOBCTL
Change, clear, hold, and release output queue (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ $^2$ )		*DTAAUT		*READ, *ADD, *DLT	None
		*OWNER		Owner <sup>3</sup>	None
			*YES		*JOBCTL
Start a writer for the queue		*DTAAUT		*CHANGE	None
(STRPRTWTR, STRRMTWTR <sup>2</sup> )			*YES		*JOBCTL

This is the authority required to direct your output to an output queue.

# **Examples: Output Queue**

Here are several examples of setting 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)
```

<sup>&</sup>lt;sup>2</sup> Use these commands or equivalent options from a display.

You must be the owner of the output queue.

<sup>&</sup>lt;sup>4</sup> Also requires \*USE authority to the printer device description.

<sup>\*</sup>CHGOUTQ requires \*OBJMGT authority to the output queue, in addition to \*READ, \*ADD, and \*DLT authorities.

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.

```
CRTOUTO OUTO(OGPL/CFOUTO) 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.

Possible Values for JOBACN:

*REJECT	The input stream is rejected. A message stating the input stream was rejected is sent to both the sender and the intended receiver.
*FILE	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.

For more information about the JOBACN attribute, see the SNA Distribution Services book.

# Client Request Access (PCSACC) Network Attribute

The PCSACC network attribute determines how the iSeries 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 iSeries system, not 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 iSeries Access clients.

*REJECT	iSeries Access rejects every request from the personal computer to access objects on the iSeries system. An error message is sent to the PC application.
*OBJAUT	The iSeries 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.
qualified- program- name	The iSeries 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 iSeries 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

#### Risks and Recommendations

Normal security measures on your system might not be sufficient protections if the iSeries 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 iSeries 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.

occurs, an error message is sent to the personal computer.

Several methods are available to prevent an iSeries workstation 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 iSeries 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 iSeries Access licensed program. Using an exit program to verify all requests is the only adequate protection measure.

The iSeries 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

For additional information about iSeries Access, see the Information Center (see "Prerequisite and Related Information" on page xvi for details).

# **DDM Request Access (DDMACC) Network Attribute**

The 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.

*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.
qualified- program- name	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.

For more information about the DDMACC network attribute and the security issues associated with DDM, see the Information Center (see "Prerequisite and Related Information" on page xvi for details).

## **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 control the ability to save and restore objects in several ways:

- Restrict physical access to save and restore devices, such as tape units, optical units, and diskette 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**

You can follow these steps to restrict the save and restore commands on your system:

- 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')
  - 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:

## **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**

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.

This chapter contains guidelines to help application developers and systems managers include security as part of the overall design. It also contains examples of techniques you can use to accomplish security objectives on your system. Some of the examples in this chapter 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 Basic System Security and Planning topic 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 information center (see "Prerequisite and Related Information" on page xvi 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 Basic System Security and Planning topic in the information center also uses a set of example applications for a fictional company called the JKL Toy Company. This chapter discusses design considerations for the same set of example applications. Figure 33 shows the relationships between user groups, applications, and libraries for the JKL Toy Company:

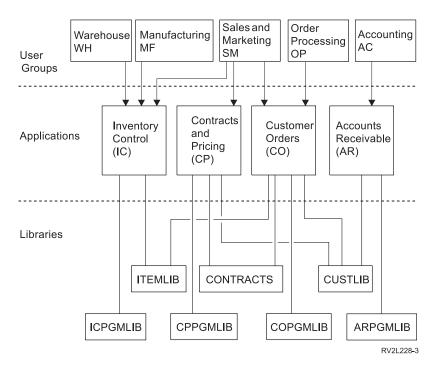


Figure 33. Example Applications

#### 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. 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 uses the Accounts Receivable application.

### Overall Recommendations

The recommendations in this chapter and in the Basic System Security and Planning topic in the information center rely on one important principle: simplicity. 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:** It is not sufficient to use only limited capabilities in the user profile and menu access control to secure your system if you use a product such as iSeries Access or have communication lines attached to your system. You must use resource security to secure those objects you do not want 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.

## 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 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 a user enters on a sign-on screen, must be upgraded to work with the new 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 new algorithm for QPWDLVL 2 or 3, even if the specific characters typed in are correct, will not be accepted. This also applies to any iSeries to iSeries 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 chang the QPWDLVL system value.

### Considerations for Changing QPWDLVL from 0 to 1

Password level 1 allows a system, which does not have a need to communicate with the Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) product, to have the NetServer passwords eliminated from the system. 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.

The functions/services that require the NetServer password include:

• iSeries Support for Windows Network Neighborhood, Windows 95/98/ME edition, (NetServer)

### 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 user profiles which do not have a password that is usable at password level 2. Depending on the profiles located, the administrator might wish to 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 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, and the user signs on through a product that sends clear text passwords, then 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. Subsequent signons will be validated against the password level 2 passwords.

Any client/service which uses password substitution will not work correctly at QPWDLVL 2 if the client/service hasn't been updated to use the new password (passphrase) substitution scheme. The administrator should check whether a client/service which hasn't been updated to the new password substitution scheme is required.

The clients/services that use password substitution include:

- TELNET
- iSeries Access
- · iSeries Host Servers
- QFileSrv.400
- iSeries 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.

It is recommended that the other password system values, such as QPWDMINLEN and QPWDMAXLEN, not be changed until after some testing at QPWDLVL 2 has occurred. This will make 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 wish 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 the administrator is comfortable with running the system at QPWDLVL 2, he can begin to change the password system values to exploit longer passwords. However, the administrator needs to be aware that longer passwords will have these effects:

- If passwords greater than 10 characters are specified, the password level 0 and 1 password is cleared. This user profile would 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, the administrator can consider moving to QPWDLVL 3 to maximize his 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 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.

Each of the following sections discusses the work required to move back to a lower password level.

### 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 (like 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, the administrator 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, the administrator should ensure 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 will cause 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 underscore.
  - The password does not begin with a numeric or underscore character.

For example, changing the password to a value of RainyDay would result in the system generating a password level 0 and 1 password of RAINYDAY. But changing the password value to Rainy Days In April would 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 QPWDLVL 1 to 0

After changing QPWDLVL to 0, the administrator 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.

The administrator can then change QPWDLVL to 0.

## **Planning Libraries**

Many factors affect how you choose to group your application information into libraries and manage libraries. This topic addresses some of the security issues associated with library design.

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.

A library is like a directory used to locate the objects in the library. \*USE authority to a library allows you to use the directory 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. See "Library Security" on page 114 for more information about the relationship between library and object authority.

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 33 on page 195 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 it. 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 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.

Library security is effective only if these rules 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.

### **Planning Applications to Prevent Large Profiles**

Because of the potential impacts on performance and security, IBM **strongly recommends** the following actions to avoid 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
  - 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 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.
- $\bullet\,$  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 cause an authorized object entry for every user granted authority to the authorization list rather than an authorized object entry for every object multiplied by the number of users that are granted the private authority.

### **Library Lists**

The library list for a job provides flexibility. It also represents a security exposure. 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. The topic "Library Lists" on page 183 provides a discussion of security issues associated with library lists.

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 technique described in the next section can reduce the security exposure.

### **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 desired list, and restore it at the end of the application. Here is a sample program to do this:

```
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 ' )')
                            QCMDEXC PARM(&CMD 2800)
                   CALL
                            &ERROR SNDPGMMSG MSGID(CPF9898) +
                   ΙF
                            MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
                            MSGDTA('The xxxx error occurred')
                   ENDPGM
```

Figure 34. 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, 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**

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 34, with the following changes:

- Instead of using the RTVJOBA command, use the Retrieve System Values (RTVSYSVAL) 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 desired value.
- 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 which 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 35 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  $\star OBJMGT$  authority.

Figure 35. 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 204 gives an example of how to do this.

- · Consider controlling access to the System Request Menu or some of the options on this menu. See "System Request Menu" on page 208 for more information.
- · 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.

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. Ouerv
         5. Office
Enter option ==>
F1=Help F12=Return
```

Figure 36. Sample Inquiry Menu

### **Using Adopted Authority in Menu Design**

The availability of decision-support tools, such as Query/400, poses challenges for security design. 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.

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.

**Note:** "Objects That Adopt the Owner's Authority" on page 128 describes how adopted authority works. "Flowchart 8: How Adopted Authority Is Checked" on page 160 describes how the system checks for adopted authority.

Figure 37 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)
       Customer Orders (COSTART)
       Query
                             (QRYSTART)
       4. Office
                             (OFCSTART)
(no command line)
```

Figure 37. 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).

PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM

Figure 38. 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 39 shows the QRYSTART program:

PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM

Figure 39. Sample Program for Query with Adopted Authority

The menu system uses three types of user profiles, shown in Table 119. Table 120 describes the objects used by the menu system.

Table 119. 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 <sup>1</sup>	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

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 120. 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		
Files not available for Query in ITEMLIB	OWNIC	*EXCLUDE		
Programs in ICPGMLIB	OWNIC	*USE		
Note: A special owner profile can	be created for object	s used by multiple ap	oplications.	

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 program 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 169 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.

### **Ignoring Adopted Authority**

Using Adopted Authority in Menu Design shows a technique for providing query capability without allowing uncontrolled changes to application files. This technique 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.

Note: "Programs That Ignore Adopted Authority" on page 131 provides more information about ignoring adopted authority. "Flowchart 8: How Adopted Authority Is Checked" on page 160 describes how the system checks for adopted authority.

Figure 40 on page 207 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 40. Sample Application Menu with Query

The authority information for the QRYSTART program is the same as shown in Table 120 on page 205. 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 program stacks when USERA selects query from MENU1 (see Figure 37 on page 204) and from ICMENU:

### Program stack when query selected from MENU1

MENU1 (no adopted authority)
QRYSTART (adopted authority QRYUSR)

### Program 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 query from ICMENU without having the ability to change and delete files, because the authority of OWNIC is not used by the QRYSTART program.

When USERA ends 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 36 on page 204) 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 program stack.

## **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. Typical information needed is:

- 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 41 on page 208 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 41. Format for Menu Security Requirements

### 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.

When your system is shipped, public authority to the System Request Menu is \*USE. 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 121 on page 209 shows the commands associated with the menu options:

Table 121. 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.)
50	End Request on Remote System (ENDRDBRQS). (See note below.)
80	Disconnect Job (DSCJOB)
90	Sign-Off (SIGNOFF)

#### Notes:

- 1. 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.
- 2. Option 12 is only displayed when 3270 emulation is active.
- 3. Option 50 is displayed only if a remote jobs is active.
- 4. 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.

## **Planning Command Security**

Menu security is a good technique for users who need applications and limited system functions. Some users need a more flexible environment and the capability to run commands. 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 it. Appendix C 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 i5/OS 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. "Using Adopted Authority in Menu Design" on page 204 gives an example of this method.

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.

## **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. See the DB2 Universal Database<sup>™</sup> for iSeries topic in the information center for more information. See "Prerequisite and Related Information" on page xvi for details.

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 42 on page 211 shows an example of a physical file and three different logical files associated with it.

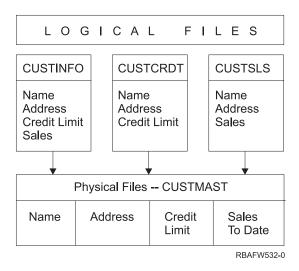


Figure 42. Using a Logical File for Security

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 122. Physical File Example: CUSTMAST File

Authority	Users: *PUBLIC		
Object Authorities			
*OBJOPR			
*OBJMGT			
*OBJEXIST			
*OBJALTER			
*OBJREF			
Data Authorities			
*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
                      CUSTLIB
 Library . . . . :
                                   Primary group . . . :
                                                          *NONE
Object type ...:
                      *FILE
                                   ASP device . . . . :
                                                          *SYSBAS
Object secured by authorization list . . . . . . . . :
                                                          *NONE
                      Object
User
                     Authority
          Group
*PUBLIC
                      *USE
```

```
Display Object Authority
Object . . . . . :
                       CUSTCRDT
                                     Owner . . . . . :
                                                            OWNAR
                       CUSTLIB
                                                            DPTAR
 Library . . . . :
                                     Primary group . . . :
Object type . . . :
                       *FILE
                                    ASP device . . . . :
                                                            *SYSBAS
Object secured by authorization list . . . . . . . . :
                                                            *NONE
                      Ob.ject
User
           Group
                      Authority
DPTAR
                      *CHANGE
*PUBLIC
                      *USE
```

```
Display Object Authority
                      CUSTSLS
Object . . . . . :
                                  Owner . . . . . :
                                                         OWNSM
                                  Primary group . . . :
 Library . . . . :
                      CUSTLIB
                                                         DPTSM
Object type . . . :
                      *FILE
                                  ASP device . . . . :
                                                         *SYSBAS
Object secured by authorization list .....:
                                                         *NONF
                     Object
User
          Group
                     Authority
DPTSM
                     *CHANGE
*PUBLIC
                     *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 165 shows how using primary group authority affects the authority checking process.

You can specify data authorities for logical files beginning with V3R1 of the i5/OS licensed program. When you move to V3R1 from an earlier version, the system converts your logical files when the system is installed. 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.

### **Overriding Files**

Override commands can be used 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.

### File Security and SQL

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.

You should take care 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.

### **Planning Authorization Lists**

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) or ALWOBJDIF(\*AUTL) is specified on the restore command.

# **Advantages of Using an Authorization List**

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 would be 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.

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.

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)
```

## **Planning Group Profiles**

A group profile is a useful tool when several users have similar security requirements. They 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.

You can create profiles specifically to be group profiles, or you can make an existing profile into a group profile. A group profile is simply 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.

## **Planning 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. "Case 2: Using Primary Group Authority" on page 165 shows an example of this.

### **Planning 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). 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.

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 148. 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 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 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 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 123 shows the characteristics of the two methods:

Table 123. Authorization List and Group Profile Comparison

Item Being Compared	<b>Authorization List</b>	<b>Group Profile</b>	
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 <sup>1</sup>	
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	No <sup>2</sup>	

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.

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 CRTxxxx 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. They 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.

Primary group authority is saved with the object.

Follow these guidelines when setting up an environment for application programmers:

- Do not grant **all** special authorities to programmers. However, if you must give programmers special authorities, give them **only** the special authority required to perform the jobs or tasks 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 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 122 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 designated for the application.
  - Application objects should not be owned by a programmer because the programmer would 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**

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 move them to production.

When a source file is created on the system, the default public authority is \*CHANGE, which 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 to add new members. The public authority should probably 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
- 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 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).

### Planning Security for System Programmers or Managers

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.

### Planning the Use of Validation List Objects

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 implement 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 an iSeries user id and password.

An internet user can be permitted or denied access to the iSeries from the Web server. The user, however, has no authority to any iSeries resources or authority to sign-on or run jobs. An iSeries 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. For more information and examples, see the API topic in the information center (see "Prerequisite and Related Information" on page xvi for details).

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, which is encrypted, rather than the application performing the verification itself.

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. For information about controlling the storage of decryptable data in validation lists, see "Retain Server Security (QRETSVRSEC)" on page 26.

# **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 limit access to program function provides APIs to perform the following tasks:

- · 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

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, the application calls the check usage API to see if the user is allowed to use the function that is associated with the code block, before invoking the code block. If the user is allowed to use the registered function, the code block is run. 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 iSeries Navigator.

# Chapter 8. Backup and Recovery of Security Information

This chapter discusses how security relates to backup and recovery on your system:

- · How security information is saved and restored
- · How security affects saving and restoring objects
- · Security issues associated with \*SAVSYS special authority

The *Backup and Recovery* book provides more information about backup and recovery. You might also refer to the Backup and Recovery topics in the iSeries Information Center (see "Prerequisite and Related Information" on page xvi for details).

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.

Planning adequate backup and recovery procedures for security information requires understanding how the information is stored, saved, and restored.

Table 124 shows the commands used to save and restore security information. The sections that follow discuss saving and restoring security information in more detail.

Table 124. How Security Information Is Saved and Restored

	Save and Restore Commands Used				
Security Information Saved or Restored	SAVSECDTA SAVSYS	SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG	RSTUSRPRF	RSTOBJ RSTLIB RSTDLO RSTCFG	RSTAUT
User profiles	X		X		
Object ownership <sup>1</sup>		X		X	
Primary group <sup>1</sup>		X		X	
Public authorities <sup>1</sup>		X		X	
Private authorities	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 <sup>2</sup>		X		X	
Function usage information	X		X		X
Validation lists		X		X	

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).

The object to save/restore is QUSEXRGOBJ, type \*EXITRG in QUSRSYS library.

### **How Security Information is Stored**

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.

#### **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.

## **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

#### **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.

#### **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 usual 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).

The Backup and Recovery book provides more information about planning recovery.

# **Restoring User Profiles**

Some changes might be made to a user profile when it is restored. The following rules applies:

- If profiles are being restored individually (RSTUSRPRF USRPRF(\*ALL) is not specified), SECDTA(\*PWDGRP) is not requested, and the profile 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 user profiles are being restored to your system, all the fields in any profiles that already exist on the system are restored from the save media, including the password.

Attention: 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 would not be valid on a system running password level 0 or 1.

Attention: Keep a record of the security officer (QSECOFR) password associated with each version of your security information that is saved to make sure 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. See Service tools topic in the information center for instructions. See "Prerequisite and Related Information" on page xvi for more information about accessing the information center.

- 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 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 the same 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 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

# **Restoring Objects**

When you restore an object to the system, the system uses the authority information stored with the object. The following applies to the security of the restored object:

### **Object ownership:**

- If the profile that owns the object is 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) or ALWOBJDIF(\*OWNER) is specified. In that case, the object is restored and the owner on the system is used.
- See "Restoring Programs" on page 227 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 being restored does not exist on the system, public authority is set to the public authority of the saved object.
- If the object 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) or ALWOBJDIF(\*AUTL) is specified, the object is restored. The object is linked to the authorization list associated with the existing object.
- If a document or folder that already exists on the system is restored, the authorization list 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) or ALWOBJDIF(\*AUTL) 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, not with objects.
- If user profiles have private authority to an object being restored, those private authorities are typically not affected. Restoring certain types of programs might result in private authorities being revoked. See "Restoring Programs" on page 227 for more information.
- If an object is deleted from the system and then restored from a saved version, 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 private authorities need to be recovered, 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 being restored does not exist on the system, the object auditing (OBJAUD) value of the saved object is restored.
- If the object 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 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 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 and 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:**

• For systems running Version 2 Release 3 or later of the i5/OS licensed program, 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.

# **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 using the information from the authority table. The grant authority operation is run for each private authority in the authority table. If authority is being restored for many profiles and many private authorities exist in the authority tables, this can be a lengthy process.

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 created by the SAVSECDTA or SAVSYS command or the QSRSAVO API to find the profiles you want to restore.

#### **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. 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 QVFYOBJRST, QFRCCVNRST, and QALWOBJRST system values to prevent these object types from being restored to your system. See Security-Related Restore System Values for more information about these system values.

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 that are created for iSeries Version 5 Release 1 or later 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. The action of re-creating the program at restore time is not new to iSeries Version 5 Release 1. In previous releases, any program validation error that was encountered at restore time resulted in the program being re-created if possible (if observability existed in the program being restored). The difference with iSeries Version 5 Release 1 or later programs is that the information needed to re-create the program remains even when observability was removed from the program.

#### **Restoring Programs That Adopt the Owner's Authority:**

When a program is restored that adopts owner authority, the ownership and authority to the program may 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.

# **Restoring Licensed Programs**

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 created using the SystemView® System Manager/400 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. Use a program that adopts \*ALLOBJ special authority to run the RSTLICPGM command, instead of having a user with \*ALLOBJ authority run the command directly.

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. For the example, the user profile is called OWNCP.
- 2. Write a program to install the application. For the example, the program is called CPINST:

```
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

Authorization lists are saved by either the SAVSECDTA command or the SAVSYS command. Authorization lists are restored by the command:

```
RSTUSRPRF USRPRF(*ALL)
```

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. See "Restoring Objects" on page 224 for more information. Users' private authorities to the list are restored using the RSTAUT command.

### Recovering from a Damaged Authorization List

When an object is secured by an authorization list and the authorization list 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.

Recovering the Authorization List: If users' authorities to the authorization list are known, just delete the authorization list, create the authorization list again, and then add users to it.

If it is not possible to create the authorization list again because you do not know all the user authorities, the authorization list can be restored and the users restored to the authorization list using your last SAVSYS or SAVSECDTA 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 using the RSTAUT command.

**Attention:** This procedure restores user profile values from the save media. See "Restoring User Profiles" on page 223 for more information.

**Recovering the Association of Objects to the Authorization List:** When the damaged authorization list is deleted, the objects 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 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 (DSPAUTLOBJ) command to list the objects associated with the QRCLAUTL authorization list.
- 3. Use the Grant Object Authority (GRTOBJAUT) command to secure each object with the correct authorization list:

**Note:** If a large number of objects are associated with the QRCLAUTL authorization list, create a database file by specifying OUTPUT(\*OUTFILE) on the DSPAUTLOBJ 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 the iSeries System

This chapter 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 chapter are appropriate for all these situations. Which things you audit and how often depends on the size and security needs of your organization. The purpose of this chapter 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 chapter 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 on the iSeries system 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 chapter 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.

# **Checklist for Security Officers and Auditors**

This checklist can be used both to plan and to audit system security. As you plan security, choose the items from the list that meet your security requirements. When you audit the security of your system, use the list to evaluate the controls you have in place and to determine if additional controls are needed.

This list serves as a review of the information in this book. The list contains brief descriptions of how to do each item and how to monitor that it has been done, including what entries in the QAUDJRN journal to look for. Details about the items are found throughout the book.

## **Physical Security**

**Note:** The Basic System Security and Planning topic in the information center contains a complete discussion of physical security on the iSeries system. See "Prerequisite and Related Information" on page xvi for details.

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 key is removed. The keys are kept separately, both under tight physical security. See the information center for more information about the keylock switch (see "Prerequisite and Related Information" on page xvi for details).

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**

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 QSECURITY (security level) and QPWDLVL (password level) values, and the current setting of the security related system (whether the values can be changed).

Decisions about system values are reviewed periodically, particularly when the system environment changes, such as the installation of new applications or a communications network.

# **IBM-Supplied User Profiles**

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.

**Note:** See "IBM-Supplied User Profiles" on page 108 and Appendix B for more information about IBM-supplied user profiles.

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. See the topic "Working with Service Tools User IDs" on page 109 for more information.

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 281, except QSECOFR, have a password of \*NONE.

## **Password Control**

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 will attempt to create an equivalent password that is usable at the other password levels, if possible. 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 would 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**

Each user is assigned a unique user profile. The QLMTDEVSSN system value should be set 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. The DSPUSRPRF command can be used to check the special authorities for user profiles and to determine which profiles are group profiles. The topic "Printing Selected User Profiles" on page 268 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 268 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 216 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 269 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. The DO (Delete Object) entries in the audit journal can be reviewed to make sure user profiles are deleted immediately after employees leave.

Management regularly verifies the users authorized to the system. You can use the DSPAUTUSR command for this 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 268 gives an example of how to determine this.

### **Authorization Control**

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(\*JOBD) ASPDEV(\*ALLAVL) OUTPUT(\*PRINT)

To check the User parameter of a job description, use the Display Job Description (DSPJOBD) 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 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 183 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 270 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**

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 ensure that no subsystem descriptions have a workstation entry which uses a job description that has a user profile name.

## **Unauthorized Programs**

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 270.

### Communications

Telephone communications is protected by call-back procedures.

Encryption is used on sensitive data.

Remote sign-on is controlled. The QRMTSIGN system value is set to \*FRCSIGNON or a pass-through validation program is used.

Access to data from other systems, including personal computers, is controlled using the JOBACN, PCSACC, and DDMACC network attributes. 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. A security auditor inside or outside your organization can use the auditing function 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" on page 236 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. An application program or a query tool can be used to analyze the data.

The security auditing function is optional. You must take specific steps to set up security auditing.

The following sections describe how to plan, set up, and manage security auditing, what information is recorded, and how to view that information. Appendix F shows record layouts for the audit journal entries. Appendix E describes what operations are audited for each type of object.

# **Planning Security Auditing**

To plan the use of security auditing on your system:

- · 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 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.

Which events you choose to log depends on both your security objectives and your potential exposures. Table 125 on page 237 describes the possible audit level values and how you might use them. It shows whether they are available as a system value, a user profile parameter, or both.

Table 126 on page 241 provides more 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

- 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.
- 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.

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	No	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), 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	<b>Deleting objects</b> : The system writes a journal entry when an object is deleted.
*JOBDTA	Yes	Yes	Job tasks: Actions that affect a job are logged, such as starting or stopping the job, holding, releasing, canceling, or changing it. *JOBDTA can be used to monitor who is running batch jobs.
*NETBAS	Yes	No	<b>Network base functions</b> : IP rules actions, sockets connections, APPN directory search filter, APPN end point filter.
*NETCLU	Yes	No	Cluster or cluster resource group operations: Ar audit journal entry is written when these events occur:
			<ul> <li>A cluster node or cluster resource group is added, created, or deleted.</li> </ul>
			<ul> <li>A cluster node or cluster resource group is started, ended, updated, or removed.</li> </ul>
			<ul> <li>Automatic failure of a system that switches access to another system.</li> </ul>
			<ul> <li>Access is manually switched from one system to another system in a cluster.</li> </ul>

Table 125. Action Auditing Values (continued)

Possible Value	Available on QAUDLVL and QAUDLVL2 System Values	Available on CHGUSRAUD Command	Description
*NETCMN	Yes	No	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	No	<b>Network failures</b> : 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.
*NETSCK	Yes	No	<b>Socket tasks</b> : An audit journal entry is written when these events occur:
			<ul> <li>An inbound TCP/IP socket connection is accepted.</li> </ul>
			<ul> <li>An outbound TCP/IP socket connection is established.</li> </ul>
			<ul> <li>An IP address is assigned through DHCP (Dynamic Host Configuration Protocol).</li> </ul>
			<ul> <li>An IP address is unable to be assigned through DHCP because all of the IP addresses are being used.</li> </ul>
			<ul> <li>Mail is filtered or rejected.</li> </ul>
*OBJMGT	Yes	Yes	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.
*OPTICAL	Yes	Yes	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.
*PGMADP	Yes	Yes	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.
*PGMFAIL	Yes	No	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.

Table 125. Action Auditing Values (continued)

Possible Value	Available on QAUDLVL and QAUDLVL2 System Values	Available on CHGUSRAUD Command	Description
*PRTDTA	Yes	No	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.
*SAVRST	Yes	Yes	<b>Restore operations</b> : *SAVRST can be used to detect attempts to restore unauthorized objects.
*SECCFG	Yes	No	<b>Security configuration</b> : An audit journal entry is written when these events occur:
			<ul> <li>User profiles are created, changed, deleted, or restored.</li> </ul>
			<ul> <li>Changes are made to programs, system values, subsystem routing, or to the auditing attributes of an object.</li> </ul>
			<ul> <li>The QSECOFR password is reset to the shipped value.</li> </ul>
			<ul> <li>The service tools security officer password is defaulted.</li> </ul>
*SECDIRSRV	Yes	No	<b>Directory service functions</b> : An audit journal entry is written when these events occur:
			<ul> <li>Changes or updates are made to auditing, authority, passwords, and ownership.</li> </ul>
			<ul> <li>Successful binds and unbinds.</li> </ul>
			<ul> <li>Changes are made to directory security policies (for example, password policy)</li> </ul>
*SECIPC	Yes	No	<b>Interprocess communications</b> : An audit journal entry is written when these events occur:
			<ul> <li>Changes are made to the ownership or authority of an IPC object.</li> </ul>
			A create, delete, or get of an IPC object.
			Shared memory attach.

Table 125. Action Auditing Values (continued)

Possible Value	Available on QAUDLVL and QAUDLVL2 System Values	Available on CHGUSRAUD Command	Description
*SECNAS	Yes	No	Network authentication service actions: An audit journal entry is written when these events occur:
			Service ticket invalid.
			Service principals do not match.
			• Client principals do not match.
			Ticket IP address mismatch.
			Decryption of the ticket failed.
			<ul> <li>Decryption of the authentication failed.</li> </ul>
			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.
			<ul> <li>For KRB_AP_PRIV or KRB_AP_SAFE:         Timestamp error, replay error, or sequence order error.     </li> </ul>
			<ul> <li>For GSS accept: Expired credentials, checksun error, or channel bindings.</li> </ul>
			<ul> <li>For GSS unwrap or GSS verify: Expired context, decrypt/decode, checksum error, or sequence error.</li> </ul>
*SECRUN	Yes	No	<b>Security runtime functions</b> : Changes to object ownership, authority, and primary group are written to the audit journal.
*SECSCKD	Yes	No	Socket descriptors: An audit journal entry is written when these events occur:
			<ul> <li>A socket descriptor is given to another job.</li> </ul>
			<ul> <li>A socket descriptor is received.</li> </ul>
*SECVFY	Yes	No	<ul> <li>A socket descriptor is unusable.</li> <li>Verification functions: An audit journal entry is written when these events occur:</li> </ul>
			<ul> <li>A profile handle or token is generated.</li> </ul>
			All profile tokens were invalidated.
			• The maximum number of profile tokens has been generated.
			<ul> <li>All profile tokens for a user have been removed.</li> </ul>
			<ul> <li>A user profile has been authenticated.</li> </ul>
			<ul> <li>A target profile was changed during a pass-through session.</li> </ul>

Possible Value	Available on QAUDLVL and QAUDLVL2 System Values	Available on CHGUSRAUD Command	Description
*SECVLDL	Yes	No	<b>Validation list operations</b> : An audit journal entry is written when these events occur:
			<ul> <li>An add, change, remove, or find of a validation list entry.</li> </ul>
			<ul> <li>Successful or unsuccessful verification of a validation list entry.</li> </ul>
*SECURITY	Yes	Yes	<b>Security tasks</b> : 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.
			*SECURITY is composed of several values to allow you to better customize your auditing. The following values make up *SECURITY:
			*SECCFG *SECDIRSRV *SECIPC *SECNAS
			*SECRUN *SECSCKD *SECVFY *SECVLDL
*SERVICE	Yes	Yes	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.
*SPLFDTA	Yes	Yes	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.
*SYSMGT	Yes	Yes	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.

Table 126. Security Auditing Journal Entries

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
*AUTFAIL <sup>1</sup>	AF	QASYAFJE/J4/J5	A	Attempt made to access an object or perform an operation to which the user was not authorized.
			K	Attempt made to perform an operation for which the user did not have the required special authority.
			S	Default signon attempt.
	X1	QASYX1J5	F	Delegate of identity token failed.
			U	Get user from identity token failed.
			F	ICAPI authorization error.
			G	ICAPI authentication error.
			Н	Scan exit program action.
			J	Attempt 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.
			N	Profile token not a regenerable profil token.
			P	Attempt made to use a profile handl that is not valid on the QWTSETP API.
			S	Attempt made to sign on without entering a user ID or a password.
			T	Not authorized to TCP/IP port.
			U	A user permission request was not valid.
			V	Profile token not valid for generating new profile token.
			W	Profile token not valid for swap.
			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.
	DI	QASYDIJ4/J5	AF	Authority failures.
			PW	Password failures.
			R	Connection rejected.
	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.
			С	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
			S	SQL decrypt a password that was no valid.
			U	User name not valid.
			X	Service tools user is disabled.
			Y	Service tools user not valid.
			Z	Service tools password not valid.
	VO	QASYVOJ4/J5	Ü	Unsuccessful verification of a validation list entry.
	VC	QASYVCJE/J4/J5	R	A connection was rejected because of incorrect password.
	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.
*CMD <sup>2</sup>	CD	QASYCDJE/J4/J5	С	A command was run.
CIVID	CD	WINT CDIL/ 14/ 10	L	An S/36E control language statement was run.
			0	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 <sup>3</sup>	СО	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.
*DELETE <sup>3</sup>	DO	QASYDOJE/J4/J5	A	Object deleted.
		V	С	Pending delete committed.
			D	Pending create rolled back.
			P	Delete pending.
			R	Pending delete rolled back.
	DI	QASYDIJ4/J5	DO	Object deleted.
*JOBDTA	JS	QASYJSJE/J4/J5	A	The ENDJOBABN command was used.
			В	A job was submitted.
			С	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	Description
	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.
		V	O	Logon requested.
	VS	QASYVSJE/J4/J5	S	A server session was started.
		V	E	A server session was ended.
*NETBAS	CV	QASYCVJE/J4/J5	С	Connection established.
		<b>V</b>	E	Connection ended normally.
			R	Rejected connection.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file
	110	QASTIIW4/ JJ	N	IP rules have been unloaded for an II
				Security connection.
			Р	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.
		v	2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A violation was detected by the
		V		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
*NIPTOLLI	CII	OACVOLUE /IA /IF	1.6	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	С	Connection established.
	٠.	V- 10 1 0 1 0 1 0 0	E	Connection ended normally.
	IR	QASYIRJ4/J5	L	IP rules have been loaded from a file.
	IIV	QA311W4/ JJ	N	IP rule have been unloaded for an IP
			11	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.
	10	AU011014/10	1 2	Phase 2 negotiation.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	Description
	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
		V	С	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
IVEIDOR	SIL .	Q1151511111111111111111111111111111111	C	Connect
			D	DHCP address assigned
			F	Filtered mail
			R	Reject mail
			U	DHCP address denied
*OBJMGT <sup>3</sup>	DI	QASYDIJ4/J5	OM	Object rename
ObJMG1	OM	QASYOMJE/J4/J5	M	An object was moved to a different library.
			R	An object was renamed.
*OFCSRV	ML	QASYMLJE/J4/J5	O	An object was renamed.  A mail log was opened.
Oresky	SD	QASYSDJE/J4/J5	S	A change was made to the system distribution directory.
*OPTICAL	O1	QASY01JE/J4/J5	R	Open file or directory
OI HOIL	O1	Q1151013E/31/30	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
	OΣ	QAD1021E/ 14/ 13	R	Rename file
			В	Back up file or directory
			S	
			M	Save held optical file Move file
	O3	QASY03JE/J4/J5	I	Initialize volume
	U3	QA5105JE/J4/J5	В	
				Backup volume Rename volume
			N	
			C	Convert backup volume to primary
			M	Import
			E	Export
			L	Change authorization list
			A	Change volume attributes
		0 4 0774 777 /74 /74	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 program stack.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	Description
			E	A program ended that adopts owner authority. The end entry is written when the program leaves the program stack. If the same program occurs more than once in the program 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 <sup>1</sup>	AF	QASYAFJE/J4/J5	В	A program ran a restricted machine interface instruction.
			С	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)
*PRTDTA 1	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 <sup>3</sup>	OR	QASYORJE/J4/J5	N	A new object was restored to the system.
			Е	An object was restored that replaces an existing object.
	RA	QASYRAJE/J4/J5	A	The system changed the authority to an object being restored. 4
	RJ	QASYRJJE/J4/J5	A	A job description that contains a use profile name was restored.
	RO	QASYROJE/J4/J5	A	The object owner was changed to QDFTOWN during restore operation. <sup>4</sup>
	RP	QASYRPJE/J4/J5	A	A program that adopts owner authority was restored.
	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
			0	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.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
			0	Auditing of an object was changed with CHGOBJAUD command.
			U	Auditing for a user was changed with CHGUSRAUD command.
	AU	QASYAUJ5	E	Enterprise Identity Mapping (EIM) configuration change
	СР	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
			С	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.
			С	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
		<b>V</b>	C	Change.
			D	Delete.
	GR	QASYGRJ4/J5	A	Exit program added
		V	D	Exit program removed
			F	Function registration operation
			R	Exit program replaced
	JD	QASYJDJE/J4/J5	A	The USER parameter of a job description was changed.
	KF	QASYKFJ4/J5	С	Certificate operation.
		v	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
			C	Change entry.
			R	Remove entry.
	SV	QASYSVJE/J4/J5	A	A system value was changed.
			В	Service attributes were changed.
			C	Change to system clock.
	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
*SECIPC	IP	QASYIPJE/J4/J5	A	The ownership or authority of an IP object was changed.
			С	Create an IPC object.
			D	Delete an IPC object.
			G	Get an IPC object.
*SECNAS	X0	QASYX0J4/J5	1	Service ticket valid.
5201112	110	q1151110017 00	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 faile
			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
			В	Remote IP address mismatch
			С	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

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
			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.
*SECSCKD	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.
			0	Auditing of an object was changed with CHGOBJAUD command.
			U	Auditing for a user was changed with CHGUSRAUD command.
			S	Scan attribute change by CHGATR command or Qp01SetAttr API
	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.
	СР	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.
	CV	Q/101C V 147 10	E	Connection ended normally.
			R	Connection rejected.
	CY	QASYCYJ4/J5	A	Access Control function
	CI	QA51C114/10	F	Facility Control function
			M	Master Key function
	DI	QASYDIJ4/J5	AD	Audit change
	DI	QA31DD4/13	BN	Successful bind
			CA	Authority change
			CA CP	ŷ ĕ
			OW	Password change Ownership change
			PO	Policy change
	DO		UB	Successful unbind
	DO	QASYDOJE/J4/J5	A	Object was deleted not under commitment control
			С	A pending object delete was committed

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	Description
			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.
			С	DST profile changed.
	EV	QASYEVJ4/J5	A	Add.
		V	С	Change.
			D	Delete.
	GR	QASYGRJ4/J5	A	Exit program added
		<b>V</b>	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.
			С	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	С	Certificate operation.
		V	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.
			Н	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.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
			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.
			В	Service attributes were changed.
			C	Change to system clock.
	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
			A	Decrypt of KRB_AP_PRIV or KRB_AP_SAFE checksum error
			В	Remote IP address mismatch
			С	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
			0	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.
	X1	QASYX1J5	D	Delegate of identity token successful

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	<b>Detailed Entry</b>	Description
			G	Get user from identity token successful
			E	An office user ended work on behalof another user.
			Н	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 beha of another user.
			V	User profile authenticated.
*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	С	The service status was changed.
		V	E	The server was stopped.
			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 someon other than the owner.
			С	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.
			U	A spooled file was changed.
*SYSMGT	DI	QASYDIJ4/J5	CF	Configuration changes
DIDIVIGI	21	Q11512117 V	RM	Replication management
	SM	QASYSMJE/J4/J5	В	Backup options were changed using xxxxxxxxxxx.
			С	Automatic cleanup options were changed using xxxxxxxxxxx.
			D	A DRDA* change was made.
			F	An HFS file system was changed.
			N	A network file operation was performed.
			0	A backup list was changed using xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
			P	The power on/off schedule was changed using xxxxxxxxxx.
			S	The system reply list was changed.
			T	The access path recovery times wer changed.
	VL	QASYVLJE/J4/J5	A	The account is expired.
	٧L	AUDI AFIE\ 14\ 10	D A	The account is expired.  The account is disabled.
			L L	Logon hours were exceeded.
			ட	9
			U	Unknown or unavailable.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
Object Auditing:				
*CHANGE	DI	QASYDIJ4/J5	IM	LDAP directory import
			ZC	Object change
	ZC	QASYZCJ4/J5	С	Object changes
			U	Upgrade of open access to an object
	AD	QASYADJEJ4/J5	D	Auditing of an object was changed with CHGOBJAUD command.
			0	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 <sup>6</sup>
	LD	QASYLDJE/J4/J5	L	Link a directory.
		V	U	Unlink a directory.
			K	Search 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.
		•	С	Change validation list entry.
			F	Find validation list entry.
			R	Remove validation list entry.
	VR	QASYVRJE/J4/J5	F	Resource access failed.
		•	S	Resource access was successful.
	YC	QASYYCJE/J4/J5	C	A document library object was changed.
	ZC	QASYZCJE/J4/J5	С	An object was changed.
			U	Upgrade of open access to an object.

Table 126. Security Auditing Journal Entries (continued)

Action or Object Auditing Value	Journal Entry Type	Model Database Outfile	Detailed Entry	Description
*ALL 5	CD	QASYCDJ4/J5	C	Command run
	DI	QASYDIJ4/J5	EX	LDAP directory export
			ZR	Object read
	GR	QASYGRJ4/J5	F	Function registration operations <sup>6</sup>
	YR	QASYYRJE/J4/J5	R	A document library object was read.
	ZR	QASYZRJE/J4/J5	R	An object was read.

<sup>1</sup> This value can only be specified for the QAUDLVL system value. It is not a value for the AUDLVL parameter of a user profile.

- See the topic "Restoring Objects" on page 224 for information about authority changes which might occur when an object is restored.
- 5 When \*ALL is specified, the entries for both \*CHANGE and \*ALL are written.
- When the QUSRSYS/QUSEXRGOBJ \*EXITRG object is being audited.

### **Planning the Auditing of Object Access**

The system provides the ability to log accesses to an object in the security audit journal. 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 127 shows how the OBJAUD values for the object and the user profile work together.

Table 127. How Object and User Auditing Work Together

	OBJAUD Value for User			
<b>OBJAUD Value for Object</b>	*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 accessing a critical object on the system. You can also use object auditing to keep track of all the object accesses by a particular user. Object auditing is a flexible tool that allows 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, and 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.

The following 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:

This value can only be specified for the AUDLVL parameter of a user profile. It is not a value for the QAUDLVL system value.

<sup>3</sup> 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.

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 using the techniques described in "Analyzing Audit Journal Entries with Query or a Program" on page 263.
- If you are concerned about who is using a particular file, you can collect information about all accesses of that 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 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 263.
- 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.

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 new objects that are created. 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, it balances the performance effect against the potential loss of information in a power outage. \*SYS is the default and the recommended 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 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 does the following things 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:

- The system turns 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, a user with \*ALLOBJ and \*AUDIT special authority must sign on at the console.
- 3. The system starts in a restricted state with a message indicating that an auditing error caused the system to stop.
- 4. The QAUDCTL system value is set to \*NONE.
- 5. 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 attempt to reset the QAUDCTL value again.

## **Choosing to not Audit QTEMP Objects**

The value, \*NOQTEMP, can be specified as a value for system value QAUDCTL. If specified, you must also specify either \*OBJAUD or \*AUDLVL. 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.

See Table 230 on page 621 for more information about CHGSECAUD command.

# **Setting up Security Auditing**

#### 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.

To set up security auditing, do the following steps. Setting up auditing requires \*AUDIT special authority.

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')
```

- 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.
- 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. Using this type of naming convention is also useful if you choose to have the system manage changing your journal receivers (which is strongly recommended).
- · 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 you choose to audit. If you use system change-journal management support, the journal receiver threshold must be at least 100 000 KB. For more information about journal receiver threshold, refer to Journal management.
- Specify \*EXCLUDE on the AUT parameter to limit access to the information 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 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 when the journal receiver was created. 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. Ensure 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 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 236.
- 4. Set action auditing for individual users, if necessary, using the CHGUSRAUD command. See "Planning the Auditing of Actions" on page 236.
- 5. Set object auditing for specific objects, if necessary, using the CHGOBJAUD, CHGAUD, and CHGDLOAUD commands. See "Planning the Auditing of Object Access" on page 254.
- 6. Set object auditing for specific users, if necessary, 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 256.
- 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 256.
- 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 auditing journal, QSYS/QAUDJRN, is intended <u>solely</u> 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.

Special locking protection is used to ensure that the system 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
- ENDJRNxxx (End Journaling) commands
- · APYJRNCHG command
- · RMVJRNCHG command
- · DMPOBJ or DMPSYSOBJ command
- Moving the journal
- Restoring the journal
- · Operations that work with authority, such as the GRTOBJAUT command
- · WRKJRN command

The information recorded in the security journal entries is described in Appendix F. 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 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 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 might want to 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 is completed. You can monitor for this message to know when to do a save of the detached journal receivers.

Attention: The automatic cleanup function provided using Operational Assistant menus does not clean up the QAUDJRN receivers. You should regularly detach, save, and delete QAUDJRN receivers to avoid problems with disk space.

See the Journal management topic for complete information about managing journals and journal receivers.

Note: 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.

## Saving and Deleting Audit Journal Receivers

#### Overview:

#### **Purpose:**

To attach a new audit journal receiver; to save and delete the old receiver

#### How To:

- CHGJRN QSYS/QAUDJRN JRNRCV(\*GEN)
- 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, in addition to taking valuable space on auxiliary storage.

Having the system manage receivers automatically is the recommended approach. 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:** 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 status.
- 3. Use the SAVOBJ command to save each receiver, except the currently attached receiver, which has not already been saved.
- 4. Use the DLTJRNRCV command to delete each receiver after it is saved.

**Note:** An alternative to the preceding procedure can be done using the journal message queue and monitoring for the CPF7020 message which indicates that the system change journal has completed successfully. See the *Backup and Recovery* for more information about this support.

**User-Managed Journal Receivers:** 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 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 might want to leave the QAUDJRN journal on the system. However, 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:

- · Viewing selected entries at your workstation using the Display Journal (DSPJRN) command
- · Copying 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
- Using 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.

You can also 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
  - 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 . . . . . :
Type options, press Enter.
 5=Display entire entry
0pt
      Sequence Code Type Object
                                     Library
                                                 Job
                                                          Time
                      PR
                                                 SCPF
                                                          10:24:55
            1
                J
            2
                      CA
                                                 SCPF
                                                          10:24:55
                Τ
            3
               Τ
                      CO
                                                 SCPF
                                                          10:24:55
            4
                Τ
                      \mathsf{C}\mathsf{A}
                                                 SCPF
                                                          10:24:55
            5
                Τ
                      CO
                                                 SCPF
                                                          10:24:55
            6
                Т
                     CA
                                                 SCPF
                                                          10:24:55
            7
                Τ
                     CO
                                                 SCPF
                                                          10:24:55
            8
                     CA
                                                 SCPF
                                                          10:24:56
                Т
                                                          10:24:56
            9
                Τ
                      CO
                                                 SCPF
            10
                      \mathsf{C}\mathsf{A}
                                                 SCPF
                                                          10:24:57
            11
                Τ
                      CO
                                                 SCPF
                                                          10:24:57
            12
                Τ
                      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 . . . . . :
                      No
                                     Minimized entry data: *None
Incomplete data . . :
Sequence . . . . : 1198
                      T - Audit trail entry
Code . . . . . . :
Type . . . . . . : CO - Create object
          Entry specific data
Co1umn
          *...+....1....+....2....+....3....+....4....+....5
          'NISAVLDCK QSYS *PGM CLE
00001
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 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 query or program, or Run 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 Table 150 on page 507 for more information.

For more information about other records and their output file formats, see Appendix F.

If you want to perform a detailed analysis of a particular entry type, use one of the model database outfiles provided. 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) ... +
   JRNCDE(T) ENTTYP(AF) OUTPUT(*OUTFILE) +
   OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)
```

3. Use Query or a program to analyze the information in the AUDJRNAF5 file.

Table 126 on page 241 shows the name of the model database output file for each entry type. Appendix F shows the file layouts for each model database output 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 126 on page 241 shows which journal entry is written for each authority violation message.

# Relationship of Object Change Date/time to Audit Records

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 was 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 would be affected if the Change Date/Time field was updated each time a record in the file was updated, added, or deleted.

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 updates 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 updates 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, you can 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.

# 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 619. This appendix 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**

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 in the information center 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. <u>Do not</u> journal any objects to the QAUDJRN journal.

Journal entries can include:

- · Identification of the job and user and the time of access
- · Before- and after-images of all object changes
- Records of when the object was opened, closed, changed, saved, 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, 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)
```

For example, if journal JRNCUST in library CUSTLIB is used to record information about file CUSTFILE (also in library CUSTLIB), the command would 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 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 outfile 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 outfile for a particular data queue.
DSPJRN JRN(library/journal) +
                   OBJPATH(('path name')) +
              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.

The Journal management topic collection provides complete information about journaling.

# **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			
		Password		
Group	User	Last	No	
Profile DPTSM	Profile	Changed	Password	Text
	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	Χ	Sales and Marketing
	DPTWH	08/13/0x	Χ	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**

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:

- 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" on page 270.

Appendix B provides information about all the IBM-supplied user profiles and their functions.

# **Analyzing Object Authorities**

You can use the following method to determine who has authority to libraries on the system:

- 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:

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. The following method can be used to find and inspect those programs:

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 268 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 have 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 have to be \*PGM, \*SQLPKG, or \*SRVPGM as indicated by the DSPPGMADP report.

# Checking for Objects That Have Been Altered

You can use the Check Object Integrity (CHKOBJITG) command to look for objects that have been altered. An altered object is often an indication that someone is attempting to tamper with your system. 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 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 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 CRTDUPOBJ (Create Duplicate Object) command each time a new release is loaded.

## **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.

## **Auditing the Security Officer's Actions**

You might want to keep a record of all actions performed by users with \*ALLOBJ and \*SECADM special authority. You can use the action auditing value in the user profile to do this:

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 *OFCSRV *PGMADP +
*SAVRST *SERVICE, +
*SPLFDTA *SYSMGT)
```

Note: Table 125 on page 237 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.

**Note:** 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 263.

# **Appendix A. Security Commands**

This appendix contains the system commands related to security. You can use these commands in place of the system menus, if you prefer, by typing these commands on a command line. The commands are divided into task-oriented groups.

The CL topic in the Information Center contains more detailed information about these commands. See "Prerequisite and Related Information" on page xvi for details. The tables in Appendix D show what object authorities are required to use these commands.

Table 128. Commands for Working with Authority Holders

<b>Command Name</b>	Descriptive Name	Function
CRTAUTHLR	Create Authority Holder	Allows you to secure a file before the file exists. Authority holders are valid only for program-described database files.
DLTAUTHLR	Delete Authority Holder	Allows you to delete an authority holder. If the associated file exists, the authority holder information is copied to the file.
DSPAUTHLR	Display Authority Holder	Allows you to display all the authority holders on the system.

Table 129. Commands for Working with Authorization Lists

<b>Command Name</b>	<b>Descriptive Name</b>	Function
ADDAUTLE	Add Authorization List Entry	Allows you to 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	Allows you to change users' authorities to the objects on the authorization list.
CRTAUTL	Create Authorization List	Allows you to create an authorization list.
DLTAUTL	Delete Authorization List	Allows you to delete an entire authorization list.
DSPAUTL	Display Authorization List	Allows you to display a list of users and their authorities to an authorization list.
DSPAUTLOBJ	Display Authorization List Objects	Allows you to display a list of objects secured by an authorization list.
EDTAUTL	Edit Authorization List	Allows you to add, change, and remove users and their authorities on an authorization list.
RMVAUTLE	Remove Authorization List Entry	Allows you to 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.
WRKAUTL	Work with Authorization Lists	Allows you to work with authorization lists from a list display.

Table 130. Commands for Working with Object Authority and Auditing

<b>Command Name</b>	Descriptive Name	Function
CHGAUD	Change Auditing	Allows you to change the auditing value for an object.
CHGAUT	Change Authority	Allows you to change the authority of users to objects.
CHGOBJAUD	Change Object Auditing	Allows you to specify whether access to an object is audited.
CHGOBJOWN	Change Object Owner	Allows you to change the ownership of an object from one user to another.
CHGOBJPGP	Change Object Primary Group	Allows you to change the primary group for an object to another user or to no primary group.
CHGOWN	Change Owner	Allows you to change the ownership of an object from one user to another.
CHGPGP	Change Primary Group	Allows you to change the primary group for an object to another user or to no primary group.
DSPAUT	Display Authority	Allows you to display users' authority to an object.
DSPLNK	Display Links	Allows you to 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	Allows you to add, change, or remove a user's authority for an object.
GRTOBJAUT	Grant Object Authority	Allows you to 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	Allows you to remove one or more (or all) of the authorities given specifically to a user for the named objects.
WRKAUT	Work with Authority	Allows you to work with object authority by selecting options on a list display.
WRKLNK	Work with Links	Allows you to show a list of names of specified objects in directories and options to work with the objects.
WRKOBJ	Work with Objects	Allows you to work with object authority by selecting options on a list display.
WRKOBJOWN	Work with Objects by Owner	Allows you to work with the objects owned by a user profile.
WRKOBJPGP	Work with Objects by Primary Group	Allows you to 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	Allows you to work with the objects for which a profile is privately authorized, using options from a list display.

Table 131. Commands for Working with Passwords

<b>Command Name</b>	Descriptive Name	Function
CHGDSTPWD	Change Dedicated Service Tools Password	Allows you to reset the DST security capabilities profile to the default password shipped with the system.
CHGPWD	Change Password	Allows a user to change the user's own password.
CHGUSRPRF	Change User Profile	Allows you to change the values specified in a user's profile, including the user's password.
CHKPWD	Check Password	Allows verification of 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 <sup>1</sup>	Create User Profile	When you add a user to the system, you assign a password to the user.

When a CRTUSRPRF is done, you can't 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, is the owner of an object on an independent ASP, or 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.

Table 132. Commands for Working with User Profiles

<b>Command Name</b>	Descriptive Name	Function
CHGPRF	Change Profile	Allows a user to change some of the attributes of the user's own profile.
CHGUSRAUD	Change User Audit	Allows you to specify the action and object auditing for a user profile.
CHGUSRPRF	Change User Profile	Allows you to 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.
СНКОВЛТС	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	Allows you to 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	Allows you to delete a user profile from the system. This command provides an option to delete or change ownership of objects owned by the user profile.
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.
DSPUSRPRF	Display User Profile command	Allows you to display a user profile in several different formats.
GRTUSRAUT	Grant User Authority	Allows you to copy private authorities from one user profile to another user profile.
PRTPRFINT	Print Profile Internals	Allows you to print a report of internal information about the number of entries.
PRTUSRPRF	Print User Profile	Allows you to 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	Allows you to work with user profiles by entering options on a list display.

Table 133. Related User Profile Commands

<b>Command Name</b>	Descriptive Name	Function
DSPPGMADP	Display Programs That Adopt	Allows you to display a list of programs and SQL packages that adopt a specified user profile.
RSTAUT	Restore Authority	Allows you to 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	Allows you to 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.

Table 134. Commands for Working with Auditing

<b>Command Name</b>	Descriptive Name	Function
CHGAUD	Change Auditing	Allows you to specify the auditing for an object.
CHGDLOAUD	Change Document Library Object Auditing	Allows you to specify whether access is audited for a document library object.
CHGOBJAUD	Change Object Auditing	Allows you to specify the auditing for an object.
CHGUSRAUD	Change User Audit	Allows you to specify the action and object auditing for a user profile.

Table 135. Commands for Working with Document Library Objects

<b>Command Name</b>	<b>Descriptive Name</b>	Function
ADDDLOAUT	Add Document Library Object Authority	Allows you to 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	Allows you to specify the object auditing level for a document library object.
CHGDLOAUT	Change Document Library Object Authority	Allows you to 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	Allows you to change the primary group for a document library object.
DSPAUTLDLO	Display Authorization List Document Library Objects	Allows you to 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	Allows you to display authority information for a document or a folder.
EDTDLOAUT	Edit Document Library Object Authority	Used to add, change, or remove users' authorities to a document or folder.

Table 135. Commands for Working with Document Library Objects (continued)

<b>Command Name</b>	Descriptive Name	Function
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	Used to 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.

Table 136. Commands for Working with Server Authentication Entries

<b>Command Name</b>	Descriptive Name	Function
ADDSVRAUTE	Add Server Authentication Entry	Allows you to add server authentication information for a user profile.
CHGSVRAUTE	Change Server Authentication Entry	Allows you to change existing server authentication entries for a user profile.
DSPSVRAUTE	Display Server Authentication Entries	Allows you to display server authentication entries for a user profile.
RMVSVRAUTE	Remove Server Authentication Entry	Allows you to 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.

Table 137. Commands for Working with the System Distribution Directory

<b>Command Name</b>	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.
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.
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.

Table 138. Commands for Working with Validation Lists

<b>Command Name</b>	Descriptive Name	Function
CRTVLDL	Create Validation List	Allows you to 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	Allows you to delete the specified validation list from a library.

Table 139. Commands for Working with Function Usage Information

<b>Command Name</b>	Descriptive Name	Function
CHGFCNUSG	Change function usage	Allows you to change the usage information for a registered function.
DSPFCNUSG	Display function usage	Allows you to display a list of function identifiers and the detailed usage information for a specific function.
WRKFCNUSG	Work with function usage	Allows you to display a list of function identifiers and change or display function usage information.

The following tables describe several different kinds of security tools. For more information about the security tools, see Appendix G, "Commands and Menus for Security Commands."

Table 140. Security Tools for Working with Auditing

<b>Command Name</b>	Descriptive Name	Function
CHGSECAUD	Change Security Auditing	Allows you to set up security auditing and to change the system values that control security auditing.
CPYAUDJRNE	Copy Audit Journal Entries	Allows you to 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	Display Audit Journal Entries	Allows you to 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	Allows you to display information about the security audit journal and the system values that control security auditing.

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 does support.

Table 141. Security Tools for Working with Authorities

<b>Command Name</b>	Descriptive Name	Function
PRTJOBDAUT	Print Job Description Authority	Allows you to 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	Allows you to print a list of objects of the specified type whose public authority is not *EXCLUDE.
PRTPVTAUT	Print Private Authorities	Allows you to print a list of private authorities for objects of the specified type.

Table 141. Security Tools for Working with Authorities (continued)

<b>Command Name</b>	Descriptive Name	Function
PRTQAUT	Print Queue Authority	Allows you 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.
PRTSBSDAUT	Print Subsystem Description Authority	Allows you to print a list of subsystem descriptions in a library that contains a default user in a subsystem entry.
PRTTRGPGM	Print Trigger Programs	Allows you to print a list of trigger programs that are associated with database files on your system.
PRTUSROBJ	Print User Objects	Allows you to print a list of the user objects (objects not supplied by IBM) that are in a library.

Table 142. Security Tools for Working with System Security

<b>Command Name</b>	Descriptive Name	Function
CHGSECA <sup>1</sup>	Change Security Attributes	Allows you to 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	Allows you to set security-relevant system values to their recommended settings. The command also sets up security auditing on your system.
CLRSVRSEC	Clear Server Security Data	Allows you to 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	Allows you to display the current and pending values of some system security attributes.
PRTCMNSEC	Print Communications Security	Allows you to print the security attributes of the *DEVD, *CTL, and *LIND objects on the system.
PRTSYSSECA	Print System Security Attributes	Allows you to 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	Allows you to set the public authority to *EXCLUDE for a set of security-sensitive commands on your system.

To use this command, you must have \*SECADM special authority.

For more information about tools and suggestions about how to use the security tools, see the *Tips for Making Your iSeries 400 Secure* book, GC41-0615.

# **Appendix B. IBM-Supplied User Profiles**

This appendix 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.

Table 143 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 144 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:

Table 144 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 iSeries system and poses a security exposure until it is changed. However, do **not** change any other values for IBM-supplied user profiles. Changing these profiles may 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 may cause system functions to fail.

Table 143. Default Values for User Profiles

	Default Values		
User Profile Parameter	IBM-Supplied User Profi	les Create User Profile Display	
Password (PASSWORD)	*NONE	*USRPRF <sup>4</sup>	
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)	*ALLOBJ¹ *SAVSYS¹	*USRCLS <sup>2</sup>	
Special environment (SPCENV)	*SYSVAL	*SYSVAL	
Display sign-on information (DSPSGNINF)	*SYSVAL	*SYSVAL	
Password expiration interval (PWDEXPITV)	*SYSVAL	*SYSVAL	
Limit device sessions (LMTDEVSSN)	*SYSVAL	*SYSVAL	

Table 143. Default Values for User Profiles (continued)

	Default Values		
User Profile Parameter	IBM-Supplied User Profiles	<b>Create User Profile Display</b>	
Keyboard buffering (KBDBUF)	*SYSVAL	*SYSVAL	
Maximum storage (MAXSTG)	*NOMAX	*NOMAX	
Priority limit (PTYLMT)	0	3	
Job description (JOBD)	QDFTJOBD	QDFTJOBD	
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	
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	
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	
Authority (AUT)	*EXCLUDE	*EXCLUDE	
Action auditing (AUDLVL) <sup>3</sup>	*NONE	*NONE	
Object auditing (OBJAUD) <sup>3</sup>	*NONE	*NONE	

- When the system security level is changed from level 10 or 20 to level 30 or above, this value is removed.
- When a user profile is automatically created at security level 10, the \*USER user class gives \*ALLOBJ and \*SAVSYS special authority.
- <sup>3</sup> Action and object auditing are specified using the CHGUSRAUD command.
- 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 in 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.

Table 144. IBM-Supplied User Profiles

Profile Name	Descriptive Name	Parameters Different from Default Values
QADSM	ADSM user profile	<ul> <li>USERCLS: *SYSOPR</li> <li>CURLIB: QADSM</li> <li>TEXT: ADSM profile used by ADSM server</li> <li>SPCAUT: *JOBCTL, *SAVSYS</li> <li>JOBD: QADSM/QADSM</li> <li>OUTQ: QADSM/QADSM</li> </ul>
QAFOWN	APD user profile	<ul> <li>USRCLS: *PGMR</li> <li>SPCAUT: *JOBCTL</li> <li>JOBD: QADSM/QADSM</li> <li>TEXT: Internal APD User Profile</li> </ul>
QAFUSR	APD user profile	TEXT: Internal APD User Profile
QAFDFTUSR	APD user profile	<ul> <li>INLPGM: *LIBL/QAFINLPG</li> <li>LMTCPB: *YES</li> <li>TEXT: Internal APD User Profile</li> </ul>
QAUTPROF	IBM authority user profile	
QBRMS	BRM user profile	
QCLUMGT	Cluster management profile	<ul><li>STATUS: *DISABLED</li><li>MSGQ: *NONE</li><li>ATNPGM: *NONE</li></ul>
QCLUSTER	High availability cluster profile	SPCAUT: *IOSYSCFG
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	<ul> <li>LMTCPB: *YES</li> <li>JOBD: QGPL/QBATCH</li> <li>DSPSGNINF: *NO</li> <li>LMTDEVSSN: *NO</li> <li>DLVRY: *HOLD</li> <li>SPCENV: *NONE</li> <li>ATNPGM: *NONE</li> </ul>
QDLFM	DataLink File Manager profile	• SRTSEQ: *HEX
QDOC	Document profile	• AUT: *CHANGE
QDSNX	Distributed systems node executive profile	<ul><li>PTYLMT: 3</li><li>CCSID: *HEX</li><li>SRTSEQ: *HEX</li></ul>

Table 144. IBM-Supplied User Profiles (continued)

Profile Name	<b>Descriptive Name</b>	Parameters Different from Default Values
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	<ul> <li>USRCLS: *SYSOPR</li> <li>INLMNU: *SIGNOFF</li> <li>SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG</li> <li>INLPGM: QSYS/QLPINATO</li> <li>DLVRY: *HOLD</li> <li>SEV: 99</li> </ul>
QLPINSTALL	Licensed program install profile	<ul> <li>USRCLS: *SYSOPR</li> <li>DLVRY: *HOLD</li> <li>SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG</li> </ul>
QMGTC	Management central profile	• JOBD: QSYS/QYPSJOBD
QMSF	Mail server framework profile	CCSID: *HEX     SRTSEQ: *HEX
QMQM	MQSeries <sup>®</sup> user profile	<ul> <li>USRCLS: *SECADM</li> <li>SPCAUT: *NONE</li> <li>PRTDEV: *SYSVAL</li> <li>TEXT: MQM user which owns the QMQM library</li> </ul>
QNFSANON	NFS user profile	
QNETSPLF	Network spooling profile	
QNETWARE	ECS user profile	STATUS: *DISABLED     TEXT: QFPNTWE USER PROFILE
QNTP	Network time profile	<ul><li>JOBD: QTOTNTP</li><li>JOBD LIBRARY: QSYS</li></ul>

Table 144. IBM-Supplied User Profiles (continued)

<b>Profile Name</b>	Descriptive Name	Parameters Different from Default Values
QOIUSER	OSI Communication Subsystem	<ul> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG</li> <li>CURLIB: QOSI</li> <li>MSGQ: QOSI/QOIUSER</li> <li>DLVRY: *HOLD</li> <li>OUTQ: *DEV</li> <li>PRTDEV: *SYSVAL</li> <li>ATNPGM: *NONE</li> <li>CCSID: *HEX</li> <li>TEXT: Internal OSI Communication Subsystem User Profile</li> </ul>
QOSIFS	OSI File Server User Profile	<ul> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *JOBCTL, *SAVSYS</li> <li>OUTQ: *DEV</li> <li>CURLIB: *QOSIFS</li> <li>CCSID: *HEX</li> <li>TEXT: Internal OSI File Services User Profile</li> </ul>
QPGMR	Programmer profile	<ul> <li>USRCLS: *PGMR</li> <li>SPCAUT: *ALLOBJ <sup>1</sup> *SAVSYS *JOBCTL</li> <li>PTYLMT: 3</li> <li>ACGCDE: *BLANK</li> </ul>
QPEX	Performance Explorer user profile	<ul><li>PTYLMT: 3</li><li>ATNPGM: *SYSVAL</li><li>TEXT: IBM-supplied User Profile</li></ul>
QPM400	IBM Performance Management for eServer <sup>™</sup> iSeries (PM iSeries)	SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Parts and projects owner user profile	<ul> <li>STATUS: *DISABLED</li> <li>CURLIB: QADM</li> <li>TEXT: User profile of parts and projects owner</li> </ul>
QRDARSADM	R/DARS user profile	<ul><li>INLMNU: *SIGNOFF</li><li>TEXT: R/DARS Administration Profile</li></ul>
QRDAR	R/DARS owning profile	<ul> <li>USRCLS: *PGMR</li> <li>INLMNU: *SIGNOFF</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile</li> </ul>
QRDARS4001	R/DARS owning profile 1	<ul> <li>INLMNU: *SIGNOFF</li> <li>GRPPRF: QRDARS400</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile 1</li> </ul>

Table 144. IBM-Supplied User Profiles (continued)

Profile Name	Descriptive Name	Parameters Different from Default Values	
QRDARS4002	R/DARS owning profile 2	<ul> <li>INLMNU: *SIGNOFF</li> <li>GRPPRF: QRDARS400</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile 2</li> </ul>	
QRDARS4003	R/DARS owning profile 3	<ul> <li>INLMNU: *SIGNOFF</li> <li>GRPPRF: QRDARS400</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile 3</li> </ul>	
QRDARS4004	R/DARS owning profile 4	<ul> <li>INLMNU: *SIGNOFF</li> <li>GRPPRF: QRDARS400</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile 4</li> </ul>	
QRDARS4005	R/DARS owning profile 5	<ul> <li>INLMNU: *SIGNOFF</li> <li>GRPPRF: QRDARS400</li> <li>OUTQ: *DEV</li> <li>TEXT: R/DARS-400 owning profile 5</li> </ul>	
QRMTCAL	Remote Calendar user profile	• TEXT: OfficeVision® Remote Calendar User	
QRJE	Remote job entry profile	USRCLS: *PGMR  SPCAUT: *ALLOBJ 1 *SAVSYS 1 *JOBCTL	
QSECOFR	Security officer profile	<ul> <li>PWDEXP: *YES</li> <li>USRCLS: *SECOFR</li> <li>SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG</li> <li>UID: 0</li> <li>PASSWORD: QSECOFR</li> </ul>	
QSNADS	SNA distribution services profile	• CCSID: *HEX • SRTSEQ: *HEX	
QSOC	OptiConnect user profile	<ul> <li>USRCLS: *SYSOPR</li> <li>CURLIB: *QSOC</li> <li>SPCAUT: *JOBCTL</li> <li>MSGQ: QUSRSYS/QSOC</li> </ul>	
QSPL	Spool profile		
QSPLJOB	Spool job profile	• AUT: *USE	
QSRV	Service profile	<ul> <li>USRCLS: *PGMR</li> <li>SPCAUT: *ALLOBJ ¹, *SAVSYS ¹, *JOBCTL, *SERVICE</li> <li>ASTLVL: *INTERMED</li> <li>ATNPGM: QSYS/QSCATTN</li> </ul>	
QSRVAGT	Service Agent user profile		

Table 144. IBM-Supplied User Profiles (continued)

Profile Name	Descriptive Name	Parameters Different from Default Values
QSRVBAS	Service basic profile	<ul> <li>USRCLS: *PGMR</li> <li>SPCAUT: *ALLOBJ <sup>1</sup> *SAVSYS <sup>1</sup> *JOBCTL</li> <li>ASTLVL: *INTERMED</li> <li>ATNPGM: QSYS/QSCATTN</li> </ul>
QSVCCS	CC Server user profile	<ul> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *JOBCTL</li> <li>SPCENV: *SYSVAL</li> <li>TEXT: CC Server User Profile</li> </ul>
QSVCM	Client Management Server user profile	• TEXT: Client Management Server User Profile
QSVSM	ECS user profile	<ul> <li>USRCLS: *SYSOPR</li> <li>STATUS: *DISABLED</li> <li>SPCAUT: *JOBCTL</li> <li>SPCENV: *SYSVAL</li> <li>TEXT: SystemView System Manager User Profile</li> </ul>
QSVSMSS	Managed System Service user profile	<ul> <li>STATUS: *DISABLED</li> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *JOBCTL</li> <li>SPCENV: *SYSVAL</li> <li>TEXT: Managed System Service User Profile</li> </ul>
QSYS	System profile	<ul> <li>USRCLS: *SECOFR</li> <li>SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG</li> </ul>
QSYSOPR	System operator profile	<ul> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *ALLOBJ ¹, *SAVSYS, *JOBCTL</li> <li>INLMNU: SYSTEM</li> <li>LIBRARY: *LIBL</li> <li>MSGQ: QSYSOPR</li> <li>DLVRY: *BREAK</li> <li>SEV: 40</li> </ul>
QTCM	Triggered cache manager profile	STATUS: *DISABLED
QTCP	Transmission control protocol (TCP) profile	<ul> <li>USRCLS: *SYSOPR</li> <li>SPCAUT: *JOBCTL</li> <li>CCSID: *HEX</li> <li>SRTSEQ: *HEX</li> </ul>
QTFTP	Trivial File Transfer Protocol	
QTMPLPD	Transmission control protocol/Internet protocol (TCP/IP) printing support profile	• PTYLMT: 3 • AUT: *USE

Table 144. IBM-Supplied User Profiles (continued)

Profile Name	Descriptive Name	Parameters Different from Default Values
QTMPLPD	Remote LPR user profile	<ul><li>JOBD: QGPL/QDFTJOBD</li><li>PWDEXPITV: *NOMAX</li><li>MSGQ: QTCP/QTMPLPD</li></ul>
QTMTWSG	HTML Workstation Gateway Profile user profile	MSGQ: QUSRSYS/QTMTWSG     TEXT: HTML Workstation Gateway Profile
QTMHHTTP	HTML Workstation Gateway Profile user profile	MSGQ: QUSRSYS/QTMHHTTP     TEXT: HTTP Server Profile
QTMHHTP1	HTML Workstation Gateway Profile user profile	MSGQ: QUSRSYS/QTMHHTTP     TEXT: HTTP Server CGI Profile
QTSTRQS	Test request profile	
QUMB	Ultimedia System Facilities user profile	
QUMVUSER	Ultimedia Business Conferencing user profile	
QUSER	Workstation user profile	• PTYLMT: 3
QX400	OSI Messages Services File Services User Profile	<ul> <li>CURLIB: *QX400</li> <li>USRCLS: *SYSOPR</li> <li>MSGQ: QX400/QX400</li> <li>DLVRY: *HOLD</li> <li>OUTQ: *DEV</li> <li>PRTDEV: *SYSVAL</li> <li>ATNPGM: *NONE</li> <li>CCSID: *HEX</li> <li>TEXT: Internal OSI Messages Services User Profile</li> </ul>
QYCMCIMOM	Server user profile	
QYPSJSVR	Management Central Java Server profile	
QYPUOWN	Internal APU user profile	TEXT: Internal APU — User profile

# **Appendix C. Commands Shipped with Public Authority \*EXCLUDE**

Table 145 identifies which commands have restricted authorization (public authority is \*EXCLUDE) when your system is shipped. It shows what IBM-supplied user profiles are authorized to use these restricted commands. For more information about IBM-supplied user profiles, see the topic "IBM-Supplied User Profiles" on page 108.

In Table 145, commands that are restricted to the security officer, and any user profile with \*ALLOBJ authority, have an  $\bf R$  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  $\bf S$  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 301.

If you choose to grant other users or the public \*USE authority to these commands, update this table to indicate that commands are no longer restricted on your system. Using some commands may require the authority to certain objects on the system as well as to the commands themselves. See Appendix D, "Authority Required for Objects Used by Commands," on page 301 for the object authorities required for commands.

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
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				
ADDIMGCLGE	R				
ADDMFS	R				
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZPFRDTA	R				
ANZPGM	R				
ANZPRB		S	S	S	S
ANZPRFACT	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				
CHGCLUCFG	R				
CHGCLUNODE	R				
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDSTPWD <sup>1</sup>	R				
CHGDSTQ		S	S		
CHGDSTRTE		S	S		
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
СНGGPHPKG	R				
 CHGIMGCLG	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

<b>Command Name</b>	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGIMGCLGE	R				
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	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	
CHGS34LIBM	R				
CHKASPBAL	R				
CHKCMNTRC				S	
CHKPRDOPT		S	S	S	S
CPHDTA	R				
CPYFCNARA	R				
CPYGPHFMT	R				
СРҮСРНРКС	R				
CPYPFRDTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CRTADMDMN	R				
CRTAUTHLR	R				
CRTBESTMDL	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

<b>Command Name</b>	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CRTCLS	R				
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTIMGCLG	R				
CRTJOBD	R				
CRTNWSCFG	R				
CRTPFRDTA	R				
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	R				·
CRTQSTLOD	R				
CRTSBSD		S	S		
CRTUDFS	R				
CRTUDFS	R				
CRTVLDL	R				
CVTBASSTR	R				
CVTBASUNF	R				
CVTBGUDTA	R				
CVTDIR	R				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36CFG	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS36QRY	R				
CVTS38JOB	R				
CVTTCPCL		S	S	S	S
DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DLTGPHPKG	R				
DLTHSTDTA	R				
DLTIMGCLG	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
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
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPSYSOBJ		S	S	S	S
DMPTRC	R	S		S	
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMFSINF	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				
DSPPFRDTA	R				
DSPPFRGPH	R				
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
DSPUDFS	R				
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ENCTOMSTK	R				
ENDASPBAL	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDHOSTSVR		S	S	S	S
ENDIDXMON	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				
ENDMGDSYS		S	S	S	S
ENDMGRSRV		S	S	S	S
ENDMSF			S	S	S
ENDNFSSVR	R		S	S	S
ENDPEX		S		S	
ENDPFRTRC	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		
INSPTF <sup>3</sup>				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
 INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

<b>Command Name</b>	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
LODIMGCLG	R				
LODOPTFMW	R				
LODPTF				S	
LODQSTDB	R				
MGRS36	R				
MGRS36APF	R				
MGRS36CBL	R				
MGRS36DFU	R				
MGRS36DSPF	R				
MGRS36ITM	R				
MGRS36LIB	R				
MGRS36MNU	R				
MGRS36MSGF	R				
MGRS36QRY	R				
MGRS36RPG	R				
MGRS36SEC	R				
MGRS38OBJ	R				
MIGRATE	R				
PKGPRDDST		S	S	S	S
PRTACTRPT	R				
PRTCMNTRC				S	
PRTCPTRPT	R				
PRTJOBRPT	R				
PRTJOBTRC	R				
PRTLCKRPT	R				
PRTPOLRPT	R				
PRTRSCRPT	R				
PRTSYSRPT	R				
PRTTNSRPT	R				
PRTTRCRPT	R				
PRTDSKINF	R				
PRTERRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	R				
PWRDWNSYS	R		S		
RCLDBXREF	R				
RCLOBJOWN	R				
RCLOPT	R				
RCLSPLSTG		S	S	S	S
RCLSTG		S	S	S	S

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
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				
RMVCLUNODE	R				
RMVCRGDEVE	R				
RMVCRGNODE	R				
RMVCRSDMNK	R				
RMVDEVDMNE	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVEXITPGM	R				
RMVIMGCLGE	R				
RMVJRNCHG		S		S	
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 <sup>4</sup>					
RSTCFG	R				
RSTDLO	R				·
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ <sup>4</sup>					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

Command Name	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RSTUSFCNR <sup>5</sup>					
RSTUSRPRF	R				
RTVDSKINF	R				
RTVIMGCLG	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				
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
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				
STRBEST	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJOBTRC	R				
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF <sup>2</sup>			S	S	S

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

<b>Command Name</b>	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
STRNFSSVR	R				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	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
VFYIMGCLG	R				
VFYLNKLPDA		S	S	S	S
VFYMSTK	R				
VFYPIN	R				
VFYPRT		S	S	S	S
VFYTAP		S	S	S	S
WRKCNTINF				S	S
WRKDEVTBL	R				
WRKDPCQ		S	S		
WRKDSTQ		S	S		
WRKFCNARA	R				
WRKIMGCLGE	R				
WRKJRN		S	S	S	
WRKLIB					

Table 145. Authorities of IBM-Supplied User Profiles to Restricted Commands (continued)

<b>Command Name</b>	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
WRKLIBPDM					
WRKLICINF	R				
WRKNWSCFG	R				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
WRKTRC	R				
WRKTXTIDX	R				
WRKUSRTBL	R				
WRKWCH	R				

The CHGDSTPWD command is shipped with public authority \*USE, but you must be signed on as QSECOFR to use this command.

<sup>&</sup>lt;sup>2</sup> The QMSF user profile is also authorized to this command.

<sup>&</sup>lt;sup>3</sup> QSRV can only run this command if an IPL is not being done.

In addition to QSYS, user profile QRDARS400 has authority.

In addition to QSYS, user profile QUMB has authority.

# Appendix D. Authority Required for Objects Used by Commands

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

The tables are organized in alphabetical order according to object type. In addition, tables are included for items that are not i5/OS objects (jobs, spooled files, network attributes, and system values) and for some functions (device emulation and finance). Additional considerations (if any) for the commands are included as footnotes to the table.

Following are descriptions of the columns in the tables:

### **Referenced Object**

The objects listed in the *Referenced Object* column are objects to which the user needs authority when using the command.

# **Authority Required for Object**

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

# **Authority Required for Library**

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

Table 146. Description of Authority Types

Authority	Name	Functions Allowed			
Object Authorities:					
*OBJOPR	Object Operational	Look at the description of an object. Use the object as determined by the user's data authorities.			
*OBJMGT	Object Management	Specify the security for the object. Move or rename the object. All functions defined for *OBJALTER and *OBJREF.			
*OBJEXIST	Object Existence	Delete the object. Free storage of the object. Perform save and restore operations for the object <sup>1</sup> . 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.			

#### **Authority Required for Library**

Table 146. Description of Authority Types (continued)

Authority	Name	Functions Allowed			
*OBJREF	Object Reference	Specify a database file as the parent in a referential constraint. For example, you want to define a rule that a customer record must exist in the CUSMAS file before an order for the customer can be added to the CUSORD file. You need *OBJREF authority to the CUSMAS file to define this rule.			
*AUTLMGT	Authorization List Management	Add and remove users and their authorities from the authorization list <sup>2</sup> .			
Data Authorities:					
*READ	Read	Display the contents of the object, such as viewing records in a file.			
*ADD	Add	Add entries to an object, such as adding messages to a message queue or adding records to a file.			
*UPD	Update	Change the entries in an object, such as changing records in a file.			
*DLT	Delete	Remove entries from an object, such as removing messages from a message queue or deleting records from a file.			
*EXECUTE	Execute	Run a program, service program, or SQL package. Locate an object in a library or a directory.			
	save system (*SAVSYS) special a ore operations on the object.	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 may show system-defined subsets of these authorities. The following table shows the subsets of object authorities and data authorities.

Table 147. System-Defined Authority

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

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

Table 148. System-Defined Authority

Authority	*RWX	*RW	*RX	*R	*WX	* <b>W</b>	*X
Object Authoritie	es X	X	X	X	X	X	X

Refer to the iSeries Security Reference for more information.

Table 148. System-Defined Authority (continued)

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

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

### **Command Usage Assumptions**

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

# **General Rules for Object Authorities on Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
Change (CHG) with F4 (Prompt) <sup>7</sup>	Current values	The current values are displayed if the user has authority to those values.	*EXECUTE
Command accessing	Directories in path prefix	*X	
object in directory	Directory when pattern is specified (* or ?)	*R	
Creating object in	Directories in path prefix	*X	
directory	Directory to contain new object	*WX	
Copy (CPY) where	Object to be copied	*OBJOPR, *READ	*EXECUTE
to-file is a database file	CRTPF command, if CRTFILE (*YES) is specified	*OBJOPR	*EXECUTE
	To-file, if CRTFILE (*YES) is specified <sup>1</sup>		*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

### **Rules for Object Authorities on Commands**

		Authority	y Needed
Command	Referenced Object	For Object	For Library
Create (CRT)	Object to be created <sup>2</sup>		*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	Object to be created (and replaced) <sup>2</sup>	*OBJMGT, *OBJEXIST, *READ <sup>5</sup>	*READ, *ADD
specified <sup>6, 9</sup>	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	Object to be displayed	*USE	*EXECUTE
operation using output file	Output file, if file does not exist <sup>3</sup>		*ADD, *EXECUTE
(OUTPUT(*OUTFILE))	Output file, if file exists and new member is added and *REPLACE option specified and member did not previously exist	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Output file, if file exists and new member is added and *ADD option specified and member did not previously exist	OBJOPR, *OBJMGT or *OBJALTER, *ADD	*ADD, *EXECUTE
	Output file, if file and member exist and *ADD option is specified	*OBJOPR, *ADD	*EXECUTE
	Output file, if file and member exist and *REPLACE option is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*EXECUTE
	Format file (QAxxxxx), if output file does not exist	*OBJOPR	
Display (DSP) using	Object to be displayed	*USE	*EXECUTE
*PRINT or Work (WRK) using *PRINT	Output queue <sup>4</sup>	*READ	*EXECUTE
(vvivis) using 1 iviivi	Printer file (QPxxxxx in QSYS)	*USE	*EXECUTE
Save (SAV) or other	Device description	*USE	*EXECUTE
operation using device description	Device file associated with device description, such as QSYSTAP for the TAP01 device description	*USE	*EXECUTE

		Authority Needed		
Command	Referenced Object	For Object	For Library	

- 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.
- 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.
- The user profile running the display command becomes the owner of the newly created output file, unless the user is a member of a group profile and has OWNER(\*GRPPRF). If the user's profile specifies OWNER(\*GRPPRF), the group profile becomes the owner of the output file. Public authority to the output file is controlled by the CRTAUT parameter of the output file library.
- If the output queue is defined as OPRCTL (\*YES), a user with \*JOBCTL special authority does not need any authority to the output queue. A user with \*SPLCTL special authority does not need any authority to the output queue.
- For device files, \*OBJOPR authority is also required.
- 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.
- Authority to the corresponding (DSP) command is also required.
- The \*UPDADD option in only available on the MBROPT parameter of the CPYF command.
- This does not apply to the REPLACE parameter on the CRTJVAPGM command.

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

Table 149. Common commands for most objects

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
ALCOBJ 1,2,11	Object	*OBJOPR	*EXECUTE
ANZUSROBJ 20			
CHGOBJAUD 18	ASP Device (if specified)	*USE	
CHGOBJD <sup>3</sup>	Object, if it is a file	*OBJOPR, *OBJMGT	*EXECUTE
	Object, if it is not a file	*OBJMGT	*EXECUTE
CHGOBJOWN 3,4	Object	*OBJEXIST	*EXECUTE
	Object (if file, library, subsystem description)	*OBJOPR, *OBJEXIST	*EXECUTE
	Object (if *AUTL)	Ownership or *ALLOBJ	*EXECUTE
	Old user profile	*DLT	*EXECUTE
	New user profile	*ADD	*EXECUTE
	ASP Device (if specified)	*USE	

Table 149. Common commands for most objects (continued)

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGOBJPGP <sup>3</sup>	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 <sup>3</sup>	Object	Authority specified by AUT parameter <sup>14</sup>	*EXECUTE
CPROBJ	Object	*OBJMGT	*EXECUTE
CHKOBJITG <sup>11</sup> (Q)			
CRTDUPOBJ 3,9,11,21	New object		*USE, *ADD
	Object being copied, if it is an *AUTL	*AUTLMGT	*USE, *ADD
	Object being copied, all other types	*OBJMGT, *USE	*USE
	CRTSAVF command (if the object is a save file)	*OBJOPR	
	ASP Device (if specified)	*USE	
DCPOBJ	Object	*USE	*EXECUTE
DLCOBJ 1,11	Object	*OBJOPR	*EXECUTE
DMPOBJ (Q) <sup>3</sup>	Object	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Object	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT <sup>3</sup>	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	
DSPOBJD <sup>2, 28</sup>	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	

Table 149. Common commands for most objects (continued)

		Authority Needed	
Command	Referenced Object	For Object	For Library
GRTOBJAUT 3,5,6,15	Object	*OBJMGT	*EXECUTE
	Object (if file)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, if used to secure object	Not *EXCLUDE	
	ASP Device (if specified)	*USE	
	Reference ASP Device (if specified)	*EXECUTE	
	Reference object	*OBJMGT or Ownership	*EXECUTE
MOVOBJ 3,7,12	Object	*OBJMGT	
	Object (if *FILE)	*ADD, *DLT, *EXECUTE	
	Object (not *FILE),	*DLT, *EXECUTE	
	From-library		*CHANGE
	To-library		*READ, *ADD
	ASP Device (if specified)	*USE	
PRTADPOBJ <sup>26</sup> (Q)			
PRTPUBAUT <sup>26</sup>			
PRTUSROBJ <sup>26</sup>			
PRTPVTAUT <sup>26</sup>			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Object	*OBJMGT	*EXECUTE
RNMOBJ 3,11	Object	*OBJMGT	*UPD, *EXECUTE
	Object, if *AUTL	*AUTLMGT	*EXECUTE
	Object (if *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	ASP Device (if specified)	*USE	
RSTOBJ 3,13 (Q)	Object, if it already exists in the library	*OBJEXIST <sup>8</sup>	*EXECUTE, *ADD
	Object, if it is *CFGL, *CNNL, *CTLD, *DEVD, *LIND, or *NWID	*CHANGE and *OBJMGT	*EXECUTE
	Media definition	*USE	*EXECUTE
	Message queues being restored to library where they already exist	*OBJOPR, *OBJEXIST	*EXECUTE, *ADD
	User profile owning objects being created	*ADD <sup>8</sup>	
	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 <sup>8</sup>	
	Save file	*USE	*EXECUTE
	1	I .	-1

Table 149. Common commands for most objects (continued)

		Authorit	ty Needed
Command	Referenced Object	For Object	For Library
RSTOBJ <sup>3,13</sup> (Q)	Tape unit, diskette unit or optical unit	*USE	*EXECUTE
	Tape (QSYSTAP) file or diskette (QSYSDKT) file	*USE <sup>8</sup>	*EXECUTE
	Optical File (OPTFILE) <sup>22</sup>	*R	Not applicable
	Parent Directory of optical file (OPTFILE) <sup>22</sup>	*X	Not applicable
	Path prefix of OPTFILE <sup>22</sup>	*X	Not applicable
	Optical volume <sup>24</sup>	*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
	ASP device description <sup>25</sup>	*USE	
RSTSYSINF	Save file	*USE	*EXECUTE
	Tape unit, diskette unit or optical unit	*USE	*EXECUTE
	Optical File (OPTFILE) <sup>22</sup>	*R	N/A
	Parent Directory of optical file (OPTFILE) <sup>22</sup>	*X	N/A
	Path prefix of OPTFILE <sup>22</sup>	*X	N/A
	Optical volume <sup>24</sup>	*USE	N/A
RVKPUBAUT <sup>20</sup>	Tape (QSYSTAP) file or diskette (QSYSDKT) file	*USE <sup>8</sup>	*EXECUTE
RTVOBJD <sup>2, 29</sup>	Object	Some authority other than *EXCLUDE	*EXECUTE
RVKOBJAUT 3,5,15, 27	Path prefix of OPTFILE <sup>22</sup>	*X	Not applicable
	Optical volume <sup>24</sup>	*USE	Not applicable
	QSYS/QPSRLDSP printer output, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	ASP Device (if specified)	*USE	
SAVCHGOBJ <sup>3</sup>	Object (8)	*OBJEXIST	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Save active message queue	*OBJOPR, *ADD	*EXECUTE
	Command user space, if specified	*USE	*EXECUTE

Table 149. Common commands for most objects (continued)

		Authori	ity Needed
Command	Referenced Object	For Object	For Library
SAVCHGOBJ <sup>3</sup>	Optical File (OPTFILE) <sup>22</sup>	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) <sup>22</sup>	*WX	Not applicable
	Path prefix of optical file (OPTFILE) <sup>22</sup>	*X	Not applicable
	Root Directory (/) of optical volume <sup>22, 23</sup>	*RWX	Not applicable
	Optical volume <sup>24</sup>	*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 <sup>8</sup>	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE <sup>8</sup>	*EXECUTE
	ASP device description <sup>25</sup>	*USE	
SAVOBJ <sup>3</sup>	Object	*OBJEXIST <sup>8</sup>	*EXECUTE
	Media definition	*USE	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Save active message queue	*OBJOPR, *ADD	*EXECUTE
	Command user space, if specified	*USE	*EXECUTE
SAVOBJ <sup>3</sup>	Optical File (OPTFILE) <sup>22</sup>	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) <sup>22</sup>	*WX	Not applicable
	Path prefix of OPTFILE <sup>22</sup>	*X	Not applicable
	Root directory (/) of optical volume <sup>22, 23</sup>	*RWX	Not applicable
	Optical volume <sup>24</sup>	*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 <sup>8</sup>	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE <sup>8</sup>	*EXECUTE
	ASP device description <sup>25</sup>	*USE	
SAVSTG 10			
SAVSYS 10	Tape unit, optical unit	*USE	*EXECUTE
	Root directory (/) of optical volume <sup>22</sup>	*RWX	Not applicable
	Optical volume <sup>24</sup>	1	1

Table 149. Common commands for most objects (continued)

		Authority Needed	
Command	Referenced Object	For Object	For Library
SAVSYSINF	Media definition	*USE	*EXECUTE
	Tape unit, diskette unit, optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*OBJMGT, *USE, *ADD	*EXECUTE
	Optical File (OPTFILE) <sup>22</sup>	*RW	N/A
	Parent Directory of optical file (OPTFILE) <sup>22</sup>	*WX	N/A
	Path prefix of OPTFILE <sup>22</sup>	*X	N/A
	Root directory (/) of optical volume <sup>22, 23</sup>	*RWX	N/A
	Optical volume <sup>24</sup>	*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 <sup>25</sup>	*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 <sup>25</sup>	*USE	
SETOBJACC	Object	*OBJOPR	*EXECUTE
STROBJCVN (Q) <sup>30</sup>			
WRKOBJ 19	Object	Any authority	*USE
WRKOBJLCK	Object		*EXECUTE
	ASP Device	*EXECUTE	
WRKOBJOWN <sup>17</sup>	User profile	*READ	*EXECUTE
WRKOBJPGP <sup>17</sup>	User profile	*READ	*EXECUTE
WRKOBJPVT <sup>17</sup>	User profile	*READ	*EXECUTE

See the OBJTYPE keyword of the ALCOBJ command for the list of object types that can be allocated and deallocated.

Some authority to the object (other than \*EXCLUDE) is required.

This command cannot be used for documents or folders. Use the equivalent Document Library Object (DLO) command.

You must have \*ALLOBJ and \*SECADM special authority to change the object owner of a program, service program, or SQL package that adopts authority.

You must be the owner or have \*OBJMGT authority and the authorities being granted or revoked.

Table 149. Common commands for most objects (continued)

		Authority Needed	
Command	Referenced Object	For Object	For Library

- You must be the owner or have \*ALLOBJ special authority to grant \*OBJMGT or \*AUTLMGT authority.
- This command cannot be used for user profiles, controller descriptions, device descriptions, line descriptions, documents, document libraries, and folders.
- If you have \*SAVSYS special authority, you do not need the authority specified.
- If the user running the CRTDUPOBJ command has OWNER(\*GRPPRF) in his user profile, the owner of the new object is the group profile. To successfully copy authorities to a new object owned by the group profile, the following applies:
  - The user running the command must have authority to the from-object. Authorities can be obtained from adopted authority or through the group profile.
  - · If an error occurs while copying authorities to the new object, the newly created object is deleted.
- You must have \*SAVSYS special authority.
- This command cannot be used for journals and journal receivers.
- 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.
- You must have \*ALLOBJ special authority to specify a value other than \*NONE for the Allow object differences (ALWOBJDIF) parameter.
- 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.
- To secure an object with an authorization list or remove the authorization list from the object, you must do one of the following actions:
  - · Own the object.
  - · Have \*ALL authority to the object.
  - · Have \*ALLOBJ special authority.
- If either the original file or the renamed file has an associated authority holder, \*ALL authority to the authority holder is required.
- This command does not support the QOPT file system.
- You must have \*AUDIT special authority.
- To use an individual operation, you must have the authority required by the individual operation.
- You must have \*ALLOBJ special authority.
- All authorities on the from-object are duplicated to the new object. The primary group of the new object is determined by the group authority type (GRPAUTTYP) field in the user profile that is running the command. If the from-object has a primary group, the new object may not have the same primary group, but the authority that the primary group has on the from-object will be duplicated to the new object.
- This authority check is only made when the Optical media format is Universal Disk Format.
- This authority check is only made if you are clearing the optical volume.
- 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.
- Authority required only if save or restore operation requires a library namespace switch.

Table 149. Common commands for most objects (continued)

				Authority	y Needed
	Comma	nd	Referenced Object	For Object	For Library
	You must have *ALLOBJ or *AUDIT special authority to use this command.				
	*** Security Risk *** Revoking all authorities specifically given to a user for an object can result in the u having more authority than before the revoke operation. If a user has *USE authority for and object and *CHANGE authority on the authorization list that secures the object, revoking *USE authority results in tuser having *CHANGE authority to the object.				for and object and
   	28		e either *ALLOBJ or *AUDIT special authority nerwise, the value *NOTAVL is displayed to inc		
	29		e either *ALLOBJ or *AUDIT special authority e value *NOTAVL is returned to indicate that the		
 	30		GM, CHGSRVPGM, and CHGMOD command vice programs, and modules.	s to determine the author	ority needed to convert

### **Access Path Recovery Commands: Authorities Required**

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

These commands do not require object authorities.

		Aut	ıthority Needed	
Command	Referenced Object	For Object	For Library	
CHGRCYAP 1 (Q)	ASP Device (if specified)	*USE		
DSPRCYAP <sup>1</sup>	ASP Device (if specified)	*USE		
EDTRBDAP <sup>2</sup> (Q)				
EDTRCYAP 1 (Q)	ASP Device (if specified)	*USE		
You must have	re *JOBCTL special authority to use this comma	and.		
You must have	re *ALLOBJ special authority to use this comma	and.		

## **Advanced Function Presentation (AFP) Commands: Authorities** Required

		Authority Needed	
Command	Referenced Object	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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTFNTTBL	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
DLTFNTTBL	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
DSPFNTTBL	DBCS font table	*USE	*EXECUTE
RMVFNTTBLE	DBCS font table	*CHANGE	*EXECUTE
WRKFNTRSC <sup>1</sup>	Font resource	*USE	*USE
WRKFORMDF <sup>1</sup>	Form definition	*USE	*USE
WRKOVL 1	Overlay	*USE	*USE
WRKPAGDFN 1	Page definition	Any authority	*USE
WRKPAGSEG <sup>1</sup>	Page segment	*USE	Any authority

AF\_INET Sockets over SNA Commands: Authorities Required

Commands identified by (Q) are shipped with public authority \*EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant \*USE authority to others. These commands do not require any authority to objects:

These commands do not require any authority to objects:

#### **AF\_INET Sockets Over SNA Commands**

ADDIPSIFC <sup>1</sup>	CHGIPSIFC <sup>1</sup>	CVTIPSLOC	RMVIPSLOC <sup>1</sup>		
ADDIPSRTE <sup>1</sup>	CHGIPSLOC <sup>1</sup>	ENDIPSIFC (Q)	RMVIPSRTE <sup>1</sup>		
ADDIPSLOC <sup>1</sup>	CHGIPSTOS <sup>1</sup>	PRTIPSCFG	STRIPSIFC (Q)		
CFGIPS	CVTIPSIFC	RMVIPSIFC <sup>1</sup>			
You must ha	You must have *IOSYSCFG special authority to use this command.				

# **Alerts: Authorities Required**

		Autl	hority Needed	
Command	Referenced Object	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 <sup>1</sup>	Physical file QAALERT	*USE	*EXECUTE	
WRKALRD <sup>1</sup>	Alert table	*USE	*EXECUTE	
WRKALRTBL <sup>1</sup>	Alert table	*READ	*USE	
<sup>1</sup> To use indiv	To use individual operations, you must have the authority required by the individual operation.			

# **Application Development Commands: Authorities Required**

		Authority Needed	
Command	Referenced Object	For Object	For Library
FNDSTRPDM	Source part	*READ	*EXECUTE
MRGFORMD	Form description	*READ	*EXECUTE
STRAPF <sup>1</sup>	Source file	*OBJMGT, *CHANGE	*READ, *ADD
	Commands CRTPF, CRTLF, ADDPFM, ADDLFM, and RMVM	*USE	*EXECUTE
STRBGU <sup>1</sup>	Chart	*OBJMGT, *CHANGE	*EXECUTE

### **Application Development Commands**

Command STRDFU <sup>1</sup>	Referenced Object Program (if create program option)	For Object	For Library
STRDFU <sup>1</sup>	Program (if create program option)		J
			*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 <sup>1</sup>			
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 <sup>1</sup>	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 <sup>1, 4</sup>			
WRKMBRPDM <sup>1</sup>	Source file	*USE	*EXECUTE
WRKOBJPDM <sup>1</sup>	File	*READ or Ownership	*EXECUTE

To use the individual operations, you must have the authority required by the individual operation.

<sup>&</sup>lt;sup>2</sup> A group corresponds to a library.

<sup>&</sup>lt;sup>3</sup> A project consists of one or more groups (libraries).

This command requires \*ALLOBJ special authority.

### **Authority Holder Commands: Authorities Required**

		Authority Needed	
Command	Referenced Object	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: Authorities Required**

	Referenced Object	Authority Needed	
Command		For Object	For QSYS Library
ADDAUTLE 1	*AUTL	*AUTLMGT or ownership	*EXECUTE
CHGAUTLE <sup>1</sup>	*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 <sup>1</sup>	*AUTL	*AUTLMGT or ownership	*EXECUTE
RMVAUTLE <sup>1</sup>	*AUTL	*AUTLMGT or ownership	*EXECUTE
RTVAUTLE <sup>2</sup>	*AUTL	*AUTLMGT or ownership	*EXECUTE
WRKAUTL 3,4,5	*AUTL		

You must be the owner or have authorization list management authority and have the authorities being given or taken away.

- You must not be excluded (\*EXCLUDE) from the authorization list.
- Some authority to the authorization list is required.

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.

To use an individual operation, you must have the authority required by the operation.

# **Binding Directory Commands: Authorities Required**

		Authority Needed	
Command	Referenced Object	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 <sup>1</sup>	Binding directory	Any authority	*USE
WRKBNDDIRE <sup>1</sup>	Binding directory	*READ, *OBJOPR	*USE
<sup>1</sup> To use indi	vidual operations, you must have the	authority required by the operati	ion.

# **Change Request Description Commands**

		Authority Needed	
Command	Referenced Object	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
RMVCRQDA	Change request description	*CHANGE	*EXECUTE
WRKCRQD <sup>1</sup>	Change request description		*EXECUTE

To use an individual operation, you must have the authority required by the operation.

### **Chart Commands**

		Aut	hority Needed
Command	Referenced Object	For Object	For Library
DLTCHTFMT	Chart format	*OBJEXIST	*EXECUTE
DSPCHT	Chart format	*USE	*USE
	Database file	*USE	*USE

#### **Chart Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
DSPGDF	Database file	*USE	*USE
STRBGU (Option 3) <sup>2</sup>	Chart format	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT <sup>1</sup>	Chart format	Any authority	*USE

To use an individual operation, you must have the authority required by the operation.

### **Class Commands**

		Authori	Authority Needed	
Command	Referenced Object	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	

To use an individual operation, you must have the authority required by the operation.

### **Class-of-Service Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGCOSD <sup>3</sup>	Class-of-service description	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD <sup>3</sup>	Class-of-service description		
DLTCOSD	Class-of-service description	*OBJEXIST	*EXECUTE
DSPCOSD	Class-of-service description	*USE	*EXECUTE
WRKCOSD 1,2	Class-of-service description	*OBJOPR	*EXECUTE

To use individual operations, you must have the authority required by the individual operation.

#### **Cluster Commands**

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

		<b>Authority Needed</b>	
Command	Referenced Object	For Object	For Library
ADDCLUNODE (Q) <sup>1</sup>	QCSTCTL service program	*USE	

Option 3 on the BGU menu (shown when STRGBU is run) is the Change chart format option.

<sup>2</sup> Some authority to the object is required.

To use this command, you must have \*IOSYSCFG special authority.

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDCRGDEVE (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
ADDCRGNODE (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
	Distribute information user queue	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q) <sup>1</sup>	QCSTDD service program	*USE	
CHGCLUCFG (Q) <sup>1</sup>	QCSTCTL2 service program	*USE	
CHGCLUNODE (Q) <sup>1</sup>	QCSTCTL service program	*USE	
CHGCLURCY	Cluster resource group	*USE	
		*JOBCTL	
		*SERVICE or Service Trace function	
CHGCLUVER (Q) <sup>1</sup>	QCSTCTL2 service program	*USE	
CHGCRG (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
CHGCRGDEVE (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
CHGCRGPRI (Q) <sup>1</sup>	QCSTCRG2 service program	*USE	
	Cluster Resource Group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Vary configuration (VFYCFG) command	*USE	

#### **Cluster Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTADMDMN (Q) <sup>1, 3</sup>	QCLUSTER user profile	*USE	
CRTCLU (Q) <sup>1</sup>	QCSTCTL service program	*USE	
CRTCRG (Q) 1	QCSTCRG1 service program	*USE	
	Cluster resource group library		*OBJOPR, *ADD, *READ (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
	Distribute information user queue	*OBJOPR, *ADD	*EXECUTE
	Failover message queue	*OBJOPR, *ADD	*EXECUTE
DLTADMDMN (Q) 1	Cluster resource group	*OBJEXIST, *USE	
	QUSRSYS	*EXECUTE	
	QCLUSTER	*USE	
DLTCLU (Q) <sup>1</sup>	QCSTCTL service program	*USE	
DLTCRG <sup>1</sup>	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCRGCLU (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster resource group	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
DMPCLUTRC	Cluster resource group	*USE	
		*SERVICE or Service Trace function	
DSPCLUINF			
DSPCRGINF	Cluster resource group	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q) <sup>1</sup>	QCSTCTL service program	*USE	
ENDCHTSVR (Q)	Authorization list	*CHANGE	
ENDCRG (Q) <sup>1</sup>	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE (QUSRSYS)
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
RMVCLUNODE (Q) <sup>1</sup>	QCSTCTL service program	*USE	
RMVCRGDEVE (Q) <sup>1</sup>	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	

		Authority Needed	
Command	Referenced Object	For Object	For Library
RMVCRGNODE (Q) 1	QCSTCRG1 service program	*USE	
	Cluster resource group	*CHANGE, *OBJEXIST	*EXECUTE
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
RMVDEVDMNE (Q) <sup>1</sup>	QCSTDD service program	*USE	
STRCHTSVR	Authorization list	*CHANGE	
STRCLUNOD (Q) <sup>1</sup>	QCSTCTL service program	*USE	
STRCRG (Q) <sup>1</sup>	QCSTCRG2 service program	*USE	
	Cluster resource group	*CHANGE	*EXECUTE
	Exit program	*EXECUTE <sup>2</sup>	*EXECUTE <sup>2</sup>
	User profile to run exit program	*USE	
	Device description	*USE, *OBJMGT	
WRKCLU <sup>4</sup>	Cluster resource group	*USE	*EXECUTE

You must have \*IOSYSCFG special authority to use this command.

## Command (\*CMD) Commands

		Authority Needed	
Command	Referenced Object	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

The authority applies to calling user profile and user profile to run exit program.

The calling user profile is granted \*CHANGE and \*OBJEXIST authority to the cluster resource group.

You must have \*SERVICE special authority or be authorized to the Service Trace Function of the operating system through Application Administration in iSeries 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

		Authority Needed	
Command	Referenced Object	For Object	For Library
GENCMDDOC <sup>3</sup>	Command	*USE	*EXECUTE
	Panel group (associated)	*USE	*EXECUTE
	Output file: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Command	*OBJOPR	*EXECUTE
	DDM file	*USE	*EXECUTE
SLTCMD <sup>1</sup>	Command	Any authority	*USE
WRKCMD <sup>2</sup>	Command	Any authority	*USE

Ownership or some authority to the object is required.

### **Commitment Control Commands**

		Autho	rity Needed
Command	Referenced Object	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			

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**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGCSI	Communications side information object	*USE, *OBJMGT	*EXECUTE
	Device description <sup>1</sup>	*CHANGE	
CRTCSI	Communications side information object		*READ, *ADD
	Device description <sup>1</sup>	*CHANGE	
DLTCSI	Communications side information object	*OBJEXIST	*EXECUTE

<sup>2</sup> To use individual operations, you must have the authority required by the individual operation.

<sup>3</sup> 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.

		Authority Needed	
Command	Referenced Object	For Object	For Library
DSPCSI	Communications side information object	*READ	*EXECUTE
WRKCSI	Communications side information objects	*USE	*EXECUTE
<sup>1</sup> Authority is verified when the communications side information object is used.			

# **Configuration Commands**

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

	Referenced Object	Authority Needed	
Command		For Object	For Library
PRTDEVADR	Controller description (CTL)	*USE	*EXECUTE
	Device description	*USE	*EXECUTE
RSTCFG (Q) <sup>5</sup>	Every object being restored over by a saved version	*OBJEXIST <sup>1</sup>	*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 <sup>2</sup>	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 <sup>4</sup>	Object	*OBJOPR	*EXECUTE

#### **Configuration Commands**

	Authority Neede		Authority Needed	
Command	Referenced Object	For Object	For Library	
If you have *SAVSYS special authority, you do not need the authority specified.				
? You	You must have *SAVSYS special authority.			
If a	If a user has *JOBCTL special authority, authority to the object is not needed.			
To u	To use the individual operations, you must have the authority required by the individual operation.			
You must have *ALLOBJ special authority to specify a value other than *NONE for the Allow object differences (ALWOBJDIF) parameter, or RESETSYS(*YES).				
	must have *IOSYSCFG special authority when the ol. OCATE or *DEALLOCATE.	bject is a media li	brary and the status is	

You must have \*IOSYSCFG and \*SECADM special authorities to specify GENPTHCERT(\*YES).

## **Configuration List Commands**

		Authori	ty Needed
Command	Referenced Object	For Object	For Library
ADDCFGLE <sup>2</sup>	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL <sup>2</sup>	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE <sup>2</sup>	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL <sup>2</sup>	Configuration list	*USE, *OBJMGT	*ADD
CRTCFGL <sup>2</sup>	Configuration list		
DLTCFGL	Configuration list	*OBJEXIST	*EXECUTE
DSPCFGL <sup>2</sup>	Configuration list	*USE, *OBJMGT	*EXECUTE
RMVCFGLE <sup>2</sup>	Configuration list	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL 1, 2	Configuration list	*OBJOPR	*EXECUTE

To use the individual operations, you must have the authority required by the individual operation.

### **Connection List Commands**

		Aut	Authority Needed	
Command	Referenced Object	For Object	For Library	
DLTCNNL	Connection list	*OBJEXIST	*EXECUTE	
DSPCNNL	Connection list	*USE	*EXECUTE	
WRKCNNL 1	Connection list	*OBJOPR	*EXECUTE	

To use the individual operations, you must have the authority required by the individual operation.

To use this command, you must have \*IOSYSCFG special authority.

# **Controller Description Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGCTLAPPC <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CHGCTLNET <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
	Line description (SWTLINLST)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP <sup>2</sup>	Controller description	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS <sup>2</sup>	Controller	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLASC <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLBSC <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLFNC <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		

#### **Controller Description Commands**

		Au	thority Needed
Command	Referenced Object	For Object	For Library
CRTCTLHOST <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLLWS <sup>2</sup>	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 <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLRWS <sup>2</sup>	Line description (LINE or SWTLINLST)	*USE	*EXECUTE
	Device description (DEV)	*USE	*EXECUTE
	Connection list (CNNLSTOUT)	*USE	*EXECUTE
	Controller description		
CRTCTLTAP <sup>2</sup>	Device description (DEV)	*USE	*EXECUTE
	Controller description		
CRTCTLVWS <sup>2</sup>	Device description (DEV)	*USE	*EXECUTE
	Controller description		
DLTCTLD	Controller description	*OBJEXIST	*EXECUTE
DSPCTLD	Controller description	*USE	*EXECUTE
ENDCTLRCY	Controller description	*USE	*EXECUTE
PRTCMNSEC <sup>3</sup>			
RSMCTLRCY	Controller description	*USE	*EXECUTE
WRKCTLD <sup>1</sup>	Controller description	*OBJOPR	*EXECUTE

To use the individual operations, you must have the authority required by the individual operation.

# **Cryptography Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE

<sup>2</sup> To use this command, you must have \*IOSYSCFG special authority.

To use this command, you must have \*ALLOBJ and \*IOSYSCFG, or \*AUDIT special authority.

### **Cryptography Commands**

		Author	rity Needed
Command	Referenced Object	For Object	For Library
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE
CPHDTA (Q)			
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGENX *FILE	*OBJOPR, *READ	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	QHST message queue	*OBJOPR, *ADD	*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	QHST message queue	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE

### **Data Area Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGDTAARA 1	Data area	*CHANGE	*EXECUTE
CRTDTAARA 1	Data area		*READ, *ADD
	APPC device description <sup>4</sup>	*CHANGE	
DLTDTAARA	Data area	*OBJEXIST	*EXECUTE
DSPDTAARA	Data area	*USE	*EXECUTE
RTVDTAARA <sup>2</sup>	Data area	*USE	*EXECUTE
WRKDTAARA <sup>3</sup>	Data area	Any authority	*USE

#### **Data Area Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library

- If the create and change data area commands are run using high-level language functions, these authorities are still required although authority to the command is not.
- 2 Authority is verified at run time, but not at compilation time.
- To use an individual operation, you must have the authority required by the operation.
- Authority is verified when the data area is used.

#### **Data Queue Commands**

		Authority Needed		Authority Needed
Command	Referenced Object	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 <sup>2</sup>	*CHANGE		
DLTDTAQ	Data queue	*OBJEXIST	*EXECUTE	
WRKDTAQ 1	Data queue	*READ	*USE	

To use individual operations, you must have the authority required by the individual operation.

# **Device Description Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CFGDEVMLB <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGDEVAPPC <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Mode description (MODE)	*USE	*EXECUTE
CHGDEVASC <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVCRP <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Printer (PRINTER)	*USE	*EXECUTE
CHGDEVFNC <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE

Authority is verified when the data area is used.

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGDEVNET <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNWSH <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVOPT <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPRT <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
	Validation list (if specified)	*READ	*EXECUTE
CHGDEVRTL <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNUF <sup>4</sup>	Device description	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP <sup>4</sup>	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 <sup>4</sup>	Device description		*EXECUTE
CRTDEVDKT 4	Device description		*EXECUTE
CRTDEVDSP <sup>4</sup>	Printer description (PRINTER)	*USE	*EXECUTE
	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVFNC 4	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVHOST <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVINTR <sup>4</sup>	Device description		
CRTDEVMLB <sup>4</sup>	Device description		*EXECUTE
CRTDEVNET <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVNWSH <sup>4</sup>	Device description		*EXECUTE
CRTDEVOPT <sup>4</sup>	Device description		*EXECUTE
CRTDEVPRT <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
	Device description		
	Validation list (if specified)	*READ	*EXECUTE
CRTDEVRTL <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
	Device description		
CRTDEVSNPT <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
	Device description		

#### **Device Description Commands**

	Authority Ne		hority Needed	
- 0	Command	Referenced Object	For Object	For Library
(	CRTDEVSNUF 4	Controller description (CTL)	*USE	*EXECUTE
		Device description		
(	CRTDEVTAP <sup>4</sup>	Controller description (CTL)	*USE	*EXECUTE
		Device description		
]	DLTDEVD <sup>1</sup>	Device description	*OBJEXIST	*EXECUTE
	DSPASPSTS	Device description	*USE	
]	DSPCNNSTS	Device description	*OBJOPR	*EXECUTE
[]	DSPDEVD	Device description	*USE	*EXECUTE
[]	ENDASPBAL (Q)			
]	ENDDEVRCY	Device description	*USE	*EXECUTE
]	HLDCMNDEV <sup>2</sup>	Device description	*OBJOPR	*EXECUTE
[]	PRTCMNSEC 4, 5			
	RLSCMNDEV	Device description	*OBJOPR	*EXECUTE
]	RSMDEVRCY	Device description	*USE	*EXECUTE
	SETASPGRP <sup>6</sup>	All device descriptions in ASP group	*USE	
		All the specified libraries in the library list before the library name space and the library list are changed	*USE	
	STRASPBAL (Q)			
	TRCASPBAL (Q)			
7	WRKDEVD <sup>3</sup>	Device description	*OBJOPR	*EXECUTE

To remove an associated output queue, object existence (\*OBJEXIST) authority to the output queue and read (\*READ) authority to the QUSRSYS library are required.

- To use individual operations, you must have the authority required by the individual operation.
- You must have \*IOSYSCFG special authority to run this command.
- You must have \*ALLOBJ special authority to run this command.
- 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 listed in your user profile and execute (\*EXECUTE) authority to the library where the job description is located.

#### **Device Emulation Commands**

		Authority Needed	
Command	Referenced Object	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

You must have job control (\*JOBCTL) special authority and object operational authority to the device description.

		Au	Authority Needed		
Command	Referenced Object	For Object	For Library		
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		
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**

These commands do not require any object authorities:					
ADDDIRE <sup>2</sup> ADDDIRSHD <sup>1</sup> CHGSYSDIRA <sup>2</sup> CHGDIRE <sup>3</sup>	CHGDIRSHD <sup>1</sup> CPYFRMDIR <sup>1</sup> CPYTODIR <sup>1</sup> DSPDIRE	ENDDIRSHD <sup>4</sup> RMVDIRE <sup>1</sup> RMVDIRSHD <sup>1</sup> RNMDIRE <sup>2</sup>	STRDIRSHD <sup>4</sup> WRKDIRE <sup>3,5</sup> WRKDIRLOC <sup>1,5</sup> WRKDIRSHD <sup>1,5</sup>		

You must have \*SECADM special authority.

You must have \*SECADM or \*ALLOBJ special authority.

A user with \*SECADM special authority can work with all directory entries. Users without \*SECADM special authority can work only with their own entries.

You must have \*JOBCTL special authority.

To use an individual operation, you must have the authority required by the operation.

#### **Disk Commands**

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

These commands do not	require authority to any obje	cts:	
ENDDSKRGZ (Q) 1	STRDSKRGZ (Q) 1	WRKDSKSTS	
1 To use this com	nand, you must have *ALLC	BJ special authority.	

## **Display Station Pass-through Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ENDPASTHR			
STRPASTHR	APPC device on source system	*CHANGE	*EXECUTE
	APPC device on target system	*CHANGE	*EXECUTE
	Virtual controller on target system <sup>1</sup>	*USE	*EXECUTE
	Virtual device on target system 1,2	*CHANGE	*EXECUTE
	Program specified in the QRMTSIGN system value on target system, if any <sup>1</sup>	*USE	*USE
TFRPASTHR			

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.

#### **Distribution Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			

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.

		Au	thority Needed
Command	Referenced Object	For Object	For Library
CHGDSTD <sup>1</sup>	Document <sup>2</sup>	*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)			
RMVDSTQ (Q)			
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST 1	Requested file or document	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			

If the user is asking for distribution for another user, the user must have the authority to work on behalf of the other user.

### **Distribution List Commands**

These commands de	o not require any object au	thorities:			
ADDDSTLE <sup>1</sup> CHGDSTL <sup>1</sup>	CRTDSTL DLTDSTL <sup>1</sup>	DSPDSTL RMVDSTLE <sup>1</sup>	RNMDSTL <sup>1</sup> WRKDSTL <sup>2</sup>		
You must have *SECADM special authority or own the distribution list.					
To use an individual operation, you must have the authority required by the operation.					

# **Document Library Object Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDDLOAUT	Document library object	*ALL or owner	*EXECUTE
CHGDLOAUD 1			
CHGDLOAUT	Document library object	*ALL or owner	*EXECUTE

When the Distribution is filed.

### **Document Library Object Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
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 <sup>2</sup>	Document description	*CHANGE	*EXECUTE	
CHKDLO <sup>2</sup>	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 <sup>3</sup>	Document library object	*ALL	*EXECUTE	
DLTDOCL <sup>20</sup>	Document list	*ALL <sup>4</sup>	*EXECUTE	
DMPDLO 15				
DSPAUTLDLO	Authorization list	*USE	*EXECUTE	
	Document library object	*USE	*EXECUTE	
DSPDLOAUD <sup>21</sup>	Output file, if specified	Refer to the general rules.	Refer to the general rules.	
DSPDLOAUT	Document library object	*USE or owner	*EXECUTE	
DSPDLONAM <sup>22</sup>	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 <sup>2</sup>	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	

		Authority Needed	
Command	Referenced Object	For Object	For Library
MRGDOC <sup>5</sup>	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
PRTDOC	Folder	*USE	*EXECUTE
	Document	*USE	*EXECUTE
	DLTPF, DLTF, and DLTOVR commands, if an <i>INDEX</i> instruction is specified	*USE	*EXECUTE
	CRTPF, OVRPRTF, 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 <sup>2,6</sup>	Requested file	*USE	*EXECUTE
	Document list, if it exists	*CHANGE	*EXECUTE
RCLDLO	Document library object		
	Internal documents or all documents and folders <sup>16</sup>		
RGZDLO	Document library object	*CHANGE or owner	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY), or DLO(*ALL) FLR(*ANY) MAIL(*YES) <sup>16</sup>		
RMVDLOAUT	Document library object	*ALL or owner	*EXECUTE
RNMDLO	Document library object	*ALL	*EXECUTE
	In-folder	*CHANGE	*EXECUTE
RPLDOC <sup>2</sup>	Requested file	*READ	*EXECUTE
	Document	*CHANGE	*EXECUTE
RSTDLO (Q) <sup>7, 8, 9</sup>	Document library object, if replacing	*ALL <sup>10</sup>	*EXECUTE
	Parent folder, if new DLO	*CHANGE <sup>10</sup>	*EXECUTE
	Owning user profile, if new DLO	*ADD <sup>10</sup>	*EXECUTE
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	Save file	*USE	*EXECUTE
	Optical file (OPTFILE) <sup>17</sup>	*R	Not applicable
	Path prefix of optical file (OPTFILE) <sup>17</sup>	*X	Not applicable
	Optical volume <sup>19</sup>	*USE	Not applicable
	Tape, diskette, and optical unit	*USE	*EXECUTE

#### **Document Library Object Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
RSTS36FLR 11,12,14	S/36 folder	*USE	*EXECUTE
	To-folder	*CHANGE	*EXECUTE
	Device file or device description	*USE	*EXECUTE
RTVDLONAM <sup>22</sup>	Document library object	*USE	*EXECUTE
RTVDOC <sup>2</sup>	Document if checking out	*CHANGE	*EXECUTE
	Document if not checking out	*USE	*EXECUTE
	Requested file	*CHANGE	*EXECUTE
SAVDLO 7,13	Document library object	*ALL <sup>10</sup>	*EXECUTE
	Tape unit, diskette unit, and optical unit	*USE	*EXECUTE
	Save file, if empty	*USE, *ADD	*EXECUTE
	Save file, if records exist in it	*USE, *ADD, *OBJMGT	*EXECUTE
	Output file, if specified	Refer to the general rules.	Refer to the general rules.
	Optical File (OPTFILE) <sup>17</sup>	*RW	Not applicable
	Parent directory of optical file (OPTFILE) <sup>17</sup>	*WX	Not applicable
	Path Prefix of optical file (OPTFILE) <sup>17</sup>	*X	Not applicable
	Root Directory (/) of volume <sup>17, 18</sup>	*RWX	Not applicable
	Optical Volume <sup>19</sup>	*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	

- You must have \*AUDIT special authority.
- If the user is working on behalf of another user, the other user's authority to the object is checked.
- 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.
- If you have \*ALLOBJ or \*SECADM special authority, you do not need all \*ALL authority to the document library list.
- 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.
- 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.
- You must have \*SAVSYS, \*ALLOBJ special authority, or have been enrolled in the system distribution directory.
- You must have \*SAVSYS or \*ALLOBJ special authority to use the following parameter combination: RSTDLO DLO(\*MAIL).
- You must have \*ALLOBJ special authority to specify a value other than \*NONE for the Allow object differences (ALWOBJDIF) parameter.
- If you have \*SAVSYS or \*ALLOBJ special authority, you do not need the authority specified.

				Auth	ority Needed
	Comma	nd	Referenced Object	For Object	For Library
	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	SAVDLO E SAVDLO E SAVDLO E	e *SAVSYS or *ALLOBJ special authority to use DLO(*ALL) FLR(*ANY) DLO(*MAIL) DLO(*CHG) DLO(*SEARCH) OWNER(not *CURRENT)	e the following para	nmeter combinations:
ı	14			the source folder is	a dagument folder
	15	You must be enrolled in the system distribution directory if the source folder is a document folder.  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 H	Format is Universal	Disk Format (UDF).
	18	This authority	check is only made when you are clearing the	e optical volume.	
	19		es are not actual system objects. The link between the volume is maintained by the optical s		ame and the authorization
	20		e *ALLOBJ special authority when OWNER (*Approfile as the caller.	ALL) or OWNER (n	ame) and Name is a
1	21	You must have	e all object (*ALLOBJ) or audit (*AUDIT) speci	al authority to use t	this command.
	22		e all object (*ALLOBJ) special authority to use at is to be located.	this command when	n specifying *DST for the

# **Double-byte Character Set Commands**

		Authority Needed	
Command	Referenced Object	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

### **Double-Byte Character Set Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
STRFMA	DBCS font table, if copy-to option specified	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	DBCS font table, if copy-from option specified	*OBJOPR, *READ	*EXECUTE
	Font management aid work file (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

# **Edit Description Commands**

		Auth	Authority Needed	
Command	Referenced Object	For Object	For Library	
CRTEDTD	Edit description		*EXECUTE, *ADD	
DLTEDTD	Edit description	*OBJEXIST	*EXECUTE	
DSPEDTD	Edit description	*OBJOPR	*EXECUTE	
WRKEDTD <sup>1</sup>	Edit description	Any authority	*USE	
To use an individual operation, you must have the authority required by the operation.				

### **Environment Variable Commands**

These commands do not require any object authorities.				
ADDENVVAR <sup>1</sup>	CHGENVVAR 1	RMVENVVAR <sup>1</sup>	WRKENVVAR <sup>1</sup>	
To update system-level environment variables, you need *JOBCTL special authority.				

# **Extended Wireless LAN Configuration Commands**

		Au	Authority Needed	
Command	Referenced Object	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	

#### **Extended Wireless LAN Configuration Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
RMVEWCPTCE	Source file	*USE	*EXECUTE

### **File Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
ADDLFM	Logical file	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE, *ADD
	File referenced in DTAMBRS parameter, when logical file is keyed	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE
	File referenced in DTAMBRS parameter, when logical file is not keyed	*OBJOPR	*EXECUTE
ADDPFCST	Dependent file, if TYPE(*REFCST) is specified	*OBJMGT or *OBJALTER	*EXECUTE
	Parent file, if TYPE(*REFCST) is specified	*OBJMGT or *OBJREF	*EXECUTE
	File, if TYPE(*UNQCST) or TYPE(*PRIKEY) is specified	*OBJMGT	*EXECUTE
ADDPFM	Physical file	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Physical file, to insert trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Physical file, to delete trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Physical file, to update trigger	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Trigger program	*EXECUTE	*EXECUTE
CHGDDMF	DDM file	*OBJOPR, *OBJMGT	*EXECUTE
	Device description <sup>7</sup>	*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

		Authori	ty Needed
Command	Referenced Object	For Object	For Library
CHGICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Logical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGLFM	Logical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPF	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFCST	Dependent file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFM	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPFTRG	Physical file	*OBJMGT or *OBJALTER	*EXECUTE
CHGPRTF	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
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

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
CPYFRMQRYF <sup>1</sup>	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	*X, *ADD	*X
	Target database file, if MBROPT(*REPLACE) specified	*X, *ADD, *DLT, *OBJMGT	*X
	Target database file, if new member created	*X, *OBJMGT, *ADD	*X, *ADD
	Conversion table *TBL used to translate data	*OBJOPR	*X
	Target save file exists	*RX, *ADD, *OBJMGT	*X
	Target save file is created		*RX, *ADD
CPYFRMTAP	From-file	*OBJOPR, *READ	*EXECUTE
	To-file (device file)	*OBJOPR, *READ	*EXECUTE
	To-file (physical file)	Refer to 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.
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	
	Conversion table *TBL used to translate data	*OBJOPR	*X
СРҮТОТАР	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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTDDMF	DDM file: REPLACE(*NO)		*READ, *ADD
	DDM file: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD
	Device description <sup>7</sup>	*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
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 REFACCPTH keywords	*OBJOPR	*EXECUTE
	Tables specified in the ALTSEQ keyword	*OBJOPR	*EXECUTE
	Logical file		*EXECUTE, *ADD
	File referenced in DTAMBRS parameter, when logical file is keyed	*OBJOPR, *OBJMGT or *OBJALTER	*EXECUTE
	File referenced in DTAMBRS parameter, when logical file is not keyed	*OBJOPR	*EXECUTE
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

		Authority Needed	
Command	Referenced Object	For Object	For Library
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
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 <sup>2</sup>	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

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
EDTCPCST	Data area, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*CHANGE	*EXECUTE
	Files, as specified on NFYOBJ keyword for the associated STRCMTCTL command.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
INZPFM	Physical file, when RECORD(*DFT) is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD	*EXECUTE
	Physical file, when RECORD(*DLT) is specified	*OBJOPR, *OBJMGT or *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Target file	*CHANGE, *OBJMGT	*CHANGE
	Maintenance file	*USE	*EXECUTE
	Root file	*USE	*EXECUTE
OPNDBF	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
OPNQRYF	Database file	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
PRTTRGPGM 11			
RGZPFM	File containing member	*OBJOPR, *OBJMGT or *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	ICF file	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	File containing member	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPFCST	File	*OBJMGT or *OBJALTER	*EXECUTE
RMVPFTRG	Physical file	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	File containing member	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F <sup>4</sup> (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

		Authority Needed	
Command	Referenced Object	For Object	For Library
SAVSAVFDTA	Tape, diskette, or optical device description	*USE	*EXECUTE
	Save file	*USE	*EXECUTE
	Optical Save/Restore File <sup>8</sup> (if previously exists)	*RW	Not applicable
	Parent Directory of OPTFILE <sup>8</sup>	*WX	Not applicable
	Path Prefix of OPTFILE <sup>8</sup>	*X	Not applicable
	Root Directory (/) of Optical Volume <sup>8,9</sup>	*RWX	Not applicable
	Optical Volume <sup>10</sup>	*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 <sup>3</sup>	Source file	*OBJMGT, *CHANGE	*READ, *ADD
	Commands CRTPF, CRTLF, ADDPFM, ADDLFM, and RMVM	*USE	*EXECUTE
STRDFU <sup>3</sup>	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
WRKDDMF <sup>3</sup>	DDM file	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF 3,5	Files	*OBJOPR	*USE
WRKPFCST <sup>3</sup>			*EXECUTE
	ı	_1	1

The CPYFRMQRYF command uses a FROMOPNID parameter rather than a FROMFILE parameter. A user must have sufficient authority to perform the OPNQRYF command before running the CPYFRMQRYF command. If CRTFILE(\*YES) is specified on the CPYFRMQRYF command, the first file specified on the corresponding OPNQRYF FILE parameter is considered to be the from-file when determining the authorities for the new to-file.

- Ownership or operational authority to the file is required.
- To use individual operations, you must have the authority required by the individual operation.
- 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.
- Some authority to the object is required.

			Au	Authority Needed	
C	ommand	Referenced Object	For Object	For Library	
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).				

- 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.
- You must have \*ALLOBJ or \*AUDIT special authority to use this command.

#### **Filter Commands**

		Auth	ority Needed
Command	Referenced Object	For Object	For Library
ADDALRACNE	Filter	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filter	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filter	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filter	*USE, *ADD	*EXECUTE
CHGALRACNE	Filter	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filter	*USE, *UPD	*EXECUTE
CHGFTR	Filter	*OBJMGT	*EXECUTE
CHGPRBACNE	Filter	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filter	*USE, *UPD	*EXECUTE
CRTFTR	Filter		*READ, *ADD
DLTFTR	Filter	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filter	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filter	*USE, *DLT	*EXECUTE
WRKFTR 1	Filter	Any authority	*EXECUTE
WRKFTRACNE <sup>1</sup>	Filter	*USE	*EXECUTE
WRKFTRSLTE 1	Filter	*USE	*EXECUTE

### **Finance Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
SBMFNCJOB (Q)	Job description and message queue <sup>1</sup>	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Job description and message queue <sup>1</sup>	*OBJOPR	*EXECUTE

		Authority Needed		
Command	Referenced Object	For Object	For Library	
WRKDEVTBL (Q)	Device description <sup>1</sup>	At least one data authority	*EXECUTE	
WRKPGMTBL (Q)				
WRKUSRTBL (Q)				
The QFNC user profile must have this authority.				

# i5/OS Graphical Operations

		Auth	ority Needed
Command	Referenced Object	For Object	For Library
CHGFCNUSG <sup>5</sup>			
DSPFCNUSG			
EDTWSOAUT	Workstation object <sup>1</sup>	*OBJMGT <sup>2,3,4</sup>	*EXECUTE
GRTWSOAUT	Workstation object <sup>1</sup>	*OBJMGT <sup>2,3,4</sup>	*EXECUTE
RVKWSOAUT	Workstation object <sup>1</sup>	*OBJMGT <sup>2,3,4</sup>	*EXECUTE
SETCSTDTA	Copy-from user profile	*CHANGE	*EXECUTE
	Copy-to user profile	*CHANGE	*EXECUTE
WRKFCNUSG			

The workstation object is an internal object that is created when you install the i5/OS Graphical Operations feature. It is shipped with public authority of \*USE.

Own the workstation object.

Have \*ALL authority to the workstation object.

Have \*ALLOBJ special authority.

You must have security administrator (\*SECADM) special authority to change the usage of a function.

# **Graphics Symbol Set Commands**

		Authority Needed		
Command	Referenced Object	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	

Ownership or some authority to the object is required.

You must be the owner or have \*OBJMGT authority and the authorities being granted or revoked.

You must be the owner or have \*ALLOBJ authority to grant \*OBJMGT or \*AUTLMGT authority.

To secure the workstation object with an authorization list or remove the authorization list, you must have one of the following authorities:

#### **Host Server Commands**

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

These commands do not require object authorities.	
ENDHOSTSVR (Q)	STRHOSTSVR (Q)

# **Image Catalog Commands**

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

			Author	ity Needed
Command	Referenced Object	Object Type	For Object	For Library <sup>1</sup>
ADDIMGCLGE (Q)	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	*X	
	Device name when FROMDEV specified	*DEVD	*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 (Q)	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 (Q)	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the	general rules
CRTIMGCLG (Q)	QUSRSYS	*LIB		*READ, *AD
	Image catalog if DIR(*REFIMGCLG) specified	*IMGCLG	*USE	*OBJOPR, *READ, *AD *EXECUTE
	Image catalog directory path prefix <sup>2</sup>	*DIR	Refer to the	general rules
DLTIMGCLG (Q)	Image catalog	*IMGCLG	*OBJEXIST	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the	general rules
LODIMGCLG (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
	Image catalog when WRTPTC(*ALL) or WRTPTC(*NONE) is specified	*IMGCLG	*CHANGE	*EXECUTE
	Virtual device	*DEVD	*USE	
	Image catalog directory path prefix	*DIR	Refer to the	general rules
LODIMGCLGE (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the	general rules

C
R
R
V
ν
ν

			Authority Needed	
Command	Referenced Object	Object Type	For Object	For Library <sup>1</sup>
RMVIMGCLGE (Q)	Image catalog	*IMGCLG	*CHANGE	*EXECUTE
	Image catalog directory path prefix	*DIR	Refer to the g	general rules
RTVIMGCLG (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
	Device description if DEV parameter specified	*DEVD	*USE	
VFYIMGCLG (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
	Virtual device	*DEVD	*USE	
	Image catalog directory path prefix	*DIR	Refer to the general rules	
WRKIMGCLG (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE (Q)	Image catalog	*IMGCLG	*USE	*EXECUTE
			•	•

The library that image catalog objects reside in is QUSRSYS.

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

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
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 ge	neral rules.	1

If a directory is created, you also need write (\*W) authority to the directory to contain the new directory.

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
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
	*DİSKSTGOPT, *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 <sup>26</sup>	*DIR and *STMF	QOpenSys, "root" (/), UDFS	
	Object when setting the following attributes: *SETUID, *SETGID, *RSTDRNMUNL	Any	All except QSYS.LIB and QDLS	Ownership <sup>15</sup>
	*CRTOBJAUD <sup>28</sup>			
	Path prefix <sup>28</sup>	Refer to the gen	eral rules.	
CHGAUD <sup>4</sup>				
CHGAUT	Object	All	QOpenSys, "root" (/), UDFS	Ownership <sup>15</sup>
			QSYS.LIB, QOPT <sup>11</sup>	Ownership or *ALLOBJ
			QDLS	Ownership, *ALL, or *ALLOBJ
				*OBJMGT
	Optical volume	*DDIR	QOPT <sup>8</sup>	*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 <sup>8</sup>	*X
	Path prefix	Refer to the gen	eral rules.	

	Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
	CHGOWN <sup>24</sup>	Object	All	QSYS.LIB	*OBJEXIST
			*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
			All	QOpenSys, "root" (/), UDFS	Ownership and *OBJEXIST <sup>15</sup>
			All	QDLS	Ownership or *ALLOBJ
				QOPT <sup>11</sup>	Ownership or *ALLOBJ
	CHGOWN <sup>24</sup>	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 <sup>8</sup>	*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 <sup>5, 15</sup>
			All	QDLS	Ownership or *ALLOBJ
				QOPT <sup>11</sup>	Ownership or *ALLOBJ
	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 <sup>8</sup>	*CHANGE
		Directory that contains objects when SUBTREE(*ALL) is specified	Any directory or library	All	*RX

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
CHKIN	Object, if the user who checked it out.	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Object, if not the user who checked it out.	*STMF	QOpenSys, "root" (/), UDFS	*ALL or *ALLOBJ or Ownership
		*DOC	QDLS	*ALL or *ALLOBJ or Ownership
	Path, if not the user who checked out	*DIR	QOpenSys, "root" (/), UDFS	*X
	Path prefix	Refer to the ge	neral rules.	,
CHKOUT	Object	*STMF	QOpenSys, "root" (/), UDFS	*W
		*DOC	QDLS	*W
	Path prefix	Refer to the general rules.		
CPY <sup>25</sup>	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 <sup>11</sup>	*R
	Destination object when REPLACE(*YES) specified (if destination object already exists)	Any	All <sup>10</sup>	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT <sup>11</sup>	*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

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
CPY <sup>25</sup>	Path (target), parent directory of destination object	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR QDLS *RW	*RWX	
		*DDIR	QOPT <sup>11</sup>	*WX
	Source Optical volume	*DDIR	QOPT <sup>8</sup>	*USE
	Target Optical volume	*DDIR	QOPT <sup>8</sup>	*CHANGE
CPY <sup>25</sup>	Parent directory of origin object	*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR	QDLS	*X
		Others	QSYS.LIB	*RX
		*DDIR	QOPT <sup>11</sup>	*X
	Path prefix (target destination)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, "root" (/), UDFS	*X
		*FLR QDLS	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
	Path prefix (origin object)	*DDIR	QOPT <sup>11</sup>	*X
CRTDIR <sup>21, 22</sup>	Parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Any		*ADD
		*DDIR	QOPT <sup>11</sup>	*WX
CRTDIR	Path prefix	Refer to the ge	neral rules.	
	Optical volume	*DDIR	QOPT <sup>8</sup>	*CHANGE
CVTDIR (Q) <sup>16</sup>				
DSPAUT	Object	All	QDLS	*ALL
		All	All others	*OBJMGT or ownership
		ALL	QOPT <sup>11</sup>	None
	Optical volume	*DDIR	QOPT <sup>8</sup>	*USE
	Path prefix	Refer to the ge	neral rules.	

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
DSPCURDIR	Path prefix	*DIR	QOpenSys, "root" (/), UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT <sup>11</sup>	*RX
DSPCURDIR	Current directory	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT <sup>11</sup>	*X
	Optical volume	*DDIR*	QOPT <sup>8</sup>	*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 gen	neral rules.	
DSPLNK	Any	Any	"root" (/), QOpenSys, UDFS QSYS.LIB <sup>27</sup> , QDLS, QOPT <sup>11</sup>	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 <sup>8</sup>	*USE
	Parent directory of referenced object - No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
DSPLNK	Parent directory of referenced object - Pattern specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*R
		*FLR	QDLS	*R
		*DDIR	QOPT <sup>11</sup>	*R
		*DDIR		*R
	Parent directory of referenced object- Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*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 <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
DSPLNK	Prefix of parent referenced object - No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
DSPLNK	Prefix of parent referenced object - Pattern specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
DSPLNK	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*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 <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
DSPLNK	Relative Path Name <sup>14</sup> : Current working directory containing object -No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R
	Relative Path Name <sup>14</sup> : Current working directory containing object -Pattern Specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R
DSPLNK	Relative Path Name <sup>14</sup> : Prefix of current working directory containing object -No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
DSPLNK	Relative Path Name <sup>14</sup> : Prefix of current working directory containing object -Pattern specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R
DSPMFSINF	Object	Any	Any	None
	Path Prefix	Refer to the gen	eral 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.		
ENDJRN	Object	*DIR if Subtree (*ALL)	QOpenSys, "root" (/), UDFS	*R, *X, *OBJMGT
		*DIR if Subtree (*NONE), *SYMLNK, *STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMG
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Parent Directory	*DIR	QOpenSys, "root" (/), UDFS	*X
		*LIB	QSYS.LIB	*X
	Path Prefix	Refer to the gen	eral rules.	
	Journal			*OBJMGT, *OBJOPR

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
MOV <sup>19</sup>	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 <sup>11</sup>	*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 <sup>11</sup>	*WX
MOV	Path prefix (target)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	others	*X
		*DDIR	QOPT <sup>11</sup>	*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 <sup>11</sup>	*RW
MOV	Moved into QSYS *MBR	*STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT <sup>11</sup>	*RW

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
MOV	Path (source) moved across file systems, parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS. LIB	ownership, *RX, *OBJEXIST
		*DDIR	QOPT <sup>11</sup>	*WX
	Path Prefix	Refer to the ge	neral rules.	•
	Optical volume (Source and Target)	*DDIR	QOPT <sup>8</sup>	*CHANGE
RCLLNK <sup>16</sup>				
RLSIFSLCK <sup>18</sup>	some_stmf	*STMF	"root" (/), QOpenSys, UDFS	*R
	Path prefix	Refer to the ge	neral rules.	•
RMVDIR <sup>19,20</sup>	Directory	*DIR	QOpenSys, "root" (/), UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT <sup>11</sup>	*W
RMVDIR	Parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT <sup>11</sup>	*WX
	Path Prefix	Refer to the ge	neral rules.	
	Optical volume	*DDIR	QOPT <sup>8</sup>	*CHANGE
RMVLNK <sup>19</sup>	Object	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		other	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT <sup>11</sup>	*W
		any	QOpenSys, "root" (/), UDFS	*OBJEXIST

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
RMVLNK	Parent Directory	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, "root" (/), UDFS	*WX
		*DDIR	QOPT <sup>11</sup>	*WX
	Path prefix	Refer to the ge	neral rules.	
	Optical volume	*DDIR	QOPT <sup>8</sup>	*CHANGE
RNM <sup>19</sup>	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 <sup>11</sup>	*W
	Optical Volume (Source and Target)	*DDIR	QOPT <sup>8</sup>	*CHANGE
RNM	Parent directory	*DIR	QOpenSys, "root" (/), UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT <sup>11</sup>	*WX
	Path prefix	*LIB	QSYS.LIB	*X, *UPD
		Any	QOpenSys, "root" (/), UDFS, QDLS	*X
RST (Q) <sup>23</sup>	Object, if it exists <sup>2</sup>	Any	QOpenSys, "root" (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Varies 10
			QDLS	*ALL
	Path prefix	Refer to the ge	neral rules.	
	Parent directory created by the restore operation due to CRTPRNDIR(*YES) <sup>2</sup>	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Parent directory owner specified on parameter PRNDIROWN <sup>2, 6</sup>	*USRPRF	QSYS.LIB	*ADD

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
RST (Q)	Parent directory of object being restored <sup>2</sup>	*DIR	QOpenSys, "root" (/), UDFS	*WX
	Parent directory of object being restored, if	*FLR	QDLS	*CHANGE
	the object does not exist <sup>2</sup>	*DIR		*OBJMGT, *OBJALTER, *READ, *ADD *UPD
	User profile owning new object being restored <sup>2</sup>	*USRPRF	QSYS.LIB	*ADD
	Tape unit, diskette unit, optical unit, or save file	*DEVD, *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
RST (Q)	Optical volume if restoring from optical device	*DDIR	QOPT <sup>8</sup>	*USE
	Optical path prefix and parent if restoring from optical device	*DDIR	QOPT <sup>11</sup>	*X
	Optical file if restoring from optical device	*DSTMF	QOPT <sup>11</sup>	*R
RTVCURDIR	Path prefix	*DIR	QOpenSys, "root" (/), UDFS, QDLS, QOPT <sup>11</sup>	*RX
		*DDIR	QOPT <sup>11</sup>	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Any		*R
RTVCURDIR	Current directory	*DIR	QOpenSys, "root" (/), UDFS, QOPT	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Any		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
SAV	Object <sup>2</sup>	Any	QOpenSys, "root" (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Varies 10
			QDLS	*ALL
	Path prefix	Refer to the ge	neral rules.	
	Tape unit, diskette unit, or optical unit	*DEVD	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
SAV	Optical volume, if saving to optical device	*DDIR	QOPT <sup>8</sup>	*CHANGE
	Optical path prefix if saving to optical device	*DDIR	QOPT <sup>11</sup>	*X
	Optical parent directory if saving to optical device	*DDIR	QOPT <sup>11</sup>	*WX
	Optical file (If it previously exists)	*DSTMF	QOPT <sup>11</sup>	*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 ge	neral rules.	

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>	
STRJRN	Object	*DIR if Subtree (*ALL)	QOpenSys, "root" (/), UDFS	*R, *X, *OBJMGT	
		*DIR if subtree (*NONE), *SYMLNK, *STMF	QOpenSys, "root" (/), UDFS	*R, *OBJMGT	
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT	
	Parent Directory	*DIR	QOpenSys, "root" (/), UDFS	*X	
		*LIB	QSYS.LIB	*X	
	Path Prefix	Refer to the gen	eral rules.		
	Journal	*JRN		*OBJMGT, *OBJOPR	
WRKAUT <sup>6, 7</sup>	Object	*DOC or *FLR	QDLS	*ALL	
		All	not QDLS	*OBJMGT or ownership	
		*DDIR and *DSTMF	QOPT <sup>11</sup>	*NONE	
	Path prefix	Refer to the gen	Refer to the general rules.		
	Optical volume	*DDIR	QOPT <sup>8</sup>	*USE	
WRKLNK	Any	Any	"root" (/), QOpenSys, UDFS, QSYS.LIB <sup>27</sup> , QDLS, QOPT <sup>11</sup>	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 <sup>8</sup>	*USE	
WRKLNK	Parent directory of referenced object - No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X	
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X	
		*FLR	QDLS	*X	
		*DDIR	QOPT <sup>11</sup>	*X	
		*DDIR		*R	

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
WRKLNK	Parent directory of referenced object - Pattern Specified	*DIR	"root" (/), QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*R
		*FLR	QDLS	*R
		*DDIR	QOPT <sup>11</sup>	*R
		*DDIR		*R
WRKLNK	Parent directory of referenced object- Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*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 <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
WRKLNK	Prefix of parent referenced object - No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
WRKLNK	Prefix of parent referenced object - Pattern specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
WRKLNK	Prefix of parent referenced object - Option 8 (Display Attributes)	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*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 <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*X
		*DDIR		*R
WRKLNK	Relative Path Name <sup>14</sup> : Current working directory containing object -No Pattern <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*X
		*FLR	QDLS	*X
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R
	Relative Path Name <sup>14</sup> : Current working directory containing object -Pattern Specified <sup>13</sup>	*DIR	"root" (/), QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB <sup>27</sup>	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT <sup>11</sup>	*RX
		*DDIR		*R

- Adopted authority is not used for integrated file system commands.
- If you have \*SAVSYS special authority, you do not need the authority specified for the QSYS.LIB, QDLS, QOpenSys, and "root" (/) file systems.
- The authority required varies by object type. See the description of the QLIRNMO API in the Information Center. If the object is a database member, see the authorities for the Rename Member (RNMM) command.
- You must have \*AUDIT special authority to change an auditing value.
- If the user issuing the command does not have \*ALLOBJ authority, the user must be a member of the new primary group.
- 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.
- These commands require the authority shown plus the authorities required for the DSPCURDIR command.
- 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.
- <sup>9</sup> See Chapter 7 of iSeries Optical Support book for information about restrictions regarding this command.
- Authority required varies by the native command used. See the respective SAVOBJ or RSTOBJ command for the required authority.
- Authority required by QOPT against media formatted in "Universal Disk Format" (UDF).
- \*ADD is needed only when object being moved to is a \*MRB.
- 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.
- Relative path name: If a path name does not begin with a slash, the predecessor of the first component of the path name is taken to be the current working directory of the process. For example, if a path name of 'a/b' is specified, and the current working directory is '/home/john', then the object being accessed is '/home/john/a/b'.
- 15 If you have \*ALLOBJ special authority, you do not need the listed authority.

Comm	nand	Referenced Object	Object Type	File System	Authority Needed for Object <sup>1</sup>
16	You must ha	ve *ALLOBJ special authority to use thi	is command.		
17	In the above system.	table, QSYS.LIB refers to independent	ASP QSYS.LIB file syste	ems as well as Q	SYS.LIB file
18	To use this command, you must have *IOSYSCFG special authority.				
19	If the restricted renames and unlinks attribute (also known as S_ISVTX bit) is on for a directory, it will restrict unlinking objects from that directory unless one of these authorities is met: *ALLOBJ; the user is the owner of the object being unlinked; or the user is the owner of the directory.				
20	If RMVLNK directory.	(*YES) is specified, the user must also h	nave *OBJEXIST author	ity to all objects	in the specified
21		B, "root" (/), QOpenSys, and user-define value other than *SYSVAL is specified			cial authority is
22		ust have all object (*ALLOBJ) and securious for the Scanning option for objects (			
23		ive *ALLOBJ special authority to specify ALWOBJDIF) parameter.	a value other than *N	ONE for the All	ow object
24	changing the	ast have all object (*ALLOBJ) and securi e owner of a stream file (*STMF) with a ogram is running includes the user and	n attached Java prograi		
25	The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority when copying a stream file (*STMF) with an attached Java program whose authority checking includes the user and the owner.				
26	The user must have all object (*ALLOBJ) and security administrator (*SECADM) special authority to specify the *CRTOBJSCAN and *SCAN attributes.				
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		ed any of the normal path name prefix a		AUD attribute, a	and the user

# **Interactive Data Definition Commands**

		Authori	Authority Needed	
Command	Referenced Object	For Object	For Library	
ADDDTADFN	Data dictionary	*CHANGE	*EXECUTE	
	File	*OBJOPR, *OBJMGT	*EXECUTE	
CRTDTADCT	Data dictionary		*READ, *ADD	
DLTDTADCT <sup>3</sup>	Data dictionary	OBJEXIST, *USE		
DSPDTADCT	Data dictionary	*USE	*EXECUTE	
LNKDTADFN 1	Data dictionary	*USE	*EXECUTE	
	File	*OBJOPR, *OBJMGT	*EXECUTE	
STRIDD				
WRKDTADCT <sup>2</sup>	Data dictionary	*OBJOPR	*EXECUTE	

#### **Interactive Data Definition Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
WRKDBFIDD <sup>2</sup>	Data dictionary	*USE <sup>4</sup> *EXECUTE	
	Database file	*OBJOPR	*EXECUTE
WRKDTADFN <sup>1</sup>	Data dictionary	*USE, *CHANGE	*EXECUTE

- 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.
- Before the dictionary is deleted, all linked files are unlinked. Refer to the LNKDTADFN command for authority required to unlink a file.
- You need use authority to the data dictionary to create a new file. No authority to the data dictionary is needed to enter data in an existing file.

# **Internetwork Packet Exchange (IPX) Commands**

Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant \*USE authority to others.

		Authority Needed	
Command	Referenced Object	For Object	For Library
DLTIPXD	IPX description	*OBJEXIST	*EXECUTE
DSPIPXD	IPX description	*USE	*EXECUTE
WRKIPXD	IPX description	*OBJOPR	*EXECUTE

#### **Information Search Index Commands**

		Aut	thority Needed
Command	Referenced Object	For Object	For Library
ADDSCHIDXE	Search index	*CHANGE	*USE
	Panel group	*USE	*EXECUTE
CHGSCHIDX	Search index	*CHANGE	*USE
CRTSCHIDX	Search Index		*READ, *ADD
DLTSCHIDX	Search index	*OBJEXIST	*EXECUTE
RMVSCHIDXE	Search index	*CHANGE	*USE
STRSCHIDX	Search index	*USE	*EXECUTE
WRKSCHIDX <sup>1</sup>	Search index	*ANY	*USE
WRKSCHIDXE	Search index	*USE	*USE

#### **IPL Attribute Commands**

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

These commands do not require authorities to objects:

- 1	CHGIPLA (Q) <sup>1</sup> DSPIPLA
	To use this command, you must have *SECADM and *ALLOBJ special authorities.

#### **Java Commands**

		Au	Authority Needed	
Command	Referenced Object	For Object	For Library	
ANZJVM	QSYS/STRSRVJOB command	*USE		
	QSYS/STRDBG command	*USE		
DSPJVMJOB1	Java Virtual Machine jobs			
You must have *JOBCTL special authority to use this command.				

#### **Job Commands**

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

		Aut	hority Needed
Command	Referenced Object	For Object	For Library
ВСНЈОВ	Job description <sup>9,11</sup>	*USE	*EXECUTE
	Libraries in the library list (system, current, and user) <sup>7</sup>	*USE	
	User profile in job description <sup>10</sup>	*USE	
	Sort sequence table <sup>7</sup>	*USE	*EXECUTE
	Message queue 10	*USE, *ADD	*EXECUTE
	Job queue <sup>10,11</sup>	*USE	*EXECUTE
	Output queue <sup>7</sup>	*READ	*EXECUTE
CHGACGCDE 1			
CHGGRPA <sup>4</sup>	Message queue if associating a message queue with a group	*OBJOPR	*EXECUTE
CHGJOB <sup>1,2,3</sup>	New job queue, if changing the job queue <sup>10,11</sup>	*USE	*EXECUTE
	New output queue, if changing the output queue <sup>7</sup>	*READ	*EXECUTE
	Current output queue, if changing the output queue	*READ	*EXECUTE
	Sort sequence table <sup>7</sup>	*USE	*EXECUTE
CHGPJ	User profile for the program start request to specify *PGMSTRRQS	*USE	*EXECUTE
	User profile and job description	*USE	*EXECUTE
CHGSYSJOB(Q) 13			

#### **Job Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
CHGUSRTRC <sup>14</sup>	User trace buffer when CLEAR (*YES) is used. <sup>15</sup>	*OBJOPR	*EXECUTE	
	User trace buffer when MAXSTG is used <sup>15</sup>	*CHANGE, *OBJMGT	*USE	
	User trace buffer when TRCFULL is used. 15	*OBJOPR	*EXECUTE	
DLTUSRTRC	User trace buffer 15	*OBJOPR, *OBJEXIST	*EXECUTE	
DLYJOB <sup>4</sup>				
DMPUSRTRC	User trace buffer 15	*OBJOPR	*EXECUTE	
DSCJOB <sup>1</sup>				
DSPACTPJ				
DSPJOB <sup>1</sup>				
DSPJOBTBL				
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 <sup>1</sup>				
ENDLOGSVR <sup>6</sup>				
ENDPJ <sup>6</sup>				
HLDJOB <sup>1</sup>				
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 <sup>2, 12</sup>	Job description 9,11	*USE	*EXECUTE	
	Libraries in the library list (system, current, and user) <sup>7</sup>	*USE		
	Message queue <sup>10</sup>	*USE, *ADD	*EXECUTE	
	User profile 10,11	*USE		
	User profile in job description <sup>10</sup>	*USE (at level 40)		
	Job queue 10,11	*USE	*EXECUTE	
	Output queue <sup>7</sup>	*READ	*EXECUTE	
	Sort sequence table <sup>7</sup>	*USE	*EXECUTE	
	ASP devices in the initial ASP group	*USE		
SBMNETJOB	Database file	*USE	*EXECUTE	
STRLOGSVR <sup>6</sup>				

		Authority Needed	
Command	Referenced Object	For Object	For Library
STRPJ <sup>6</sup>	Subsystem description	*USE	
	Program	*USE	*EXECUTE
TFRBCHJOB	Job queue	*READ	*EXECUTE
TFRGRPJOB	First group program	*USE	*EXECUTE
TFRJOB <sup>8</sup>	Job queue	*USE	*EXECUTE
	Subsystem description to which the job queue is allocated	*USE	
TFRSECJOB			
WRKACTJOB			
WRKASPJOB	Device description	*USE	
WRKJOB <sup>1</sup>			
WRKJOBLOG			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

- 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.
- You must have the authority (specified in your user profile) for the scheduling priority and output priority specified.
- 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.
- This command only affects the job in which it was specified.

- 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 iSeries 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.
- To use this command, job control \*JOBCTL special authority is required.
- 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.
- If the job being transferred is an interactive job, the following restrictions apply:
  - · The job queue where the job is placed must be associated with an active subsystem.
  - The 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.
- Both the user submitting the job and the user profile under which the job will run are checked for authority to the referenced object.
- The user submitting the job is checked for authority to the referenced object.

			Authorit	y Needed	
Command Referenced Object		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	0	tain job attributes, even in the user's own job, ecial authorities.	requires job control (*JC	BCTL) and all object	
14		run these commands for jobs running under hecial authority can run these commands for an		ser with job control	
15	A user trace b	uffer is a user space (*USRSPC) object in librar	y QUSRSYS by the nam	ne QPOZ <i>nnnnnn</i> , where	

# **Job Description Commands**

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

'nnnnnn' is the job number of the job using the user trace facility.

		Authori	ty Needed		
Command	Referenced Object	For Object	For Library		
CHGJOBD	Job description	*OBJOPR, *OBJMGT, *READ	*EXECUTE		
	User profile (USER)	*USE			
CPYAUDJRNE <sup>8</sup>	Output file already exists	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE		
	Output file does not exist		*EXECUTE *ADD		
CRTJOBD (Q)	Job description		*READ, *ADD		
	User profile (USER)	*USE			
DLTJOBD	Job description	*OBJEXIST	*EXECUTE		
DSPJOBD	Job description	*OBJOPR, *READ	*EXECUTE		
PRTJOBDAUT 1					
WRKJOBD Job description		Any	*USE		
You must have *ALLOBJ or *AUDIT special authority to use this command.					

### **Job Queue Commands**

	Referenced	Job Queu	Job Queue Parameters <sup>4</sup>		Authorit	Authority Needed	
Command	Object	AUTCHK	OPRCTL Special Authority		For Object	For Library	
CLRJOBQ 1	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE	
		*OWNER			Owner <sup>2</sup>	*EXECUTE	
			*YES	*JOBCTL		*EXECUTE	
CRTJOBQ 1	Job queue					*READ, *ADD	
DLTJOBQ	Job queue				*OBJEXIST	*EXECUTE	

Command	Referenced Object	Job Queue Parameters <sup>4</sup>		Special	Authority Needed	
		AUTCHK	OPRCTL	Authority	For Object	For Library
HLDJOBQ <sup>1</sup>	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner <sup>2</sup>	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT <sup>5</sup>						
RLSJOBQ 1	Job queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner <sup>2</sup>	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ 1,3	Job queue	*DTAAUT			*READ	*EXECUTE
		*OWNER			Owner <sup>2</sup>	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

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.

# **Job Schedule Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
ADDJOBSCDE	Job schedule	*CHANGE	*EXECUTE	
	Job description <sup>1</sup>	*USE	*EXECUTE	
	Job queue <sup>1,2</sup>	*READ	*EXECUTE	
	User profile	*USE	*EXECUTE	
	Message queue <sup>1</sup>	*USE, *ADD	*EXECUTE	
CHGJOBSCDE <sup>3</sup>	Job schedule	*CHANGE	*EXECUTE	
	Job description <sup>1</sup>	*USE	*EXECUTE	
	Job queue <sup>1,2</sup>	*READ	*EXECUTE	
	User profile	*USE	*EXECUTE	
	Message queue <sup>1</sup>	*USE, *ADD	*EXECUTE	
HLDJOBSCDE <sup>3</sup>	Job schedule	*CHANGE	*EXECUTE	
RLSJOBSCDE 3	Job schedule	*CHANGE	*EXECUTE	
RMVJOBSCDE <sup>3</sup>	Job schedule	*CHANGE	*EXECUTE	
WRKJOBSCDE <sup>4</sup>	Job schedule	*USE	*EXECUTE	

You must be the owner of the job queue.

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.

To display the job queue parameters, use the QSPRJOBQ API.

You must have \*ALLOBJ or \*AUDIT special authority to use this command.

#### **Job Schedule Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	

- 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.
- You must have \*JOBCTL special authority or have added the entry.
- To display the details of an entry (option 5 or print format \*FULL), you must have \*JOBCTL special authority or have added the entry.

### **Journal Commands**

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

		Authority Needed		
Command	Referenced Object	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	
	Non-integrated file system objects whose journaled changes are being applied	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD	
	integrated file system objects whose journal changes are being applied	*RW, *OBJMGT	*RX (if subtree *ALL)	
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	
CHGJRNOBJ 9		*OBJOPR, *OBJMGT		
	Non-integrated file system objects	*READ, *OBJMGT		
	Integrated file system objects *R	*OBJMGT		
	Object path SUBTREE(*ALL) *RX	*OBJMGT		
	Object path SUBTREE(*NONE) *R	*OBJMGT		
	Parent directory *X			
CHGRMTJRN	Source journal	*CHANGE, *OBJMGT	*EXECUTE	
	Source journal	*USE, *OBJMGT	*EXECUTE	

		Authority Needed	
Command	Referenced Object	For Object	For Library or Directory
CMPJRNIMG	Journal	*USE	*EXECUTE
	Journal receiver	*USE	*EXECUTE
	File	*USE	*EXECUTE
CPYAUDJRNE <sup>8</sup>	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 <sup>8</sup>			
DSPJRN <sup>6</sup>	Journal	*USE	*EXECUTE
	Journal if FILE(*ALLFILE) is specified, no object selection is specified, the specified object has been deleted from the system, *IGNFILSLT or *IGNOBJSLT is specified for any selected journal codes, 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 could be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
DSPJRNMNU <sup>1</sup>			
ENDJRN	See "Integrated File System Commands" on	page 349.	
ENDJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP <sup>2</sup>			
JRNPF <sup>3</sup>			

#### **Journal Commands**

		Authority Needed	
Command	Referenced Object	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, *IGNFILSLT or *IGNOBJSLT is specified for any selected journal codes, 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 could be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
	Exit program	*EXECUTE	*EXECUTE
RMVJRNCHG (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, *IGNFILSLT or *IGNOBJSLT is specified for any selected journal codes, 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 could be *X as well if object is a directory and SUBTREE (*ALL) is specified)	*X
RMVRMTJRN	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 p	page 349.	1
STRJRNAP	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNPF	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	File	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Journal	*OBJOPR, *OBJMGT	*EXECUTE
	Object	*OBJOPR, *READ, *OBJMGT	*EXECUTE

		Authori	Authority Needed	
Command	Referenced Object	For Object	For Library or Directory	
WRKJRN 4 (Q)	Journal	*USE	*READ <sup>7</sup>	
	Journal receiver	*USE	*EXECUTE	
WRKJRNA <sup>6</sup>	Journal	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE	
	Journal receiver <sup>5</sup>	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE	

- See the WRKJRN command (this command has the same function).
- See the STRJRNAP command.
- <sup>3</sup> See the STRJRNPF command.
- 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.
- \*OBJOPR and \*OBJEXIST authority is required for journal receivers if the option is chosen to delete receivers.
- To specify JRN(\*INTSYSJRN), you must have \*ALLOBJ special authority.
- \*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.
- You must have \*AUDIT special authority to use this command.
- To specify PTLTNS(\*ALWUSE), you must have \*ALLOBJ special authority.

### **Journal Receiver Commands**

	Referenced Object	Authority Needed	
Command		For Object	For Library
CRTJRNRCV	Journal receiver		*READ, *ADD
DLTJRNRCV	Journal receiver	*OBJOPR, *OBJEXIST, and a data authority other than *EXECUTE	*EXECUTE
	Journal	*OBJOPR	*EXECUTE
DSPJRNRCVA	Journal receiver	*OBJOPR and a data authority other than *EXECUTE	*EXECUTE
	Journal, if attached	*OBJOPR	*EXECUTE
WRKJRNRCV <sup>1</sup> , <sup>2</sup> , <sup>3</sup>	Journal receiver	Any authority	*USE

To use an individual operation, you must have the authority required by the operation.

<sup>\*</sup>OBJOPR and \*OBJEXIST authority is required for journal receivers if the option is chosen to delete receivers.

<sup>\*</sup>OBJOPR and a data authority other than \*EXECUTE is required for journal receivers if the option is chosen to display the description.

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTBNDC	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to 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
CRTBNDCL	Source file	*USE	*EXECUTE
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Refer to the general rules.	Refer to the general rules.
	Table specified in SRTSEQ parameter	*USE	*EXECUTE
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

			Authority Needed	
Command	Referenced Object	For Object	For Library	
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	
CRTCBLMOD	Source file	*USE	*EXECUTE	
	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE	
	Module: REPLACE(*NO)		*READ, *ADD	
	Module: REPLACE(*YES)	Refer to 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	
	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	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.	Refer to the general rules.	
	Table specified in SRTSEQ parameter	*USE	*EXECUTE	
CRTCBLPGM	Source file	*USE	*EXECUTE	
(COBOL/400* licensed program or S/38 environment)	Externally described device files and database files referred to in source program	*OBJOPR	*EXECUTE	
z. oo onvironiiciity	Program: REPLACE(*NO)		*READ, *ADD	
	Program: REPLACE(*YES)	Refer to the general rules.	*READ, *ADD	
	Table specified in SRTSEQ parameter	*USE	*EXECUTE	

		Authority Needed	
Command	Referenced Object	For Object	For Library
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
CRTRPGPGM	Source file	*USE	*EXECUTE
(RPG/400* licensed program and S/38 environment)	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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTRPTPGM (RPG/400 licensed program and S/38 environment)	Source file	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Refer to 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	Source file	*USE	*EXECUTE
environment)	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®	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTSQLCBL (DB2 Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
CRTSQLPLI (DB2	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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	Source file	*OBJOPR, *READ	*EXECUTE
Query Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	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 <sup>1</sup>	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

	Referenced Object	Authority Needed	
Command		For Object	For Library
ENDCBLDBG (COBOL/400® licensed program or S/38 environment)	Program	*CHANGE	*EXECUTE
ENTCBLDBG (S/38 environment)	Program	*CHANGE	*EXECUTE
DLTCLD	Locale object	*OBJEXIST, *OBJMGT	*EXECUTE
RTVCLDSRC	Locale object	*USE	*EXECUTE
	To-file	Refer to the general rules.	Refer to the general rules.
RUNSQLSTM <sup>1</sup>	Source file	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRREXPRC	Source file	*USE	*EXECUTE
	Exit program	*USE	*EXECUTE
STRSQL (DB2 Query	Sort sequence table	*USE	*EXECUTE
Manager and SQL Development for i5/OS licensed program) <sup>1</sup>	Printer device description	*USE	*EXECUTE
	Printer output queue	*USE	*EXECUTE
	Printer file	*USE	*EXECUTE

See the **Authorization**, **privileges and object ownership** information in the **DB2 for iSeries SQL Reference** (located in the iSeries Information Center) for more information about security requirements for structured query language (SQL) statements.

# **Library Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library Being Acted On
ADDLIBLE	Library		*USE
CHGCURLIB	New current library		*USE
CHGLIB <sup>8</sup>	Library		*OBJMGT
CHGLIBL	Every library being placed in the library list		*USE
CHGSYSLIBL (Q)	Libraries in new list		*USE
CLRLIB <sup>3</sup>	Every object being deleted from library	*OBJEXIST	*USE
	Object types *DTADCT <sup>14</sup> , *JRN <sup>14</sup> ,*JRNRCV <sup>14</sup> , *MSGQ <sup>14</sup> , *SBSD <sup>14</sup>	See the authority required by the DLTxxx command for the object type	
	ASP device (if specified)	*USE	

### **Library Commands**

		Authorit	y Needed	
Command	Referenced Object	For Object	For Library Being Acted On	
CPYLIB <sup>4</sup>	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 <sup>3</sup>	Every object being deleted from library	*OBJEXIST	*USE, *OBJEXIST	
	Object types *DTADCT <sup>14</sup> , *JRN <sup>14</sup> ,*JRNRCV <sup>14</sup> , *MSGQ, *SBSD <sup>14</sup>	See the authority required by the DLTxxx command for the object type		
	ASP device (if specified)	*USE		
DSPLIB	Library		*READ	
	Objects in the library <sup>5</sup>	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	

### **Library Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library Being Acted On
RSTLIB 7 (Q)	Media definition	*USE	*EXECUTE
	Library, if it does exist		*READ, *ADD
	Message queues being restored to library where they already exist	*OBJOPR, *OBJEXIST <sup>7</sup>	*EXECUTE. *READ, *ADD
	Programs that adopt authority	Owner or *ALLOBJ and *SECADM	*EXECUTE
	Library saved if VOL(*SAVVOL) is specified		*USE <sup>6</sup>
	Every object being restored over in the library	*OBJEXIST <sup>3</sup>	*EXECUTE, *READ, *ADD
	User profile owning objects being created	*ADD <sup>6</sup>	
	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 7 (Q)	Tape (QSYSTAP) or diskette (QSYSDKT) file	*USE <sup>6</sup>	*EXECUTE
	QSYS/QPSRLDSP printer output, if OUTPUT(*PRINT) specified	*USE	*EXECUTE
	Save file	*USE	*EXECUTE
	Optical File (OPTFILE) <sup>12</sup>	*R	Not applicable
	Path prefix of optical file (OPTFILE) <sup>12</sup>	*X	Not applicable
	Optical volume <sup>11</sup>	*USE	
	ASP device description <sup>15</sup>	*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

		Authority Needed	
Command	Referenced Object	For Object	For Library Being Acted On
SAVLIB	Every object in the library	*OBJEXIST <sup>6</sup>	*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 <sup>6</sup>	*EXECUTE
	QSYS/QPSAVOBJ printer output	*USE <sup>6</sup>	*EXECUTE
	Command user space, if specified	*USE	*EXECUTE
SAVLIB	Optical File <sup>12</sup>	*RW	Not applicable
	Parent Directory of optical file (OPTFILE) <sup>12</sup>	*WX	Not applicable
	Path Prefix of optical file (OPTFILE) <sup>12</sup>	*X	Not applicable
	Root Directory (/) of Optical Volume <sup>12, 13</sup>	*RWX	Not applicable
	Optical volume <sup>11</sup>	*CHANGE	
	ASP device description <sup>15</sup>	*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

#### **Library Commands**

			Authority Needed	
			For Library Being Acted	
Command	Referenced Object	For Object	On	

- 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 ADDLIBLE command requires Use authority to the CUSTLIB library.
- The authority needed for the QSYS library is indicated in this column, because all libraries are in QSYS library.
- 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.
- <sup>4</sup> All restrictions that apply to the CRTDUPOBJ command, also apply to this command.
- If you do not have authority to an object in the library, the text for the object says \*NOT AUTHORIZED.
- If you have \*SAVSYS special authority, you do not need the authority specified.
- You must have \*ALLOBJ special authority to specify a value other than \*NONE for the Allow object differences (ALWOBJDIF) parameter.
- 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.
- You must have \*AUDIT special authority to specify a CRTOBJAUD value other than \*SYSVAL.
- You must have the authority required by the operation to use an individual operation.
- 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.
- This authority check is only made when the Optical media format is Universal Disk Format.
- This authority check is only made when you are clearing the optical volume.
- This object is allowed on independent ASP.
- Authority required only if save or restore operation requires a library namespace switch.
- This command requires \*ALLOBJ special authority.

# **License Key Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDLICKEY (Q)	Output file	*USE	*EXECUTE
DSPLICKEY (Q)	Output file	Refer to the general rules.	Refer to the general rules.
RMVLICKEY (Q)	Output file	*CHANGE	*EXECUTE

### **Licensed Program Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGLICINF (Q)	WRKLICINF command	*USE	*EXECUTE
DLTLICPGM 1,2 (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM 1,2 (Q)			
SAVLICPGM 1,2 (Q)			
WRKLICINF (Q)			

Some licensed programs can be deleted, saved, or restored only if you are enrolled in the system distribution directory.

# **Line Description Commands**

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
CHGLINASC <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Controller description (SWTCTLLST)	*USE	*EXECUTE
	Connection list (CNNLSTIN or CNNLSTOUT)	*USE	*EXECUTE
	Network interface description (SWTNWILST)	*USE	*EXECUTE

If deleting, restoring, or saving a licensed program that contains folders, all restrictions that apply to the DLTDLO command also apply to this command.

To use individual operations, you must have the authority required by the individual operation.

### **Line Description Commands**

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
CHGLINWLS <sup>2</sup>	Line description	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CRTLINASC <sup>2</sup>	Controller description (CTL and SWTCTLLST)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINBSC <sup>2</sup>	Controller description (SWTCTLLST and CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINDDI <sup>2</sup>	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Controller description (NETCTL)	*USE	*EXECUTE
CRTLINETH <sup>2</sup>	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 <sup>2</sup>	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Controller description (NETCTL)	*USE	*EXECUTE
CRTLINPPP <sup>2</sup>	Controller description (NETCTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINSDLC <sup>2</sup>	Controller description (CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINTDLC <sup>2</sup>	Controller description (WSC and CTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
CRTLINTRN <sup>2</sup>	Controller description (NETCTL)	*USE	*EXECUTE
	Line description		*READ, *ADD
	Network interface description (NWI)	*USE	*EXECUTE
	Network server description (NWS)	*USE	*EXECUTE
CRTLINX25 <sup>2</sup>	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 <sup>2</sup>	Line description		*READ, *ADD
	Controller description (NETCTL)	*USE	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE

		Authority Needed		Authority Needed
Command	Referenced Object	For Object	For Library	
DLTLIND	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	

To use individual operations, you must have the authority required by the individual operation.

## Local Area Network (LAN) Commands

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

These commands do n	ot require any object authorities	S:		
ADDLANADPI CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT	

### **Locale Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTLOCALE	Source file	*USE	*USE, *ADD
DLTLOCALE	Locale	*OBJEXIST	*USE

#### **Mail Server Framework Commands**

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

This command does no	t require any object authorities:	
ENDMSF (Q)	STRMSF (Q)	

### **Media Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDTAPCTG	Tape Library description	*USE	*EXECUTE
CFGDEVMLB <sup>1</sup>	Tape Library description	*CHANGE, *OBJMGT	*EXECUTE

To use this command, you must have \*IOSYSCFG special authority.

To use this command, you must have \*ALLOBJ special authority.

#### **Media Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGDEVMLB (Q)	Tape Library description	*CHANGE, *OBJMGT	*EXECUTE
CHGJOBMLBA <sup>4</sup>	Tape Library description	*CHANGE	*EXECUTE
CHGTAPCTG	Tape Library description	*USE	*EXECUTE
CHKDKT	Diskette unit description	*USE	*EXECUTE
СНКТАР	Tape device description	*USE	*EXECUTE
CLRDKT	Diskette unit description	*USE	*EXECUTE
CRTTAPCGY	Tape Library description		
DLTDKTLBL	Diskette unit description	*USE	*EXECUTE
DLTMEDDFN	Media definition	*OBJEXIST	*EXECUTE
DLTTAPCGY	Tape Library description		
DMPTAP (Q) <sup>5</sup>	Tape device description	*USE	*EXECUTE
DSPDKT	Diskette unit description	*USE	*EXECUTE
DSPTAP	Tape device description	*USE	*EXECUTE
DSPTAPCGY	Tape Library description		
DSPTAPCTG	Tape Library description	*USE	*EXECUTE
DSPTAPSTS	Tape Library description	*USE	*EXECUTE
DUPDKT	Diskette unit description	*USE	*EXECUTE
DUPTAP	Tape device description	*USE	*EXECUTE
INZDKT	Diskette unit description	*USE	*EXECUTE
INZTAP	Tape device description	*USE	*EXECUTE
RMVTAPCTG	Tape Library description	*USE	*EXECUTE
RNMDKT	Diskette unit description	*USE	*EXECUTE
SETTAPCGY	Tape Library description	*USE	*EXECUTE
WRKMLBRSCQ <sup>3</sup>	Tape Library description	*USE	*EXECUTE
WRKMLBSTS <sup>2</sup> (Q)	Tape Library description	*USE	*EXECUTE
WRKTAPCTG	Tape Library description	*USE	*EXECUTE

To use this command, you must have \*IOSYSCFG special authority.

## **Menu and Panel Group Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGMNU	Menu	*CHANGE	*USE

To use individual operation, you must have the authority required by the operation.

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.

To change the priority or work with another user's job you must have \*JOBCTL special authority.

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**

		Authority Needed	
Command	Referenced Object	For Object	For Library
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
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 <sup>1</sup>	Menu	Any	*USE
WRKPNLGRP 1	Panel group	Any	*EXECUTE
1 To use an i	individual operation, you must have the authority	y required by the operat	ion.

# **Message Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
DSPMSG	Message queue	*USE	*USE
	Message queue that receives the reply to an inquiry message	*USE, *ADD	*USE
	Remove messages from message queue	*USE, *DLT	*USE
RCVMSG	Message queue	*USE	*EXECUTE
	Remove messages from queue	*USE, *DLT	*EXECUTE
RMVMSG	Message queue	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Message file	*USE	*EXECUTE
SNDBRKMSG	Message queue that receives the reply to inquiry messages	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Message queue	*OBOPR, *ADD	*EXECUTE
	Message queue that receives the reply to inquiry message	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Message queue	*OBJOPR, *ADD	*EXECUTE
	Message file, when sending predefined message	*USE	*EXECUTE
	Message queue that receives the reply to inquiry message	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Message queue	*USE, *ADD	*EXECUTE
	Remove messages from queue	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Message queue	*OBJOPR, *ADD	*EXECUTE
	Message file, when sending predefined message	*USE	*EXECUTE
WRKMSG	Message queue	*USE	*USE
	Message queue that receives the reply to inquiry message	*USE, *ADD	*USE
	Remove messages from message queue	*USE, *DLT	*USE

# **Message Description Commands**

		Autho	Authority Needed	
Command	Referenced Object	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 <sup>1</sup>	Message file	*USE	*EXECUTE	

# **Message File Commands**

		Authority Needed	ity Needed
Command	Referenced Object	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

# **Message Queue Commands**

		Autho	rity Needed	
Command	Referenced Object	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 <sup>1</sup>	Message queue	Any authority	*USE	
To use individual operations, you must have the authority required by the individual operation.				

# **Migration Commands**

		Aut	Authority Needed	
Command	Referenced Object	For Object	For Library	
RCVMGRDTA	File	*ALL	*READ, *ADD	
	Device	*CHANGE	*EXECUTE	
SNDMGRDTA	File	*ALL	*READ, *ADD	
	Device	*CHANGE	*EXECUTE	

The following commands do not require any object authorities.

They are shipped with public authority \*EXCLUDE. You must have \*ALLOBJ special authority to use these commands.

### **Migration Commands**

		Auth	ority Needed
Command	Referenced Object	For Object	For Library
ANZS34OCL	CVTS36JOB	MGRS36DSPF	MIGRATE
ANZS36OCL	CVTS36QRY	MGRS36ITM	QMUS36
CHGS34LIBM	CVTS38JOB	MGRS36LIB	RESMGRNAM
CHKS36SRCA	GENS36RPT	MGRS36MNU	RSTS38AUT
CVTBASSTR	GENS38RPT	MGRS36MSGF	STRS36MGR
CVTBASUNF	MGRS36	MGRS36QRY <sup>1</sup>	STRS38MGR
CVTBGUDTA	MGRS36APF <sup>1</sup>	MGRS36RPG	
CVTS36CFG	MGRS36CBL	MGRS36SEC	
CVTS36FCT	MGRS36DFU <sup>1</sup>	MGRS38OBJ	
You must have *ALLOBJ special authority and have i5/OS option 4 installed.			

# **Mode Description Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGMODD <sup>2</sup>	Mode description	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD <sup>2</sup>	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 <sup>1</sup>	Mode description	*OBJOPR	*EXECUTE

To use individual operations, you must have the authority required by the individual operation.

# **Module Commands**

		Authority Needed	
Command	Referenced Object	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

To use this command, you must have \*IOSYSCFG special authority.

			y Needed
Command	Referenced Object	For Object	For Library
RTVBNDSRC 1	Module	*USE	*EXECUTE
	*SRVPGMs and modules specified with *SRVPGMs	*USE	*EXECUTE
	Database source file if file and member exists and MBROPT(*REPLACE) is specified.	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Database source file if file and member exists and MBROPT(*ADD) is specified	*OBJOPR, *ADD	*EXECUTE
	Database source file if file exists and member needs to be created.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Database source file if file and member needs to be created.		*EXECUTE, *READ, *ADD
	CRTSCRPF command if file does not exist		*EXECUTE
	ADDPFM command if member does not exist		*EXECUTE
	RGZPFM command to reorganize source file member	*OBJMGT	*EXECUTE
WRKMOD <sup>2</sup>	Module	Any authority	*USE

- You need \*USE authority to the:
  - · CRTSRCPF command if the file does not exist.
  - · ADDPFM command if the member does not exist.
  - RGZPFM command so the source file member is reorganized. Either \*CHANGE and \*OBJALTER authorities or \*OBJMGT authority is required to reorganize the source file member. The RTVBNDSRC command function then completes with the source file member reorganized with sequence numbers of zero.
- To use individual operations, you must have the authority required by the individual operation.

# **NetBIOS Description Commands**

		Authority	y Needed
Command	Referenced Object	For Object	For Library
CHGNTBD <sup>2</sup>	NetBIOS description	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD <sup>2</sup>	NetBIOS description		*EXECUTE
DLTNTBD	NetBIOS description	*OBJEXIST	*EXECUTE
DSPNTBD	NetBIOS description	*USE	*EXECUTE
WKRNTBD1	NetBIOS description	*OBJOPR	*EXECUTE

<sup>&</sup>lt;sup>1</sup> To use individual operations, you must have the authority required by the individual operation.

#### **Network Commands**

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

To use this command, you must have \*IOSYSCFG special authority.

#### **Network Commands**

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
ADDNETJOBE (Q)	User profile in the network job entry	*USE	
APING	Device description	*CHANGE	
AREXEC	Device description	*CHANGE	
CHGNETA (Q) <sup>4</sup>			
CHGNETJOBE (Q)	User profile in the network job entry	*USE	
DLTNETF <sup>2</sup>	Output file	Refer to the general rules.	Refer to the general rules.
DSPNETA			
RCVNETF <sup>2</sup>	To-file member does not exist, MBROPT(*ADD) specified	*OBJMGT, *USE	*EXECUTE, *ADD
	To-file member does not exist, MBROPT(*REPLACE) specified	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	To-file member exists, MBROPT(*ADD) specified	*USE	*EXECUTE
	To-file member exists, MBROPT(*REPLACE) specified	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	User profile in the network job entry	*USE	
RTVNETA			
RUNRMTCMD	Device description	*CHANGE	
SNDNETF	Physical file or save file	*USE	*EXECUTE
SNDNETMSG to a local user	Message queue	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Device description	*CHANGE	
WRKNETF <sup>2,3</sup>			
WRKNETJOBE <sup>3</sup>	QUSRSYS/QANFNJE	*USE	*EXECUTE

You must have \*ALLOBJ special authority.

# **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 ge	eneral rules.	
ENDNFSSVR 1,4	none			

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.

To use an individual operation, you must have the authority required by that operation.

To change some network attributes, you must have \*IOSYSCFG, or \*ALLOBJ and \*IOSYSCFG special authorities.

Command	Referenced Object	Object Type	File System	Authority Needed for Object
EXPORTFS 1,2	Path prefix	Refer to the g	eneral rules.	
MOUNT 1,3	dir_to_be_ mounted_over	*DIR	"root" (/)	*W
RLSIFSLCK <sup>1</sup>	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 g	eneral rules.	
STRNFSSVR 1	none			
UNMOUNT 1				

To use this command, you must have \*IOSYSCFG special authority.

# **Network Interface Description Commands**

		Authori	ty Needed
Command	Referenced Object	For Object	For Library
CHGNWIFR <sup>2</sup>	Network interface description	*CHANGE, *OBJMGT	*EXECUTE
CRTNWIFR <sup>2</sup>	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

To use the individual operations, you must have the authority required by the individual operation.

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.

The directory that is mounted over (dir\_to\_be\_mounted\_over) is any integrated file system directory that can be mounted over.

To end any daemon jobs started by someone else, you must have \*JOBCTL special authority.

To use this command, you must have \*IOSYSCFG special authority.

### **Network Server Commands**

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDNWSSTGL <sup>2</sup>	Path (/QFPNWSSTG)	*DIR	"root" (/)	*X
	Parent directory (name of the storage space)	*DIR	"root" (/)	*WX
	Files that make up the storage space	*FILE	"root" (/)	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG <sup>2</sup>	Path (root and /QFPNWSSTG)	*DIR	"root" (/)	*WX
CHGNWSUSRA <sup>4</sup>	User Profile	*USRPRF		*OBJMGT, *USE
CRTNWSSTG <sup>2</sup>	Path (root and /QFPNWSSTG)	*DIR	"root" (/)	*WX
DLTNWSSTG <sup>2</sup>	Path (/QFPNWSSTG)	*DIR	"root" (/)	*WX
	Parent directory (name of the storage space)	*DIR	"root" (/)	*RWX, *OBJEXIST
	Files that make up the storage space	*FILE	"root" (/)	*OBJEXIST
DLTWNTSVR <sup>5</sup>	Network server description	*NWSD	QSYS.LIB	*OBJEXIST
	Line description	*LIND	QSYS.LIB	*OBJEXIST
	Network server configuration	*NWSCFG	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	*FILE	"root" (/)	*OBJEXIST
DSPNWSSTG	Path to the storage space	*DIR	"root" (/)	*X
	Files that make up the storage space	*FILE	"root" (/)	*R
INSWNTSVR <sup>6, 7</sup>	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 <sup>2</sup>	Path (/QFPNWSSTG)	*DIR	"root" (/)	*X
	Parent directory (name of the storage space)	*DIR	"root" (/)	*WX
	Files that make up the storage space	*FILE	"root" (/)	*RW
	Network server description	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Path to the storage space	*DIR	"root" (/)	*X
	Files that make up the storage space	*FILE	"root" (/)	*R

Command	Referenced Object	Object Type	File System	Authority Needed for Object
ADDRMTSVR	DSPNWSALS		SNDNWSMSC	x x
CHGNWSA 4(Q)	DSPNWSSSN		WRKNWSALS	S
CHGNWSALS	DSPNWSSTC		WRKNWSENI	3
CRTNWSALS	DSPNWSUSR		WRKNWSSSN	I
DLTNWSALS	DSPNWSUSRA		WRKNWSSTS	
DSPNWSA	SBMNWSCMD (Q) <sup>3</sup>			

- Adopted authority is not used for Network Server commands.
- To use this command, you must have \*IOSYSCFG special authority.
- To use this command, you must have \*JOBCTL special authority.
- You must have \*SECADM special authority to specify a value other than \*NONE for the NDSTREELST and the NTW3SVRLST parameters.
- To use this command, you must have \*IOSYSCFG and \*ALLOBJ special authorities.
- To use this command, you must have \*IOSYSCFG, \*ALLOBJ, and \*JOBCTL special authorities.
- You must have \*SECADM special authority to specify a nondefault value for the IPSECRULE, CHAPAUT, or SPCERTID parameter.

## **Network Server Configuration Commands**

		- I	Authority Needed
Command	Referenced Object	For Object	For QUSRSYS Library
CHGNWSCFG <sup>1, 3</sup>	Network server configuration	*CHANGE	*EXECUTE
CRTNWSCFG <sup>1, 3</sup>	Network server configuration	*USE	*READ, *ADD
DLTNWSCFG <sup>1, 3</sup>	Network server configuration	*OBJEXIST	*EXECUTE
DSPNWSCFG <sup>1, 3</sup>	Network server configuration	*USE	*EXECUTE
INZNWSCFG <sup>1, 2</sup>	Network server configuration	*CHANGE	*EXECUTE
WRKNWSCFG <sup>1</sup>	Network server configuration	*USE	*EXECUTE

- To use this command, you must have \*IOSYSCFG special authority.
- To use this command, you must have \*SECADM special authority.
- 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**

		Authorit	Authority Needed		
Command	Referenced Object	For Object	For QSYS Library		
CHGNWSD <sup>2</sup>	Network server description	*CHANGE, *OBJMGT	*EXECUTE		
	NetBIOS description (NTB)	*USE	*EXECUTE		
CRTNWSD <sup>2</sup>	NetBIOS description (NTB)	*USE	*EXECUTE		
	Line description (PORTS)	*USE	*EXECUTE		
DLTNWSD	Network server description	*OBJEXIST	*EXECUTE		
DSPNWSD	Network server description	*USE	*EXECUTE		
WRKNWSD1	Network server description	*OBJOPR	*EXECUTE		

To use an individual operation, you must have the authority required by the operation.

### **Node List Commands**

		Author	Authority Needed	
Command	Referenced Object	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	

**Office Services Commands** 

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

These commands do not require object authorities.			
ADDACC (Q) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT <sup>2,3,6</sup> (Q) GRTUSRPMN <sup>1,2</sup> RMVACC <sup>1</sup> (Q) RVKACCAUT <sup>1</sup>	RVKUSRPMN <sup>1,2</sup> WRKDOCLIB <sup>4</sup> WRKDOCPRTQ <sup>5</sup>	

To use this command, you must have \*IOSYSCFG special authority.

- You must have \*ALLOBJ special authority to grant or revoke access code authority or document authority for other users.
- Access is restricted to documents, folders, and mails that are not personal.
- 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.
- 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.
- You must have all object (\*ALLOBJ) or security administrator (\*SECADM) special authority to grant access code authority for other users.

### **Online Education Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
CVTEDU			
STREDU			

# **Operational Assistant Commands**

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

		Au	thority Needed
Command	Referenced Object	For Object	For Library
CHGBCKUP 1	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP <sup>2</sup>			
CHGPWRSCD <sup>3</sup>			
CHGPWRSCDE <sup>3</sup>			
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 <sup>1</sup>	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE
ENDCLNUP <sup>4</sup>	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, member QCURRENT	*USE	*EXECUTE
	ASP device (if specified)	*USE	

### **Operational Assistant Commands**

		Au	thority Needed
Command	Referenced Object	For Object	For Library
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) <sup>5</sup>	ASP device (if specified)	*USE	
RTVPWRSCDE	DSPPWRSCD command	*USE	
RUNBCKUP 1	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Commands: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP <sup>4</sup>	QPGMR User profile	*USE	
	Job queue	*USE	*EXECUTE

You must have \*ALLOBJ or \*SAVSYS special authority.

# **Optical Commands**

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

		Authority Needed			
Command	Referenced Object	Object	Library	Optical Volume 1	
ADDOPTCTG (Q)	Optical Device	*USE	*EXECUTE		
ADDOPTSVR (Q)	Server CSI	*USE	*EXECUTE		
CHGDEVOPT⁴	Optical Device	*CHANGE, *OBJMGT	*EXECUTE		
CHGOPTA (Q)					
CHGOPTVOL	Root directory (/) of volume when changing the Text Description <sup>5</sup>	*W	N/A	N/A	
	Optical Device	*USE	*EXECUTE	*CHANGE <sup>3</sup>	
	Server CSI	*USE	*EXECUTE	N/A	
CHKOPTVOL	Optical device	*USE	*EXECUTE	*USE	
	Root directory (/) of volume	*RWX	N/A	N/A	

You must have \*ALLOBJ, \*SECADM, and \*JOBCTL special authorities.

You must have \*ALLOBJ and \*SECADM special authorities.

You must have \*JOBCTL special authority.

You must have \*ALLOBJ special authority.

			Authority Need	ded
Command	Referenced Object	Object	Library	Optical Volume 1
СРҮОРТ	Optical Device	*USE	*EXECUTE	*USE - Source Volume
				*ALL - Target Volume
	Each preceding dir in path of source file	*X	N/A	N/A
	Each preceding dir in path of target file	*X	N/A	N/A
	Source file (*DSTMF) <sup>5</sup>	*R	N/A	N/A
	Parent dir of target file	*WX	N/A	N/A
	Parent of parent dir if creating dir	*WX	N/A	N/A
СРҮОРТ	Target file if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target file if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
	Each dir in path that precedes source dir	*X	N/A	N/A
	Each dir in path that precedes target dir	*X	N/A	N/A
СРҮОРТ	Dir being copied <sup>5</sup>	*R	N/A	N/A
	Dir being copied if it contains entries	*RX	N/A	N/A
	Parent of target dir	*WX	N/A	N/A
	Target dir if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target dir if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
	Target dir if entries are to be created	*WX	N/A	N/A
СРҮОРТ	Source files	*R	N/A	N/A
	Target file if replaced due to SLTFILE(*ALL)	*W	N/A	N/A
	Target file if replaced due to SLTFILE(*CHANGED)	*RW	N/A	N/A
CRTDEVOPT <sup>4</sup>	Optical Device		*EXECUTE	
CVTOPTBKU	Optical Device	*USE	*EXECUTE	*ALL
DSPOPT	Path Prefix when DATA (*SAVRST) <sup>5</sup>	*X	N/A	N/A
	File Prefix when (*SAVRST) <sup>2</sup>	*R	N/A	N/A
	Optical Device	*EXECUTE	*USE	
	Server CSI	*USE	*EXECUTE	
DSPOPTLCK				

#### **Optical Commands**

			Authority Need	led		
Command	Referenced Object	Object	Library	Optical Volume 1		
DSPOPTSVR	Server CSI	*USE	*EXECUTE			
DUPOPT	Optical Device	*USE	*EXECUTE	*USE - Source Volume		
				*ALL - Target Volume		
INZOPT	Root directory (/) of volume	*RWX	N/A	N/A		
	Optical Device	*USE	*EXECUTE	*ALL		
LODOPTFMW	Stream file	*R	N/A	N/A		
	Path prefix	Refer to the general rules.				
RCLOPT (Q)	Optical Device	*USE	*EXECUTE			
RMVOPTCTG (Q)	Optical Device	*USE	*EXECUTE			
RMVOPTSVR (Q)	Server CSI	*USE	*EXECUTE			
WRKHLDOPTF <sup>2</sup>	Optical Device	*USE	*EXECUTE	*USE		
	Server CSI	*USE	*EXECUTE			
WRKOPTDIR <sup>2</sup>	Optical Device	*USE	*EXECUTE	*USE		
	Server CSI	*USE	*EXECUTE			
WRKOPTF <sup>2</sup>	Optical Device	*USE	*EXECUTE	*USE		
	Server CSI	*USE	*EXECUTE			
WRKOPTVOL <sup>2</sup>	Optical Device	*USE	*EXECUTE			

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.

There are seven options that can be invoked from the optical utilities that are not commands themselves. These options and their required authorities to the optical volume are shown below.

Delete File: \*CHANGE Rename File: \*CHANGE Delete Directory: \*CHANGE Create Directory: \*CHANGE Rename Volume: \*ALL

Release Held Optical File: \*CHANGE

Save Held Optical File: \*USE - Source Volume, \*Change - Target Volume

- 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.
- To use this command, you must have \*IOSYSCFG special authority.
- 5 This authority check is only made when the Optical media format is Universal Disk Format (UDF).

# **Output Queue Commands**

	Referenced	Output Qu	ueue Parameters	Special	Authorit	Authority Needed	
Command	Object	AUTCHK	OPRCTL	Authority	For Object	For Library	
CHGOUTQ 1	Data queue				*READ	*EXECUTE	
	Output queue	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE	
		*OWNER			Owner <sup>2</sup>	*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 <sup>2</sup>	*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 <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE	
		*OWNER			Owner <sup>2</sup>	*EXECUTE	
			*YES	*JOBCTL		*EXECUTE	
PRTQAUT <sup>4</sup>							
RLSOUTQ 1	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE	
		*OWNER			Owner <sup>2</sup>	*EXECUTE	
			*YES	*JOBCTL		*EXECUTE	
WRKOUTQ 1,3	Output queue				*READ	*EXECUTE	
			*YES	*JOBCTL		*EXECUTE	
WRKOUTQD	Output queue				*READ	*EXECUTE	
1,3			*YES	*JOBCTL		*EXECUTE	

#### **Output Queue Commands**

	Referenced	erenced Output Queue Parameters		Special	Authority Needed	
Command	Object	AUTCHK	OPRCTL	1	For Object	For Library

- 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.
- You must be the owner of the output queue.
- 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.
- You must have \*ALLOBJ special authority to use this command.

# **Package Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
CRTSQLPKG	Program	*OBJOPR, *READ	*EXECUTE	
	SQL package: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE	
	SQL package: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE	
DLTSQLPKG	Package	*OBJEXIST	*EXECUTE	
PRTSQLINF	Package	*OBJOPR, *READ	*EXECUTE	
	Program	*OBJOPR, *READ	*EXECUTE	
	Service program	*OBJOPR, *READ	*EXECUTE	
STRSQL				

### **Performance Commands**

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

		Autho	ority Needed
Command	Referenced Object	For Object	For Library
ADDPEXDFN (Q) 5	PGM Library		*EXECUTE
ADDPEXFTR (Q) <sup>5</sup>	PGMTRG Library		*EXECUTE
	PGMFTR Library		*EXECUTE
	JVAFTR Path	*X for directory	
	PATHFTR Path	*X for directory	
ANZBESTMDL (Q) <sup>4</sup>	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Application libraries that contain the database files to be analyzed		*EXECUTE
	Job description	*USE	*EXECUTE
ANZDBF (Q) <sup>4</sup>	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Job description	*USE	*EXECUTE

#### **Performance Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
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 <sup>2</sup>		*ADD, *READ	
ANZPFRDTA (Q) <sup>4</sup>	QPFR/QACVPP *PGM	*USE	*EXECUTE	
	Performance data <sup>2</sup>		*ADD, *READ	
ANZPFRDT2 (Q) <sup>4</sup>	QPFR/QAVCPP *PGM	*USE	*EXECUTE	
	QAPTAPGP *FILE	*CHANGE	*EXECUTE	
	DLTFCNARA command (Q)	*USE	*EXECUTE	
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE	
CFGPFRCOL (Q)	Collection library		*EXECUTE	
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE	
	QAPGGPHF *FILE	*CHANGE	*EXECUTE	
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE	
	QAPGPKGF *FILE	*CHANGE	*EXECUTE	
	QAPGGPHF *FILE	*USE	*EXECUTE	
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE	
	QAPMDMPT *FILE	*CHANGE	*EXECUTE	
CHGJOBTYP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE	
CHGPEXDFN (Q) <sup>5</sup>	PGM Library		*EXECUTE	
CHKPFRCOL (Q)				
CPYFCNARA (Q) <sup>4</sup>	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE	
	QAPGGPHF *FILE in "From" library	*USE	*EXECUTE	
	"To" library (if QAPGGPHF *FILE does not exist)		*EXECUTE, *ADD	
	QAPGGPHF *FILE in "To" library (if adding a new graph format or replacing an existing one)	*CHANGE	*EXECUTE	
CPYGPHFMT (Q) <sup>4</sup>	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	

#### **Performance Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE	
	From library		*EXECUTE	
	To library		*EXECUTE, *ADD	
	Job description	*USE	*EXECUTE	
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE	
	Performance data (all QAPM* files)	*USE	*EXECUTE	
	Model library		*EXECUTE, *ADD	
	Job description	*USE	*EXECUTE	
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE	
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE	
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE	
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE	
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE	
	Library where the Functional Area is created		*EXECUTE, *ADD	
	QAPTAPGP *FILE in target library (if adding a new functional area)	*CHANGE	*EXECUTE	
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE	
	Library where the Graph Format is created		*EXECUTE, *ADD	
	QAPGGPHF *FILE in target library (if adding a new graph format)	*CHANGE	*EXECUTE	
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE	
	Library where the Graph Package is created		*EXECUTE, *ADD	
	QAPGGPHF *FILE	*CHANGE	*EXECUTE	
	QAPGPKGF *FILE in target library (if adding a new graph package)	*USE	*EXECUTE	
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE	
	Library where the historical data is created		*ADD, *READ	
	Job description	*USE	*EXECUTE	
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE	
	To Library		*ADD, *READ	
CRTPEXDTA (Q) <sup>5</sup>	*MGTCOL Library		*EXECUTE	
	Data library <sup>1</sup>		*READ, *ADD <sup>2</sup>	
CRTPFRDTA (Q)	From Library		*EXECUTE	
	To Library		*ADD, *READ	
	From Library		*USE	
CVTPFRDTA (Q)	Job description	*USE	*EXECUTE	
CVTPFRTHD (Q)	Performance data <sup>2</sup>		*ADD, *READ	
	Model library		*EXECUTE, *ADD	
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE	
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE	

		Authority Needed	
Command	Referenced Object	For Object	For Library
DLTBESTMDL (Q) <sup>4</sup>	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE in the functional area library	*CHANGE	*EXECUTE
DLTFCNARA (Q) <sup>4</sup>	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE in the graph format library	*CHANGE	*EXECUTE
DLTGPHFMT (Q) <sup>4</sup>	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE in the graph package library	*CHANGE	*EXECUTE
DLTGPHPKG (Q) <sup>4</sup>	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) <sup>4</sup>	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE
DLTPEXDTA (Q) <sup>5</sup>	Data Library <sup>1</sup>		*EXECUTE, *DELETE
DLTPFRDTA (Q) <sup>4</sup>	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	Output file	Refer to the general rules	Refer to the general rules
DMPTRC (Q) <sup>5</sup>	Library where the trace data will be stored		*EXECUTE, *ADD
	Output file (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q) <sup>4</sup>	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Historical data library		*EXECUTE
DSPPFRDTA (Q) <sup>4</sup>	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Format or package library		*EXECUTE
	Performance data <sup>2</sup>		*EXECUTE
	Output file library		*EXECUTE, *ADD
	Output queue	*USE	*EXECUTE
	Job description	*USE	*EXECUTE
DSPPFRGPH (Q) <sup>4</sup>	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Output file library		*EXECUTE
	Job description	*USE	*EXECUTE
ENDJOBTRC (Q) <sup>4</sup>	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDPEX (Q) <sup>5</sup>	Data Library <sup>1</sup>		*READ, *ADD <sup>2</sup>
ENDPFRCOL (Q)			
PRTACTRPT (Q) <sup>4</sup>	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Performance data <sup>2</sup>	*USE	*ADD, *READ
	Job description	*USE	*EXECUTE

### **Performance Commands**

		Autho	thority Needed	
Command	Referenced Object	For Object	For Library	
PRTCPTRPT (Q) <sup>4</sup>	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE	
	Performance data <sup>2</sup>		*ADD, *READ	
	Job description	*USE	*EXECUTE	
PRTJOBRPT (Q) <sup>4</sup>	QPFR/QPTITVXC *PGM	*USE	*EXECUTE	
	Performance data <sup>2</sup>		*ADD, *READ	
	Job description	*USE	*EXECUTE	
PRTJOBTRC (Q) <sup>4</sup>	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE	
	Job trace file (QAPTTRCJ) library		*EXECUTE	
	Job description	*USE	*EXECUTE	
PRTLCKRPT (Q) <sup>4</sup>	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE	
PRTPEXRPT <sup>5</sup>	Data Library <sup>1</sup>		*EXECUTE <sup>2</sup>	
	Output file	*USE	*EXECUTE, *ADD	
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE	
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE	
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE	
PRTPOLRPT (Q) <sup>4</sup>	QPFR/QPTITVXC *PGM	*USE	*EXECUTE	
	Performance data <sup>2</sup>		*ADD, *READ	
	Job description	*USE	*EXECUTE	
PRTRSCRPT (Q) <sup>4</sup>	QPFR/QPTITVXC *PGM	*USE	*EXECUTE	
	Performance data <sup>2</sup>		*ADD, *READ	
	Job description	*USE	*EXECUTE	
PRTSYSRPT (Q) <sup>4</sup>	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE	
	QAPMDMPT *FILE		*EXECUTE	
	Job description	*USE	*EXECUTE	
PRTTNSRPT (Q) <sup>4</sup>	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE	
	Trace file (QTRJOBT) library		*EXECUTE	
	Job description	*USE	*EXECUTE	
PRTTRCRPT (Q) <sup>4</sup>	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE	
RMVPEXDFN (Q) <sup>5</sup>				
RMVPEXFTR (Q) <sup>5</sup>				
STRBEST (Q) <sup>4</sup>	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE	
STRDBMON <sup>3, 4</sup>	Output file	*OBJOPR, *ADD	*EXECUTE	
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE	
STRPEX (Q) <sup>5</sup>				
STRPFRCOL (Q)				
STRPFRG (Q) <sup>4</sup>	QPFR/QPGSTART *PGM	*USE	*EXECUTE	

Authority I		ty Needed	
Command	Referenced Object	For Object	For Library
STRPFRT (Q) <sup>4</sup>	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) <sup>4</sup>	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	Output file (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q) <sup>5</sup>			
WRKPEXFTR (Q) <sup>5</sup>			
WRKSYSACT (Q) <sup>3, 4</sup>	QPFR/QITMONCP *PGM	*USE	*EXECUTE

These commands do not require any object authorities:

- ENDDBMON<sup>3</sup>
- ENDPFRTRC (Q)
- STRPFRTRC (Q)
- If the default library (QPEXDATA) is specified, authority to that library is not checked.
- Authority is needed to the library that contains the set of database files. Authority to the individual set of database files is not checked.
- To use this command, you must have \*JOBCTL special authority.
- To use this command, you must have \*SERVICE special authority.
- To use this command, you must have \*SERVICE special authority or you must be authorized to the Service Trace function of i5/OS through Application Administration in iSeries 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.

# **Print Descriptor Group Commands**

		Aut	thority Needed
Command	Referenced Object	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<sup>™</sup> Configuration Commands

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGPSFCFG 1, 2			
CRTGPSFCFG 1, 2			*READ, *ADD
DLTPSFCFG 1, 2	PSF Configuration	*OBJEXIST	*EXECUTE
DSPPSFCFG <sup>1</sup>	PSF Configuration	*USE	*EXECUTE
WRKPSFCFG 1	PSF Configuration	*READ	*EXECUTE

The PSF/400 feature is required to use this command.

### **Problem Commands**

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

	Referenced Object	Authority Needed	
Command		For Object	For Library
ADDPRBACNE (Q)	Filter	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Filter	*USE, *ADD	*EXECUTE
ANZPRB (Q)	SNDSRVRQS command	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filter	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filter	*USE, *UPD	*EXECUTE
DLTPRB (Q) <sup>3</sup>	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 <sup>1</sup>	*USE	*EXECUTE
	Controller description <sup>1</sup>	*USE	*EXECUTE
	Network ID <sup>1</sup>	*USE	*EXECUTE
VFYOPT (Q)	Device description	*USE	*EXECUTE
VFYTAP <sup>4</sup> (Q)	Device description	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Device description	*USE	*EXECUTE
WRKPRB (Q) <sup>2</sup>	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE	*EXECUTE

<sup>\*</sup>IOSYSCFG special authority is required to use this command.

		Authority Needed	
Command	Referenced Object	For Object	For Library

- You need \*USE authority to the communications object you are verifying.
- You must have \*USE authority to the SNDSRVRQS command to be able to report a problem.
- 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.
- <sup>4</sup> You must have \*IOSYSCFG special authority when the device description is allocated by a media library device.

# **Program Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
The object authorities r Commands" on page 3	required for the CRTxxxPGM commands are list78.	sted in the Languages ta	ble in "Language
ADDBKP <sup>1</sup>	Breakpoint handling program	*USE	*EXECUTE
ADDPGM 1,2	Program	*CHANGE	*EXECUTE
ADDTRC <sup>1</sup>	Trace handling program	*USE	*EXECUTE
CALL	Program	*OBJOPR, *EXECUTE	*EXECUTE
	Service program <sup>4</sup>	*EXECUTE	*EXECUTE
CHGDBG	Debug operation	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR <sup>1</sup>			
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 <sup>7</sup>	*USE, *ADD, *DLT
CHGPGMVAR <sup>1</sup>			
CHGPTR <sup>1</sup>			
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 <sup>7</sup> , *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA 1			

### **Program Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
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
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 <sup>3</sup>
DSPBKP <sup>1</sup>			
DSPDBG <sup>1</sup>			
DSPDBGWCH			
DSPMODSRC <sup>2, 4</sup>	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 <sup>1</sup>			
DSPSRVPGM	Service program	*READ	*EXECUTE
	Service program, if DETAIL(*MODULE) specified	*USE	*EXECUTE
DSPTRC <sup>1</sup>			
DSPTRCDTA <sup>1</sup>			

		Authority Needed	
Command	Referenced Object	For Object	For Library
ENDCBLDBG (COBOL/400 licensed program or S/38 environment)	Program	*CHANGE	*EXECUTE
ENDDBG <sup>1</sup>	Source debug program	*USE	*USE
ENDRQS <sup>1</sup>			*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 <sup>1</sup>			
RMVTRC <sup>1</sup>			
RSMBKP <sup>1</sup>			
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Database source file	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	Attention-key-handling program	*EXECUTE	*EXECUTE
SETPGMINF	Database files	*OBJOPR	*EXECUTE
	Source file	*USE	*EXECUTE
	Root program	*CHANGE	*READ, *ADD
	Subprogram	*USE	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRDBG	Program <sup>2</sup>	*CHANGE	*EXECUTE
	Source file <sup>4</sup>	*USE	*EXECUTE
	Any include files <sup>4</sup>	*USE	*EXECUTE
	Source debug program	*USE	*EXECUTE
	Unmonitored message program	*USE	*EXECUTE
TFRCTL <sup>4</sup>	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

#### **Program Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
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 <sup>6</sup>	Program	Any authority	*USE
WRKSRVPGM <sup>6</sup>	Service program	Any authority	*USE

- When a program is in a debug operation, no further authority is needed for debug commands.
- If you have \*SERVICE special authority, you need only \*USE authority to the program.
- 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.
- Applies only to ILE programs.
- See the Authorization, privileges and object ownership topic in the SQL Reference (located in the iSeries Information Center) for more information about security requirements for SQL statements.
- To use individual operations, you need the authority required by the individual operation.
- You must own the program or have \*ALLOBJ and \*SECADM special authorities.

# **QSH Shell Interpreter Commands**

The commands listed in this table do not require any authorities to objects.

		Authority Needed	
Command	Referenced Object	For Object	For Library
STRQSH 1, 2			
QSH <sup>1, 2</sup>			

QSH is an alias for the STRQSH CL command.

You need \*RX authority to all scripts and \*X authority to all directories in the path to the script.

# **Query Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
ANZQRY	Query definition	*USE	*EXECUTE
CHGQRYA <sup>4</sup>			

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTQMFORM	Query management form: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Query management form: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE
CRTQMQRY	Query management query: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Query management query: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE
	OVRDBF command	*USE	*EXECUTE
DLTQMFORM	Query management form	OBJEXIST	*EXECUTE
DLTQMQRY	Query management query	*OBJEXIST	*EXECUTE
DLTQRY	Query definition	*OBJEXIST	*EXECUTE
RTVQMFORM	Query manager form	*OBJEXIST	*EXECUTE
	Target source file	*ALL	*READ, *ADD, *EXECUTE
	ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RTVQMQRY	Query manager query	*USE	*EXECUTE
	Target source file	*ALL	*READ, *ADD
	ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM commands	*USE	*EXECUTE
RUNQRY	Query definition	*USE	*USE
	Input files	*USE	*EXECUTE
	Output files	Refer to the general rules.	Refer to the general rules.
STRQMQRY <sup>1</sup>	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, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM commands (if OUTPUT(*OUTFILE) is specified)	*USE	*EXECUTE
STRQMPRC <sup>1</sup>	Source file containing query manager procedure	*USE	*EXECUTE
	Source file containing command source file, if specified	*USE	*EXECUTE
	OVRPRTF command, if statements result in printed report or query object.	*USE	*EXECUTE

#### **Query Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
STRQRY			*EXECUTE
WRKQMFORM <sup>3</sup>	Query management form	Any authority	*USE
WRKQMQRY <sup>3</sup>	Query management query	Any authority	*USE
WRKQRY <sup>3</sup>			

- 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.
- Ownership or some authority to the object is required.
- To use individual operations, you must have the authority required by the individual operation.
- To use individual command, you must have \*JOBCTL special authority.

### **Question and Answer Commands**

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

		Au	thority Needed
Command	Referenced Object	For Object	For Library
ANSQST (Q)	Database file QAQAxxBQPY 1	*READ	*READ
ASKQST	Database file QAQAxxBBPY <sup>1</sup> or QAQAxxBQPY <sup>1</sup>	*READ	*READ
CHGQSTDB (Q)	Database file QAQAxxBQPY 1	*READ	*READ
CRTQSTDB <sup>2</sup> (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 <sup>2</sup> (Q)	Database file QAQAxxBQPY <sup>1,3</sup>	*READ	*READ, *ADD, *EXECUTE
STRQST <sup>4</sup>	Database file QAQAxxBBPY <sup>1</sup> or QAQAxxBQPY <sup>1</sup>	*READ	*READ
WRKQST	Database file QAQAxxBBPY <sup>1</sup> QAQAxxBQPY <sup>1</sup>	*READ	*USE
WRKCNTINF			*EXECUTE

		Authority Needed	
Command	Referenced Object	For Object	For Library

- 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.
- 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.
- Authority to the file is required only if loading a previously existing Question and Answer database.
- The command displays the Question and Answer menu. To use individual options, you must have the authority required by those options.

### **Reader Commands**

		Authority Needed	
Command	Referenced Object	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 of	do not require any authority to objects:	,	
ENDRDR 1	HLDRDR <sup>1</sup>	RLSRDR 1	
	be the user who started the reader, or .) special authority.	you must have all object (*ALLOF	BJ) or job control

# **Registration Facility Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

### **Relational Database Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE

### **Relational Database Commands**

Autho			rity Needed	
Command	Referenced Object	For Object	For Library	
CHGRDBDIRE	Output file, if specified	*EXECUTE	*EXECUTE	
	Remote location device description <sup>7</sup>	*CHANGE		
DSPRDBDIRE	Output file, if specified	Refer to the general rules.	Refer to the general rules.	
These commands do n	not require any authority to objects:			
RMVRDBDIRE Wrkrdbdire				
Authority ver	rified when the RDB directory entry is used.			

# **Resource Commands**

		Autho	Authority Needed	
Command	Referenced Object	For Object	For Library	
DSPHDWRSC				
DSPSFWRSC	Output file, if specified	Refer to the general rules.	Refer to the general rules.	
EDTDEVRSC				
WRKHDWRSC <sup>1</sup>				

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

	Referenced Object	Authorit	Authority Needed	
Command		For Object	For Library	
ADDFCTE	Forms control table	*DELETE, *USE, *ADD	*READ, *EXECUTE	
	Device file <sup>1,2</sup>	*USE	*READ, *EXECUTE	
	Physical file <sup>1,2</sup> (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD	
	Physical file <sup>1,2</sup> (member specified)	*USE, *ADD	*READ, *EXECUTE	
	Program <sup>1,2</sup>	*USE	*READ, *EXECUTE	
	Message queue <sup>1,2</sup>	*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 <sup>2</sup>	*USE	*READ, *EXECUTE	
	QUSER user profile	*USE	*READ, *EXECUTE	
ADDRJERDRE	Session description	*READ, *ADD, *DLT	*READ, *EXECUTE	
	Job queue <sup>2</sup>	*READ	*READ, *EXECUTE	
	Message queue <sup>2</sup>	*READ, *ADD	*READ, *EXECUTE	

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDRJEWTRE	Session description	*READ, *ADD, *DLT	*READ, *EXECUTE
	Device file <sup>1,2</sup>	*USE	*READ, *EXECUTE
	Physical file <sup>1,2</sup> (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file <sup>1.2</sup> (member specified)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program <sup>1,2</sup>	*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 <sup>1,2</sup>	*USE	*READ, *EXECUTE
	Physical file <sup>1,2</sup> (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file <sup>1,2</sup> (member specified)	*USE, *ADD	*READ, *EXECUTE
	Program <sup>1,2</sup>	*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 <sup>2</sup>	*USE	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
CHGRJERDRE	Session description	*USE, *ADD, *DLT	*READ, *EXECUTE
	Job queue <sup>2</sup>	*USE	*READ, *EXECUTE
	Message queue <sup>2</sup>	*USE, *ADD	*READ, *EXECUTE
CHGRJEWTRE	Session description	*USE	*READ, *EXECUTE
	Device File <sup>1,2</sup>	*USE	*READ, *EXECUTE
	Physical file <sup>1,2</sup> (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Physical file <sup>1,2</sup> (member specified)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program <sup>1,2</sup>	*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 <sup>1,2</sup>	*USE	*EXECUTE
	Message queue <sup>1,2</sup>	*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

		Autho	ority Needed
Command	Referenced Object	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 <sup>3</sup>	*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 <sup>1,2</sup>	*USE	*EXECUTE
	Message queue 1,2	*USE, *ADD	*EXECUTE
	Forms control table <sup>1,2</sup>	*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

		Authority Needed	
Command	Referenced Object	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 <sup>4</sup>	*OBJEXIST	*EXECUTE
	Controller description <sup>4</sup>	*OBJEXIST	*EXECUTE
	Line description <sup>4</sup>	*OBJEXIST	*EXECUTE
DLTSSND	Session description	*OBJEXIST	*EXECUTE
DSPRJECFG	Session description	*READ	*EXECUTE
ENDRJESSN <sup>5</sup>	Session description	*USE	*EXECUTE
RMVFCTE	Forms control table	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJECMNE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Session description	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Session description	*USE	*EXECUTE
SBMRJEJOB	Session description	*USE	*EXECUTE
	Input file <sup>6</sup>	*USE	*EXECUTE
	Message queue	*USE, *ADD	*EXECUTE
	Job-related objects <sup>7</sup>		
SNDRJECMD	Session description	*USE	*EXECUTE
STRRJECSL	Session description	*USE	*EXECUTE
	Message queue	*USE	*EXECUTE
STRRJERDR	Session description	*USE	*USE
STRRJESSN <sup>5</sup>	Session description	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	User profile QUSER	*USE	*EXECUTE
	Job-related objects <sup>7</sup>		*EXECUTE

		Authorit	y Needed
Command	Referenced Object	For Object	For Library
STRRJEWTR	Session description	*USE	*USE
	Program <sup>1</sup>	*USE	*READ, *EXECUTE
	Device file <sup>1</sup>	*USE, *ADD	*READ, *EXECUTE
	Physical file <sup>1</sup> (RJE generates members)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Physical file <sup>1</sup> (member specified)	*READ, *ADD	*READ, *EXECUTE
	Message queue <sup>1</sup>	*USE, *ADD	*READ, *EXECUTE
	QUSER user profile	*USE	*READ, *EXECUTE
WRKFCT <sup>8</sup>	Forms control table	*USE	*EXECUTE
WRKRJESSN <sup>8</sup>	Session description	*USE	*EXECUTE
WRKSSND <sup>8</sup>	Session description	*CHANGE	*EXECUTE

- User profile QUSER requires authority to this object.
- 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.
- This authority is required to create job description QRJESSN.
- This authority is only required when DLTCMN(\*YES) is specified.
- <sup>5</sup> You must have \*JOBCTL special authority.
- Input files include those imbedded using the .. READFILE control statement.
- Review the authorities that are required for the SBMJOB command.
- To use an individual operation, you must have the authority required by the operation.

# **Security Attributes Commands**

		Au	thority Needed
Command	Referenced Object	For Object	For Library
CHGSECA 1			
CHGSECAUD 2,3			
CFGSYSSEC 1,2,3			
DSPSECA			
DSPSECAUD <sup>3</sup>			
PRTSYSSECA <sup>4</sup>			

- You must have \*SECADM special authority to use this command.
- You must have \*ALLOBJ special authority to use this command.
- You must have \*AUDIT special authority to use this command.
- You must have \*ALLOBJ or \*AUDIT special authority to use this command.

# **Server Authentication Entry Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDSVRAUTE <sup>1</sup>			
CHGSVRAUTE <sup>1</sup>			
DSPSVRAUTE	User profile	*READ	*EXECUTE
RMVSVRAUTE <sup>1</sup>			

If the user profile for this operation is not \*CURRENT or the current user for the job, you must have \*SECADM special authority and \*OBJMGT and \*USE authority to the profile.

### **Service Commands**

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

		Authority Needed	
Command	Referenced Object	For Object	For Library
ADDTRCFTR <sup>11</sup>			
APYPTF (Q)	Product library	*OBJMGT	
CHGSRVA <sup>3</sup> (Q)			
CHKCMNTRC <sup>3</sup> (Q)			*EXECUTE
CHKPRDOPT (Q)	All objects in product option <sup>4</sup>		
CPYPTF <sup>2</sup> (Q)	From file	*USE	*EXECUTE
	To-file <sup>8</sup>	Same requirements as the SAVOBJ command	Same requirements as the SAVOBJ command
	Device description	*USE	*EXECUTE
	Licensed program		*USE
	Commands: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF, and OVRTAPF	*USE	*EXECUTE
	QSRV library	*USE	*EXECUTE
CPYPTFGRP <sup>2</sup> (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 <sup>3</sup> (Q)	NWID (network ID) or line description	*USE	*EXECUTE
DLTPTF (Q)	Cover letter file <sup>4</sup>		*EXECUTE
	PTF save file <sup>4</sup>		*EXECUTE

### **Service Commands**

		Authori	ty Needed
Command	Referenced Object	For Object	For Library
DLTTRC (Q)	RMVM command	*USE	
	QSYS Library	*EXECUTE	
	Database Files	*OBJEXIST, *OBJOPR	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Output file	Refer to the general rules.	Refer to the general rules.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
ENDCMNTRC <sup>3</sup> (Q)	NWID or line description	*USE	*EXECUTE
ENDCPYSCN (Q)	Device description	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	QSYS Library	*ADD, *EXECUTE	
	Database files	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Commands: PTRTRC, DLTTRC	*USE	
EDNWCH <sup>16</sup> (Q)	Watch sessions watching for a message within a job log <sup>18</sup>		
INSPTF <sup>9</sup> (Q)			
LODPTF (Q)	Device Description	*USE	*EXECUTE
LODRUN <sup>2</sup>	RSTOBJ command	*USE	*EXECUTE
PRTCMNTRC <sup>3</sup> (Q)	NWID (network ID) or line description	*USE	*EXECUTE
	Output file	Refer to the general rules.	Refer to the general rules.
PRTERRLOG (Q)	Output file	Refer to the general rules.	Refer to the general rules.
PRTINTDTA <sup>12,13</sup> (Q)			
PRTTRC <sup>11</sup> (Q)	QSYS Library	*EXECUTE	
	Database Files	*USE	
	DLTTRC command	*USE	
RMVPTF (Q)	Product library	*OBJMGT	
RMVTRCFTR <sup>11</sup>			
RUNLPDA (Q)	Line description	*READ	*EXECUTE
SAVAPARDTA <sup>6</sup> (Q)	Commands: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERRLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB, and WRKSYSVAL	*USE	*EXECUTE
	Existing problem <sup>7</sup>	*CHANGE	*EXECUTE
SNDPTFORD 10 (Q)			

### **Service Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
SNDSRVRQS (Q)			
STRCMNTRC <sup>11</sup> (Q)	NWID (network ID) or line description	*USE	*EXECUTE
	Watched job <sup>17</sup>		
	Trace 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 <sup>3</sup> (Q)			
STRTRC (Q) <sup>11, 15</sup>	Watched job <sup>17</sup>		
	Trace program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
STRWCH <sup>16</sup> (Q)	Watched job <sup>17</sup>		
	Watch program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
TRCCNN <sup>11</sup> (Q)	Watched job <sup>17</sup>		
	Trace program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT <sup>11</sup> (Q)	Watched job <sup>17</sup>		
	Trace 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
TRCTCPAPP <sup>11</sup> (Q)	Line description	*USE	
	Network interface	*USE	
	Network interface	*USE	
	Watched job <sup>17</sup>		
	Trace program	*OBJOPR and *EXECUTE	*EXECUTE
	Message queue	*USE	*USE

#### **Service Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
VFYCMN (Q)	Line description <sup>5</sup>	*USE	*EXECUTE
	Controller description <sup>5</sup>	*USE	*EXECUTE
	Network ID <sup>5</sup>	*USE	*EXECUTE
VFYLNKLPDA (Q)	Line description	*READ	*EXECUTE
VFYPRT (Q)	Device description	*USE	*EXECUTE
VFYOPT (Q)	Device description	*USE	*EXECUTE
VFYTAP <sup>14</sup> (Q)	Device description	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QPVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB 1, 10 (Q)	Line, controller, NWID (Network ID), and device based on problem analysis action	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKSRVPVD (Q)			
WRKTRC <sup>11</sup> (Q)			
WRKWCH <sup>19</sup> (Q)			

- You need authority to the PRTERRLOG command for some analysis procedures or if the error log records are being saved.
- All restrictions for the RSTOBJ command also apply.
- Service (\*SERVICE) special authority is required to run this command.
- 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.
- You need \*USE authority to the communications object that you are verifying.
- You must have \*SPLCTL special authority to save a spooled file.
- 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.
- The option to add a new member to an existing output file is not valid for this command.
- This command has the same authorities and restrictions as the APYPTF command and the LODPTF command.
- 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:
  - · You must have \*X authority to each directory in the path.
  - You must have \*WX authority to the directory that contains optical image.

|

430

Command		Referenced Object	Aut	thority Needed	
			For Object	For Library	
11	To use this command, you must have *SERVICE special authority, or be authorized to the Service Trace function of i5/OS through Application Administration in iSeries Navigator. The Change Function Usage Information (CHGFCNUSG) command, with a function ID of QIBM_SERVICE_TRACE, can also be used change the list of users that are allowed to perform trace operations.				
12	Function of Information	ommand, you must have *SERVICE speci5/OS through Application Administration (CHGFCNUSG) command, with a function of users that are allowed to perform of	on in iSeries Navigator. Th ion ID of QIBM_SERVICE_	e Change Function Usage	
13	command m internal data	nd must be issued from within the job wast be running under a user profile which being printed, or the issuer of the community.	ch is the same as the job u	ser identity of the job with	
14	You must ha device.	ve *IOSYSCFG special authority when the	he device description is all	ocated by a media library	
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 i5/OS through Application Administration in iSeries 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.				
16	To use this command, you must have service (*SERVICE) special authority, or be authorized to the service watch function of the operating system through Application Administration in iSeries 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 specific 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 Operating System through Application Administration in iSeries 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	Same author	ity required on STRWCH command.			
19	To use this of trace function iSeries Navig	ommand, you must have service (*SERV n and service watch function of the oper gator. You can also use the Change Func SERVICE_TRACE and QIBM_SERVICE_race operations.	rating system through App tion Usage (CHGFCNUSG	olication Administration in ) command, with a function	

# **Spelling Aid Dictionary Commands**

		Authori	ty Needed
Command	Referenced Object	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

### **Spelling Aid Dictionary Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
<sup>1</sup> To use an indi	vidual operation, you must have the authority	required by the operation	on.

# **Sphere of Control Commands**

		Aut	hority Needed
Command	Referenced Object	For Object	For Library
ADDSOCE	Sphere of control <sup>1</sup>	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sphere of control <sup>1</sup>	*USE, *DLT	*EXECUTE
WRKSOC	Sphere of control <sup>1</sup>	*USE	*EXECUTE
1 The spher	re of control is physical file QUSRSYS	/QAALSOC.	

# **Spooled File Commands**

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

	Referenced	Output	Queue Para	ameters	Special	Authority	Needed
Command	Object	DSPDTA	AUTCHK	OPRCTL	Authority	For Object	For Library
CHGSPLFA 1,2	Output queue <sup>3</sup>		*DTAAUT			*READ, *DLT, *ADD	
			*OWNER			Owner <sup>4</sup>	
				*YES	*JOBCTL		
CHGSPLFA <sup>1</sup> , if moving	Original output queue <sup>3</sup>		*DTAAUT			*READ, *ADD, *DLT	
spooled file			*OWNER			Owner <sup>4</sup>	
				*YES	*JOBCTL		
	Spooled file	*OWNER				Owner <sup>6</sup>	
	Target output					*READ	*EXECUTE
	queue <sup>7</sup>			*YES	*JOBCTL		*EXECUTE
	Target device					*USE	

	Referenced	Output Queue Parameters		Special	Authority Needed		
Command	Object	DSPDTA	AUTCHK	OPRCTL	Authority	For Object	For Library
CPYSPLF <sup>1</sup>	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 <sup>6</sup>	
	Output queue <sup>3</sup>	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner <sup>4</sup>	
		*YES or *NO		*YES	*JOBCTL		
DLTEXPSPLF (Q)	Independent disk pool				*SPLCTL	*EXECUTE	
DLTSPLF <sup>1</sup>	Output queue <sup>3</sup>		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner <sup>4</sup>	
				*YES	*JOBCTL		
DSPSPLF <sup>1</sup>	Output queue <sup>3</sup>	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner <sup>4</sup>	
		*YES or *NO		*YES	*JOBCTL		
	Spooled file	*OWNER				Owner <sup>6</sup>	
HLDSPLF <sup>1</sup>	Output queue <sup>3</sup>		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner <sup>4</sup>	
				*YES	*JOBCTL		
RCLSPLSTG (Q)							
RLSSPLF 1, 8	Output queue <sup>3</sup>		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Owner <sup>4</sup>	
				*YES	*JOBCTL		
SNDNETSPLF	Output queue <sup>3</sup>	*YES				*READ	
,		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner <sup>4</sup>	
		*YES or *NO		*YES	*JOBCTL		
	Spooled file	*OWNER				Owner <sup>6</sup>	

### **Spooled File Commands**

	Referenced	Output Queue Parameters		Special	Authority Needed		
	Object	DSPDTA	AUTCHK	OPRCTL	Authority	For Object	For Library
SNDTCPSPLF	Output queue <sup>3</sup>	*YES				*READ	
1,5		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Owner <sup>4</sup>	
		*YES or *NO		*YES	*JOBCTL		
	Spooled file	*OWNER				Owner <sup>6</sup>	
WRKSPLF							

- Users are always authorized to control their own spooled files.
- 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.
- If you have \*SPLCTL special authority, you do not need any authority to the output queue.
- You must be the owner of the output queue.
- 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.
- You must be the owner of the spooled file.
- 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.
- When the spooled file has been held with HLDJOB SPLFILE(\*YES) and the spooled file was also decoupled from the job, the user will need to have \*USE authority to the RLSJOB command and either have \*JOBCTL special authority or be the owner of the spooled file.

# **Subsystem Description Commands**

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

		Authori	ty Needed
Command	Referenced Object	For Object	For Library
ADDAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Job description	*OBJOPR, *READ	*EXECUTE
	User profile	*USE	
ADDJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	User profile	*USE	
	Job description	*OBJOPR, *READ	*EXECUTE

### **Subsystem Description Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
ADDRTGE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
ADDWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
	Job description	*OBJOPR, *READ	*EXECUTE	
CHGAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
	Job description	*OBJOPR, *READ	*EXECUTE	
CHGCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
	Job description	*OBJOPR, *READ	*EXECUTE	
	User profile	*USE		
CHGJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
CHGPJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
	User profile	*USE		
	Job description	*OBJOPR, *READ	*EXECUTE	
CHGRTGE	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE	
CHGSBSD <sup>5</sup>	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE	
	signon display file <sup>4</sup>	*USE	*EXECUTE	
CHGWSE	Subsystem description	*OJBOPR, *OBJMGT, *READ	*EXECUTE	
	Job description	*OBJOPR, *READ	*EXECUTE	
CRTSBSD <sup>5</sup> (Q)	Subsystem description		*READ, *ADD	
	signon display file <sup>4</sup>	*USE	*EXECUTE	
DLTSBSD	Subsystem description	*OBJEXIST, *USE	*EXECUTE	
DSPSBSD	Subsystem description	*OBJOPR, *READ	*EXECUTE	
ENDSBS <sup>1</sup>				
PRTSBSDAUT <sup>6</sup>				
RMVAJE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
RMVCMNE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	
RMVJOBQE	Subsystem description	*OBJOPR, *OBJMGT, *EXECUTE *READ		
RMVPJE	Subsystem description	*OBJOPR, *OBJMGT, *EXECUTE *READ		
RMVRTGE	Subsystem description	*OBJOPR, *OBJMGT, *EXECUTE *READ		
RMVWSE	Subsystem description	*OBJOPR, *OBJMGT, *READ	*EXECUTE	

### **Subsystem Description Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
STRSBS <sup>1</sup>	Subsystem description	*USE	*EXECUTE
WRKSBS <sup>2, 3</sup>	Subsystem description	Any authority	*USE
WRKSBSD <sup>3</sup>	Subsystem description	Any authority	*USE

- You must have job control (\*JOBCTL) special authority to use this command.
- Requires some authority (anything but \*EXCLUDE)
- To use an individual operation, you must have the authority required by the operation.
- 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.
- You must have \*SECADM or \*ALLOBJ special authority to specify a specific library for the subsystem library.
- You must have \*ALLOBJ or \*AUDIT special authority to use this command.

# **System Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
PWRDWNSYS <sup>1</sup>	Image catalog (if specified)	*USE		
These commands do not require any object authorities:				
CHGSHRPOOL DSPSYSSTS ENDSYS <sup>1</sup> RCLACTGRP <sup>1</sup>	RCLRSC RETURN RTVGRPA	SIGNOFF WRKSHRPOOL	WRKSYSSTS	
You must have job control (*JOBCTL) special authority to use this command.				

# **System Reply List Commands**

These commands do n	ot require object authorities:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE	

# **System Value Commands**

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

These commands do not	require any authority to	objects:		
CHGSYSVAL (Q) 1,2	DSPSYSVAL <sup>3</sup>	RTVSYSVAL <sup>3</sup>	WRKSYSVAL 1,2, 3	

- To change some system values, you must have \*ALLOBJ, \*ALLOBJ and \*SECADM, \*AUDIT, \*IOSYSCFG, or \*JOBCTL special authorities.
- To use this command as shipped by IBM, you must be signed on as QPGMR, QSYSOPR, or QSRV, or have \*ALLOBJ special authority.
- To display or retrieve auditing-related system values, you must have either \*AUDIT or \*ALLOBJ special authority.

# **System/36 Environment Commands**

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

		Authority N		
Command	Referenced Object	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	

### **System/36 Environment Commands**

		Authority Needed			
Command	Referenced Object	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		
DSPS36	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		

		Authority Needed		
Command	Referenced Object	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 <sup>1,2,3</sup> (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	

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.

### **Table Commands**

		Au	thority Needed
Command	Referenced Object	For Object	For Library
CRTTBL	Table		*READ, *ADD, *EXECUTE
	Source file	*USE	*EXECUTE

If used for a data dictionary, only the authority to the command is required.

You must be enrolled in the system distribution directory if the source folder is a document folder.

### **Table Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
DLTTBL	Table	*OBJEXIST	*EXECUTE
WRKTBL <sup>1</sup>	Table	Any authority	*USE
To use an individual operation, you must have the authority required by the operation.			

### **TCP/IP Commands**

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

		Au	thority Needed
Command	Referenced Object	For Object	For Library
ADDTCPSVR <sup>1</sup>	Program to call	*EXECUTE	*EXECUTE
CHGTCPSVR <sup>1</sup>	Program to call	*EXECUTE	*EXECUTE
CVTTCPCL (Q)	File objects	*USE	*EXECUTE
ENDTCP (Q)	Line description <sup>4</sup>	*USE	*EXECUTE
	Controller description <sup>4</sup>	*USE	*EXECUTE
	Device description <sup>4</sup>	*USE	*EXECUTE
	File Objects	*USE	*EXECUTE
ENDTCPIFC (Q)	File objects	*USE	*EXECUTE
	Line description <sup>4</sup>	*USE	*EXECUTE
	Controller description <sup>4</sup>	*USE	*EXECUTE
	Device description <sup>4</sup>	*USE	*EXECUTE
ENDTCPPTP	Line description <sup>4</sup>	*USE	*EXECUTE
	Controller description <sup>4</sup>	*USE	*EXECUTE
	Device description <sup>4</sup>	*USE	*EXECUTE
	File Objects	*USE	*EXECUTE
ENDTCPSRV (Q)	File objects	*USE	*EXECUTE
FTP	File objects	*USE	*EXECUTE
	Table objects	*USE	*EXECUTE
LPR <sup>2</sup>	Workstation customizing object	*USE	*EXECUTE
SETVTTBL	Table objects	*USE	*EXECUTE
SNDTCPSPLF <sup>2</sup>	Workstation customizing object	*USE	*EXECUTE
STRTCP (Q)	File objects	*USE	*EXECUTE
	Line description <sup>4</sup>	*USE	*EXECUTE
	Controller description <sup>4</sup>	*USE	*EXECUTE
	Device description <sup>4</sup>	*USE	*EXECUTE
STRTCPFTP	Table objects	*USE	*EXECUTE
	File objects	*USE	*EXECUTE

### **Transmission Control Protocol/Internet Protocol Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
STRTCPIFC (Q)	File objects	*USE	*EXECUTE	
	Line description <sup>4</sup>	*USE	*EXECUTE	
	Controller description <sup>4</sup>	*USE	*EXECUTE	
	Device description <sup>4</sup>	*USE	*EXECUTE	
STRTCPPTP	Line description <sup>4</sup>	*USE	*EXECUTE	
	Controller description <sup>4</sup>	*USE	*EXECUTE	
	Device description <sup>4</sup>	*USE	*EXECUTE	
	File Objects	*USE	*EXECUTE	
STRTCPSVR (Q)	Table objects	*USE	*EXECUTE	
	File objects	*USE	*EXECUTE	
STRTCPTELN	Table objects	*USE	*EXECUTE	
	File objects	*USE	*EXECUTE	
	Virtual workstation device <sup>5</sup>	*USE	*EXECUTE	
TELNET	Table objects	*USE	*EXECUTE	
	File objects	*USE	*EXECUTE	
	Virtual workstation device <sup>5</sup>	*USE	*EXECUTE	
These commands do	not require any object authorities:			
ADDCOMSNMP ADDNETTBLE ADDPCLTBLE ADDSRVTBLE ADDTCPHTE ADDTCPHTE ADDTCPIFC ADDTCPPORT ADDTCPRSI ADDTCPRTE CFGTCP CFGTCPAPP CFGTCPLPD CFGTCPLPD ADDNETTBLE ADDTCPTP CFGTCPLPD ADDTCPTP AD	CFGTCPSMTP CFGTCPSNMP CFGTCPTELN CHGCOMSNMP <sup>1</sup> CHGFTPA <sup>1</sup> CHGLPDA <sup>1</sup> CHGSMTPA <sup>1</sup> CHGSNMPA <sup>1</sup> CHGTCPA <sup>1</sup> CHGTCPATCHGTCPHTE <sup>1</sup> CHGTCPHTE <sup>1</sup> CHGTCPRTE <sup>1</sup> CHGTCPRTE <sup>1</sup> CHGTCPRTE <sup>1</sup> CHGTCPRTE <sup>1</sup> CHGTCPLNA <sup>1</sup>	CHGVTMAP DSPVTMAP ENDTCPCNN MGRTCPHT <sup>1</sup> NETSTAT PING RMVCOMSNMP <sup>1</sup> RMVNETTBLE <sup>1</sup> RMVPCLTBLE <sup>1</sup> RMVSRVTBLE <sup>1</sup> RMVTCPHTE <sup>1</sup> RMVTCPHTE <sup>1</sup> RMVTCPFC <sup>1</sup>	RMVTCPRSI <sup>1</sup> RMVTCPRTE <sup>1</sup> RMVTCPSVR <sup>1</sup> RNMTCPHTE <sup>1</sup> SETVTMAP VFYTCPCNN WRKNAMSMTP <sup>3</sup> WRKNETTBLE <sup>1</sup> WRKPCLTBLE <sup>1</sup> WRKSRVTBLE <sup>1</sup> WRKTCPSTS	

You must have \*IOSYSCFG special authority to use this command.

# **Time Zone Description Commands**

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

The SNDTCPSPLF command and the LPR command use the same combinations of referenced object authorities as the SNDNETSPLF command.

You must have \*SECADM special authority to change the system alias table or another user profile's alias table.

If you have \*JOBCTL special authority, you do not need the specified authority to the object.

If you have \*JOBCTL special authority, you do not need the specified authority to the object on the remote system.

### **Time Zone Description Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CHGTIMZON	Time zone description	*CHANGE	*EXECUTE
CRTTIMZON	Time zone description		*READ, *ADD
DLTTIMZON1	Time zone description	*OBJEXIST	*EXECUTE
WRKTIMZON <sup>2</sup>	Time zone description	*USE	*USE

The time zone description specified in the QTIMZON system value cannot be deleted.

# **Upgrade Order Information Data Commands**

These commands are shipped with public authority \*EXCLUDE. Appendix C shows which IBM-supplied user profiles are authorized to the command. The security officer can grant \*USE authority to others.

		Auth	Authority Needed	
Command	Referenced Object	For Object	For Library	
WRKORDINF	QGPL/QMAHFILE file	*CHANGE, *OBJALTER	*EXECUTE	

# 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**

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 ge	eneral rules.	
CRTUDFS 1,2,6,7 (Q)	/dev/QASPxx or /dev/IASPname	*DIR	"root" (/)	*RWX
DLTUDFS 1,2,4,5,8,9 (Q)	/dev/QASPxx or /dev/IASPname	*DIR	"root" (/)	*RWX
	any_epfs_object		"root" (/)	*RWX, *OBJEXIST
DSPUDFS	some_dirsxx	*DIR	"root" (/)	*RX
MOUNT 1,2,3	dir_to_be_ mounted_over	*DIR	"root" (/)	*W
	Path Prefix	Refer to the ge	eneral rules.	
RMVMFS <sup>1</sup>				

<sup>2</sup> 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.

Command	Referenced Object	Object Type	Authority Needed for Object
UNMOUNT 1			

- To use this command, you must have \*IOSYSCFG special authority.
- There are two directory naming conventions depending on the location of the user-defined file system (UDFS). Use one of the following conventions:
  - /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.

- The directory that is mounted over (dir\_to\_be\_mounted\_over) is any integrated file system directory that can be mounted over.
- 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.
- When using the DLTUDFS commands, you must have \*OBJEXIST authority on every object in the UDFS or no objects are deleted.
- 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.
- The audit (\*AUDIT) special authority is required when specifying a value other than \*SYSVAL on the Auditing value for objects (CRTOBJAUD) parameter.
- You must have write (\*W) and execute (\*X) authority to all of the non-empty directory objects in the UDFS.
- 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:
  - · 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.

### **User Profile Commands**

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

		Au	thority Needed
Command	Referenced Object	For Object	For Library
ANZDFTPWD <sup>3, 14,</sup> <sub>15(Q)</sub>			
ANZPRFACT <sup>3, 14,</sup> <sub>15(Q)</sub>			
CHGACTPRFL <sup>14</sup> (Q)			
CHGACTSCDE <sup>3, 14,</sup> <sub>15(Q)</sub>			
CHGDSTPWD <sup>1</sup>			
CHGEXPSCDE <sup>3, 14,</sup> <sub>15</sub> (Q)			

### **User Profile Commands**

		Authority Needed		
Command	Referenced Object	For Object	For Library	
CHGPRF	User profile	*OBJMGT, *USE		
	Initial program <sup>2</sup>	*USE	*EXECUTE	
	Initial menu <sup>2</sup>	*USE	*EXECUTE	
	Job description <sup>2</sup>	*USE	*EXECUTE	
	Message queue <sup>2</sup>	*USE	*EXECUTE	
	Output queue <sup>2</sup>	*USE	*EXECUTE	
	Attention-key- handling program <sup>2</sup>	*USE	*EXECUTE	
	Current library <sup>2</sup>	*USE	*EXECUTE	
CHGPWD				
CHGUSRAUD <sup>11</sup> (Q)				
CHGUSRPRF <sup>3</sup>	User profile	*OBJMGT, *USE	*EXECUTE	
	Initial program <sup>2</sup>	*USE	*EXECUTE	
	Initial menu <sup>2</sup>	*USE	*EXECUTE	
	Job description <sup>2</sup>	*USE	*EXECUTE	
	Message queue <sup>2</sup>	*USE	*EXECUTE	
	Output queue <sup>2</sup>	*USE	*EXECUTE	
	Attention-key-handling program <sup>2</sup>	*USE	*EXECUTE	
	Current library <sup>2</sup>	*USE	*EXECUTE	
	Group profile (GRPPRF or SUPGRPPRF) <sup>2,4</sup>	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE	
CHGUSRPRTI	User profile	*CHANGE		
CHKPWD				
CRTUSRPRF 3, 12, 17	Initial program	*USE	*EXECUTE	
	Initial menu	*USE	*EXECUTE	
	Job description	*USE	*EXECUTE	
	Message queue	*USE	*EXECUTE	
	Output queue	*USE	*EXECUTE	
	Attention-key- handling program	*USE	*EXECUTE	
	Current library	*USE	*EXECUTE	
	Group profile (GRPPRF or SUPGRPPRF) <sup>4</sup>	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE	
CVTUSRCERT <sup>3, 14</sup>				
DLTUSRPRF <sup>3,9</sup>	User profile	*OBJEXIST, *USE	*EXECUTE	
	Message queue <sup>5</sup>	*OBJEXIST, *USE, *DLT	*EXECUTE	
DSPACTPRFL <sup>14</sup> (Q)				
DSPACTSCD <sup>14</sup> (Q)				
DSPAUTUSR <sup>6</sup>	User profile	*READ		
DSPEXPSCD <sup>14</sup> (Q)				

- This command can be run only if you are signed on as QSECOFR.
- You need authority only to the objects for fields you are changing in the user profile.
- \*SECADM special authority is required.
- \*OBJMGT authority to the group profile cannot come from adopted authority.
- 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.
- The display includes only user profiles to which the user running the command has the specified authority.
- See the authorities required for the GRTOBJAUT command.
- \*SAVSYS special authority is required.
- 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.
- You must have \*ALLOBJ special authority to specify a value other than \*NONE for the Allow object differences (ALWOBJDIF) parameter.
- You must have \*AUDIT special authority.
- The user whose profile is created is given these authorities to it: \*OBJMGT, \*OBJOPR, \*READ, \*ADD, \*DLT, \*UPD, \*EXECUTE.
- To use an individual operation, you must have the authority required by the operation.
- You must have \*ALLOBJ special authority to use this command.
- You must have \*JOBCTL special authority to use this command.

### **User Profile Commands**

			Au	Authority Needed		
Command		Referenced Object	For Object	For Library		
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 hav	You must have *ALLOBJ or *AUDIT special authority to use this command.				
19	and action au	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 hav	ve either *ALLOBJ or *AUDIT specia	l authority to retrieve the cur	rent OBJAUD and AUDLVL		

### **Validation List Commands**

		Authority Needed	
Command	Referenced Object	For Object	For Library
CRTVLDL	Validation list		*ADD, *READ
DLTVLDL	Validation list	*OBJEXIST	*EXECUTE

values. Otherwise, the value \*NOTAVL is displayed to indicate that the values are unavailable for retrieval.

# **Workstation Customization Commands**

	Author		ity Needed	
Command	Referenced Object	For Object	For Library	
CRTWSCST	Source file	*USE	*EXECUTE	
	Workstation customizing object, if REPLACE(*NO)		*READ, *ADD	
	Workstation customizing object, if REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD	
DLTWSCST	Workstation customizing object	*OBJEXIST	*EXECUTE	
RTVWSCST	To-file, if it exists and a new member is added	*OBJOPR, *OBJMGT, *ADD	*EXECUTE	
	To-file, if file and member exist	*OBJOPR, *ADD, *DLT	*EXECUTE	
	To-file, if the file does not exist		*READ, *ADD	

# **Writer Commands**

Command	Referenced Object	<b>Output Queue Parameters</b>		Special	Authority Needed	
		AUTCHK	OPRCTL	Authority	For Object	For Library
CHGWTR <sup>2, 4</sup>	Current output queue <sup>1</sup>	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner <sup>3</sup>	
			*YES	*JOBCTL		
	New output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner <sup>3</sup>	
			*YES	*JOBCTL		
HLDWTR <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner <sup>3</sup>	
			*YES	*JOBCTL		
RLSWTR <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Owner <sup>3</sup>	
			*YES	*JOBCTL		
STRDKTWTR <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner <sup>3</sup>	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Message queue				*OBJOPR, *ADD	*EXECUTE
	Device description				*OBJOPR, *READ	

# **Writer Commands**

Command	Referenced Object	<b>Output Queue Parameters</b>		Special	Authority Needed	
		AUTCHK	OPRCTL	Authority	For Object	For Library
STRPRTWTR <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner <sup>3</sup>	*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 <sup>1</sup>	Output queue	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Owner <sup>3</sup>	*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						

If you have \*SPLCTL special authority, you do not need any authority to the output queue.

To change the output queue for the writer, you need one of the specified authorities for the new output queue.

You must be the owner of the output queue.

You must have \*EXECUTE authority to the new output queue's library even if the user has \*SPLCTL special authority.

# **Appendix E. Object Operations and Auditing**

This appendix 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 254 describes how to set up auditing for objects.

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:**

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 Journaled Changes** 

### **CHGJRNOBJ**

Change Journaled Object

#### **CHGOBJD**

Change Object Description

### **CHGOBJOWN**

Change Object Owner

### **CRTxxxxx**

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**

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.

### **MOVOBJ**

Move Object

### 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 Journaled Changes

#### **RNMOBJ**

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

### Prompt <sup>2</sup>

Prompt override program for a change command (if one exists)

### **CHKOBJ**

Check Object

#### **ALCOBJ**

Allocate Object

### **CPROBJ**

Compress Object

#### **DCPOBJ**

**Decompress Object** 

### **DLCOBJ**

Deallocate Object

### **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.

<sup>2.</sup> 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.

### **QSYRUSRA**

Retrieve User's Authority to Object API

### **RCLTMPSTG**

**Reclaim Temporary Storage** 

#### **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:**

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):**

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):**

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** 

### **DSPAUTLOBJ**

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):**

· 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):**

Read operation

#### **CRTPGM**

Create Program

### **CRTSRVPGM**

Create Service Program

### **RTVBNDSRC**

**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):**

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):**

See Operations for Stream File (\*STMF) for \*CHRSF auditing.

### **Operations for Chart Format (\*CHTFMT):**

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):**

· 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):

· 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):**

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):**

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 **ENDPGM RCVF CALLPRC ENDRCV** RETURN **CHGVAR GOTO SNDF** COPYRIGHT **SNDRCVF** TFRCTL DCL MONMSG **DCLF** PGM WAIT

DO ELSE ENDDO

# **Operations for Connection List (\*CNNL):**

· Read operation

None

· Change operation

**ADDCNNLE** 

Add Connection List Entry

**CHGCNNL** 

**Change Connection List** 

**CHGCNNLE** 

Change Connection List Entry

**RMVCNNLE** 

Remove Connection List Entry

**RNMCNNLE** 

Rename Connection List Entry

· Operations that are not audited

**Copy** Option 3 of WRKCNNL

**DSPCNNL** 

**Display Connection List** 

RTVCFGSRC

Retrieve source of connection list

WRKCNNL

Work with Connection List

**WRKCNNLE** 

Work with Connection List Entry

# **Operations for Class-of-Service Description (\*COSD):**

· Read operation

None

Change operation

**CHGCOSD** 

Change Class-of-Service Description

CALL is audited if it is run interactively. It is not audited if it is run within a CL program.

· 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):**

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):**

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 Cross System Product Table (\*CSPTBL):**

· 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 (\*CTLD):**

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 (\*DEVD):**

· 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

#### **HLDDEVxxx**

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

### **DSPDEVD**

**Display Device Description** 

### **DSPMODSTS**

**Display Mode Status** 

### **ENDDEVRCY**

**End Device Recovery** 

#### **HLDCMNDEV**

Hold Communications Device

### **RLSCMNDEV**

Release Communications Device

#### **RSMDEVRCY**

Resume Device Recovery

### **RTVCFGSRC**

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):**

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:**

**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 \*OFCSRV 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):**

· 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

# CPYDOC <sup>3</sup>

**Copy Document** 

Note: A change entry is written if the target document already exists.

# **CRTFLR**

Create Folder

<sup>3.</sup> A change entry is written for both the document and the folder if the target of the operation is in a folder.

CVTTOFLR <sup>3</sup>

Convert to Folder

DLTDLO $^3$ 

Delete DLO

**DLTSHF** 

Delete Bookshelf

DTLDOCL <sup>3</sup>

Delete Document List

DLTDST <sup>3</sup>

**Delete Distribution** 

**EDTDLOAUT** 

Edit DLO Authority

**EDTDOC** 

**Edit Document** 

FILDOC <sup>3</sup>

File Document

**GRTACCAUT** 

**Grant Access Code Authority** 

**GRTUSRPMN** 

**Grant User Permission** 

MOVDOC <sup>3</sup>

Move Document

MRGDOC<sup>3</sup>

Merge Document

**PAGDOC** 

Paginate Document

**QHFCHGAT** 

Change Directory Entry Attributes API

**QHFSETSZ** 

Set Stream File Size API

**QHFWRTSF** 

Write Stream File API

QRYDOCLIB<sup>3</sup>

Query Document Library

Note: A change entry is written if an existing document resulting from a search is replaced.

RCVDST <sup>3</sup>

Receive Distribution

**RGZDLO** 

Reorganize DLO

**RMVACC** 

Remove access code, for any DLO to which the access code is attached

**RMVDLOAUT** 

Remove DLO authority

RNMDLO <sup>3</sup>

Rename DLO

**RPLDOC** 

Replace Document

RSTDLO <sup>3</sup>

Restore DLO

**RSTSHF** 

Restore Bookshelf

**RTVDOC** 

Retrieve Document (check out)

**RVKACCAUT** 

Revoke Access Code Authority

**RVKUSRPMN** 

**Revoke User Permission** 

SAVDLO<sup>3</sup>

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

**QHFFRCSF** 

Force Buffered Data API

**QHFLULSF** 

Lock/Unlock Stream File Range API

**QHFRTVAT** 

Retrieve Directory Entry Attributes API

**RCLDLO** 

Reclaim DLO (\*ALL or \*INT)

**WRKDOCLIB** 

Work with Document Library

**WRKDOCPRTQ** 

Work with Document Print Queue

# **Operations for Data Area (\*DTAARA):**

· 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):**

· 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):**

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

· Operations that are not audited

### **WRKDTAQ**

Work with Data Queue

### **QMHQRDQD**

Retrieve Data Queue Description API

# **Operations for Edit Description (\*EDTD):**

· 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):**

· 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):**

• No Read or Change operations are audited for the \*FCT object type.

# Operations for File (\*FILE):

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)

#### **CRTCMNF**

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)

### **CRTLF**

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

# **RMVPFCST**

Remove Physical File Constraint

#### **RMVPFTGR**

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

### **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

### **WRKPFCST**

Work with Physical File Constraints

#### WRKF

Work with File

### **Operations for First-in First-out Files (\*FIFO):**

• See Operations for Stream File (\*STMF) for the \*FIFO auditing.

# **Operations for Folder (\*FLR):**

• See operations for Document Library Object (\*DOC or \*FLR)

### **Operations for Font Resource (\*FNTRSC):**

· 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):**

· 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):**

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):**

· 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):**

Read operation

### **DSPIGCDCT**

Display IGC Dictionary

Change operation

#### **EDTIGCDCT**

**Edit IGC Dictionary** 

# **Operations for Double-Byte Character Set Sort (\*IGCSRT):**

· Read operation

#### **CPYIGCSRT**

Copy IGC Sort (from-\*ICGSRT-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-\*ICGSRT-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):**

· 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 (\*JOBD):**

Read operation

### None

Change operation

### **CHGJOBD**

Change Job Description

• Operations that are not audited

### **DSPJOBD**

Display Job Description

### **WRKJOBD**

Work with Job Description

# **QWDRJOBD**

Retrieve Job Description API

# Batch job

When used to establish a job

### **Operations for Job Queue (\*JOBQ):**

Read operation

#### None

Change operation

**Entry** When an entry is placed on or removed from the queue

### **CLRJOBQ**

Clear Job Queue

### **HLDJOBQ**

Hold Job Queue

### **RLSJOBQ**

Release Job Queue

Operations that are not audited

### ADDJOBQE "Subsystem Descriptions" on page 181

Add Job Queue Entry

### **CHGJOB**

Change Job from one JOBQ to another JOBQ

# CHGJOBQE "Subsystem Descriptions" on page 181

Change Job Queue Entry

<sup>4.</sup> An audit record is written if object auditing is specified for the subsystem description (\*SBSD).

### **QSPRJOBQ**

Retrieve job queue information

# RMVJOBQE "Subsystem Descriptions" on page 181

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

# **Operations for Job Scheduler Object (\*JOBSCD):**

· 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):**

Read operation

### **CMPJRNIMG**

**Compare Journal Images** 

### **DSPJRN**

Display Journal Entry for user journals

### **QJORJIDI**

Retrieve Journal Identifier (JID) Information

### QjoRetrieveJournalEntries

**Retrieve Journal Entries** 

### **RCVJRNE**

Receive Journal Entry

#### **RTVJRNE**

Retrieve Journal Entry

· Change operation

#### **ADDRMTJRN**

Add Remote Journal

### **APYJRNCHG**

**Apply Journaled 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 Journaled 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):**

· 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):**

· 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

#### **Notes:**

- 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):**

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:**

**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):**

· 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):**

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):**

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

#### **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

### **RTVBNDSRC**

Retrieve Binder Source

#### **WRKMOD**

Work with Module

### **Operations for Message File (\*MSGF):**

· 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):**

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

## **QMHRMVM**

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):**

· Read operation

#### **DSPNODGRP**

Display Node Group

· Change operation

## **CHGNODGRPA**

Change Node Group

## **Operations for Node List (\*NODL):**

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):**

· 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):**

· 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):**

Read operation

#### **SAVCFG**

Save Configuration

Change operation

## **CHGNWSD**

Change Network Server Description

#### **VRYCFG**

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):**

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 5

Change Spooled File Attributes, if moved to a different output queue and either output queue is audited

## **CLROUTQ**

Clear Output Queue

## DLTSPLF 5

Delete Spooled File

## **HLDOUTQ**

**Hold Output Queue** 

#### **RLSOUTQ**

Release Output Queue

· Operations that are not audited

# CHGSPLFA 5

**Change Spooled File Attributes** 

## CPYSPLF 5

Copy Spooled File

#### Create <sup>5</sup>

Create a spooled file

## DSPSPLF <sup>5</sup>

Display Spooled File

## HLDSPLF 5

Hold Spooled File

## **QSPROUTQ**

Retrieve output queue information

## RLSSPLF 5

Release Spooled File

## SNDNETSPLF 5

Send Network Spooled File

#### **WRKOUTO**

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):**

· 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

## **Operations for Page Definition (\*PAGDFN):**

Read operation

**Print** Printing a spooled file that refers to the page definition

· Change operation

None

<sup>5.</sup> This is also audited if action auditing (QAUDLVL system value or AUDLVL user profile value) includes \*SPLFDTA.

· 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):**

· 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):**

Read operation

**Open** When the page descriptor group is opened for read access by a PrintManager<sup>™</sup> 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):**

· 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

## **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):**

Read operation

#### **ADDSCHIDXE**

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):**

· 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):**

· 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):**

· 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):**

Read operation

## **STRQMQRY**

Start Query Management Query

## **RTVQMFORM**

Retrieve Query Management Form

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 UDB for iSeries Query Manger and SQL Development Kit.

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):**

· Read operation

#### **RTVQMQRY**

Retrieve Query Manager Query

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):**

· 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

## **ORYRUN**

Run Query

#### **RTVQMFORM**

Retrieve Query Management Form

## **RTVQMQRY**

Retrieve Query Management Query

Run Run query using WRKQRY prompt display

Run (Query Management command)

#### **RUNQRY**

Run Query

## **STRQMQRY**

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 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):**

· Read operation

None

· Change operation

None

· Operations that are not audited

None

## **Operations for Reply List:**

**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):**

· 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):**

· Read operation

**STRSCHIDX** 

Start Index Search

**WRKSCHIDXE** 

Work with Search Index Entry

• Change operation (audited if OBJAUD is \*CHANGE or \*ALL)

**ADDSCHIDXE** 

Add Search Index Entry

#### **CHGSCHIDX**

**Change Search Index** 

## **RMVSCHIDXE**

Remove Search Index Entry

· Operations that are not audited

## **WRKSCHIDX**

Work with Search Index

## **Operations for Local Socket (\*SOCKET):**

Read operation

#### connect

Bind a permanent destination to a socket and establish a connection.

## **DSPLNK**

**Display Links** 

## givedescriptor

Give File Access API

## ${\bf Qp0lGetPathFromFileID}$

Get Path Name of Object from File ID API

## **Qp0lRenameKeep**

Rename File or Directory, Keep New API

## **Qp0lRenameUnlink**

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

writev Write to File (Vector) API

## **Operations for Spelling Aid Dictionary (\*SPADCT):**

· 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:**

**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 (CLROUTQ)
- Deleting the spooled file using the DLTSPLF 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):**

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):**

· 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** 

#### **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

#### **QBNLSPGM**

List Service Program Information API

#### **QBNRSPGM**

Retrieve Service Program Information API

#### WRKSRVPGM

Work with Service Program

## **Operations for Session Description (\*SSND):**

No Read or Change operations are audited for the \*SSND object type.

## **Operations for Server Storage Space (\*SVRSTG):**

• No Read or Change operations are audited for the \*SVRSTG object type.

## **Operations for Stream File (\*STMF):**

· 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

writev Write to File (Vector) API

#### **Operations for Symbolic Link (\*SYMLNK):**

· 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

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

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):**

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):**

· Read operation

## **QDCXLATE**

Translate character string

#### **QTBXLATE**

Translate character string

#### **QLGRTVSS**

Retrieve sort sequence table

#### **CRTLF**

Translation Table during CRTLF 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):**

· 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

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.

Retrieve User Index Attributes API

# **Operations for User Profile (\*USRPRF):**

· 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

#### **GRTUSRAUT**

Grant 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

## **GRTUSRAUT**

Grant 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):

- 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):**

· 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):**

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):**

· 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 appendix 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 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 of the information center.

Table 152 on page 510 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.

**Note:** TYPE2 and \*TYPE 4 output formats are no longer updated; therefore, IBM recommends that you stop using \*TYPE2 and \*TYPE4 formats and use only \*TYPE5 formats.

Table 151 on page 509 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.

Table 154 on page 512 through Table 227 on page 614 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 263 provides examples of using the model database outfiles. See also the Journal management topic.

Table 150 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.

Table 150. Standard Heading Fields for Audit Journal Entries. QJORDJE5 Record Format (\*TYPE5)

Offset	Field	Format	Description	
1 Length of Entry Zoned		Zoned(5,0)	Total length of the journal entry including the entry length field.	
6	Sequence	Char(20)	Applied to each journal entry. Initially set to 1 for each new or restored	
	Number		journal. Optionally, reset to 1 when a new receiver is attached.	
26	Journal Code	Char(1)	Always T.	
27	Entry Type	Char(2)	See Table 153 on page 510 for a list of entry types and descriptions.	
29	Timestamp of	Char(26)	Date and time that the entry was made in SAA® timestamp format.	
	Entry			
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 <sup>1</sup> .	
75	Job Number	Zoned(6,0)	The job number.	

Table 150. Standard Heading Fields for Audit Journal Entries (continued). QJORDJE5 Record Format (\*TYPE5)

Offset	Field	Format	Description	
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:	
			The program name does not apply to this entry type.	
91	Program library	Char(10)	<ul> <li>The program name was not available.</li> <li>Name of the library that contains the program that added the journal entry.</li> </ul>	
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 <sup>1</sup> .	
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.	
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.	

Table 150. Standard Heading Fields for Audit Journal Entries (continued). QJORDJE5 Record Format (\*TYPE5)

Offset	Field	Format	Description
606	Entry specific data length	Binary(5)	Length of the entry specific data.

**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 swap user profiles, the User profile name field contains the name of the new (swapped) user profile.

Table 151. 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.		
16	Journal Code	Char(1)	Always T.		
17	Entry Type	Char(2)	See Table 153 on page 510 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 <sup>1</sup> .		
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> <li>The program name does not apply to this entry type.</li> </ul>		
			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 <sup>1</sup> .		
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.		

**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 swap user profiles, the User profile name field contains the name of the new (swapped) user profile.

Table 152. 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 Table 153 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 job¹.	
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> <li>The program name does not apply to this entry type.</li> </ul>	
			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 <sup>1</sup> .	
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 swap user profiles, the <i>User profile name</i> field contains the name of the new (swapped) user profile.			

Table 153. 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

Table 153. Audit Journal (QAUDJRN) Entry Types. (continued)

		3. Addit Journal (QAODJKN) Entry Types. (continued)							
	rtry pe	Description							
DS	S	DST security password reset							
EV		System environment variables							
GF	R	Generic record							
GS	S	Socket description was given to another job							
IM	1	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	7	Key ring file							
LD	)	Link, unlink, or look up directory entry							
M	L	Office services mail actions							
NA	A	Network attribute changed							
NI	D	APPN directory search filter violation							
NI	Е	APPN end point filter violation							
Ol	M	Object move or rename							
OF	R	Object restore							
IO	W	Object ownership changed							
01	1	(Optical Access) Single File or Directory							
O2		(Optical Access) Dual File or Directory							
O3	3	(Optical Access) Volume							
PA		Program changed to adopt authority							
PC		Change of an object's primary group							
PC		Printed output							
PS		Profile swap							
PV		Invalid password							
RA		Authority change during restore							
RJ		Restoring job description with user profile specified							
RC		Change of object owner during restore							
RF		Restoring adopted authority program							
RG RU		Restoring a *CRQD object							
RZ		Restoring user profile authority  Changing a primary group during restore							
SD		Changing a primary group during restore Changes to system distribution directory							
SE		Subsystem routing entry changed							
SF		Actions to spooled files							
SG		Asynchronous Signals							
SK		Secure sockets connections							
SN		Systems management changes							
SC		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							
VI		Account limit exceeded							
VN		Logging on and off the network							
VC		Validation list actions							
VF		Network password error							
VF		Network resource access							

Table 153. Audit Journal (QAUDJRN) Entry Types. (continued)

Entry	
Type	Description
VS	Starting or ending a server session
VU	Changing a network profile
VV	Changing service status
X0	Network Authentication
X1	Identify Token
YC	DLO object accessed (change)
YR	DLO object accessed (read)
ZC	Object accessed (change)
ZR	Object accessed (read)

Table 154. AD (Auditing Change) Journal Entries. QASYADJE/J4/J5 Field Description File

	Offs	set				
JE	J4	J5	Field	Format	Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.	
156	224	610	Entry Type	Char(1)	D CHGDLOAUD command	
					O CHGAUD command	
					S The scan attribute was changed using CHGATR command or the Qp0lSetAttr API, or when the object was created.	
157	225	611	Object Name	Char(10)	U CHGUSRAUD command  Name of the object for which auditing was	
107	005	001	T.11 . N.1	CI (10)	changed.	
167	235	621	Library Name	Char(10)	Name of the library for the object.	
177 185	245 253	631 639	Object Type Object Audit	Char(8) Char(10)	The type of object.  If the entry type is D, O, or U, the field contains	
100	233	039	Value	Char(10)	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 *JOBDTA	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 *OFCSRV	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.	

Table 154. AD (Auditing Change) Journal Entries (continued). QASYADJE/J4/J5 Field Description File

	Offs	set			
JE	J4	<b>J</b> 5	Field	Format	Description
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = Write an audit record when this user manipulates spooled files.
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	(Reserved Area)	Char(19)	•
227	295	681	DLO Name	Char(12)	Name of the DLO object for which auditing was changed.
239	307	693	(Reserved Area)	Char(8)	-
247 310	315	701	Folder Path (Reserved Area)	Char(63) Char(20)	Path of the folder.
	378	764	(Reserved Area)	Char(18)	
	396	782	Object Name Length <sup>1</sup>	Binary(4)	The length of the object name.
330	398	784	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
334	402	788	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
336	404	790	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
339	407	793	(Reserved area)	Char(3)	
342	410	796	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
358	426	812	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
374	442	828	Object Name <sup>1</sup>	Char(512)	The name of the object.
	954	1340	Object File ID <sup>1</sup>	Char(16)	The file ID of the object.
	970	1356	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	980	1366	ASP Number <sup>5</sup>	Char(5)	The number of the ASP device.
	985	1371	Path Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the path name.
	989	1375	Path Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the absolute path name.
	991	1377	Path Name Language ID <sup>1</sup>	Char(3)	The language ID for the absolute path name.
	994	1380	Path Name Length <sup>1</sup>	Binary(4)	The length of the absolute path name.

Table 154. AD (Auditing Change) Journal Entries (continued). QASYADJE/J4/J5 Field Description File

	Offs	set			
JE	<b>J4</b>	<b>J5</b>	Field	Format	Description
	996	1382	Path Name	Char(1)	Path name indicator:
			Indicator <sup>1</sup>		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.
	997	1383	Relative Directory File ID <sup>1, 3</sup>	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. <sup>3</sup>
	1013	1399	Path Name <sup>1, 4</sup>	Char(5002)	The path name of the object.

These fields are used only for objects in the QOpenSys, "root" (/) file systems, and user-defined file systems.

Table 155. AF (Authority Failure) Journal Entries. QASYAFJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.

<sup>2</sup> An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

<sup>3</sup> 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.

<sup>4</sup> This is a variable length field. The first two bytes contain the length of the path name.

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.

Table 155. AF (Authority Failure) Journal Entries (continued). QASYAFJE/J4/J5 Field Description File

Offset						
JE	J4	J5	Field	Format	Desci	ription
156	224	610	Violation Type <sup>1</sup>	Char(1)	A	Not authorized to object
					В	Restricted instruction
					C	Validation failure (see J5 offset 639)
					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
					Н	Scan exit program action (see J5 offset 639)
					$I^7$	System Java inheritance not allowed
					J	Submit job profile error
					K	Special authority violation
					N	Profile token not a regenerable token
					0	Optical Object Authority Failure
					P	Profile swap error
					R	Hardware protection error
					S	Default sign-on attempt
					T	Not authorized to TCP/IP port
					U	User permission request not valid
					V	Profile token not valid for generating new profile token
					W	Profile token not valid for swap
					X	System violation — see J5 offset 723 for violation codes
					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.
157	225	611	Object Name 1,	Char(10)	The r	name of the object.
167	235	621	5, 12 Library Name <sup>13</sup>	Char(10)	The name of the library where the object is store or the Licensed Internal Code fix number that	
177	245	631	Object Type <sup>14</sup>	Char(8)		to apply. <sup>11</sup> ype of object.

Table 155. AF (Authority Failure) Journal Entries (continued). QASYAFJE/J4/J5 Field Description File

Offset							
JE	J4	<b>J</b> 5	Field	Format	Description		
185	253	639	Validation Error Action	Char(1)	Action taken after validation error detected, set only if the violation type (J5 offset 610) is C or H		
					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.	
					В	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.	
					С	The translation of the object was successful. The translated copy was restored on the system.	
					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.	
					E	System install time error detected.	
					F	The object was not restored because the signature is not i5/OS format.	
					G	Unsigned system or inherit state object found when checking system.	
					Н	Unsigned user state object found when checking system.	
					I	Mismatch between object and its signature found when checking system.	
					J	IBM certificate not found when checking system.	
					K	Invalid signature format found when checking system.	
					M	Scan exit program modified the object that was scanned	
					X	Scan exit program wanted object marked as having a scan failure	
186	254	640	Job Name	Char(10)	The name of the job.		

Table 155. AF (Authority Failure) Journal Entries (continued). QASYAFJE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Descri	ption
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 <sup>2</sup>	Char(10)	The name of the user that caused the authorit failure.	
242	310	696	Workstation Name	Char(10)	The name of the workstation or workstation	
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)		pe of operation violation that occurred, se the violation type (J5 offset 610) is X.
					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 commathat has been disabled by a system administrator.
272	340	726	Office User	Char(10)	The na	me of the office user.
282	350	736	DLO Name	Char(12)		me of the document library object.
294	362	748	(Reserved Area)			
302	370	756	Folder Path <sup>15</sup>	Char(63)	The path of the folder.	
365	433	819	Office on Behalf of User		User working on behalf of another user.	
375			(Reserved Area)	Char(20)		
	443	829	(Reserved Area)	Char(18)		
	461	847	Object Name Length <sup>3</sup>	Binary(4)	The ler	ngth of the object name.
395	463	849	Object Name CCSID <sup>3</sup>	Binary(5)	The coded character set identifier for the object name.	
399	467	853	Object Name Country or Region ID <sup>3</sup>	Char(2)	The Country or Region ID for the object nam	
401	469	855	Object Name Language ID <sup>3</sup>	Char(3)	The language ID for the object name.	
404	472	858	(Reserved area)	Char(3)		
407	475	861	Parent File ID <sup>3,4</sup>	` '	The file ID of the parent directory.	
423	491	877	Object File ID <sup>3,4</sup>	Char(16)	The file ID of the object.	
439	507	893	Object Name <sup>3,6</sup>	Char(512)	The name of the object.	
	1019	1405	Object File ID <sup>3</sup>	Char(16)	The file ID of the object.	
	1035	1421	ASP Name <sup>10</sup>	Char(10)		me of the ASP device.
	1045	1431	ASP Number <sup>10</sup>	Char(5)	The number of the ASP device.	

Table 155. AF (Authority Failure) Journal Entries (continued). QASYAFJE/J4/J5 Field Description File

	Offset					
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description	
	1050	1436	Path Name CCSID <sup>3</sup>	Binary(5)	The coded character set identifier for the path name.	
	1054	1440	Path Name Country or Region ID <sup>3</sup>	Char(2)	The Country or Region ID for the absolute path name.	
	1056	1442	Path Name Language ID <sup>3</sup>	Char(3)	The language ID for the absolute path name.	
	1059	1445	Path Name Length <sup>3</sup>	Binary(4)	The length of the absolute path name.	
	1061	1447	Path Name	Char(1)	Path name indicator:	
			Indicator <sup>3</sup>		Y Absolute 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.	
	1062	1448	Relative Directory File ID <sup>3, 8</sup>	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. <sup>3</sup>	
	1078	1464	Path Name <sup>3, 9</sup>	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	

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 Table 126 on page 241.

- · offsets 41 and 118 for \*TYPE2 records
- offsets 55 and 132 for \*TYPE4 records
- · offsets 65 and 187 for \*TYPE5 records

- <sup>4</sup> An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
- 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.

This field contains the name of the user that caused the entry. QSYS may be the user for the following entries:

These fields are used only for objects in the QOpenSys file system, the "root" (/) file system, user-defined file systems, and QFileSvr.400.

Table 155. AF (Authority Failure) Journal Entries (continued). QASYAFJE/J4/J5 Field Description File

	Offset					
JE	J4	J5	Field	Format	Description	

- 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.
- The Java class object being created may not extend its base class because the base class has system Java attributes.
- 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.
- This is a variable length field. The first two bytes contain the length of the path name.
- 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.
- 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.
- 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.
- 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.
- When the violation type is "K", the object type contains the object type of the command or program that detected the error.
- 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.

Table 156. AP (Adopted Authority) Journal Entries. QASYAPJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.
156	224	610	Entry Type	Char(1)	S Start
					<b>E</b> 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 <sup>1</sup>	Char(10)	The name of the ASP device.
	289	675	ASP Number <sup>1</sup>	Char(5)	The number of the ASP device.

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.

Table 157. AU (Attribute Changes) Journal Entries. QASYAUJ5 Field Description File

Offse	et		
J5	Field	Format	Description
610	Entry type	Char(1)	The type of entry.
611	Action	Char(3)	E EIM configuration attributes Action
614	Name	Char(100)	CHG Attributes changed Attribute name
714	New Value Length	Binary(4)	New value length
716	New Value CCSID	Binary(5)	New value CCSID
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 fi	eld. The first two	bytes contain the length of the field.

Table 158. CA (Authority Changes) Journal Entries. QASYCAJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 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
207	275	661	Object Operational	Char(1)	Y *OBJOPR

Table 158. CA (Authority Changes) Journal Entries (continued). QASYCAJE/J4/J5 Field Description File

	Offs	et				
JE	J4	J5	Field	Format	Descri	ption
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	Char(3)	The ty	pe of command used.
			Type		GRT	Grant
					RPL	Grant with replace
					RVK	Revoke
					USR	GRTUSRAUT operation
225 235	293 303	679	Field name (Reserved Area)	Char(10) Char(10)	The na	ame of the field.
		689	Object Attribute	Char(10)	The att	tribute of the object.
245	313	699	Office User	Char(10)		me of the office user.
255 267	323 335	709 721	DLO Name (Reserved Area)	Char(12) Char(8)	The na	me of the DLO.
275	343	729	Folder Path	Char(63)	The pa	th of the folder.
338	406	792	Office on Behalf of User	Char(10)	_	orking on behalf of another user.
348	416	802	Personal Status	Char(1)	Y	Personal status changed
349	417	803	Access Code	Char(1)	A	Access code added
0 2 6				GI (C	R	Access code removed
350 354	418	804	Access Code (Reserved Area)	Char(4) Char(20)	Access	code.
	422	808	(Reserved Area)	Char(18)		

Table 158. CA (Authority Changes) Journal Entries (continued). QASYCAJE/J4/J5 Field Description File

	Offse	et			
JE	J4	J5	Field	Format	Description
	440	826	Object Name Length <sup>1</sup>	Binary(4)	The length of the object name.
374	442	828	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
378	446	832	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
380	448	834	Object Name Language ID¹	Char(3)	The language ID for the object name.
383	451	837	(Reserved area)	Char(3)	
386	454	840	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
402	470	856	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
418	486	872	Object Name <sup>1</sup>	Char(512)	The name of the object.
	998	1384	Object File ID	Char(16)	The file ID of the object.
	1014	1400	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	1024	1410	ASP Number <sup>5</sup>	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 absolute path name.
	1035	1421	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	1038	1424	Path Name Length	Binary(4)	The length of the absolute path name.
	1040	1426	Path Name Indicator	Char(1)	Path name indicator:
			Hulcator		Y Absolute 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.
	1041	1427	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>
	1057	1443	Path Name <sup>4</sup>	Char(5002)	The path name of the object.

Table 158. CA (Authority Changes) Journal Entries (continued). QASYCAJE/J4/J5 Field Description File

	Offset					
JE	J4	J5	Field	Format	Description	

- These fields are used only for objects in the QOpenSys file system, the "root" (/) file system, user-defined file systems, and QFileSvr.400.
- An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
- 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.
- This is a variable length field. The first two bytes contain the length of the path name.
- 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.

Table 159. CD (Command String) Journal Entries. QASYCDJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. 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		
157 167	225 235	611 621	Object Name Library Name	Char(10) Char(10)	U Utility control statement The name of the object. 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		
186	254	640	Command String	Char(6000)	N No 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		

Table 160. CO (Create Object) Journal Entries. QASYCOJE/J4/J5 Field Description File

	Offs	set			
JE	J4	J5	Field	Format	Description
1 156	224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
100	££4	010	Liftiy Type	Char(1)	N Create of new object
					·
157	225	611	Object Name	Char(10)	<b>R</b> Replacement of existing object The name of the object.
167	235	621	Library Name	Char(10)	The name of the object.  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)	
	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 <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
372	440	826	Object Name <sup>1</sup>	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	978	1364	ASP Number <sup>5</sup>	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 absolute path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the absolute path name.

Table 160. CO (Create Object) Journal Entries (continued). QASYCOJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	992	1378	Path Name Length	Binary(4)	The length of the absolute path name.
	994	1380	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.
	995	1381	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>
	1011	1397	Path Name <sup>4</sup>	Char(5002)	The path name of the object.

These fields are used only for objects in the QOpenSys, "root" (/) file systems, and user-defined file systems.

Table 161. CP (User Profile Changes) Journal Entries. QASYCPJE/J4/J5 Field Description File

	Offs	et					
JE J4		<b>J</b> 5	Field Format		Description		
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 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	Char(3)	The type of command used.		
			Name		CRT CRTUSRPRF		
					CHG CHGUSRPRF		
					RST RSTUSRPRF		
					DST QSECOFR password reset using DST		
					<b>RPA</b> QSYRESPA API		

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

<sup>&</sup>lt;sup>4</sup> This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 161. CP (User Profile Changes) Journal Entries (continued). QASYCPJE/J4/J5 Field Description File

	Offs	et				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Descr	iption
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
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	Char(1)	Y	*SECADM special authority
195	263	649	Authority 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	<b>Group Profile</b>	Char(10)		ame of a group profile.
222	290	676	Owner	Char(10)	profile	
232	300	686	Group Authority	Char(10)	_	profile authority.
242	310	696	Initial Program	Char(10)		ame of the user's initial program.
252	320	706	Initial Program Library	Char(10)	is fou	
262	330	716	Initial Menu	Char(10)		ame of the user's initial menu.
272	340	726	Initial Menu Library	Char(10)	found	
282	350	736	Current Library	Char(10)		ame of the user's current library.
292	360	746	Limited Capabilities	Char(10)		alue of limited capabilities parameter.
302	370	756	User Class	Char(10)		ser class of the user.
312	380	766	Priority Limit	Char(1)		alue of the priority limit parameter.
313	381	767	Profile Status	Char(10)		profile status.
323	391	777	Group Authority Type	Char(10)		ralue of the GRPAUTTYP parameter.
333	401	787	Supplemental Group Profiles	Char(150)		ames of up to 15 supplemental group es for the user.

Table 161. CP (User Profile Changes) Journal Entries (continued). QASYCPJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
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	Char(10)	Indicates whether the new password conforms to the password composition rules.
			Conformance		*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.
		977	Password Expiration	Char(7)	*NOCHECK Not checked; password was changed. This field has meaning only when the Password Changed field contains a <i>Y</i> . Specifies the value that the password expiration interval has been changed to.
			Interval		*NOMAX No expiration interval.
					*SYSVAL The system value QPWDEXPITV is used
					number  The size of the expiration interval in days.

Table 162. CQ (\*CRQD Changes) Journal Entries. QASYCQJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. 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

Table 163. CU (Cluster Operations) Journal Entries. QASYCUJ4/J5 Field Description File

	Offset					
JE	<b>J4</b>	<b>J</b> 5	Field	Format Char(1)	Description	
	1 224	1 610 Entry	Entry Type		Heading fields common to all entry types. See Table 150 on page 507 and Table 151 on page 509 for field listing. The type of entry.	
					M Cluster control operation	
	225	611	Entry Action	Char(3)	R Cluster Resource Group (*GRP) management operation The type of action.	
	220	011	Lifty / Tetion	Char (o)	ADD Add	
					CRT Create	
					DLT Delete	
					<b>DST</b> Distribute	
					END End	
					FLO Fail over	
					LST List information	
					RMV Remove	
					STR Start	
					SWT Switch	
	228	614	Status	Char(3)	<b>UPC</b> Update attributes The status of the request.	
					ABN The request ended abnormally	
					AUT Authority Failure, *IOSYSCFG is required	
					<b>END</b> The request ended successfully	
	231	617	CRG Object	Char(10)	STR The request was started The Cluster Resource Group object name.	
			Name		<b>Note:</b> This value is filled in when the entry type is R.	
	241	627	CRG Library	Char(10)	The Cluster Resource Group object library.	
			Name		<b>Note:</b> 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	

Table 164. CV (Connection Verification) Journal Entries. QASYCVJ4/J5 Field Description File

	Offset					
JE	J4	J5	Field	Format	Descrip	otion
	1 224	1 1		Char(1)	Table 15 for field	g fields common to all entry types. See 50 on page 507 and Table 151 on page 509 d listing. De of entry.
					C	Connection established
					E	Connection ended
	225	611	Action	Char(1)	<b>R</b> Action	Connection rejected 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 poi	int-to-point profile name.
	236	622	Protocol	Char(10)	The typ	pe of entry.
					L2TP	Layer Two Tunneling protocol
					PPP	Point-to-Point protocol.
	246	632	Local	Char(10)	<b>SLIP</b> The typ	Serial Line Internet Protocol. pe of entry.
			Authentication Method		CHAP	Challenge Handshake Authentication Protocol.
					PAP	Password Authentication Protocol.
					SCRIP	
						Script method.

Table 164. CV (Connection Verification) Journal Entries (continued). QASYCVJ4/J5 Field Description File

	Offset					
JE	<b>J4</b>	J5	Field	Format Char(10)	<b>Description</b> The type of entry.	
	256	642	Remote			
			Authentication Method		<b>CHAP</b> Challenge Handshake Authentication Protocol.	
					<b>PAP</b> Password Authentication Protocol.	
					RADIUS Radius method.	
					SCRIPT	
	200	0.50		GI (40)	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.	
				<b>61</b> (1)	N IP forwarding is off.	
	467	853	Proxy ARP	Char(1)	The type of entry.	
					Y Proxy ARP is enabled.	
	400	07.4	D 11 37	GI (40)	N Proxy ARP is not enabled.	
	468 478	854 864	Radius Name Authenticating IP Address	Char(10) Char(40)	The AAA profile name. 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	
					<b>6</b> 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 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	

Table 165. CY (Cryptographic Configuration) Journal Entries. QASYCYJ4/J5 Field Description File

	Off	set				
JE	<b>J4</b>	J5	Field	Format	Descri	ption
	1 224	1 610	Entry Type	Char(1)	Table 1 and Ta	ng fields common to all entry types. See 150 on page 507,Table 151 on page 509, able 152 on page 510 for field listing. pe of entry.
					A	Cryptographic Coprocessor Access Control Function
					F	Cryptographic Coprocessor Facility Control Function
					K	Cryptographic Services Master Key Function
					M	Cryptographic Coprocessor Master & Function
	225	611	Action	Char(3)	The cr	yptographic configuration function med:
					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.
	228 236 244	614 622 630 640	Card Profile Card Role Device Name Master Key ID <sup>1</sup>	Char(8) Char(8) Char(10) Binary(4)	The ro The na	Test master key.

Table 165. CY (Cryptographic Configuration) Journal Entries (continued). QASYCYJ4/J5 Field Description File

	Of	fset					
JE	J4	J5	Field	Format	Description		
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 th	When the entry type is "K", this field is blank.					
3	When the entry type is not "K", this field is blank.						

Table 166. DI (Directory Server) Journal Entries. QASYDIJ4/J5 Field Description File

	Offs	set		Format Descri		
JE	<b>J4</b>	J5	Field		iption	
	1 224	1 610	Entry Type	ntry Type Char(1)		ng fields common to all entry types. See 150 on page 507,Table 151 on page 509, and 152 on page 510 for field listing. Ope of entry.
	225	611	Operation Type	Char(2)	L The ty	LDAP Operation /pe of LDAP operation:
					AD	Audit attribute change.
					AF	Authority failure.
					BN	Successful bind.
					CA	Object authority change.
					CF	Configuration change.
					CO	Object creation.
					CP	Password change.
					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 166. DI (Directory Server) Journal Entries (continued). QASYDIJ4/J5 Field Description File

Offset						
JE	J4	J5	Field	Format	Desc	ription
	227 613 Authority Failure Code		Char(1)		for authority failures. This field is used if the operation type (J5 offset 611) is AF.	
					A	Unauthorized attempt to change audit value.
					В	Unauthorized bind attempt.
					C	Unauthorized object create attempt.
					D	Unauthorized object delete attempt.
					E	Unauthorized export attempt.
					F	Unauthorized configuration change (administrator, change log, backend library, replicas, publishing).
					G	Unauthorized replication management attempt.
					I	Unauthorized import attempt.
					M	Unauthorized change attempt.
					P	Unauthorized policy change attempt.
					R	Unauthorized read (search) attempt.
					U	Unauthorized attempt to read the audit configuration.
					X	Unauthorized proxy authorization attempt.
	228	614	Configuration Change	Char(1)		iguration changes. This field is only used if peration type (J5 offset 611) is CF.
					Α	Administrator ND change.
					C	Change log on or off.
					L	Backend library name change.
					P	Publishing agent change.
					R	Replica server change.
						operation type (J5 offset 611) is RM the wing values might be present:
					U	Suspend replication.
					V	Resume replication.
					W	Replicate pending changes now.
					X	Skip one or more pending changes.
					Y	Quiesce replication context.
					Z	Unquiesce replication context.

Table 166. DI (Directory Server) Journal Entries (continued). QASYDIJ4/J5 Field Description File

	Offset		_				
JE	J4	J5	Field	Format	Description		
	229		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 ony 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		
	257	643	Connection ID	Char(20)	U Unauthenticated 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 <sup>1</sup>	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.		
	2341	2727	Object Name <sup>1</sup>	Char(2002)	The name of the LDAP object.		

Table 166. DI (Directory Server) Journal Entries (continued). QASYDIJ4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
	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 <sup>1</sup>	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.
					• 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.
					<ul> <li>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.</li> </ul>
	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.
					• 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.
					<ul> <li>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.</li> </ul>
	6357	6743	New Name <sup>1</sup>	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.
					• For operation type OM, this field will contain the new object name.
					• For operation type OW, this field will contain the new owner name.
					<ul> <li>For operation types PO, ZC, AF+M, or AF+P, this field will contain a list of changed attribute types.</li> </ul>
	8359	8745	Object File ID <sup>2</sup>	Char(16)	The file ID of the object for export.
	8375	8761	ASP Name <sup>2</sup>	Char(10)	The name of the ASP device.
	8385	8771	ASP Number <sup>2</sup>	Char(5)	The number of the ASP device.
	8390	8776	Path Name CCSID <sup>2</sup>	Bin(5)	The coded character set identifier of the absolute path name.
	8394	8780	Path Name Country or	Char(2)	The Country or Region ID of the absolute path name.
	8396	8782	Region ID <sup>2</sup> Path Name Language ID <sup>2</sup>	Char(3)	The language ID of the absolute path name.
	8399	8785	Path Name Length <sup>2</sup>	Bin(4)	The length of the absolute path name.

Table 166. DI (Directory Server) Journal Entries (continued). QASYDIJ4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
	8401	8787	Path Name	Char(1)	Path name indicator.
			Indicator <sup>2</sup>		Y Absolute 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.
	8402	8788	Relative Directory File ID <sup>2.3</sup>	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. <sup>3</sup>
	8418	8804	Path Name <sup>1,2</sup>	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.
		13822	Proxy ID Length	Bin(4)	The length of the proxy ID.
		13826	Proxy ID <sup>1</sup>	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.

This is a variable length field. The first two bytes contain the length of the value in the field.

Table 167. DO (Delete Operation) Journal Entries. QASYDOJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.

These fields are used only if the operation type (J5 offset 611) is EX or IM.

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.

Table 167. DO (Delete Operation) Journal Entries (continued). QASYDOJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
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 committee
					D A pending object create was rolled ba
					P The object delete is pending (the delete was performed under commitment control)
					R A pending object delete was rolled ba
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	Char(20)	
			Area)		
		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.
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 <sup>1</sup>	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
372	440	826	Object Name <sup>1</sup>	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	978	1364	ASP Number <sup>5</sup>	Char(5)	The number of the ASP device.
	983	1369	Path Name CCSID	Binary5)	The coded character set identifier for the path name.

Table 167. DO (Delete Operation) Journal Entries (continued). QASYDOJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
	987	1373	Path Name Country or Region ID	Char(2)	The Country or Region ID for the absolute path name.
	989	1375	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	992	1378	Path Name Length	Binary(4)	The length of the absolute path name.
	994	1380	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.
	995	1381	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>
	1011	1397	Path Name <sup>4</sup>	Char(5002)	The path name of the object.

These fields are used only for objects in the QOpenSys, "root" (/) file systems, and user-defined file systems.

Table 168. DS (IBM-Supplied Service Tools User ID Reset) Journal Entries. QASYDSJE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	J5	Field	Format	Desc	ription
1 156	1 224	1 610	Entry Type	Char(1)	Table Table	ling fields common to all entry types. See 150 on page 507,Table 151 on page 509, and 152 on page 510 for field listing. ype 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.
157	225	611	IBM-Supplied Service Tools User ID Reset	Char(1)	Y	Request to reset an IBM-supplied service tools user ID.

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

This is a variable length field. The first two bytes contain the length of the path name.

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.

Table 168. DS (IBM-Supplied Service Tools User ID Reset) Journal Entries (continued). QASYDSJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	ld Format	Description
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.

Table 169. EV (Environment Variable) Journal Entries. QASYEVJ4/J5 Field Description File

	Offset						
JE	J4	4 J5 Field Format		Format	Description		
	1	1		GL (A)	Table Table	ing fields common to all entry types. See 150 on page 507,Table 151 on page 509, and 152 on page 510 for field listing.	
	224	610	Entry Type	Char(1)	The ty	ype of entry.	
					Α	Add	
					C	Change	
					D	Delete	
	225	611	Name Truncated	Char(1)		ates whether the environment variable name t 232) is truncated.	
					Y	Environment variable name truncated.	
					N	Environment variable name not truncated.	
	226	612	CCSID	Binary(5)	The C	CCSID of the environment variable name.	
	230	616	Length	Binary(4)	The le	ength of the environment variable name.	
	232	618	Environment Variable Name <sup>2</sup>	Char(1002)	The na	ame of the environment variable.	
	1234	1620	New Name Truncated <sup>1</sup>	Char(1)		ites whether the new environment variable (offset 1241) is truncated.	
					Y	Environment variable value truncated.	
					N	Environment variable value not truncated.	

Table 169. EV (Environment Variable) Journal Entries (continued). QASYEVJ4/J5 Field Description File

Offset						
JE	<b>J4</b>	J5	Field	Format	Description	
	1235	1621	New Name CCSID <sup>1</sup>	Binary(5)	The CCSID of the new environment variable name.	
	1239	1625	New Name Length <sup>1</sup>	Binary(4)	The length of the new environment variable name.	
	1241	1627	New Environment Variable Name <sup>1,2</sup>	Char (1002)	The new environment variable name.	

These fields are used when the entry type is C.

Table 170. GR (Generic Record) Journal Entries. QASYGRJ4/J5 Field Description File

	Off	set				
JE	<b>J4</b>	J5	Field	Format	Descr	iption
	224	1 610	Entry Type	Char(1)	Table for fie	ing fields common to all entry types. See 150 on page 507 and Table 151 on page 509 eld listing. ype of entry.
			3 31		Α	Exit program added
					C	Operations Resource Monitoring and Control Operations
					D	Exit program removed
					F	Function registration operations
	225	611	Action	Char(2)	<b>R</b> The a	Exit program replaced ction performed.
					ZC	Change
	227	613	User Name	Char(10)	<b>ZR</b> User	Read profile name
					the us	ntry type F, this field contains the name of ser the function registration operation was rmed against.
	237	623	Field 1 CCSID	Binary (5)		CCSID value for field 1.
	241	627	Field 1 Length	Binary (4)	The le	ength of the data in field 1.

This is a variable length field. The first two bytes contain the length of the environment variable name.

Table 170. GR (Generic Record) Journal Entries (continued). QASYGRJ4/J5 Field Description File

	Off	set			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	243	629	Field 1	Char(102) <sup>1</sup>	Field 1 data
					For entry type F, this field contains the description of the function registration operation that was performed. The possible values are:
					*REGISTER: Function has been registered
					*REREGISTER: Function has been updated
					*DEREGISTER: Function has been de-registered
					*CHGUSAGE: Function usage information has been changed
					*CHKUSAGE:  Function usage was checked for a user and the check passed
					*USAGEFAILURE: Function usage was checked for a user and the check failed
					For entry types A, D, and R, this field will contain the exit program information for the specific function that was performed.
					For entry type C, this field contains the name of the RMC function that is being attempted. The possible values are:
					<ul> <li>mc_reg_event_select Register event using attribute selection</li> </ul>
					<ul> <li>mc_reg_event_handle Register event using resource handle</li> </ul>
					<ul> <li>mc_reg_class_event Register event for a resource class</li> </ul>
					• mc_unreg_event Unregister event
					• mc_define_resource Define new resource
					• mc_undefine_resource Undefine resource
					<ul> <li>mc_set_select Set resource attribute values using attribute selection</li> </ul>
					<ul> <li>mc_set_handle Set resource attribute values using resource handle</li> </ul>
					<ul> <li>mc_class_set Set resource class attribute values</li> </ul>
					<ul> <li>mc_query_p_select Query resource persistent attributes using attribute selection</li> </ul>
					<ul> <li>mc_query_d_select Query resource dynamic attributes using attribute selection</li> </ul>

Table 170. GR (Generic Record) Journal Entries (continued). QASYGRJ4/J5 Field Description File

Offset					
JE	J4	<b>J</b> 5	Field	Format	Description
243 (cont)					<ul> <li>mc_query_p_handle Query resource persistent attributes using resource handle</li> </ul>
					mc_query_d_handle Query resource dynamic attributes using resource handle
					<pre>mc_class_query_p Query resource class persistent attributes</pre>
					<pre>mc_class_query_d Query resource class dynamic attributes</pre>
					<pre>mc_qdef_resource_class Query resource class definition</pre>
					<pre>mc_qdef_p_attribute Query persistent attribute definition</pre>
					<pre>mc_qdef_d_attribute Query dynamic attribute definition</pre>
					mc_qdef_sd Query Structured Data definition
					<pre>mc_qdef_valid_values Query definition of a persistent attribute's valid values</pre>
					<pre>mc_qdef_actions Query definition of a resource's actions</pre>
					<pre>mc_invoke_action Invoke action on a resource</pre>
	345 349 351	731 735 737	Field 2 CCSID Field 2 Length Field 2	Binary (5) Binary (4) Char (102) <sup>1</sup>	mc_invoke_class_action Invoke action on a resource class The CCSID value for field 2. The length of the data in field 2. Field 2 data
					For entry type F, this field contains the name of the function that was operated on.
	453 457	839 843	Field 3 CCSID Field 3 Length	Binary (5) Binary (4)	For entry type C, this field contains the name of the resource or resource class against which the operation was attempted.  The CCSID value for field 3.  The length of the data in field 3.

Table 170. GR (Generic Record) Journal Entries (continued). QASYGRJ4/J5 Field Description File

	Off	set			
JE	<b>J4</b>	J5	Field	Format	Description
	459	845	Field 3	Char(102)1	Field 3 data.
					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:
					*REGISTER:  When the operation is *REGISTER, thi field contains the default usage value. The user name will be *DEFAULT.
					*REREGISTER:  When the operation is *REREGISTER, this field contains the default usage value. The user name will be *DEFAULT.
					*CHGUSAGE:  When the operation is *CHGUSAGE, this field contains the usage value for the user specified in the user name field.
					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:
					<ul> <li>*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.</li> </ul>
					<ul> <li>*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.</li> </ul>
					<ul> <li>*AUTHORITYFAILED: When the mapped user ID indicated in the User Profile Name has failed the appropriate authorization chec for the operation indicated in field 1 against the resource or resource class indicated in field 2.</li> </ul>
	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 170. GR (Generic Record) Journal Entries (continued). QASYGRJ4/J5 Field Description File

	Offset				
E	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	567	953	Field 4	Char(102) <sup>1</sup>	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

This is a variable length field. The first two bytes contain the length of the field.

Table 171. GS (Give Descriptor) Journal Entries. QASYGSJE/J4/J5 Field Description File

	Offs	set			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. 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.)

Table 172. IM (Intrusion Monitor) Journal Entries. QASYIMJE/J4/J5 Field Description File

	Offset						
	JE	J4 J5 Field		Field	Format	Description	
 			1 610	Entry Type	Char(1)	Heading fields common to all entry types. The type of entry.	
			611	Time of Event	TIMESTAMP	P Potential intrusion event detected 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.	
Local Port Zone(5, 0) Local p   Number event.		Local port number associated with the detected event.					

| Table 172. IM (Intrusion Monitor) Journal Entries (continued). QASYIMJE/J4/J5 Field Description File

55 647 693 694 699 745	Field  Local IP Address Remote Address Family Remote Port Number Remote IP Address Probe Type Identifier	Format Char(46) Char(1) Zoned(5, 0) Char(46) Char(6)	Description  Local IP address associated with the detected event.  Remote address family associated with the detected event.  Remote port number associated with the detected event.  Remote IP address associated with the detected event.  Identifies the type of probe used to detect the
693 694 699	Address Remote Address Family Remote Port Number Remote IP Address Probe Type	Char(1)  Zoned(5, 0)  Char(46)	event. Remote address family associated with the detected event. Remote port number associated with the detected event. Remote IP address associated with the detected event.
694 699	Remote Address Family Remote Port Number Remote IP Address Probe Type	Zoned(5, 0) Char(46)	Remote address family associated with the detected event.  Remote port number associated with the detected event.  Remote IP address associated with the detected event.
699	Remote Port Number Remote IP Address Probe Type	Char(46)	detected event.  Remote IP address associated with the detecte event.
	Address Probe Type		event.
745		Char(6)	Identifies the type of probe used to detect the
			potential intrusion. Possible values include:
			ATTACK
			Attack action detected event
			TR (trace) action detected event
			SCANG Scan global action detected event
			SCANE
751	Event Correlator	Char(4)	Scan event action detected event Unique identifier for this specific intrusion ev This identifier can be used to correlate this au record with other intrusion detection information.
755	Event type	Char(8)	Identifies the type of potential intrusion that v detected. The possible values are:
			MALFPKT Malformed packet
			FLOOD Flood event
			ICMPRED ICMP (Internet Control Message Protocol) redirect
			PERPECH Perpetual echo
			IPFRAG IP fragment
			RESTPROT Restricted IP protocol
763	Reserved	Char(20)	-
783	Suspected Packet	Char(1002) <sup>1</sup>	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.
	763	763 Reserved 783 Suspected	763 Reserved Char(20) 783 Suspected Char(1002) <sup>1</sup>

Table 173. IP (Interprocess Communication) Journal Entries. QASYIPJE/J4/J5 Field Description File

	Offs	et	<u> </u>		
JE	J4	<b>J</b> 5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. 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
158 162 172 182	226 230 240 250	612 616 626 636	IPC Handle New Owner Old Owner Owner Authority	Binary(5) Char(10) Char(10) Char(3)	S Semaphore IPC handle ID New owner of IPC entity Old owner of IPC entity Owner's authority to IPC entity
					*R read
					*W write
185 195 205	253 263 273	639 649 659	New Group Old Group Group	Char(10) Char(10) Char(3)	*RW read and write Group associated with IPC entity Previous group associated with IPC entity Group's authority to IPC entity
			Authority		*R read
					*W write
208	276	662	Public	Char(3)	*RW read and write Public's authority to IPC entity
			Authority		*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.

Table 173. IP (Interprocess Communication) Journal Entries (continued). QASYIPJE/J4/J5 Field Description File

	Offset			_		
JE	J4	<b>J</b> 5	Field	Format	Descri	ption
218	285	671	Semaphore	Char(2050)	The ser	maphore name.
			Name		Note:	This is a variable length field. The first two characters contain the length of the semaphore name.

Table 174. IR (IP Rules Actions) Journal Entries. QASYIRJ4/J5 Field Description File

	Offs	set			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	1 224	1 610	0 Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507 and Table 151 on page 509 for field listing. 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
					<b>R</b> IP rules have been read and copied to a file.
	225	611	File Name	Char(10)	U IP rules have been unloaded (removed). The name of the QSYS file used to load or receive the IP rules.
					This value is blank if the file used was
	235	621	File Library	Char(10)	not in the QSYS file system.  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 CCSID¹	Binary (5)	The coded character set identifier for the file name.
	269	655	File Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the file name.
	271	657	File Language ID <sup>1</sup>	Char(3)	The language ID for the file name.
	274	660	Reserved	Char(3)	
	277	663	Parent File ID <sup>1,</sup>	Char(16)	The file ID of the parent directory.
	293	679	Object File ID <sup>1,</sup>	Char(16)	The file ID of the file.
	309	695	File Name <sup>1</sup>	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 <sup>5</sup>	Char(5)	The number of the ASP device.
	892	1278	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.

Table 174. IR (IP Rules Actions) Journal Entries (continued). QASYIRJ4/J5 Field Description File

	Offset					
JE	J4	<b>J</b> 5	Field	Format	Description	
	896	1282	Path Name Country or Region ID	Char(2)	The Country or Region ID for the absolute path name.	
	898	1284	Path Name Language ID	Char(3)	The language ID for the absolute path name.	
	901	1287	Path Name Length	Binary(4)	The length of the absolute path name.	
	903	1289	Path Name	Char(1)	Path name indicator:	
			Indicator		Y Absolute 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.	
	904	1290	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>	
	920	1306	Path Name <sup>4</sup>	Char(5002)	The path name of the object.	

<sup>1</sup> These fields are used only for objects in the QOpenSys file system and the "root" (/) file system.

Table 175. IS (Internet Security Management) Journal Entries. QASYISJ4/J5 Field Description File

	Offset						
JE	<b>J4</b>	J5	Field	Format	Desc	ription	
	1 224	1 610	Entry Type	Char(1)	Table for fi	ling fields common to all entry types. See 150 on page 507 and Table 151 on page 509 eld listing. ype 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	Char(15)	Local	IP Address.	

<sup>2</sup> If the ID has the left-most bit set and the rest of the bits zero, the ID is not set.

<sup>3</sup> 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.

This is a variable length field. The first two bytes contain the length of the field.

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.

Table 175. IS (Internet Security Management) Journal Entries (continued). QASYISJ4/J5 Field Description File

	Offse	t			
JE	<b>J4</b>	J5	Field	Format	Description
	240	626	Local Client ID Port	Char(5)	Local Client ID port.
	245	631	Remote IP Address	Char (15)	Remote IP address.
	260	646	Remote Client ID Port	Char (5)	Remote Client ID Port (valid for phase 2).
	265 521	651 907	Mobile ID Result Code	Char (256) Char(4)	Mobile ID. This field no longer used. Negotiation Result:
					0 Successful
					1–30 Protocol specific errors (documented in ISAKMP RFC2408, found at: http://www.ietf.org)
	525	911	CCSID	Bin(5)	<ul><li>82xx iSeries VPN Key Manager specific errors</li><li>The coded character set identifier for the following fields:</li><li>Local ID</li></ul>
					Local ID     Local Client ID Value
					Remote ID
					Remote Client ID Value
	529 785	915 1171	Local ID Local Client ID Type	Char(256) Char(2)	Local IKE identifier 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
					7 IP version 4 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
	1303	1689	Remote Client ID Type	Char(2)	Type of client ID (valid for phase 2)
			12 1ype		1 IP version 4 address
					2 Fully qualified domain name
					3 User fully qualified domain name
					4 IP version 4 subnet
					7 IP version 4 address range
					9 Distinguished name
	1305	1691	Remote Client ID Value	Char(256)	11 Key identifier Remote client ID (valid for phase 2)

Table 175. IS (Internet Security Management) Journal Entries (continued). QASYISJ4/J5 Field Description File

Offset					
JE	J4	<b>J</b> 5	Field	Format	Description
	1561	1947	Remote Client ID Protocol	Char(4)	Remote client ID protocol (valid for phase 2)

Table 176. JD (Job Description Change) Journal Entries. QASYJDJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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.		
185	253	639	Command	Char(3)	The type of command used.		
			Туре		<b>CHG</b> Change Job Description (CHGJOBD) command.		
					<b>CRT</b> Create Job Description (CRTJOBD) 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 JOBD library		
		672	ASP number	Char(5)	ASP number for JOBD library		

Table 177. JS (Job Change) Journal Entries. QASYJSJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.

Table 177. JS (Job Change) Journal Entries (continued). QASYJSJE/J4/J5 Field Description File

	Offse	et				
JE	J4	J5	Field	Format	Desc	ription
156	224	610	Entry Type	Char(1)	The type of entry.	
					A	ENDJOBABN command
					В	Submit
					C	Change
					E	End
					Н	Hold
					I	Disconnect
					J	The current job is attempting to interruganother job
					K	The current job is about to be interrupted
					L	The interruption of the current job has completed
					M	Change profile or group profile
					N	ENDJOB command
					P	Attach prestart or batch immediate job
					$\mathbf{Q}$	Change query attributes
					R	Release
					S	Start
					T	Change profile or group profile using a profile token.
					$\mathbf{U}$	CHGUSRTRC
					V	Virtual device changed by QWSACCDS API.
157	225	611	Job Type	Char(1)	The t	type of job.
					A	Autostart
					В	Batch
					I	Interactive
					M	Subsystem monitor
					R	Reader
					S	System
					W	Writer
					X	SCPF

Table 177. JS (Job Change) Journal Entries (continued). QASYJSJE/J4/J5 Field Description File

Offset						
JE J4 J5		Field	Format	Description		
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	
					<b>Q</b> 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)	operated on  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 <sup>2</sup>	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	
275 705	343 773	729 1159	Library List <sup>2</sup>	Char(430)	The library list for the job	
703	113	1159	Effective Group Profile Name <sup>2</sup>	Char(10)	The name of the effective group profile for the thread	
715	783	1169	Supplemental Group Profiles <sup>2</sup>	Char(150)	The names of the supplemental group profiles for the thread.	
	933	1319	JUID	Char(1)	Describes the meaning of the JUID field:	
			Description		' ' 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.	
	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.	

Table 177. JS (Job Change) Journal Entries (continued). QASYJSJE/J4/J5 Field Description File

	Offse	et				
JE	J4 J5		Field	Format	Description	
	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	Char(1)	The real user profile was changed.	
			Changed <sup>3</sup>		Y Yes	
					N No	
	985	1371	Effective User	Char(1)	The effective user profile was changed.	
			Changed <sup>3</sup>		Y Yes	
					N No	
	986	1372	Saved User	Char(1)	The saved user profile was changed	
			Changed <sup>3</sup>		Y Yes	
					N No	
	987	1373	Real Group	Char(1)	The real group profile was changed.	
			Changed <sup>3</sup>		Y Yes	
					N No	
	988	1374	Effective Group	Char(1)	The effective group profile was changed	
			Changed <sup>3</sup>		Y Yes	
					N No	
	989	1375	Saved Group	Char(1)	The saved group profile was changed.	
			Changed <sup>3</sup>		Y Yes	
					N No	
	990	1376	Supplemental	Char(1)	The supplemental group profiles were changed.	
			Groups Changed <sup>3</sup>		Y Yes	
			Changeu		N No	
	991	1377	Library list	Bin(4)	The number of libraries in the library list	
			Number <sup>4</sup>		extension field (offset 993).	
	993	1379	Library List Extension <sup>4,5</sup>	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	
		3666	Exit Job Name	Char(10)	The name of the job that interrupted the current	
					job, or the name of the job that was interrupted b the current 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	Char(6)	The number of the job that interrupted the current	
			Number <sup>6, 7</sup>		job, or the job number of the job that was	
		3692	Exit Program	Char(10)	interrupted by the current job  The exit program used to interrupt the job	
		0002	Name <sup>6</sup>	J. (10)	The one program about to interrupt the job	

Table 177. JS (Job Change) Journal Entries (continued). QASYJSJE/J4/J5 Field Description File

Offset			_			
JE	J4	<b>J</b> 5	Field	Format	Description	
		3702	Exit Program Library <sup>6</sup>	Char(10)	The library name of the exit program used to interrupt the job	

- This field is blank if the job is on the job queue and has not run.
- 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.
- This field is used only when entry type (offset 610) is M or T.
- This field is used only if the number of libraries in the library list exceeds the size of the field at offset 729.
- This is a variable length field. The first two bytes contain the length of the data in the field.
- This field is used only when entry type (offset 610) is J, K, or L.
- 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.

Table 178. KF (Key Ring File) Journal Entries. QASYKFJ4/J5 Field Description File

	Offse	et				
JE	<b>J4</b>	J5	Field	Format	Description	
	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. Stable 150 on page 507 and Table 151 on page 509 for field listing.  The type of entry.	
	224	010	Entry Type	Char(1)	·	-
					С	Certificate operation
					K	Key ring file operation
					P	Password incorrect
	225	611	Certificate	Char(3)	<b>T</b> Type o	Trusted root operation of action <sup>4</sup> .
			Operation		ADK Certificate with	Certificate with private key added
					ADD	Certificate added
					REQ	Certificate requested
					SGN	Certificate signed

Table 178. KF (Key Ring File) Journal Entries (continued). QASYKFJ4/J5 Field Description File

	Offse	et				
E	<b>J4</b>	J5	Field	Format	Descri	ption
	228	614	Key Ring	Char(3)	Туре о	f action <sup>5</sup> .
			Operation	Operation		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
	231	617	Trusted Root	Char(3)	Type o	ring file f action <sup>6</sup> .
		Operation	(-)	TRS	Key ring pair designated as trusted	
					D1437	root
					RMV	Trusted root designation removed
	234	620	Reserved	Char(18)	LST	List trusted roots
	252	638	Object Name	Binary(4)	Key rii	ng file name length.
			Length		-	
	254	640	Object Name CCSID	Binary(5)	Key rii	ng file name CCSID.
	258	644	Object Name Country or Region ID	Char(2)	Key rir	ng file name Country or Region ID.
	260	646	Object Name	Char(3)	Key rir	ng file name language ID.
	000	0.40	Language ID	Cl(0)		
	263 266	649 652	Reserved Parent File ID	Char(3) Char(16)	Kev rir	ng parent directory file ID.
	282	668	Object File ID	Char(16)	-	ng directory file name.
	298	684	Object Name	Char(512)	-	ng file name.
	810	1196	Reserved	Char(18)	v	
	828	1214	Object Name length	Binary(4)	Source	or target file name length.
	830	1216	Object Name CCSID	Binary(5)	Source	or target file name CCSID.
	834	1220	Object Name Country or Region ID	Char(2)	Source ID.	or target file name Country or Regio
	836	1222	Object Name Language ID	Char(3)	Source	or target file name language ID.
	839	1225	Reserved	Char(3)		
	842	1228	Parent File ID	Char(16)		or target parent directory file ID.
	858	1244	Object File ID	Char(16)		or target directory file ID.
	874	1260	Object Name	Char(512)	Source	or target file name.

Table 178. KF (Key Ring File) Journal Entries (continued). QASYKFJ4/J5 Field Description File

	Offse	t			
JE	J4	J5	Field	Format	Description
	1386	1772	Certificate Label Length	Binary(4)	The length of the certificate label.
	1388	1774	Certificate Label <sup>1</sup>	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 absolute path name.
	2451	2837	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	2454	2840	Path Name Length	Binary(4)	The length of the absolute path name.
	2456	2842	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute Path Name field contains complete absolute path name for the key ring file.
					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.
	2457	2843	Relative Directory File ID <sup>2</sup>	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. <sup>3</sup>
	2473	2859	Absolute Path Name <sup>1</sup>	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 target file.
	7491	7877	ASP Name	Char(10)	Source or target file ASP name
	7501	7887	ASP Number	Char(5)	Source or target 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 absolute path name
	7512	7898	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	7515	7901	Path Name Length	Binary(4)	The length of the absolute path name.

Table 178. KF (Key Ring File) Journal Entries (continued). QASYKFJ4/J5 Field Description File

	Offse	t				
JE	<b>J4</b>	J5	Field	Format	Description	
	7517	7903	Path Name	Char(1)	Path name indicator:	
			Indicator		Y Absolute Path Name field contains complete absolute path name for the source or target file.	
					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.	
	7518	7904	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>	
	7534	7920	Absolute Path Name <sup>1</sup>	Char(5002)	The absolute path name of the source or target file.	

This is a variable length field. The first 2 bytes contain the length of the path name.

Table 179. LD (Link, Unlink, Search Directory) Journal Entries. QASYLDJE/J4/J5 Field Description File

	Of	fset				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Descr	iption
1 156	224	1 610	Entry Type	Char(1)	See Ta 509, a	ing fields common to all entry types. See able 150 on page 507, Table 151 on page nd Table 152 on page 510 for field listing. ype 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 <sup>1</sup>	Binary (4)	The le	ength of the object name.
177	245	631	Object Name CCSID <sup>1</sup>	Binary(5)	The contains	oded character set identifier for the object

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.

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.

The field will be blanks when it is not a certificate operation.

The field will be blanks when it is not a key ring file operation.

The field will be blanks when it is not a trusted root operation.

Table 179. LD (Link, Unlink, Search Directory) Journal Entries (continued). QASYLDJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
181	249	635	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
183	251	637	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
186	254	640	(Reserved area)	Char(3)	
189	257	643	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
205	273	659	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
221	289	675	Object Name <sup>1</sup>	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 absolute path name
	838	1224	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	841	1227	Path Name Length	Binary(4)	The length of the absolute path name.
	843	1229	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.
	844	1230	Relative Direcotry File ID <sup>1</sup>	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. <sup>3</sup>
	860	1246	Path Name <sup>2</sup>	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.

This is a variable length field. The first 2 bytes contain the length of the path name.

Table 180. ML (Mail Actions) Journal Entries. QASYMLJE/J4/J5 Field Description File

Offset						
JE	J4	<b>J</b> 5	Field Format		Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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	

Table 181. NA (Attribute Change) Journal Entries. QASYNAJE/J4/J5 Field Description File

	Offset				
JE J4		<b>J</b> 5	Field	Format	Description
1 156	224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
			3 31		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.

Table 182. ND (APPN Directory Search Filter) Journal Entries. QASYNDJE/J4/J5 Field Description File

	Offset					
JE	J4	<b>J</b> 5	Field	Format	Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 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.	

Table 182. ND (APPN Directory Search Filter) Journal Entries (continued). QASYNDJE/J4/J5 Field Description File

Offset						
JE	JE J4 J5		Field Forma		Desci	ription
205	5 273 659 Inbound Char(1)		Inbou	and session.		
			session		Y	This is an inbound session
206	274	660 Outbound Char(1)	Char(1)	N Outbo	This is not an inbound session bund session.	
			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 the Information Center (see "Prerequisite and Related Information" on page xvi for details).

Table 183. NE (APPN End Point Filter) Journal Entries. QASYNEJE/J4/J5 Field Description File

	Off	set					
JE J4		J5	Field	Format	Descr	ription	
1	1	1			Table	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.	
156	224	610	Entry Type	Char(1)		ype of entry.	
					Α	End point filter violation	
157	225	611	Local location name	Char(8)	Local	location name.	
165	233	619	Remote location name	Char(8)	Remo	te location name.	
173	241	627	Remote NETID	Char(8)	Remo	te NETID.	
181	249	635	Inbound	Char(1)	Inbou	nd session.	
			session		Y	This is an inbound session	
					N	This is not an inbound session	
182	250	636	Outbound	Char(1)	Outbo	ound session.	
			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 the Information Center (see "Prerequisite and Related Information" on page xvi for details).

Table 184. OM (Object Management Change) Journal Entries. QASYOMJE/J4/J5 Field Description File

Offset					
<b>J4</b>	J5	Field	Format	Descr	ription
1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. So Table 150 on page 507, Table 151 on page 508 and Table 152 on page 510 for field listing. The type of entry.	
				M	Object moved to a different library.
				R	Object renamed.
	<b>J4</b>	<b>J4 J5</b> 1	J4 J5 Field 1 1	J4 J5 Field Format  1 1	J4 J5 Field Format Description  1 1 Head Table and Table and Table M

Table 184. OM (Object Management Change) Journal Entries (continued). QASYOMJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
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	650	(Reserved Area)	Char(10)	The attribute of the object		
		659 669	Object Attribute (Reserved	Char(10)	The attribute of the object.		
		003	Area)	Chai (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 <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.		
435	503	889	Object Name Country or Region ID¹	Char(2)	The Country or Region ID for the object name.		
437	505	891	Object Name Language ID¹	Char(3)	The language ID for the object name.		
440	508	894	(Reserved area)	Char(3)			
443	511	897	Old Parent File ID <sup>1,2</sup>		The file ID of the old parent directory.		
459	527	913	Old Object File ID <sup>1,2</sup>		The file ID of the old object.		
475	543	929	Old Object Name <sup>1</sup>	Char(512)	The name of the old object.		

Table 184. OM (Object Management Change) Journal Entries (continued). QASYOMJE/J4/J5 Field Description File

	Offs	set			
JE	J4	J5	Field	Format	Description
987	1055	1441	New Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the new parent directory.
1003	1071	1457	New Object Name <sup>1, 2,6</sup>	Char(512)	The new name of the object.
	1583	1969	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
	1599	1985	ASP Name <sup>7</sup>	Char(10)	The name of the ASP device.
	1609	1995	ASP Number <sup>7</sup>	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 absolute path name
	1620	2006	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	1623	2009	Path Name Length	Binary(4)	The length of the absolute path name.
	1625	2011	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.
	1626	2012	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>
	1642	2028	Absolute Path Name <sup>5</sup>	Char(5002)	The old absolute path name of the object.
	6644	7030	Object File ID	Char(16)	The file ID of the object.
	6660	7046	ASP Name <sup>8</sup>	Char(10)	The name of the ASP device.
	6670	7056	ASP Number <sup>8</sup>	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 absolute path name
	6681	7067	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	6684	7070	Path Name Length	Binary(4)	The length of the absolute path name.

Table 184. OM (Object Management Change) Journal Entries (continued). QASYOMJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	6686	7072	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.
	6687	7073	Relative Directory File ID <sup>4</sup>	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. <sup>3</sup>
	6703	7089	Absolute Path Name <sup>5</sup>	Char(5002)	The new absolute path name of the object.

- These fields are used only for objects in the QOpenSys, "root" (/) file systems, and user-defined file systems.
- An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.
- 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.
- 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.
- This is a variable length field. The first 2 bytes contain the length of the path name.
- There is no associated length field for this value. The string is null padded unless it is the full 512 characters long.
- 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.
- 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.

Table 185. OR (Object Restore) Journal Entries. QASYORJE/J4/J5 Field Description File

Offset					
JE	J4	J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. 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.

Table 185. OR (Object Restore) Journal Entries (continued). QASYORJE/J4/J5 Field Description File

	Offs	et				
JE	E J4 J5		Field	Format	Description	
167	235	621	Restored Library Name	Char(10)	The n	ame of the library of the restored object.
177	245	631	Object Type.	Char(8)	-	ype of object.
185	253	639	Save Object Name	Save Object Char(10) Name		ame of the save object.
195	263	649	Save Library Name	Char(10)	The n	name of the library from which the object aved.
205	273	659	Program State <sup>1</sup>	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	Char(1)	Y	A system command was restored.
			Command <sup>2</sup>		N	A user state command was restored.
207			(Reserved Area)	Char(18)		Trasor state commune was restored.
	275	661	SETUID Mode	Char(1)	The S	ETUID 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 S	ETGID 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.
	277	663	Signature Status	Char(1)	The s	ignature status of the restored object.
			Status		В	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)		file was an integrated file system object, alue of the scan attribute for that object
					Y	*YES
					N	*NO
						*CHGONLY ne CHGATR command for descriptions of values.

Table 185. OR (Object Restore) Journal Entries (continued). QASYORJE/J4/J5 Field Description File

	Offse	et			
JE	<b>J4</b>	J5	Field	Format	Description
	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	Char(12)	The document library object name of the
			Name	, ,	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	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 <sup>3</sup>	Binary(5)	The coded character set identifier for the objection.
435	503	889	Object Name Country or Region ID <sup>3</sup>	Char(2)	The Country or Region ID for the object name
437	505	891	Object Name Language ID <sup>3</sup>	Char(3)	The language ID for the object name.
440	508	894	(Reserved area)	Char(3)	
443	511	897	Parent File ID <sup>3,4</sup>	Char(16)	The file ID of the parent directory.
459	527	913	Object File ID <sup>3,4</sup>	Char(16)	The file ID of the object.
475	543	929	Object Name <sup>3</sup>	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 medi file.
					<b>Note:</b> 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 <sup>7</sup>	Char(10)	The name of the ASP device.
	1113	1499	ASP Number <sup>7</sup>	Char(5)	The number of the ASP device.
	1118	1504	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.

Table 185. OR (Object Restore) Journal Entries (continued). QASYORJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
	1122	1508	Path Name Country or Region ID	Char(2)	The Country or Region ID for the absolute path name
	1124	1510	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	1127	1513	Path Name Length	Binary(4)	The length of the absolute path name.
	1129	1515	Path Name	Char(1)	Path name indicator:
			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.
	1130	1516	Relative Directory File ID <sup>5</sup>	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. <sup>3</sup>
	1146	1532	Path Name <sup>6</sup>	Char(5002)	The path name of the object.

<sup>1</sup> This field has an entry only if the object being restored is a program.

Table 186. OW (Ownership Change) Journal Entries. QASYOWJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
			0 01		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.

<sup>2</sup> This field has an entry only if the object being restored is a command.

<sup>3</sup> These fields are used only for objects in the QOpenSys file system and the "root" (/) file system.

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

<sup>5</sup> 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.

This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 186. OW (Ownership Change) Journal Entries (continued). QASYOWJE/J4/J5 Field Description File

	Offs	set			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
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 <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
352	420	806	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
354	422	808	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
357	425	811	(Reserved area)	Char(3)	
360	428	814	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
376	444	830	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
392	460	846	Object Name <sup>1</sup>	Char(512)	The name of the object.
	972	1358	Object File ID	Char(16)	The file ID of the object.
	988	1374	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	998	1384	ASP Number <sup>5</sup>	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 absolute path name
	1009	1395	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	1012	1398	Path Name Length	Binary(4)	The length of the absolute path name.
	1014	1400	Path Name	Char(1)	Path name indicator:
			Indicator		Y Absolute 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.

Table 186. OW (Ownership Change) Journal Entries (continued). QASYOWJE/J4/J5 Field Description File

Offset						
JE	J4	J5	Field	Format	Description	
	1015	1401	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>	
	1031	1417	Path Name <sup>4</sup>	Char(5002)	The path name of the object.	

These fields are used only for objects in the QOpenSys file system and the "root" (/) file system.

Table 187. O1 (Optical Access) Journal Entries. QASY01JE/J4/J5 Field Description File

Offset					
ΙE	J4	J5	Field	Format	Description
l	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.
56	224	610	Entry Type	Char(1)	R-Read
					U-Update
					D-Delete
					C-Create Dir
					X-Release Held File
57	225	611	Object Type	Char(1)	F-File
					D-Directory End
					S-Storage
58	226	612	Access Type	Char(1)	D-File Data
					A-File Directory Attributes
					R-Restore operation
					S-Save operation
59	227	613	Device Name	Char(10)	Library LUD name
69	237	623	CSI Name	Char(8)	Side Object Name
77	245	631	CSI Library	Char(10)	Side Object Library
87	255	641	Volume Name	Char(32)	Optical volume name
19	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

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 187. O1 (Optical Access) Journal Entries (continued). QASY01JE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description	
Note:	Γhis entry is	used to audit	the following option	al functions:		
Ope	en File or Di	rectory				
Crea	ate Directory	1				
Dele	ete File Dire	ctory				
Cha	nge or Retri	eve Attributes				
Rele	ease Held O	ptical File				

Table 188. O2 (Optical Access) Journal Entries. QASY02JE/J4/J5 Field Description File

	Off	fset			
JE	J4	<b>J</b> 5	Field	Format	Description
1	1	1 1	1 Entry Type		Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.
156	224	610		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

Table 189. O3 (Optical Access) Journal Entries. QASY03JE/J4/J5 Field Description File

	Of	fset				
JE	<b>J4</b>	J5	Field	Format	Descr	ription
1	1	1			Table	ing fields common to all entry types. Sec 150 on page 507, Table 151 on page 509, Table 152 on page 510 for the field listing
156	224	610	Entry Type	Char(1)	Α	Change Volume Attributes
					В	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)	Libra	ry LUD name
167	235	621	CSI Name	Char(8)		Object Name
175	243	629	CSI Library	Char(10)	Side (	Object Library
185	253	639	Old Volume Name	Char(32)	Old C	Optical volume name
217	285	671	New Volume Name <sup>1</sup>	Char(32)	New	Optical volume name
249	317	703	Old Auth List	Char(10)	Old A	Authorization List
259	327	713	New Auth List	Char(10)	New	Authorization List
269	337	723	Address <sup>4</sup>	Binary(5)	Starti	ng Block
273	341	727	Length <sup>4</sup>	Binary(5)	Lengt	h read
		731	ASP name	Char(10)	ASP r	name for CSI library
		741	ASP number	Char(5)	ASP r	number for CSI library
1	backup bo	lume name for		contains volu	ıme nam	d Convert functions; it contains the e for Import, Export, Change

Used for Import, Export, and Change Authorization List only.

Table 190. PA (Program Adopt) Journal Entries. QASYPAJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.

<sup>3</sup> Used for Change Authorization List only.

Used for Sector Read only.

Table 190. PA (Program Adopt) Journal Entries (continued). QASYPAJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
.56	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.
57	225	611	Program Name <sup>3</sup>	Char(10)	The name of the program.
67	235	621	Program Library <sup>3</sup>	Char(10)	The name of the library where the program is found.
77	245	631	Object Type	Char(8)	The type of object.
.85	253	639	Owner	Char(10)	The name of the owner.
.00	263	649	IXVTX mode	Char(1)	The restricted rename and unlink (ISVTX) mode
	200	040	1XV 1X mode	Char(1)	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 <sup>1</sup>	Binary (4)	The length of the object name.
	283	669	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
	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 <sup>1</sup>	Char(3)	The language ID for the object name.
	292	678	Reserved	Char(3)	
	295	681	Parent ID <sup>1, 2, 3</sup>	Char(16)	Parent File ID.
	311	697	Object File ID <sup>3</sup>	Char(16)	File ID for the object
	327	713	Object Name <sup>1</sup>	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 <sup>6</sup>	Char(10)	The name of the ASP device.
	877	1263	ASP Number <sup>6</sup>	Char(5)	The number of the ASP device.

Table 190. PA (Program Adopt) Journal Entries (continued). QASYPAJE/J4/J5 Field Description File

	Offset					
JE	J4	J5	Field	Format	Desci	ription
	882	1268	Path Name CCSID	Binary(5)	The c	oded character set identifier for the path
	886	1272	Path Name Country or Region ID	Char(2)	The C name	Country or Region ID for the absolute path
	888	1274	Path Name Language ID	Char(3)	The la	anguage ID for the absolute path name.
	891	1277	Path Name Length	Binary(4)	The le	ength of the absolute path name.
	893	1279	Path Name	Char(1)	Path	name indicator:
			Indicator		Y	Absolute 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.
	894	1280	Relative Directory File ID <sup>4</sup>	Char(16)	field conta	the Path Name Indicator field is N, this contains the file ID of the directory that ins the object identified in the Path Name Otherwise it contains hex zeros. <sup>3</sup>
	910	1296	Path Name <sup>5</sup>	Char(5002)	The p	oath name of the object.

These fields are used only for objects in the QOpenSys and "root" (/) file systems.

Table 191. PG (Primary Group Change) Journal Entries. QASYPGJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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.		

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 191. PG (Primary Group Change) Journal Entries (continued). QASYPGJE/J4/J5 Field Description File

	Offse	et			
JE	J4	<b>J</b> 5	Field	Format	Description
185	253 639 Old Primary Char(10) Group		The previous primary group for the object. <sup>5</sup>		
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
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)	
222	290	676	Add Authority	Char(1)	Y *READ
			3		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.
					<ul> <li>Do not revoke authority for previous primary group.</li> </ul>
238	306	692	(Reserved Area)	Char (20)	
258	326	712	Office User	Char(10)	The name of the office user.
268	336	722 724	DLO Name (Reserved Area)	Char(12)	The name of the document library object or fold
280 288	348 356	734 742	Folder Path	Char(8) Char(63)	The path of the folder.
351	419	805	Office on Behalf		User working on behalf of another user.
361	410	003	of User (Reserved Area)	Char(20)	Oser working on behalf of another user.
JU1	429	815	(Reserved Area)	Char(18)	
	447	833	Object Name Length <sup>1</sup>	Binary (4)	The length of the object name.
381	449	835	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
385	453	839	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.

Table 191. PG (Primary Group Change) Journal Entries (continued). QASYPGJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
387	455	841	Object Name Language ID¹	Char(3)	The language ID for the object name.		
390	458	844	(Reserved area)	Char(3)			
393	461	847	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.		
409	477	863	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.		
425	493	879	Object Name <sup>1</sup>	Char(512)	The name of the object.		
	1005	1391	Object File ID	Char(16)	The file ID of the object.		
		1407	ASP Name <sup>6</sup>	Char(10)	The name of the ASP device.		
		1417	ASP Number <sup>6</sup>	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 absolute path name		
	1042	1428	Path Name Language ID	Char(3)	The language ID for the absolute path name.		
	1045	1431	Path Name Length	Binary(4)	The length of the absolute path name.		
	1047	1433	Path Name	Char(1)	Path name indicator:		
			Indicator		Y Absolute Path Name field contains complete absolute path name for the object.		
					N The Path Name field does not contain a 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.		
	$\begin{array}{ccc} 1048 & 1434 & \text{Relative} & \text{C} \\ & \text{Directory File} \\ & \text{ID}^3 \end{array}$		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. <sup>3</sup>			
	1064	1450	Path Name <sup>4</sup>	Char(5002)	The path name of the object.		

These fields are used only for objects in the QOpenSys and "root" (/) file systems.

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

<sup>&</sup>lt;sup>5</sup> A value of \*N implies that the value of the Old Primary Group was not available.

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.

Table 192. PO (Printer Output) Journal Entries. QASYPOJE/J4/J5 Field Description File

	Offse	et					
JE	JE `J4 J5		Field	Format Char(1)	Description  Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of output.		
1 156			Output Type				
					D Direct print		
					R Sent to remote system for printing		
					S Spooled file printed		
157	225	611	Status After	Char(1)	D Deleted after printed		
		Printing		i			
					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. <sup>1</sup>		
214	282	668	Device Name	Char(10)	The device where the output was printed <sup>2</sup> .		
224	292	678	Device Type	Char(4)	The type of printer device <sup>2</sup> .		
228	296	682	Device Model	Char(4)	The model of the printer device <sup>2</sup> .		
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 <sup>1</sup>		
262	330	716	Short Spooled File Number	Char(4)	The number of the spooled file <sup>1</sup> . Set to blank if to long.		
266	334	720	Form Type	Char(10)	The form type of the spooled file.		
276 286	344	730	User Data (Reserved area)	Char(10) Char(20)	The user data associated with the spooled file <sup>1</sup> .		
	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 (CYYMMDD)		
	772	1158	Spooled File Create Time	Char(6)	The spooled file create time (HHMMSS).		

Table 192. PO (Printer Output) Journal Entries (continued). QASYPOJE/J4/J5 Field Description File

	Offset					
JE	`J4	<b>J</b> 5	Field	Format	Description	
		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.	

This field is blank if the type of output is direct print.

Table 193. PS (Profile Swap) Journal Entries. QASYPSJE/J4/J5 Field Description File

Offset						
JE	J4	J5	Field	Format	Descr	iption
1 156	1 224	1 610	Entry Type	Char(1)	Table Table	ing fields common to all entry types. See 150 on page 507,Table 151 on page 509, and 152 on page 510 for field listing. ype of entry.
					Α	Profile swap during pass-through.
					E	End work on behalf of relationship.
					Н	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)		profile name.
167	235	621	Source Location	` '		through source location.
175	243	629	Original Target User Profile	Char(10)	Origir	nal 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)		user starting or ending on behalf of onship.
205	273	659	On Behalf of User	Char(10)	User o worki	on behalf of whom the office user is ing.
215	283	669	Profile Token	Char(1)	The ty	ype of the profile token that was generated.
			Type		M	Multiple-use profile token
					R	Multiple-use regenerated profile token
					S	Single-use profile token
216	284	670	Profile Token Timeout	Binary(4)		number of seconds that the profile token is

This field is blank if the type of output is remote print.

Table 194. PW (Password) Journal Entries. QASYPWJE/J4/J5 Field Description File

	Offs	et					
JE	J4	J5	Field	Format	Descr	iption	
1 156	1 224			Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of violation		
			Type		Α	APPC bind failure.	
					С	User authentication with the CHKPWD command failed.	
					D	Service tools user ID name not valid.	
					E	Service tools user ID password not valid	
					P	Password not valid.	
					Q	Attempted signon (user authentication) failed because user profile is disabled.	
					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.	
					S	SQL Decryption password is not valid.	
					U	User name not valid.	
					X	Service tools user ID is disabled.	
					Y	Service tools user ID not valid.	
157	225	611	User Name	Char(10)	<b>Z</b> The jo	Service tools user ID password not valid bb user name or the service tools user ID	
167	235	621	Device name	Char(40)	The n	ame of the device or communications e on which the password or user ID was ed. If the entry type is X, Y, or Z, this field ontain the name of the service tool being	
207	275	661	Remote Location Name	Char(8)	Name	e of the remote location for the APPC bind.	
215	283	669	Local Location Name	Char(8)	Name	e of the local location for the APPC bind.	
223	291	677 685 <sup>2</sup> 695 705 713 723	Network ID Object Name Object Library Object Type ASP Name <sup>1</sup> ASP Number <sup>1</sup>	Char(8) Char(10) Char(10) Char(8) Char(10) Char(5)	The n The li The ty The n	ork ID for the APPC bind.  ame of the object being decrypted.  brary for the object being decrypted.  ype of object being decrypted.  ame of the ASP device.  umber of the ASP device.	

this is the ASP information for the object.

If the object name is \*N and the violation type is S, the user attempted to decrypt data in a host variable.

Table 195. RA (Authority Change for Restored Object) Journal Entries. QASYRAJE/J4/J5 Field Description File

	Of	fset			
JE	J4	J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
			J	,	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.
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 <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
325	393	779	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
327	395	781	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
330	398	784	(Reserved area)	Char(3)	
333	401	787	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
349	417	803	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
365	433	819	Object Name <sup>1</sup>	Char(512)	The name of the object.
	945	1331	Object File ID	Char(16)	The file ID of the object.
	961	1347	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	971	1357	ASP Number <sup>5</sup>	Char(5)	The number of the ASP device.
	976	1362	Path Name CCSID	Binary(5)	The coded character set identifier for the path name.

Table 195. RA (Authority Change for Restored Object) Journal Entries (continued). QASYRAJE/J4/J5 Field Description File

	Of	fset					
JE	J4	<b>J</b> 5	Field	Format	Description		
	980	1366	Path Name Country or Region ID	Char(2)	The Country or Region ID for the absolute path name		
	982	1368	Path Name Language ID	Char(3)	The language ID for the absolute path name.		
	985	1371	Path Name Length	Binary(4)	The length of the absolute path name.		
	987	1373	Path Name	Char(1)	Path name indicator:		
			Indicator		Y Absolute 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.		
	988	1374	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>		
	1004	1390	Path Name <sup>4</sup>	Char(5002)	The path name of the object.		

These fields are used only for objects in the QOpenSys and "root" (/) file systems.

Table 196. RJ (Restoring Job Description) Journal Entries. QASYRJJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
					A Restoring a job description that had a user profile specified in the USER parameter.
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.

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

<sup>&</sup>lt;sup>4</sup> This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 196. RJ (Restoring Job Description) Journal Entries (continued). QASYRJJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	Format	Description
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

Table 197. RO (Ownership Change for Restored Object) Journal Entries. QASYROJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. 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)	
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length <sup>1</sup>	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID <sup>1</sup>	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
372	440	826	Object Name <sup>1</sup>	Char(512)	The name of the object.
	952	1338	Object File ID	Char(16)	The file ID of the object.
	968	1354	ASP Name <sup>5</sup>	Char(10)	The name of the ASP device.
	978	1364	ASP Number <sup>5</sup>	Char(5)	The number of the ASP device.

Table 197. RO (Ownership Change for Restored Object) Journal Entries (continued). QASYROJE/J4/J5 Field Description File

	Offset						
JE	J4	J5	Field	Format	Description		
	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 absolute path name		
	989	1375	Path Name Language ID	Char(3)	The language ID for the absolute path name.		
	992	1378	Path Name Length	Binary(4)	The length of the absolute path name.		
	994	1380	Path Name	Char(1)	Path name indicator:		
			Indicator		Y Absolute 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 nam The Relative Directory File ID field is valid and may be used to form an absolute path name with this relative path name.		
	995	1381	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>		
	1011	1397	Path Name <sup>4</sup>	Char(5002)	The path name of the object.		

These fields are used only for objects in the QOpenSys and "root" (/) file systems.

Table 198. RP (Restoring Programs that Adopt Authority) Journal Entries. QASYRPJE/J4/J5 Field Description File

	Offse	et			
JE	J4	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 198. RP (Restoring Programs that Adopt Authority) Journal Entries (continued). QASYRPJE/J4/J5 Field Description File

	Offse	et				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Descr	iption
	263	649	(Reserved Area)	Char(18)		
	281	667	Object Name Length <sup>1</sup>	Binary (4)	The le	ength of the object name.
	283	669	Object Name CCSID <sup>1</sup>	Binary (5)	The containe.	oded character set identifier for the object
	287	673	Object Name Country or Region ID <sup>1</sup>	Char (2)	The C	ountry or Region ID for the object name.
	289	675	Object name Language ID <sup>1</sup>	Char (3)	The la	anguage ID for the object name.
	292	678	(Reserved Area)	Char (3)		
	295	681	Parent File ID <sup>1,2</sup>	Char (16)	The fi	le ID of the parent directory.
	311	697	Object File ID <sup>1,2</sup>	Char (16)	The fi	le ID of the object.
	327	713	Object Name <sup>1</sup>	Char (512)	The n	ame of the object.
	839	1225	Object File ID	Char(16)	The fi	le ID of the object.
	855	1241	ASP Name <sup>5</sup>	Char(10)	The n	ame of the ASP device.
	865	1251	ASP Number <sup>5</sup>	Char(5)	The n	umber of the ASP device.
	870	1256	Path Name CCSID	Binary(5)	The conname.	oded character set identifier for the path
	874	1260	Path Name Country or Region ID	Char(2)	The C name	ountry or Region ID for the absolute path
	876	1262	Path Name Language ID	Char(3)	The la	anguage ID for the absolute path name.
	879	1265	Path Name Length	Binary(4)	The le	ength of the absolute path name.
	881	1267	Path Name	Char(1)	Path r	name indicator:
			Indicator		Y	Absolute 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.
	882	1268	Relative Directory File ID <sup>3</sup>	Char(16)	field o contai	the Path Name Indicator field is N, this contains the file ID of the directory that ns the object identified in the Path Name Otherwise it contains hex zeros. <sup>3</sup>
	898	1284	Path Name <sup>4</sup>	Char(5002)		ath name of the object.
					_	

These fields are used only for objects in the QOpenSys and the "root" (/) file system.

If an ID that has the left-most bit set and the rest of the bits are zero, the ID is **not** set.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

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.

Table 199. RQ (Restoring Change Request Descriptor Object) Journal Entries. QASYRQJE/J4/J5 Field Description File

Offset		t			
JE	<b>J4</b>	J5	Field	ield Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 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

Table 200. RU (Restore Authority for User Profile) Journal Entries. QASYRUJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 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.
	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

Table 201. RZ (Primary Group Change for Restored Object) Journal Entries. QASYRZJE/J4/J5 Field Description File

Offset		Offset			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
1 156	224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.
100	<i>ω</i> ω 1	010	Lifty Type	Char(1)	
157	225	611	Object Name	Char(10)	A Primary group changed.
			J	` ,	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.

Table 201. RZ (Primary Group Change for Restored Object) Journal Entries (continued). QASYRZJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
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)	
245 308	313	699	Folder Path (Reserved Area)	Char(63) Char(20)	The folder into which the object was restored.
	376	762	(Reserved Area)	Char(18)	
	394	780	Object Name Length <sup>1</sup>	Binary(4)	The length of the object name.
328	396	782	Object Name CCSID <sup>1</sup>	Binary(5)	The coded character set identifier for the object name.
332	400	786	Object Name Country or Region ID <sup>1</sup>	Char(2)	The Country or Region ID for the object name.
334	402	788	Object Name Language ID¹	Char(3)	The language ID for the object name.
337	405	791	(Reserved area)	Char(3)	
340	408	794	Parent File ID <sup>1,2</sup>	Char(16)	The file ID of the parent directory.
356	424	810	Object File ID <sup>1,2</sup>	Char(16)	The file ID of the object.
372	440	826	Object Name <sup>1</sup>	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 absolute path name
	989	1375	Path Name Language ID	Char(3)	The language ID for the absolute path name.
	992	1378	Path Name Length	Binary(4)	The length of the absolute path name.
	994	1380	Path Name Indicator	Char(1)	Path name indicator:
					Y Absolute 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.

Table 201. RZ (Primary Group Change for Restored Object) Journal Entries (continued). QASYRZJE/J4/J5 Field Description File

Offset					
JE	J4	J5	Field	Format	Description
	995	1381	Relative Directory File ID <sup>3</sup>	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. <sup>3</sup>
	1011	1397	Path Name <sup>4</sup>	Char(5002)	The path name of the object.

These fields are used only for objects in the QOpenSys and "root" (/) file systems.

Table 202. SD (Change System Distribution Directory) Journal Entries. QASYSDJE/J4/J5 Field Description File

Offset						
JE	J4	<b>J</b> 5	Field	Format	Description	
1 156	224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry.	
			0 01		S System directory change	
157	225	611	Type of Change	Char(3)	ADD Add directory entry	
					CHG Change directory entry	
					COL Collector entry	
					<b>DSP</b> 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)	<b>DIRE</b> Directory	
					<b>DPTD</b> 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	

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

Table 202. SD (Change System Distribution Directory) Journal Entries (continued). QASYSDJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
190	258	644	Function	Char(6)	INIT Initialization
			Requested		
					OFFLIN
					Offline initialization
					REINIT
					Reinitialization
					SHADOW
					Normal shadowing
					STPSHD
					Stop shadowing
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

Table 203. SE (Change of Subsystem Routing Entry) Journal Entries. QASYSEJE/J4/J5 Field Description File

	Offset					
JE	J4	J5	Field	Format	Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.	
156	224	610	Entry Type	Char(1)	The type of entry.	
157	225	611	Subsystem Name	Char(10)	A Subsystem routing entry changed 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	Char(3)	The type of command used	
			Name		ADD ADDRTGE	
					CHG CHGRTGE	
					RMV RMVRTGE	
		666	ASP name for SBSD library	Char(10)	ASP name for SBSD library	
		676	ASP number for SBSD library	Char(5)	ASP number for SBSD library	
		681	ASP name for program library	Char(10)	ASP name for program library	

Table 203. SE (Change of Subsystem Routing Entry) Journal Entries (continued). QASYSEJE/J4/J5 Field Description

Offset					
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
		691	ASP number for program library	Char(5)	ASP number for program library

Table 204. SF (Action to Spooled File) Journal Entries. QASYSFJE/J4/J5 Field Description File

Offset				_		
JE	J4	J5	Field	Format	Description	
1 156	1 224	1 610	Access Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, a Table 152 on page 510 for field listing. The type of entry	
					A Spooled file read.	
					C Spooled file created.	
					<b>D</b> 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 attribut changed.	
					V Only non-security-relevant spooled fi	
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)		
195 205	263 273	649 659	Member Name Spooled File Name	Char(10) Char(10)	The name of the file member.  The name of the spooled file <sup>1</sup> .	
215	283	669	Short Spooled File Number	Char(4)	The number of the spooled file <sup>1</sup> . 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	

Table 204. SF (Action to Spooled File) Journal Entries (continued). QASYSFJE/J4/J5 Field Description File

Of		t				
JE	J4	J5	Field	Format	Description	
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	
33	401	787	New Restart Page	Char(8)	New restart page for the spooled file	
841	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.	
	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.	

Table 204. SF (Action to Spooled File) Journal Entries (continued). QASYSFJE/J4/J5 Field Description File

Offset			_			
JE	<b>J4</b>	J5	Field	Format	Description	
	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.	
	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 (CYYMMDD).	
	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.	

Table 204. SF (Action to Spooled File) Journal Entries (continued). QASYSFJE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description	
		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.	
		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	

This field is blank when the type of entry is I (inline print).

Table 205. SG (Asychronous Signals) Journal Entries. QASYSGJ4/J5 Field Description File

	Offset					
JE	<b>J4</b>	J5	Field	Format	Description	
	1 224	1 610	Entry Type	Char(1)	Table for fie	ing fields common to all entry types. See 150 on page 507 and Table 151 on page 509 eld listing.
					Α	Asynchronous iSeries signal processed
					P	Asynchronous Private Address Space Environment (PASE) signal processed
	225	611	Signal Number	Char(4)	The si	ignal number that was processed.

Table 205. SG (Asychronous Signals) Journal Entries (continued). QASYSGJ4/J5 Field Description File

	Offset						
JE	<b>J4</b>	J5 Field Format		Format	Description		
	229	615	Handle action	Char(1)	The action taken on this signal.		
					C Continue the process		
					E Signal exception		
					<ul> <li>H Handle by invoking the signal catching function</li> </ul>		
					S Stop the process		
					T End the process		
	230	616	Signal Source	Char(1)	U End the request 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.		

Table 206. SK (Secure Sockets Connections) Journal Entries. QASYSKJ4/J5 Field Description File

	Offs	set					
JE	<b>J4</b>	J5	Field	Format	Description		
	1	1			Table	ling fields common to all entry types. See 150 on page 507 and Table 151 on page 509 eld listing.	
	224	610	Entry type	Char(1)	Α	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 <sup>3</sup>	Char(15)	The l	ocal IP address.	
	240	626	Local port	Char(5)	The l	ocal port.	

Table 206. SK (Secure Sockets Connections) Journal Entries (continued). QASYSKJ4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
	245	631	Remote IP Address <sup>3</sup>	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 <sup>1</sup>	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 <sup>2</sup>	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.

This is a variable length field. The first two bytes contain the length of the field.

Table 207. SM (Systems Management Change) Journal Entries. QASYSMJE/J4/J5 Field Description File

	Offs	set				
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Desc	ription
1 156	1 224	1 610	Entry Type	Char(1)	Table Table	ling fields common to all entry types. See e 150 on page 507,Table 151 on page 509, and e 152 on page 510 for field listing. tion accessed
					В	Backup list changed
					C	Automatic cleanup options
					D	DRDA
					F	HFS file system
					N	Network file operation
					О	Backup options changed
					P	Power on/off schedule
					S	System reply list
					T	Access path recovery times changed

When the entry type is D, this field contains the IP address that the DHCP server assigned to the requesting client.

These fields only support IPv4 addresses.

Table 207. SM (Systems Management Change) Journal Entries (continued). QASYSMJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
157	225	611	Access Type	Char(1)	<b>A</b> Add
					C Change
					<b>D</b> 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
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

Table 208. SO (Server Security User Information Actions) Journal Entries. QASYSOJE/J4/J5 Field Description File

Offset  JE J4 J5					
		J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. 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.

Table 208. SO (Server Security User Information Actions) Journal Entries (continued). QASYSOJE/J4/J5 Field Description File

	Of	fset				
JE	<b>J4</b>	J5	Field	Format	Desc	ription
	235	621	User Information	Char(1)	N	Entry type not specified.
			Entry Type		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
			Stored		S	No change
					Y	Password is stored.
	237	623	Server Name	Char(200)	The 1	name of the server.
	437	823	(Reserved Area)	Char(3)		
	440	826	User ID Length	Binary (4)	The l	length of the user ID.
	442	828	(Reserved Area)	Char(20)		
	462	848	User ID	Char(1002)1	The l	ID for the user.
1	This is a	variable length	field. The first 2 byt	es contain the l	ength o	of the field.

Table 209. ST (Service Tools Action) Journal Entries. QASYSTJE/J4/J5 Field Description File

	Offs	set					
JE	J4	J5	Field	Format	Description		
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, a Table 152 on page 510 for field listing.		
156	224	610	Entry Type	Char(1)	The type	e of entry	
157	225	611	Service Tool	Char(2)	<b>A</b> The type	Service record e of entry.	
					AN	ANZJVM	
					CS	STRCPYSCN	
					CD	QTACTLDV, QTADMPDV	
					CE	QWTCTLTR	
					CT	DMPCLUTRC	
					DC	DLTCMNTRC	
					DD	DMPDLO	
					DJ	DMPJVM, QPYRTJVM	
					DM	DMPMEMINF	
					DO	DMPOBJ	

Table 209. ST (Service Tools Action) Journal Entries (continued). QASYSTJE/J4/J5 Field Description File

	Offs	set				
JE	J4	J5	Field	Format	Descri	ption
					DS	DMPSYSOBJ, QTADMPTS, QTADMPD
					EC	ENDCMNTRC
					ER	ENDRMTSPT
					HD	QYHCHCOP (DASD)
					HL	QYHCHCOP (LPAR)
					JW	QPYRTJWA
					MC	QWMMAINT (change)
					MD	QWMMAINT (dump)
					OP	Operations console
					PC	PRTCMNTRC
					PE	PRTERRLOG, QTADMPDV
					PΙ	PRTINTDTA, QTADMPDV
					PS	QP0FPTOS
					SC	STRCMNTRC
					SE	QWTSETTR
					SF	QWCCDSIC, QWVRCSTK (Display internal stack entry)
					SJ	STRSRVJOB
					SR	STRRMTSPT
					ST	STRSST
					TA	TRCTCPAPP
					TC	TRCCNN (*FORMAT specified)
					TE	ENDTRC, ENDPEX, TRCJOB(*OFF or *END specified)
					TI	TRCINT or TRCCNN (*ON, *OFF, or *END specified)
					$\mathbf{T}\mathbf{Q}$	QWCTMQTM
					TS	STRTRC, STRPEX, TRCJOB(*ON specified)
					UD	QTAUPDDV
					WE	ENDWCH, QSCEWCH
					WS	STRWCH, QSCSWCH
					WT	WRKTRC
					ww	WRKWCH
159	227	613	Object Name	Char(10)		of the library for the chiest
169 179	237 247	623 633	Library Name Object Type	Char(10) Char(8)		of the library for the object of object
187	255	641	Job Name	Char(10)		rst part of the qualified job name

Table 209. ST (Service Tools Action) Journal Entries (continued). QASYSTJE/J4/J5 Field Description File

	Offs	set			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
97	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
81	349	735	DLO Name	Char(12)	Name of the document library object
93	361	747	(Reserved Area)	Char(8)	
801	369	755	Folder Path	Char(63)	The folder containing the document library object
	432	818	JUID Field	Char(10)	The JUID of the target job.
	442	828	Early Trace	Char(10)	The action requested for early job tracing
			Action <sup>1</sup>		*ON Early tracing turned on
					*OFF Early tracing turned off
					*RESET
					Early tracing turned off and trace information deleted.
	452	838	Application	Char(1)	The trace option specified on TRCTCPAPP.
			Trace Option <sup>2</sup>		Y Collection of trace information started
					N Collection of trace information stopped and trace information written to spoole file
					E Collection of trace information ended and all trace information purged (no output created)
	453	839	Application Traced <sup>2</sup>	Char(10)	The name of the application being traced.
	463	849	Service Tools Profile <sup>3</sup>	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 <sup>4</sup>	Char(10)	The console type. Possible values are: • *DIRECT
					• *LAN
					• *HMC

Table 209. ST (Service Tools Action) Journal Entries (continued). QASYSTJE/J4/J5 Field Description File

	Offset				
JE	J4	<b>J</b> 5	Field	Format	Description
		917	Console action	Char(10)	The console action. Possible values are:
			4		• *RECOVERY
					• *TAKEOVER
		927	Address family	Char(10)	The address family.
			4		• *IPv4
					• *IPv6
		937	Previous IP address <sup>4</sup>	Char(46)	The IP address of the previous console device for *LAN.
		938	Previous device ID <sup>4</sup>	Char(10)	The service tools device ID of the previous console device for *LAN.
		993	Current IP address <sup>4</sup>	Char(46)	The IP address of the current console device for *LAN.
		1039	Current device ID <sup>4</sup>	Char(10)	The service tools device ID of the current console device for *LAN.
		1049	Watch session <sup>5</sup>	Char(10)	Watch session ID.
1	This field	d is used only	when the entry type	(offset 225)	is CE.
2	This field	d is used only	when the entry type	(offset 225)	is TA.
3	This field	d is used only	when the entry type	(offset 611)	is ST or OP.
4	This field	d is only used	when the entry type	(offset 611)	is OP.
5	This field	d is only used	when the Service To	ol value (off:	set 611) is WS or WE.

Table 210. SV (Action to System Value) Journal Entries. QASYSVJE/J4/J5 Field Description File

	Offs	et					
JE	J4	J5	Field	Format	Desci	Description	
1 156	1 224	1 610	Entry Type	Char(1)	Table Table	ling fields common to all entry types. See 150 on page 507,Table 151 on page 509, and 152 on page 510 for field listing. ype of entry.	
					A	Change to system values	
					В	Change to service attributes	
					C	Change to system clock	
157	225	611	System Value or Service Attribute	Char(10)	The n	name of the system value or service attribute	
167	235	621	New Value	Char(250)		value to which the system value or service oute was changed	
417	485	871	Old Value	Char(250)	The v	value of the system value or service attribute e it was changed	
667	735	1121	New Value Continued	Char(250)	Conti	Continuation of the value to which the system value or service attribute was changed.	
917	985	1371	Old Value Continued	Char(250)	Conti	inuation of the value of the system value or ce attribute was changed.	

Table 211. VA (Change of Access Control List) Journal Entries. QASYVAJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
1 156	1 224	1 610	Status	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. Status of request.
130	224	010	Status	Cital (1)	•
					S Successful
					<b>F</b> 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.

Table 212. VC (Connection Start and End) Journal Entries. QASYVCJE/J4/J5 Field Description File

	Offset					
JE	<b>J4</b>	J5	Field	Format	Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.	
156	224	610	Connect	Char(1)	The connection action that occurred.	
			Action.		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.	

Table 212. VC (Connection Start and End) Journal Entries (continued). QASYVCJE/J4/J5 Field Description File

	Offset						
JE	<b>J4</b>	J5	Field	Format	Description		
202 270	656	Rejection	Char(1)	The r	reason why the connection was rejected:		
			Reason		A	Automatic disconnect (timeout), share removed, or administrative permissions lacking	
					E	Error, session disconnect, or incorrect password	
					N	Normal disconnection or user name limit	
203	271	657	Network Name	Char(12)		No access permission to shared resource network name associated with the ection.	

Table 213. VF (Close of Server Files) Journal Entries. QASYVFJE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
1 156	1 224	1 610	Close Reason	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. 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.

Table 214. VL (Account Limit Exceeded) Journal Entries. QASYVLJE/J4/J5 Field Description File

	Offs	et			
JE	<b>J4</b>	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.

Table 214. VL (Account Limit Exceeded) Journal Entries (continued). QASYVLJE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	J5	Field Format	Format	Description	
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.	
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.	

Table 215. VN (Network Log On and Off) Journal Entries. QASYVNJE/J4/J5 Field Description File

	Offset						
JE	J4	<b>J</b> 5	Field	Format	Description		
1 156	1 224	1 610	Log Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. The type of event that occurred:		
			3 71	,	F Logoff requested		
					O Logon requested		
157	225	611	Server Name	Char(10)	<b>R</b> Logon rejected  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		
					<b>G</b> Guest		
					U User		

Table 215. VN (Network Log On and Off) Journal Entries (continued). QASYVNJE/J4/J5 Field Description File

Offset						
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Desci	ription
198	266	652	Reject Reason	Char(1)	The r	reason why the log on attempt was rejected:
					A	Access denied
					F	Forced off due to logon limit
199	267	653	Additional	Char(1)	<b>P</b> Detai	Incorrect password ls of why access was denied:
			Reason		A	Account expired
					D	Account disabled
					L	Logon hours not valid
					R	Requester ID not valid
					U	Unknown or unavailable

Table 216. VO (Validation List) Journal Entries. QASYVOJ4/J5 Field Description File

	Offset					
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Desci	ription
	1 224			Table for fie	ling fields common to all entry types. See 150 on page 507 and Table 151 on page 509 eld listing.	
	224	610	Entry Type	Char(1)	•	ype 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
	225	611	Unsuccessful	Char(1)	<b>V</b> Type	Successful verify of a validation list entry of unsuccessful verify.
			Type		E	Encrypted data is incorrect
					I	Entry ID was not found
	226 236	612 622	Validation List Library Name	Char(10) Char(10)		Validation list was not found name of the validation list. name of the library that the validation list is
	246	632	<b>Encrypted Data</b>	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 216. VO (Validation List) Journal Entries (continued). QASYVOJ4/J5 Field Description File

	Offset					
JE	<b>J4</b>	J5	Field	Format	Desci	ription
	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 le	ength of the entry ID.
	250 252	636 638	Data length Encrypted Data	Binary(4) Char (1)		ength of the entry data. pted data.
			Attribute		, ,	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)		entry ID.
	382	768	Entry Data	Byte(1000)		entry data.
		1768	ASP name for validation list library	Char(10)	ASP 1	name for validation list library
		1778	ASP number for validation list library	Char(5)	ASP 1	number for validation list library

Table 217. VP (Network Password Error) Journal Entries. QASYVPJE/J4/J5 Field Description File

	Offset					
JE	J4	<b>J</b> 5	Field	Format	Description	
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing.	
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.	

Table 218. VR (Network Resource Access) Journal Entries. QASYVRJE/J4/J5 Field Description File

	Offse	et			
JE	J4	J5	Field	Format	Description
1 156	1 224	1 610	Status	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. 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.
187 197	255 265	641 651	User Operation Type	Char(10) Char(1)	The name of the user requesting the resource.  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.

Table 219. VS (Server Session) Journal Entries. QASYVSJE/J4/J5 field Description File

Offset					
JE	J4	J5	Field	Format	Description
1 156	1 224	1 610	Session Action	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. The session action that occurred.
					E End session
157	225	611	Server Name	Char(10)	<b>S</b> Start session  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.

Table 219. VS (Server Session) Journal Entries (continued). QASYVSJE/J4/J5 field Description File

	Offs	et				
JE	J4	<b>J</b> 5	Field	Format	Descr	ription
179	247	633	Computer Name	Char(8)	The n	name of the computer requesting the session.
187	255	641	User	Char(10)	The n	name of the user requesting the session.
197	265	651	User Privilege	Char(1)	The p	privilege level of the user for session start:
					A	Administrator
					G	Guest
					U	User
198	266	652	Reason Code	Char(1)	The re	eason 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

Table 220. VU (Network Profile Change) Journal Entries. QASYVUJE/J4/J5 Field Description File

	Offs	et			
JE	J4	<b>J</b> 5	Field	Format	Description
1 156	1 224	1 610	Туре	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. The type of record that was changed.
					G Group record
					U User record
157	225	611	Server Name	Char(10)	<b>M</b> User profile global information  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.
197	265	651	Action	Char(1)	Action requested:
					A Addition
					C Change
					D Deletion
198	266	652	Resource Name	Char(260)	<b>P</b> Incorrect password Name of the resource.

Table 221. VV (Service Status Change) Journal Entries. QASYVVJE/J4/J5 Field Description File

	Offset				
JE	<b>J4</b>	J5	Field	Format	Description
1 156	1 224	1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing. The type of entry:
					C Service status changed
					E Server stopped
					P Server paused
					R Server restarted
157	225	611	Server Name	Char(10)	S Server started 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
173	241	627	Server Time	Zoned(6,0)	network server.  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.
187 197	255 265	641 651	User Status	Char(10) Char(1)	The name of the user requesting the change. 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
198 206 286 290	266 274 354 358	652 660 740 744	Service Code Text Set Return Value Service	Char(8) Char(80) Char(4) Char(20)	S Service stopped The code of the service requested. The text being set by the service request. The return value from the change operation. The service that was changed.

Table 222. X0 (Network Authentication) Journal Entries. QASYX0JE/J4/J5 Field Description File

	Offset				
JE	J4	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.

Table 222. X0 (Network Authentication) Journal Entries (continued). QASYX0JE/J4/J5 Field Description File

	Offset						
JE	J4	J5	 Field	Format	Desc	ription	
156	224	610	Entry Type	Char(1)	The t	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	
					В	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	
					0	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)		status of the request	
	233	619	GSS Status Value	Char(8)	GSS :	status value	
	241	627	Remote IP Address	Char(21)		ote IP address	
	262	648	Local IP Address	Char(21)	Local	l IP address	
	283	669	Encrypted Addresses	Char(256)	Encry	ypted IP addresses	

Table 222. X0 (Network Authentication) Journal Entries (continued). QASYX0JE/J4/J5 Field Description File

Offset		t			
JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description
	539	925	Encrypted	Char(1)	Encrypted IP addresses indicator
			Addresses Indicator		Y all addresses included
			21101200101		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	` '	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	Char(1)	Server principal (from ticket) indicator
			Indicator		Y server principal complete
					N server principal not complete
					X not provided
	603	989	Server Principal		Server principal (from ticket)
	1115	1501	Server Principal Parameter CCSID	Binary(5)	Server principal (from ticket) parameter CCSID
	1119	1505	Server Principal Parameter	Binary(4)	Server principal (from ticket) parameter length
	1121	1507	Length Server Principal	Char(1)	Server principal (from ticket) parameter indicator
	1121	1007	Parameter	Char(1)	Y server principal complete
			Indicator		• • •
					1 1 1
	1122	1508	Server Principal	Char(512)	X not provided Server principal parameter that ticket must match
	1634	2020	Parameter Client Principal CCSID	Binary(5)	Client principal (from authenticator) CCSID
	1638	2024	Client Principal Length	Binary(4)	Client principal (from authenticator) length
	1640	2026	Client Principal	Char(1)	Client principal (from authenticator) indicator
			Indicator		Y client principal complete
					N client principal not complete
					X not provided
	1641	2027	Client Principal	Char(512)	Client principal from authenticator

Table 222. X0 (Network Authentication) Journal Entries (continued). QASYX0JE/J4/J5 Field Description File

	Offset				
ΙE	<b>J4</b>	J5	Field	Format	Description
	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
			marcator		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	Char(1)	Server principal (from GSS credential) indicator
			Principal 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	Char(1)	GSS local principal name indicator
			Principal 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
	3714	4100	GSS Remote Principal Length	Binary(4)	GSS remote principal name length
	3716	4102	GSS Remote	Char(1)	GSS remote principal name indicator
			Principal Indicator		Y remote principal complete
			marcator		N remote principal not complete
					X not provided
	3717	4103	GSS Remote Principal	Char(512)	GSS remote principal

Table 223. X1 (Identity Token) Journal Entries. QASYX1JE/J4/J5 Field Description File

	Offse	et					
JE	J4	J5	— Field	Format	Description		
		1 610	Entry Type	Char(1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 for field listing. 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		
		611	Reason Code	Binary (5)	U Get user from identity token failed 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 bee validated up to the point of failure will be filled in th text fields.		
		615	Reserved	Char(7)	Reserved		
		622 626	Data CCSID Receiver length	Binary(5) Binary(5)	The CCSID of the data in the text fields 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	205	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.		

Table 223. X1 (Identity Token) Journal Entries (continued). QASYX1JE/J4/J5 Field Description File

	Offse	et			
JE	<b>J4</b>	J5	Field	Format	Description
		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: <pre> <sndrz><eimid>sndrz_eimID</eimid> <appid>sndrz_appID</appid> <timestamp>sndrz_timestamp </timestamp> </sndrz> <sndry></sndry></pre>
		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 may 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.
		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.

Table 224. YC (Change to DLO Object) Journal Entries. QASYYCJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.
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

Table 224. YC (Change to DLO Object) Journal Entries (continued). QASYYCJE/J4/J5 Field Description File

Offset					
JE	<b>J4</b>	J5	Field	Format	Description
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 <sup>1</sup>

Table 225. YR (Read of DLO Object) Journal Entries. QASYYRJE/J4/J5 Field Description File

Offstes		tes			
JE	<b>J4</b>	J5	Field	Format	Description
1	1	1	T . T	Cl. (1)	Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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	Char(12)	Name of the document library object
			Document		
			Name		
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 <sup>1</sup>
1	See Table	228 on pag	ge 616 for a list of th	e codes for acc	ess types.

Table 226. ZC (Change to Object) Journal Entries. QASYZCJE/J4/J5 Field Description File

Offset					
JE	J4	J5	Field	Format	Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507,Table 151 on page 509, and Table 152 on page 510 for field listing.

Table 226, ZC (Change to Object) Journal Entries (continued), QASYZCJE/J4/J5 Field Description File

Offset							
JE	J4	J5	Field	Format	Descrip	otion	
156	224	610	Entry Type	Char(1)	Object a	access	
					C	Change	e of an object
					U		le of open access to an object
157	225	611	Object Name	Char(10)		of the obj	
167 177	235 245	621 631	Library Name Object Type	Char(10) Char(8)	Type of		rary in which the object is located
185	253	639	Access Type	Packed(5,0)		access 1	
188	256	642	Access Specific	Char(50)	Specific	data abo	out the access
			Data				type is *IMGCLG, this field owing format:
					Char 3	Index rentry.	number of the image catalog
						Blank	Indicates the operation was against an image catalog.
					Char 32		
						Volume	e ID of the image catalog entry.
						Blank	Indicates the operation was against an image catalog.
					Char 1		type for the entry. The possible are listed below.
						Blank	Indicates the operation was against an image catalog.
						R	The file containing the image catalog entry is read-only.
						W	The file containing the image catalog entry is read/write capable.
					Char 1	The wr	ite protection for the entry.
						Blank	Indicates the operation was against an image catalog.
						Y	The file containing the image catalog entry is write protected.
						N	The file containing the image catalog entry is not write protected.
					Char 10	)	
						The na	me of the virtual device.
						Blank	Indicates the operation was against an image catalog or the image catalog is not in Ready status.
					Char 3	Not use	ed.
238			(Reserved Area)	Char(20)			

Table 226. ZC (Change to Object) Journal Entries (continued). QASYZCJE/J4/J5 Field Description File

	Offset						
JE	J4	<b>J</b> 5	Field	Format	Description		
	306	692	(Reserved Area)	Char(18)			
	324	710	Object Name Length <sup>2</sup>	Binary (4)	The length of the object name.		
258	326	712	Object Name CCSID <sup>2</sup>	Binary(5)	The coded character set identifier for the object name.		
262	330	716	Object Name Country or Region ID <sup>2</sup>	Char(2)	The Country or Region ID for the object name.		
264	332	718	Object Name Language ID <sup>2</sup>	Char(3)	The language ID for the object name.		
267	335	721	(Reserved area)	Char(3)			
270	338	724	Parent File ID <sup>2,</sup>	Char(16)	The file ID of the parent directory.		
286	354	740	Object File ID <sup>2,</sup> <sub>3</sub>	Char(16)	The file ID of the object.		
302	370	756	Object Name <sup>2</sup>	Char(512)	The name of the object.		
	882	1268	Object File ID	Char(16)	The file ID of the object.		
	898	1284	ASP Name <sup>6</sup>	Char(10)	The name of the ASP device.		
	908	1294	ASP Number <sup>6</sup>	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 absolute path name		
	919	1305	Path Name Language ID	Char(3)	The language ID for the absolute path name.		
	922	1308	Path Name Length	Binary(4)	The length of the absolute path name.		
	924	1310	Path Name	Char(1)	Path name indicator:		
			Indicator		Y Absolute 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.		
	925	1311	Relative Directory File ID <sup>4</sup>	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. <sup>3</sup>		
	941	1327	Path Name <sup>5</sup>	Char(5002)	The path name of the object.		
	941	1061	I atti ivallie	C11a1 (JUUL)	The paul name of the object.		

Table 226. ZC (Change to Object) Journal Entries (continued). QASYZCJE/J4/J5 Field Description File

	Offset J4 J5				
JE			Field	Format	Description
1	See Tabl	e 228 on pag	e 616 for a list of	the codes for acc	ess types.
2	These fi	elds are used	only for objects	in the QOpenSys,	"root" (/) file systems, and user-defined file systems.
3	An ID tl	nat has the le	eft-most bit set an	d the rest of the	bits zero indicates that the ID is NOT set.
4	If the Path Name Indicate error in determining the				Directory File ID is hex zeros, then there was some

This is a variable length field. The first 2 bytes contain the length of the path name.

Table 227. ZR (Read of Object) Journal Entries. QASYZRJE/J4/J5 Field Description File

Offset					
JE	JE J4 J5		Field Format		Description
1	1	1			Heading fields common to all entry types. See Table 150 on page 507, Table 151 on page 509, and Table 152 on page 510 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 <sup>1</sup>

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.

Table 227. ZR (Read of Object) Journal Entries (continued). QASYZRJE/J4/J5 Field Description File

	Offse	t					
JE	J4	J5	Field	Format	Descrip	Description	
188	256	642	Access Specific	Char(50)	Specific	data ab	out the access.
			Data				type is *IMGCLG, this field owing format:
					Char 3	Index r	number of the image catalog entry.
						Blank	Indicates the operation was against an image catalog.
					Char 32	2	
						Volume	e ID of the image catalog entry.
						Blank	Indicates the operation was against an image catalog.
					Char 1		type for the entry. The possible are listed below.
						Blank	Indicates the operation was against an image catalog.
						R	The file containing the image catalog entry is read-only.
						W	The file containing the image catalog entry is read/write capable.
					Char 1	<b>Char 1</b> The write protection for the entry.	
						Blank	Indicates the operation was against an image catalog.
						Y	The file containing the image catalog entry is write protected.
						N	The file containing the image catalog entry is not write protected.
					Char 10		
						The na	me of the virtual device.
						Blank	Indicates the operation was against an image catalog or the image catalog is not in Ready status.
238			(Reserved Area)	Char(20)	Char 3	Not us	ed.
	306	692	(Reserved Area)	Char(18)			
	324	710	Object Name Length <sup>2</sup>	Binary(4)	The len	gth of th	e object name.
258	326	712	Object Name CCSID <sup>2</sup>	Binary(5)	The cocname.	led chara	acter set identifier for the object
262	330	716	Object Name Country or Region ID <sup>2</sup>	Char(2)	The Co	untry or	Region ID for the object name.
264	332	718	Object Name Language ID <sup>2</sup>	Char(3)	The lan	guage II	) for the object name.
267	335	721	(Reserved area)	Char(3)			

Offset

Table 227. ZR (Read of Object) Journal Entries (continued). QASYZRJE/J4/J5 Field Description File

JE	<b>J4</b>	<b>J</b> 5	Field	Format	Description	
270	338	724	Parent File ID <sup>2,3</sup>	Char(16)	The file ID of the parent directory.	
286	354	740	Object File ID <sup>2,3</sup>	Char(16)	The file ID of the object.	
302	370	756	Object Name <sup>2</sup>	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 absolute path name	
	919	1305	Path Name Language ID	Char(3)	The language ID for the absolute path name.	
	922	1308	Path Name Length	Binary(4)	The length of the absolute path name.	
	924	1310	Path Name	Char(1)	Path name indicator:	
			Indicator		Y Absolute 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.	
	925	1311	Relative Directory File ID <sup>4</sup>	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. <sup>3</sup>	
	941	1327	Path Name <sup>5</sup>	Char(5002)	The path name of the object.	
1	See Table	228 for a li	st of the codes for a	ccess types.		
2	These fiel	lds are used	l only for objects in	the QOpenSys	, "root" (/) file systems, and user-defined file systems.	
3	An ID th	at has the le	eft-most bit set and	the rest of the	bits zero indicates that the ID is NOT set.	

An ID that has the left-most bit set and the rest of the bits zero indicates that the ID is NOT set.

Table 228 lists the access codes used for object auditing journal entries in files QASYYCJE/J4/J5, QASYYRJE/J4/J5, QASYZCJE/J4/J5, and QASYZRJE/J4/J5.

Table 228. 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

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.

This is a variable length field. The first 2 bytes contain the length of the path name.

Table 228. Numeric Codes for Access Types (continued)

Code	Access Type	Code	Access Type	Code	Access Type
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	Сору	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

This appendix describes the commands and menus for security tools. Examples of how to use the commands are included throughout this manual.

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**

The following 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 229 describes these menu options and the associated commands:

Table 229. Tool Commands for User Profiles

Menu <sup>1</sup> 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 <sup>2</sup>
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 <sup>2</sup>

Table 229. Tool Commands for User Profiles (continued)

Menu <sup>1</sup> Option	<b>Command Name</b>	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 <sup>2</sup>
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 <sup>2</sup>
5	DSPACTSCD	Use the Display Profile Activation Schedule command to display or print information about the schedule for enabling and disabling specific user profiles. You create the schedule with the CHGACTSCDE command.	QASECACT <sup>2</sup>
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 <sup>2</sup>
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 command to set up user profiles to expire.	QASECEXP <sup>2</sup>
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). The job looks at the QASECEXP file to determine whether any user profiles are set up to expire on that day.	QASECEXP <sup>2</sup>
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 230 describes the menu options and associated commands for security auditing:

Table 230. Tool Commands for Security Auditing

Menu <sup>1</sup> Option	<b>Command Name</b>	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 <sup>2</sup>

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 of this book.

### 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 . . . . . . . . . . . . . . . . .
                                    *.10RD
                                                  Name, *JOBD
Job description . . . . . . .
                                    *USRPRF
                                                  Name, *USRPRF
                                                  Name, *LIBL, *CURLIB
 Library . . . . . . . . . . .
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
                                    *CURRENT
                                                  Name, *CURRENT, *USRPRF...
Print device . . . . . . . . .
```

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:

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

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

### **Options on the Security Batch Menu**

Table 231 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 231. Commands for Security Reports

Menu <sup>1</sup> 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 <sup>2</sup>
2, 41	DSPAUDJRNE <sup>6</sup>	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 <sup>3</sup>

Table 231. Commands for Security Reports (continued)

Menu <sup>1</sup> Option	<b>Command Name</b>	Description	Database File Used
3, 42	PRTPVTAUT *AUTL	When you use the Print Private Authorities command for *AUTL objects, you receive a list of all the authorization lists on the system. The report includes the users who are authorized to each list and what authority the users have for the list. Use this information to help you analyze sources of object authority on your system.	QSECATLOLD <sup>2</sup>
		This report has three versions. The full report lists all authorization lists on the system. The changed report lists additions and changes to authorization since you last ran the report. The deleted report lists users whose authority to the authorization list has been deleted since you last ran the report.	
		When you print the full report, you have the option to print a list of objects that each authorization list secures. The system will create a separate report for each authorization list.	
6, 45	PRTCMNSEC	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.	QSECCMNOLD <sup>2</sup>
		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.	
15, 54	PRTJOBDAUT	Use the Print Job Description Authority command to print a list of job descriptions that specify a user profile and have public authority that is not *EXCLUDE. The report shows the special authorities for the user profile that is specified in the job description.	QSECJBDOLD <sup>2</sup>
		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.	

Table 231. Commands for Security Reports (continued)

Menu <sup>1</sup> Option	<b>Command Name</b>	Description	Database File Used
See note 4	PRTPUBAUT	Use the Print Publicly Authorized Objects command to print a list of objects whose public authority is not *EXCLUDE. When you run the command, you specify the type of object and the library or libraries for the report. Use the PRTPUBAUT command to print information about objects that every user on the system can access.  This report has two versions. The full report lists all objects that meet the selection criteria. The	QPBxxxxxx <sup>5</sup>
		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.	
See note 4.	PRTPVTAUT	Use the Print Private Authorities command to print a list of the private authorities to objects of the specified type in the specified library. Use this report to help you determine the sources of authority to objects.  This report has three versions. The full report	QPVxxxxxx <sup>5</sup>
		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.	
24, 63	PRTQAUT	Use the Print Queue Report to print the security settings for output queues and job queues on your system. These settings control who can view and change entries in the output queue or job queue.	QSECQOLD <sup>2</sup>
		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.	

Table 231. Commands for Security Reports (continued)

Menu <sup>1</sup> Option	<b>Command Name</b>	Description	Database File Used
25, 64	PRTSBSDAUT	Use the Print Subsystem Description command to print the security-relevant communications entries for subsystem descriptions on your system. These settings control how work can enter your system and how jobs run. The report prints a subsystem description only if it has communications entries that specify a user profile name.	QSECSBDOLD <sup>2</sup>
		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.	
26, 65	PRTSYSSECA	Use the Print System Security Attributes command to print a list of security-relevant system values and network attributes. The report shows the current value and the recommended value.	
27, 66	PRTTRGPGM	Use the Print Trigger Programs command to print a list of trigger programs that are associated with database files on your system.  This report has two versions. The full report lists every trigger program that is assigned and meets your selection criteria. The changed report lists trigger programs that have been assigned since the last time that you ran the report.	QSECTRGOLD <sup>2</sup>
28, 67	PRTUSROBJ	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.  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.	QSECPUOLD <sup>2</sup>
29, 68	PRTUSRPRF	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.	
30, 69	PRTPRFINT	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.	

Table 231. Commands for Security Reports (continued)

Menu <sup>1</sup> Option	<b>Command Name</b>	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.	

- Options are from the SECBATCH menu.
- <sup>2</sup> This file is in the QUSRSYS library.
- 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 of this book.
- 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.
- 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.
- The DSPAUDJRNE command is obsolete. The 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**

You can use the Security Wizard to customize system security. For more information, see the topic "Complete the Security Wizard" in the iSeries Information Center.

Table 232 describes the commands that you can use to customize the security on your system. These commands are on the SECTOOLS menu.

Table 232. Commands for Customizing Your System

Menu <sup>1</sup> Option	<b>Command Name</b>	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 628 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 630 lists the actions that the RVKPUBAUT command performs.	
Options are from the SECTOOLS menu.			

# Values That Are Set by the Configure System Security Command

Table 233 lists the system values that are set when you run the CFGSYSSEC command. The CFGSYSSEC command runs a program that is called QSYS/QSECCFGS.

Table 233. 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)	Minimum length for passwords
QPWDMAXLEN	8 (See note 4)	Maximum length for passwords
QPWDPOSDIF	1 (Yes)	Whether every position in a new password must differ from the same position in the last password
QPWDLMTCHR	See note 2	Characters that are not allowed in passwords
QPWDLMTAJC	1 (Yes)	Whether adjacent numbers are prohibited in passwords
QPWDLMTREP	2 (Cannot be repeated consecutively)	Whether repeating characters in are prohibited in passwords
QPWDRQDDGT	1 (Yes)	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
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

# System Value Name Setting System Value Description

#### **Notes:**

- 1. If you are currently running with a QSECURITY value of 30 or lower, be sure to review the information in Chapter 2 of this book 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.

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

**QSYSOPR** 

**QPGMR** 

**QUSER** 

**QSRV** 

**QSRVBAS** 

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

## **Changing the Program**

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

- \_\_ Step 1. Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the CFGSYSSEC command. The program to retrieve is QSYS/QSECCFGS. When you retrieve it, give it a *different name*.
- \_\_ Step 2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you *do not* replace the IBM-supplied QSYS/QSECCFGS program. Your program should have a different name.
- \_\_ Step 3. Use the Change Command (CHGCMD) command to change the program to process command (PGM) parameter for the CFGSYSSEC command. Set the PGM value to the name of your program. For example, if you create a program in the QGPL library that is called MYSECCFG, you would type the following 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 CFGSYSSEC 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 234 and the application programming interfaces (APIs) that are listed in Table 235. When your system arrives, these commands and APIs have their public authority set to \*USE.

The commands that are listed in Table 234 and the APIs that are listed in Table 235 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 234. 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 235 are all in the QSYS library:

Table 235. Programs Whose Public Authority Is Set by the RVKPUBAUT Command



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

- Step 1. Use the Retrieve CL Source (RTVCLSRC) command to copy the source for the program that runs when you use the RVKPUBAUT command. The program to retrieve is QSYS/QSECRVKP. When you retrieve it, give it a different name.
- Step 2. Edit the program to make your changes. Then compile it. When you compile it, make sure that you do not replace the IBM-supplied QSYS/QSECRVKP program. Your program should have a different name.

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

Listed here are the product manuals and IBM Redbooks $^{\text{\tiny TM}}$  (in PDF format), Web sites, and information center topics that relate to the security reference topic. You can view or print any of the PDFs.

## **Advanced Security**

- *Tips and Tools for Securing Your iSeries*, SC41-5300-07, 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. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- Implementing iSeries 400 Security, 3rd Edition by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communication International, 1998. Provides guidance and practical suggestions for planning, setting up, and managing your iSeries security.

#### **ISBN Order Number**

1-882419-78-2

## **Backup and Recovery**

- *Backup and Recovery*, SC41-5304-08, 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. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- Additional backup and recovery information can be found in the information center. See "Prerequisite and Related Information" on page xvi for more information.

# **Basic Security Information and Physical Security**

• The Basic System Security and Planning topic in the Information Center explains why security is necessary, defines major concepts, and provides information about planning, implementing, and monitoring basic security on the system. See "Prerequisite and Related Information" on page xvi for details.

# iSeries Access for Windows Licensed Program

• The iSeries Access for Windows topic in the Information Center provides technical information about the iSeries Access for Windows programs for all versions of iSeries Access for Windows. See "Prerequisite and Related Information" on page xvi for details.

# **Communications and Networking**

- SNA Distribution Services, SC41-5410-01, 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.
- *Remote Work Station Support*, SC41-5402-00, 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. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- The Information Center provides information about remote file processing. It describes how to define a remote file to i5/OS distributed data management (DDM), how to create a DDM file, what file utilities

- are supported through DDM, and the requirements of i5/OS DDM as related to other systems. See "Prerequisite and Related Information" on page xvi for details.
- The Information Center provides information that describes how to use and configure TCP/IP and the several TCP/IP applications, such as FTP, SMTP, and TELNET. See "Prerequisite and Related Information" on page xvi for details.

## Cryptography

• Cryptographic Support/400, SC41-3342-00, describes the data security capabilities of the Cryptographic Facility licensed program product. It explains how to use the facility and provides reference information for programmers. See the iSeries: Information Center Supplemental Manuals CD-ROM.

## **General System Operations**

• "Basic system operations" in the Information Center provides information about how to start and stop the system and work with system problems. See "Prerequisite and Related Information" on page xvi for more details.

## **IBM-Supplied Program Installation and System Configuration**

- Local Device Configuration, SC41-5121-00, provides information about how to do an initial configuration and how to change that configuration. It also contains conceptual information about device configuration. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- Install, upgrade, or delete i5/OS and related software, SC41-5120-09, provides step-by-step procedures for initial install, installing licensed programs, program temporary fixes (PTFs), and secondary languages from IBM. See the iSeries: Information Center Supplemental Manuals CD-ROM.

## Integrated File System

• The topic "Integrated File System" in the iSeries Information Center provides an overview of the integrated file system, including what it is, how it can be used, and what interfaces are available. See "Prerequisite and Related Information" on page xvi for details.

#### The Internet

- AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet SG24-4929 discusses the security issues and the risk associated with connecting your iSeries to the Internet. It provides examples, recommendations, tips, and techniques for applications.
- iSeries and the Internet, G325-6321, 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

Cool Title About the AS/400 and Internet, SG24-4815, can help you understand and then use the Internet (or your own intranet) from your iSeries. 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.

#### **IBM Lotus Domino**

The URL, http://www.lotus.com/ldd/doc, provides information about Lotus Notes, Domino, and IBM Domino for iSeries. 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.

## **Optical Support**

Optical Support, SC41-5310-04, 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. See the iSeries:
Information Center Supplemental Manuals CD-ROM.

## **Printing**

• The information center provides information about printing elements and concepts of the system, printer file and print spooling support for printing operation, and printer connectivity. See "Prerequisite and Related Information" on page xvi for details.

## **Programming**

- *CL Programming*, SC41-5721-06, 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. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- The CL topic in the information center (see "Prerequisite and Related Information" on page xvi for details) provides a description of all the iSeries control language (CL) and its i5/OS commands. The i5/OS commands are used to request functions of the i5/OS (5722-SS1) licensed program. All the non-i5/OS 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.
- The Programming topic in the Information Center provides information about many of the languages and utilities available on the iSeries. It contains summaries of:
  - All iSeries CL commands (in i5/OS 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).
- The information center contains several topics regarding Systems Management and Work Management on the iSeries. Some of these topics include performance data collection, system values management, and storage management. For details on accessing the information center, see "Prerequisite and Related Information" on page xvi.
- The work management topic in the information center provides information about how to create and change a work management.
- The API topic in the Information Center (see "Prerequisite and Related Information" on page xvi for details) provides information about how to create, use, and delete objects that help manage system performance, use spooling efficiently, and maintain database files efficiently. This topic also includes information about creating and maintaining the programs for system objects and retrieving i5/OS information by working with objects, database files, jobs, and spooling.

#### **Utilities**

- ADTS for AS/400: Source Entry Utility, SC09-2605-00, 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. See the iSeries: Information Center Supplemental Manuals CD-ROM.
- The DB2 Universal Database for iSeries topic in the information center provides an overview of how to design, write, run, and test the statements of DB2 UDB for iSeries Query Manger and SQL Development Kit. 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. See "Prerequisite and Related Information" on page xvi for details.
- The DB2 Universal Database for iSeries topic in the information center 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

See "Prerequisite and Related Information" on page xvi for details.

# **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:

IBM World Trade Asia Corporation Licensing 2-31 Roppongi 3-chome, Minato-ku Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

**IBM Corporation** 

Software Interoperability Coordinator, Department YBWA 3605 Highway 52 N Rochester, MN 55901 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

#### **COPYRIGHT LICENSE:**

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

# **Programming Interface Information**

This iSeries Security Reference publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of i5/OS.

#### **Trademarks**

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX

AS/400

COBOL/400

DB2

DB2 Universal Database

Domino

DRDA

e(logo)server

eServer

i5/OS

IBM

**iSeries** 

Lotus

**MQSeries** 

NetServer

**Notes** 

OfficeVision

OS/2

**Print Services Facility** 

PrintManager

Redbooks

RPG/400

SAA

SecureWay

System/36

System/38

SystemView

WebSphere

zSeries

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 trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or 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 112 (\*Ref) Reference authority 112 (Display Link) command object authority required 354 (Move) command

object authority required 358 (user identification number) parameter user profile 90

\*ADD (add) authority 112, 302

\*ADOPTED (adopted) authority 135

\*ADVANCED (advanced) assistance level 64

\*ALL (all) authority 113, 302

\*ALLOBJ

user class authority 8

\*ALLOBJ (all object) special authority added by system

changing security levels 10 auditing 233

failed sign-on 177 functions allowed 68 removed by system

changing security levels 10 restoring profile 224 risks 68

\*ALRTBL (alert table) object auditing 452

\*ASSIST Attention-key-handling program 86

\*AUDIT (audit) special authority functions allowed 71 risks 71

\*AUTFAIL (authority failure) audit level 242

\*AUTHLR (authority holder) object auditing 453

\*AUTL (authorization list) object auditing 453

\*AUTLMGT (authorization list management) authority 112, 302

\*BASIC (basic) assistance level 64 \*BNDDIR (binding directory) object

auditing 453 \*BREAK (break) delivery mode See also message queue

user profile 84 \*CFGL (configuration list) object auditing 454

\*CHANGE (change) authority 113, 302

\*CHRSF (Special Files) object auditing 454

\*CHTFMT (chart format) object auditing 454

\*CLD (C locale description) object auditing 455

\*CLKWD (CL keyword) user option 88,

\*CLS (Class) object auditing 456

\*CMD (command string) audit level 243

\*CMD (Command) object auditing 456

\*CNNL (connection list) object auditing 457

\*COSD (class-of-service description) object auditing 457

\*CREATE (create) audit level 243 \*CRQD

restoring

audit journal (QAUDJRN) entry 246

\*CRQD (change request description) object auditing 455

CRQD change (CQ) file layout 527

\*CSI (communications side information) object auditing 458

\*CSPMAP (cross system product map) object auditing 458

\*CSPTBL (cross system product table) object auditing 458

\*CTLD (controller description) object auditing 459

\*DELETE (delete) audit level 243

\*DEVD (device description) object auditing 459

\*DFT (default) delivery mode See also message queue user profile 84

\*DIR (directory) object auditing 460

\*DISABLED (disabled) user profile status description 62

QSECOFR (security officer) user profile 62

\*DLT (delete) authority 112, 302 \*DOC (document) object auditing 464

\*DTAARA (data area) object auditing 467

\*DTADCT (data dictionary) object auditing 468

\*DTAQ (data queue) object auditing 468

\*EDTD (edit description) object auditing 469

\*ENABLED (enabled) user profile status 62

\*EXCLUDE (exclude) authority 113

\*EXECUTE (execute) authority 112, 302

\*EXITRG (exit registration) object auditing 469

\*EXPERT (expert) user option 88, 89, 90,

\*FCT (forms control table) object auditing 470

\*FILE (file) object auditing 470

\*FNTRSC (font resource) object auditing 473

\*FORMDF (form definition) object auditing 473

\*FTR (filter) object auditing 474 \*GROUP (group) authority 135

\*GSS (graphic symbols set) object auditing 475

\*HLPFULL (full-screen help) user option 90

\*HOLD (hold) delivery mode See also message queue user profile 84

\*IGCDCT (double-byte character set dictionary) object auditing 475

\*IGCSRT (double-byte character set sort) object auditing 475

\*IGCTBL (double-byte character set table) object auditing 475

\*INTERMED (intermediate) assistance

\*IOSYSCFG (system configuration) special authority functions allowed 71

risks 72 \*JOBCTL (job control) special authority functions allowed 69 output queue parameters 187 priority limit (PTYLMT) 78

risks 69 \*JOBD (job description) object auditing 476

\*JOBDTA (job change) audit level 243

\*JOBQ (job queue) object auditing 476 \*JOBSCD (job scheduler) object

auditing 477

\*JRN (journal) object auditing 477 \*JRNRCV (journal receiver) object auditing 479

\*LIB (library) object auditing 479 \*LIND (line description) object auditing 480

\*MENU (menu) object auditing 481

\*Mgt (Management) authority 112 \*MODD (mode description) object

auditing 482

\*MODULE (module) object auditing 482

\*MSGF (message file) object auditing 482

\*MSGQ (message queue) object auditing 483

\*NODGRP (node group) object auditing 484

\*NODL (node list) object auditing 484

\*NOSTSMSG (no status message) user option 90

\*NOTIFY (notify) delivery mode See also message queue user profile 84

\*NTBD (NetBIOS description) object auditing 485

\*NWID (network interface) object auditing 485

\*NWSD (network server description) object auditing 486

\*OBJALTER (object alter) authority 112,

\*OBJEXIST (object existence) authority 112, 301

\*OBJMGT (object management) audit level 245

*OBJMGT (object management)	*SECADM (security administrator)	access (continued)
authority 112, 301	special authority 69	restricting
*OBJOPR (object operational)	functions allowed 69	console 232
authority 112, 301	*SECURITY (security) audit level 249	workstations 232
*OBJREF (object reference)	*SERVICE (service tools) audit level 252	access code
authority 112, 302	*SERVICE (service) special authority	object authority required for
*OFCSRV (office services) audit	failed sign-on 177	commands 402
level 245, 463, 481	functions allowed 70	access command (Determine File
*OUTQ (output queue) object	risks 70	Accessibility)
auditing 486	*SIGNOFF initial menu 66	object auditing 460
*OVL (overlay) object auditing 487	*SOCKET (local socket) object	access control list
*PAGDFN (page definition) object	auditing 495	changing
auditing 487	*SPADCT (spelling aid dictionary) object	audit journal (QAUDJRN)
*PAGSEG (page segment) object	auditing 497	entry 251
auditing 488	*SPLCTL (spool control) special authority	access control list change (VA) journal
*PARTIAL (partial) limit capabilities 67	functions allowed 69	entry type 251
*PDG (print descriptor group) object	output queue parameters 187	access path recovery
auditing 488	risks 70	action auditing 452
*PGM (program) object 488	*SPLFDTA (spooled file changes) audit	object authority required for
*PGMADP (adopted authority) audit	level 252, 497	commands 312
level 245	*SQLPKG (SQL package) object	accessx command (Determine File
*PGMFAIL (program failure) audit	auditing 498	Accessibility)
level 246	*SRVPGM (service program) object	object auditing 460
*PNLGRP (panel group) object	auditing 499	account limit
auditing 489	*SSND (session description) object	exceeded
*PRDAVL (product availability) object	auditing 499	audit journal (QAUDJRN)
auditing 490	*STMF (stream file) object auditing 499	entry 252
*PRDDFN (product definition) object	*STSMSG (status message) user	account limit exceeded (VL) file
auditing 490	option 90	layout 599
*PRDLOD (product load) object	*SVRSTG (server storage space)	account limit exceeded (VL) journal entry
auditing 490	object 499	type 252
*PRTDTA (printer output) audit	*SYNLNK (symbolic link) object	accounting code (ACGCDE) parameter
level 246	auditing 502	changing 82
*PRTMSG (printing message) user	*SYSMGT (systems management) audit	user profile 82
option 90	level 252	Accumulating Special Authorities 215
*QMFORM (query manager form) object	*SYSTEM (system) domain 12	ACGCDE (accounting code) parameter
auditing 490	*SYSTEM (system) state 13	changing 82
*QMQRY (query manager query) object	*TBL (table) object auditing 503	user profile 82
auditing 491	*TYPEAHEAD (type-ahead) keyboard	action auditing
*QRYDFN (query definition) object	buffering 76	access path recovery 452
auditing 491	*UPD (update) authority 112, 302	definition 236
*R (read) 113, 303	*USE (use) authority 113, 302	Directory Server 463
*RCT (reference code table) object	*USER (user) domain 12	mail services 481
auditing 492	*USER (user) state 13	office services 481
*READ (read) authority 112, 302	*USRIDX (user index) object 16	
*Ref (Reference) authority 112	*USRIDX (user index) object	planning 236 reply list 493
*ROLLKEY (roll key) user option 90	auditing 504	spooled files 497
*RW (read, write) 113, 303	9	
	*USRPRF (user profile) object	action auditing (AUDLVL) parameter
*RWX (read, write, execute) 113, 303	auditing 504	user profile 94
*RX (read, execute) 113, 303	*USRQ (user queue) object 16	action to spooled file (SF) file layout 587
*S36 (S/36 machine description) object	*USRQ (user queue) object auditing 505	action to system value (SV) file
auditing 503	*USRSPC (user space) object 16	layout 597
*S36 (System/36) special	*USRSPC (user space) object	action when sign-on attempts reached
environment 72	auditing 505	(QMAXSGNACN) system value
*SAVRST (save/restore) audit level 246	*VLDL (validation list) object	description 26
*SAVSYS (save system) special authority	auditing 506	value set by CFGSYSSEC
*OBJEXIST authority 112, 302	*W (write) 113, 303	command 628
description 230	*WX (write, execute) 113, 303	activating
functions allowed 70	*X (execute) 113, 303	security auditing function 258
removed by system		user profile 619
changing security levels 10	_	active profile list
risks 70	A	changing 619
*SBSD (subsystem description) object		AD (auditing change) file layout 512
auditing 493	access	AD (auditing change) journal entry
*SCHIDX (search index) object	preventing	type 249
auditing 494	unauthorized 235	add (*ADD) authority 112, 302
S	unsupported interface 12	· · · · · · · · · · · · · · · · · · ·

Add Authorization List Entry ADDCMNE (Add Communications ADDENVVAR (Add Environment (ADDAUTLE) command 146, 273 Entry) command Variable) command Add Directory Entry (ADDDIRE) object auditing 493 object authority required 338 command 278 object authority required 434 ADDEWCBCDE (Add Extended Wireless Add Document Library Object Authority ADDCNNLE (Add Connection List Controller Bar Code Entry) command (ADDDLOAUT) command 277 Entry) command object authority required 338 Add Job Schedule Entry (ADDJOBSCDE) ADDEWCM (Add Extended Wireless object auditing 457 command ADDCOMSNMP (Add Community for Controller Member) command SECBATCH menu 623 object authority required 338 SNMP) command Add Library List Entry (ADDLIBLE) object authority required 441 ADDEWCPTCE (Add Extended Wireless command 183, 185 ADDCRGDEVE command Controller PTC Entry) command authorized IBM-supplied user Add User display object authority required 338 profiles 289 sample 98 ADDEWLM (Add Extended Wireless ADDACC (Add Access Code) command object authority required 319 Line Member) command object auditing 467 ADDCRGNODE command object authority required 338 object authority required 402 authorized IBM-supplied user ADDEXITPGM (Add Exit Program) ADDAJE (Add Autostart Job Entry) profiles 289 command authorized IBM-supplied user command object authority required 319 object auditing 493 ADDCRSDMNK (Add Cross Domain profiles 289 object authority required 434 Key) command object auditing 469 ADDALRACNE (Add Alert Action Entry) object authority required 421 authorized IBM-supplied user ADDFCTE (Add Forms Control Table command profiles 289 object auditing 474 object authority required 326 Entry) command object authority required 346 ADDDEVDMNE command object authority required 422 ADDALRD (Add Alert Description) ADDFNTTBLE (Add DBCS Font Table authorized IBM-supplied user command profiles 289 Entry) object auditing 452 object authority required 319 object authority required for object authority required 314 ADDDIRE (Add Directory Entry) commands 312 ADDALRSLTE (Add Alert Selection command ADDICFDEVE (Add Intersystem Entry) command description 278 **Communications Function Program** object auditing 474 object authority required 331 Device Entry) command object authority required 346 ADDDIRSHD (Add Directory Shadow object auditing 471 ADDAUTLE (Add Authorization List System) command object authority required 339 object authority required 331 ADDIMGCLGE command Entry) command ADDDLOAUT (Add Document Library authorized IBM-supplied user description 273 object auditing 453 Object Authority) command profiles 289 object authority required 316 description 277 object authority required 348 using 146 object auditing 465 adding object authority required 333 ADDBKP (Add Breakpoint) command authorization list object authority required 415 ADDDSPDEVE (Add Display Device entries 146, 273 ADDBNDDIRE (Add Binding Directory Entry) command objects 147 Entry) command object auditing 471 users 146, 273 object auditing 454 ADDDSTLE (Add Distribution List Entry) directory entry 278 document library object (DLO) object authority required 317 command ADDBSCDEVE (Add BSC Device Entry) object authority required 333 authority 277 ADDDSTQ (Add Distribution Queue) library list entry 183, 185 command object auditing 471 command server authentication entry 278 ADDCFGLE (Add Configuration List authorized IBM-supplied user user authority 140 Entries) command user profiles 98 profiles 289 object auditing 454 object authority required 332 ADDIPSIFC (Add IP over SNA Interface) object authority required 324 ADDDSTRTE (Add Distribution Route) command ADDCLUNODE (Add ) command command object authority required 314 authorized IBM-supplied user authorized IBM-supplied user ADDIPSLOC (Add IP over SNA Location profiles 289 profiles 289 Entry) command ADDCLUNODE command object authority required 332 object authority required 314 ADDDSTSYSN (Add Distribution ADDIPSRTE (Add IP over SNA Route) object authority required 318 ADDCMDCRQA (Add Command Secondary System Name) command command Change Request Activity) command authorized IBM-supplied user object authority required 314 authorized IBM-supplied user ADDJOBQE (Add Job Queue Entry) profiles 289 profiles 289 object authority required 332 command object auditing 455 ADDDTADFN (Add Data Definition) object auditing 476, 493 object authority required 317 object authority required 434 command ADDCMNDEVE (Add Communications ADDJOBSCDE (Add Job Schedule Entry) object authority required 367 Device Entry) command ADDEMLCFGE (Add Emulation command object auditing 477 object auditing 471 Configuration Entry) command object authority required 373 object authority required 330 SECBATCH menu 623

ADDLANADPI (Add LAN Adapter ADDPEXDFN () command ADDRMTSVR (Add Remote Server) authorized IBM-supplied user Information) command profiles 289 object authority required 391 object authority required 401 ADDPEXDFN (Add Performance ADDRPYLE (Add Reply List Entry) ADDLFM (Add Logical File Member) command Explorer Definition) command command object auditing 471 object authority required 408 authorized IBM-supplied user object authority required 339 ADDPEXFTR () command profiles 290 ADDLIBLE (Add Library List Entry) authorized IBM-supplied user object auditing 493 command 183, 185 profiles 289 object authority required 436 object authority required 384 ADDPFCST (Add Physical File ADDRSCCRQA (Add Resource Change ADDLICKEY (Add License Key) Constraint) command Request Activity) command authorized IBM-supplied user command object auditing 471 profiles 290 object authority required 388 ADDPFM (Add Physical File Member) ADDLNK (Add Link) command command object auditing 455 object authority required 317 object auditing 495, 500 object auditing 471 object authority required 339 object authority required 349 ADDRTGE (Add Routing Entry) ADDMFS (Add Mounted File System) ADDPFTRG (Add Physical File Trigger) command command command object auditing 493 authorized IBM-supplied user object auditing 471 object authority required 435 profiles 289 object authority required 339 ADDSCHIDXE (Add Search Index Entry) object authority required 442 ADDPFVLM (Add Physical File command ADDMFS (Add Mounted File System) Variable-Length Member) command object auditing 490, 494 command) command object auditing 471 object authority required 368 object authority required 398 ADDPGM (Add Program) command ADDSOCE (Add Sphere of Control ADDMSGD (Add Message Description) object authority required 415 Entry) command object authority required 432 command ADDPJE (Add Prestart Job Entry) object auditing 483 ADDSRVTBLE (Add Service Table Entry) command object authority required 394 object auditing 493 command ADDNETJOBE (Add Network Job Entry) object authority required 434 object authority required 441 ADDPRBACNE (Add Problem Action ADDSVRAUTE (Add Server command authorized IBM-supplied user Entry) command Authentication Entry) command profiles 289 object auditing 474 object authority required 427 object authority required 398 object authority required 346, 414 ADDTAPCTG (Add Tape Cartridge) ADDPRBSLTE (Add Problem Selection ADDNETTBLE (Add Network Table command object authority required 391 Entry) command Entry) command ADDTCPHTE (Add TCP/IP Host Table object authority required 441 object auditing 474 ADDNODLE (Add Node List Entry) object authority required 346, 414 Entry) command command ADDPRDCRQA (Add Product Change object authority required 441 Request Activity) command ADDTCPIFC (Add TCP/IP Interface) object auditing 484 object authority required 402 authorized IBM-supplied user command ADDNWSSTGL (Add Network Server profiles 289 object authority required 441 Storage Link) command object auditing 455 ADDTCPPORT (Add TCP/IP Port Entry) object authority required 400 object authority required 317 command ADDOBJCRQA (Add Object Change ADDPRDLICI (Add Product License object authority required 441 ADDTCPRSI (Add TCP/IP Remote Request Activity) command Information) command authorized IBM-supplied user object auditing 490 System Information) command ADDPTFCRQA (Add PTF Change profiles 289 object authority required 441 object auditing 455 Request Activity) command ADDTCPRTE (Add TCP/IP Route) object authority required 317 authorized IBM-supplied user command ADDOFCENR (Add Office Enrollment) profiles 289 object authority required 441 object auditing 455 ADDTRC (Add Trace) command command object authority required 317 object authority required 415 object auditing 465 ADDRDBDIRE (Add Relational Database ADDOPTCTG (Add Optical Cartridge) **ADDTRCFTR** Directory Entry) command authorized IBM-supplied user command authorized IBM-supplied user object authority required 421 profiles 290 ADDRJECMNE (Add RJE profiles 289 ADDWSE (Add Workstation Entry) object authority required 404 Communications Entry) command command ADDOPTSVR (Add Optical Server) object authority required 422 object auditing 493 ADDRJERDRE (Add RJE Reader Entry) object authority required 435 command authorized IBM-supplied user command adopted object authority required 422 profiles 289 authority ADDRJEWTRE (Add RJE Writer Entry) object authority required 404 displaying 135 adopted (\*ADOPTED) authority 135 ADDPCST (Add Physical File Constraint) command command object authority required 423 adopted authority ADDRMTJRN (Add Remote Journal) \*PGMADP (program adopt) audit object authority required 339 level 245 command object auditing 478

adopted authority (continued)	AFDFTUSR (QAFDFTUSR) user	ALWLMTUSR (allow limited user)
AP (adopted authority) file	profile 283	parameter (continued)
layout 519	AFOWN (QAFOWN) user profile 283	limit capabilities 67
AP (adopted authority) journal entry	AFP (Advanced Function Printing)	ALWOBJDIF (allow object difference)
type 245	object authority required for	parameter 225
application design 204, 206, 207	commands 312	Analyze Default Passwords
Attention (ATTN) key 129	AFUSR (QAFUSR) user profile 283	(ANZDFTPWD) command
audit journal (QAUDJRN) entry 245, 519	ALCOBJ (Allocate Object) command	description 619
auditing 234	object auditing 451 object authority required 305	Analyze Profile Activity (ANZPRFACT) command
authority checking example 167, 169	alert	creating exempt users 619
bound programs 130	object authority required for	description 619
break-message-handling	commands 314	analyzing
program 129	alert description	audit journal entries, methods 262
changing	object authority required for	object authority 269
audit journal (QAUDJRN)	commands 314	program failure 270
entry 250	alert table	user profile
authority required 130	object authority required for	by special authorities 623
job 130	commands 314	by user class 623
creating program 130	alert table (*ALRTBL) object	user profiles 268
debug functions 129	auditing 452	ANSLIN (Answer Line) command
definition 128	all (*ALL) authority 113, 302	object auditing 480
displaying	all object (*ALLOBJ) special authority	ANSQST (Answer Questions) command
command description 277	added by system	authorized IBM-supplied user
critical files 210	changing security levels 10	profiles 290
programs that adopt a profile 130	auditing 233	object authority required 420
USRPRF parameter 130	failed sign-on 177	ANZBESTMDL
example 204, 206, 207	functions allowed 68	authorized IBM-supplied user
flowchart 160	removed by system	profiles 290
group authority 128	changing security levels 10	ANZBESTMDL (Analyze BEST/1 Model)
ignoring 131, 206	restoring profile 224	command
job initiation 176	risks 68	object authority required 408
library security 115	all-numeric password 60	ANZDBF
object ownership 130	allow limited user (ALWLMTUSR)	authorized IBM-supplied user
printing list of objects 623	parameter Change Command (CLICCMD)	profiles 290
purpose 128 recommendations 131	Change Command (CHGCMD) command 67	ANZDBF (Analyze Database File) command
restoring programs	Create Command (CRTCMD)	object authority required 408
changes to ownership and	command 67	ANZDBFKEY
authority 227	limit capabilities 67	authorized IBM-supplied user
risks 131	allow object difference (ALWOBJDIF)	profiles 290
service programs 130	parameter 225	ANZDBFKEY (Analyze Database File
special authority 128	allow object restore (QALWOBJRST)	Keys) command
system request function 129	system value	object authority required 409
transferring to group job 129	value set by CFGSYSSEC	ANZDFTPWD (Analyze Default
adopting owner's authority	command 628	Password) command
See adopted authority	allow object restore option	object authority required 443
ADSM (QADSM) user profile 283	(QALWOBJRST) system value 37	ANZDFTPWD (Analyze Default
advanced (*ADVANCED) assistance	allow remote sign-on (QRMTSIGN)	Passwords) command
level 58, 64	system value	authorized IBM-supplied user
advanced function printing (AFP)	value set by CFGSYSSEC	profiles 290
object authority required for	command 628	description 619
commands 312	allow user objects (QALWUSRDMN)	ANZJVM
advantages	system value 16, 21	authorized IBM-supplied user
authorization list 213	allowed function	profiles 290
AF (authority failure) file layout 514	limit capabilities (LMTCPB) 67	ANZJVM command
AF (authority failure) journal entry type default sign-on violation 13	allowing users to change passwords 233	object authority required 369
description 242, 246	users to change passwords 233 alter service function	ANZPFRDT2 (Analyze Performance Data) command
hardware protection violation 14	*SERVICE (service) special	object authority required 409
job description violation 13	authority 70	ANZPFRDTA
program validation 14, 15	ALWLMTUSR (allow limited user)	authorized IBM-supplied user
restricted instruction 15	parameter	profiles 290
unsupported interface 13, 15	Change Command (CHGCMD)	ANZPFRDTA (Analyze Performance
AF_INET sockets over SNA	command 67	Data) command
object authority required for	Create Command (CRTCMD)	object authority required 409
commands 313	command 67	• •

ANZPGM (Analyze Program) command	APYRMTPTF (Apply Remote Program	audit (QAUDJRN) journal (continued)
object auditing 489	Temporary Fix) command	CA (authority change) entry type 249
object authority required 409	authorized IBM-supplied user	CA (authority change) file layout 520
ANZPRB (Analyze Problem) command	profiles 290	CD (command string) entry type 243
authorized IBM-supplied user	ASKQST (Ask Question) command	CD (command string) file layout 523
profiles 290	object authority required 420	changing receiver 261
object authority required 414	assistance level	CO (create object) entry type 123,
ANZPRFACT	advanced 58, 64	243
authorized IBM-supplied user	basic 58, 64	CO (create object) file layout 524
profiles 290	definition 58	CP (user profile change) entry
ANZPRFACT (Analyze Profile Activity)	example of changing 64	type 247
command	intermediate 58, 64	CP (user profile change) file
creating exempt users 619	stored with user profile 64	layout 525
description 619	user profile 63	CQ (*CRQD change) file layout 527
object authority required 443	ASTLVL (assistance level) parameter	CQ (change *CRQD object) entry
ANZQRY (Analyze Query) command	See also assistance level	type 247
object auditing 492	user profile 63	creating 258
object authority required 418	ATNPGM (Attention-key-handling	CU(Cluster Operations file
ANZS34OCL (Analyze System/34 OCL)	program) parameter	layout 528
command	See also Attention-key-handling	CV(connection verification) file
authorized IBM-supplied user	program	layout 529
profiles 290	user profile 86	CY(cryptographic configuration) file
	Attention (ATTN) key	
object authority required 396	· ·	layout 531
ANZS34OCL (Analyze System/36 OCL)	adopted authority 129	damaged 260
command	Attention (ATTN) key buffering 76	detaching receiver 260, 261
object authority required 396	Attention-key-handling program	DI(Directory Server) file layout 532
ANZS36OCL (Analyze System/36 OCL)	*ASSIST 86	displaying entries 235, 262
command	changing 86	DO (delete operation) entry type 243
authorized IBM-supplied user	initial program 86	DO (delete operation) file layout 536
profiles 290	job initiation 176	DS (DST password reset) entry
AP (adopted authority) file layout 519	QATNPGM system value 86	type 247
AP (adopted authority) journal entry	QCMD command processor 86	DS (IBM-Supplied Service Tools User
type 245	QEZMAIN program 86	ID Reset) file layout 538
API (application programming interface)	setting 86	error conditions 50
security level 40 12	user profile 86	EV (Environment variable) file
application design	attribute change (AU) file layout 520	layout 539
0	AU (attribute change) file layout 520	force level 51
adopted authority 204, 207		
general security	audit (*AUDIT) special authority	GR(generic record) file layout 540
recommendations 196	functions allowed 71	GS (give descriptor) entry type 250
ignoring adopted authority 206	risks 71	GS (give descriptor) file layout 544
libraries 200	audit (QAUDJRN) journal 570	introduction 235
library lists 201	See also object auditing	IP (change ownership) entry
menus 203	AD (auditing change) entry type 249	type 250
profiles 201	AD (auditing change) file layout 512	IP (interprocess communication
Application development	AF (authority failure) entry type 246	actions) file layout 546
commands 314	default sign-on violation 13	IP (interprocess communications)
application programming interface (API)	description 242	entry type 242
security level 40 12	hardware protection violation 14	IR(IP rules actions) file layout 547
APPN directory (ND) file layout 559	job description violation 13	IS (Internet security management) file
APPN end point (NE) file layout 560	program validation 15	layout 548
approval program, password 45, 46	restricted instruction violation 15	JD (job description change) entry
approving password 44	unsupported interface 13	
11 01	* *	type 250
APYJRNCHG (Apply Journaled Changes)	unsupported interface	JD (job description change) file
command	violation 15	layout 550
authorized IBM-supplied user	AF (authority failure) file layout 514	JS (job change) entry type 243
profiles 290	analyzing	JS (job change) file layout 550
object auditing 450, 478	with query 263	KF (key ring file) file layout 554
object authority required 374	AP (adopted authority) entry	LD (link, unlink, search directory) file
APYJRNCHGX (Apply Journal Changes	type 245	layout 557
Extend) command	AP (adopted authority) file	managing 259
object auditing 471, 478	layout 519	methods for analyzing 262
APYPTF (Apply Program Temporary Fix)	AU (attribute change) file layout 520	ML (mail actions) entry type 245
command	auditing level (QAUDLVL) system	ML (mail actions) file layout 559
authorized IBM-supplied user	value 51	NA (network attribute change) entry
profiles 290	auditing level extension (QAUDLVL2)	type 250
•		V 1
object authority required 427	system value 53	NA (network attribute change) file
	automatic cleanup 260	layout 559

audit (QAUDJRN) journal (continued) audit (QAUDJRN) journal (continued) audit function activating 258 ND (APPN directory) file layout 559 SF (change to spooled file) entry type 252 starting 258 NE (APPN end point) file layout 560 SG file layout 590, 591 O1 (optical access) file layout 568, stopping 261 SM (systems management change) audit journal O3 (optical access) file layout 570 entry type 252 displaying entries 279 printing entries 623 OM (object management) entry SM (systems management change) file type 245 layout 592 working with 261 OM (object management) file SO (server security user information audit journal receiver layout 560 actions) file layout 593 creating 258 OR (object restore) entry type 246 deleting 261 ST (service tools action) entry naming 258 OR (object restore) file layout 563 type 252 OW (ownership change) entry ST (service tools action) file saving 261 type 250 layout 594 audit level (AUDLVL) parameter OW (ownership change) file stopping 261 \*AUTFAIL (authority failure) layout 566 SV (action to system value) entry value 242 PA (program adopt) entry type 250 type 251 \*CMD (command string) value 243 PG (primary group change) entry SV (action to system value) file \*CREATE (create) value 243 layout 597 \*DELETE (delete) value 243 type 250 PG (primary group change) file system entries 259 \*JOBDTA (job change) value 243 lavout 572 VA (access control list change) entry \*OBJMGT (object management) PO (printed output) entry type 246 type 251 value 245 PO (printer output) file layout 575 VA (changing access control list) file \*OFCSRV (office services) value 245 PS (profile swap) entry type 250 layout 598 \*PGMADP (adopted authority) PS (profile swap) file layout 576 VC (connection start and end) file value 245 PW (password) entry type 242 \*PGMFAIL (program failure) layout 598 PW (password) file layout 577 VC (connection start or end) entry value 246 RA (authority change for restored type 244 \*SAVRST (save/restore) value 246 object) entry type 246 VF (close of server files) file \*SECURITY (security) value 249 RA (authority change for restored layout 599 \*SERVICE (service tools) value 252 object) file layout 578 VL (account limit exceeded) entry \*SPLFDTA (spooled file changes) receiver storage threshold 260 type 252 value 252 RJ (restoring job description) entry VL (account limit exceeded) file \*SYSMGT (systems management) type 246 layout 599 value 252 RJ (restoring job description) file VN (network log on and off) file changing 107 audit level (QAUDLVL) system value layout 579 layout 600 RO (ownership change for restored VN (network log on or off) entry \*AUTFAIL (authority failure) object) entry type 246 type 244 value 242 RO (ownership change for restored VO (validation list) file layout 601 \*CREATE (create) value 243 object) file layout 580 VP (network password error) entry \*DELETE (delete) value 243 RP (restoring programs that adopt \*JOBDTA (job change) value 243 type 243 authority) entry type 246 VP (network password error) file \*OBJMGT (object management) layout 602 RP (restoring programs that adopt value 245 authority) file layout 581 VR (network resource access) file \*OFCSRV (office services) value 245 RQ (restoring \*CRQD object that layout 603 \*PGMADP (adopted authority) adopts authority) file layout 583 VS (server session) entry type 244 value 245 RQ (restoring \*CRQD object) entry VS (server session) file layout 603 \*PGMFAIL (program failure) type 246 VU (network profile change) entry value 246 RU (restore authority for user profile) \*PRTDTA (printer output) value 246 type 251 VU (network profile change) file entry type 246 \*SAVRST (save/restore) value 246 RU (restore authority for user profile) layout 604 \*SECURITY (security) value 249 VV (service status change) entry file layout 583 \*SERVICE (service tools) value 252 RZ (primary group change for \*SPLFDTA (spooled file changes) type 252 value 252 restored object) entry type 246 VV (service status change) file RZ (primary group change for layout 605 \*SYSMGT (systems management) restored object) file layout 583 X0 (kerberos authentication) file value 252 layout 605 See also audit (QAUDJRN) journal SD (change system distribution directory) entry type 245 YC (change to DLO object) file changing 259, 279, 621 displaying 279, 621 SD (change system distribution layout 610 directory) file layout 585 YR (read of DLO object) file purpose 236 SE (change of subsystem routing layout 611 user profile 94 entry) entry type 251 ZC (change to object) file layout 611 auditing ZR (read of object) file layout 614 \*ALLOBJ (all object) special SE (change of subsystem routing entry) file layout 586 audit control (QAUDCTL) system value authority 233 changing 279, 621 \*AUDIT (audit) special authority 71 SF (action to spooled file) file layout 587 displaying 279, 621 See audit (QAUDJRN) journal

nuditing (continued)	auditing (continued)	authority (continued)
See also audit level (QAUDLVL)	user profile	*Ref (Reference) 112
system value	*ALLOBJ (all object) special	*RW (read, write) 113, 303
See also object auditing	authority 233	*RWX (read, write, execute) 113, 303
abnormal end 50	administration 233	*RX (read, execute) 113, 303
access path recovery 452	using	*SAVSYS (save system) special
actions 236	journals 267	authority 70
activating 258	QHST (history) log 266	*SECADM (security administrator)
adopted authority 234	QSYSMSG message queue 235	special authority 69
authority	working on behalf 481	*SERVICE (service) special
user profiles 234	working with user 107	authority 70
authorization 234	auditing change (AD) file layout 512	*SPLCTL (spool control) special
changing	auditing change (AD) journal entry	authority 69
command description 274, 277	type 249	*UPD (update) 112, 302
checklist for 231	auditing control (QAUDCTL) system	*USE (use) 113, 302
communications 235	value	*W (write) 113, 303
controlling 50	overview 50	*WX (write, execute) 113, 303
Directory Server 463	auditing end action (QAUDENDACN)	*X (execute) 113, 303
encryption of sensitive data 235	system value 50, 256	See also authority checking
ending 50	auditing force level (QAUDFRCLVL)	adding users 140
error conditions 50	system value 51, 256	adopted 519
group profile	auditing level (QAUDLVL) system	application design 204, 206, 207
*ALLOBJ (all object) special	value 51	audit journal (QAUDJRN)
authority 233	auditing level extension (QAUDLVL2)	entry 245
membership 233	system value 53	auditing 270
password 233	AUDLVL (audit level) parameter	authority checking example 167,
IBM-supplied user profiles 232	*CMD (command string) value 243	169
inactive users 233	user profile 94	displaying 135, 210
job descriptions 234	AUT (authority) parameter	ignoring 206
library lists 234	creating libraries 136	purpose 128
limit capabilities 233	creating objects 138	assigning to new object 124
mail services 481	specifying authorization list	authorization for changing 138
methods 266	(*AUTL) 146	authorization list
network attributes 235	user profile 93	format on save media 223
object	AUTCHK (authority to check)	management (*AUTLMGT) 112,
default 256	parameter 187	302
planning 254	authentication	stored on save media 223
object authority 269	digital ID 96	storing 222
object integrity 270	Authorities, Accumulating Special 215	changing 520
office services 481	authorities, field 115	audit journal (QAUDJRN)
overview 231	Authorities, Special 215	entry 249
password controls 233	authority	command description 274
physical security 232	*ADD (add) 112, 302	procedures 138
planning	*ALL (all) 113, 302	checking 148
overview 236	*ALLOBJ (all object) special	batch job initiation 176
system values 256	authority 68	interactive job initiation 175
program failure 270	*AUDIT (audit) special authority 71	sign-on process 175
programmer authorities 233	*AUTLMGT (authorization list	commonly used subsets 113
QTEMP objects 257	management) 112, 118, 302	copying
remote sign-on 235	*CHANGE (change) 113, 302	command description 276
reply list 493	*DLT (delete) 112, 302	example 101
save operations 230	*EXCLUDE (exclude) 113	recommendations 145
security officer 271	*EXECUTE (execute) 112, 302	renaming profile 106
sensitive data	*IOSYSCFG (system configuration)	data
authority 234	special authority 71	definition 112
encrypting 235	*JOBCTL (job control) special	definition 112
setting up 258	authority 69	deleting user 140
sign-on without user ID and	*Mgt 112	detail, displaying (*EXPERT user
password 234	*OBJALTER (object alter) 112, 301	option) 88, 89, 90
spooled files 497	*OBJEXIST (object existence) 112, 301	directory 5
starting 258	*OBJMGT (object existence)** 112, 301	displaying
steps to start 258	301	command description 274
stopping 50, 261	*OBJOPR (object operational) 112,	displaying detail (*EXPERT user
system values 49, 232, 256	301	option) 88, 89, 90
unauthorized access 235	*OBJREF (object reference) 112, 302	displays 133
unauthorized programs 235	*R (read) 113, 303	field
unsupported interfaces 235	*READ (read) 112, 302	definition 112
apported miterates woo	1121 12 (1000) 11W, 00W	· · · · · · · · · · · · · · · · · · ·

authority <i>(continued)</i>	authority (continued)	authority holder (continued)
group	storing	commands for working with 273,
displaying 135	authorization list 222	278
example 164, 168	with object 222	creating 132, 273, 278
holding when deleting file 132	with user profile 222	deleting 133, 273
	•	e e e e e e e e e e e e e e e e e e e
ignoring adopted 131	system-defined subsets 113	description 132
introduction 4	user profile	displaying 132, 273
library 5	format on save media 223	maximum storage limit exceeded 124
Management authority	stored on save media 223	object auditing 453
*Mgt(*) 112	storing 222	object authority required for
multiple objects 141	user-defined 139	commands 316
1 0		
new object	using generic to grant 141	printing 279
CRTAUT (create authority)	working with	restoring 221
parameter 118, 136	command description 274	risks 133
example 124	authority (AUT) parameter	saving 221
GRPAUT (group authority)	creating libraries 136	System/36 migration 133
parameter 80, 122	creating objects 138	authority profile (QAUTPROF) user
-		
GRPAUTTYP (group authority	specifying authorization list	profile 283
type) parameter 81	(*AUTL) 146	authority table 223
QCRTAUT (create authority)	user profile 93	authority, object
system value 22	authority cache	See object authority
QUSEADPAUT (use adopted	private authorities 174	authorization
	authority change (CA) file layout 520	auditing 234
authority) system value 30		ĕ
object	authority change (CA) journal entry	authorization list
*ADD (add) 112, 302	type 249	adding
*DLT (delete) 112, 302	authority change for restored object (RA)	entries 146, 273
*EXECUTE (execute) 112, 302	file layout 578	objects 147
*OBJEXIST (object existence) 112,	authority change for restored object (RA)	users 146
•	<b>3 3</b> • • •	
301	journal entry type 246	advantages 213
*OBJMGT (object	authority checking	authority
management) 112, 301	See also authority	changing 146
*OBJOPR (object operational) 112,	adopted authority	storing 223
301	example 167, 169	authority checking
*READ (read) 112, 302	flowchart 160	example 170
*Ref (Reference) 112	authorization list	changing
	_	
*UPD (update) 112, 302	example 170	entry 273
definition 112	group authority	comparison
exclude (*EXCLUDE) 113	example 164, 168	group profile 216
format on save media 222	owner authority	creating 145, 273
stored on save media 222	flowchart 153	damaged 228
storing 222	primary group	deleting 147, 273
object alter (*OBJALTER) 112, 301	example 165	description 117
•	•	*
object reference (*OBJREF) 112, 302	private authority	displaying
primary group 111, 123	flowchart 152	document library objects
example 165	public authority	(DLO) 277
working with 104	example 166, 168	objects 147, 273
private	flowchart 159	users 273
definition 111	sequence 148	document library object (DLO)
restoring 221, 225	•	ů ů
3	authority failure	displaying 277
saving 221	audit journal (QAUDJRN) entry 246	editing 146, 273
public	default sign-on violation 13	entry
definition 111	device description 177	adding 146
example 166, 168	hardware protection violation 14	group profile
restoring 221, 225	job description violation 13	comparison 216
saving 221	job initiation 175	introduction 4
referenced object	program validation 14, 15	management (*AUTLMGT)
using 145	restricted instruction 15	authority 112, 118, 302
removing user 140	sign-on process 175	object auditing 453
restoring	unsupported interface 13, 15	object authority required for
audit journal (QAUDJRN)	authority failure (*AUTFAIL) audit	commands 316
entry 246	level 242	
· ·		printing authority information 623
command description 277	authority failure (AF) file layout 514	QRCLAUTL (reclaim storage) 229
description of process 226	authority failure (AF) journal entry	reclaim storage (QRCLAUTL) 229
overview of commands 221	type 242	recovering damaged 228
procedure 225	description 246	removing
special (SPCAUT) authority	authority holder	entries 273
parameter 68	automatically created 133	objects 147
r		00,000 11.

authorization list (continued)	batch job (continued)	CFGSYSSEC (Configure System Security)
users 146, 273	security when starting 175, 176	command (continued)
restoring	BCHJOB (Batch Job) command	object authority required 426
association with object 225	object authority required 369	CFGTCP (Configure TCP/IP) command
description of process 228	binding directory	object authority required 441
overview of commands 221	object authority required for	CFGTCPAPP (Configure TCP/IP
retrieving entries 273	commands 317	Applications) command
saving 221	binding directory object auditing 453	object authority required 441
securing IBM-supplied objects 118	bound program	CFGTCPLPD (Configure TCP/IP LPD)
securing objects 147	adopted authority 130	command
storing	definition 130	object authority required 441
authority 222, 223	break (*BREAK) delivery mode	CFGTCPSMTP (Configure TCP/IP SMTP)
user	See also message queue	command
adding 146	user profile 84	object authority required 441
working with 273	break-message-handling program	CFGTCPTELN (Change TCP/IP
Authorization lists	adopted authority 129	TELNET) command
advantages 213	BRM (QBRMS) user profile 283	object authority required 441
planning 213	buffering	change (*CHANGE) authority 113, 302
authorization methods	Attention key 76	change *CRQD object (CQ) journal entry
combining	keyboard 76	type 247
example 172		Change Accounting Code
authorized IBM-supplied user		(CHGACGCDE) command 82
profiles 291, 299	C	Change Activation Schedule Entry
authorized user	C locale description (*CLD) auditing 455	(CHGACTSCDE) command
displaying 276	CA (authority change) file layout 520	description 619
AUTOCFG (automatic device	CA (authority change) journal entry	Change Active Profile List
configuration) value 31	type 249	(CHGACTPRFL) command
automatic configuration (QAUTOCFG)	CALL (Call Program) command	description 619
system value	object authority required 415	Change Auditing (CHGAUD) command
value set by CFGSYSSEC command 628	transferring adopted authority 128	description 274, 277 using 107
automatic configuration of virtual devices	Call Program (CALL) command	Change Authority (CHGAUT)
(QAUTOVRT) system value 31	transferring adopted authority 128	command 139, 274
automatic creation	call-level interface	Change Authorization List Entry
user profile 57	security level 40 12	(CHGAUTLE) command
automatic device configuration	calling	description 273
(AUTOCFG) value 31	program	using 146
automatic device configuration	transferring adopted	Change Command (CHGCMD) command
(QAUTOCFG) system value	authority 128	ALWLMTUSR (allow limited user)
overview 31	canceling	parameter 67
automatic install (QLPAUTO) user profile	audit function 261	PRDLIB (product library)
default values 283	cartridge	parameter 185
automatic virtual-device configuration	object authority required for	security risks 185
(QAUTOVRT) system value	commands 391	Change Command Default
value set by CFGSYSSEC	CCSID (coded character set identifier)	(CHGCMDDFT) command 210
command 628	parameter	Change Current Library (CHGCURLIB)
availability 1	user profile 88	command
	CD (command string) file layout 523	restricting 185
	CD (command string) journal entry	Change Dedicated Service Tools
В	type 243 CFGDSTSRV (Configure Distribution	Password (CHGDSTPWD)
backing up	Services) command	command 275
security information 221	authorized IBM-supplied user	Change Directory Entry (CHGDIRE)
backup	profiles 290	command 278
object authority required for	object authority required 332	Change Document Library Object
commands 403	CFGIPS (Configure IP over SNA	Auditing (CHGDLOAUD) command
backup media	Interface) command	*AUDIT (audit) special authority 71
protecting 232	object authority required 314	description 277
basic (*BASIC) assistance level 58, 64	CFGRPDS (Configure VM/MVS Bridge)	QAUDCTL (Auditing Control) system
basic service (QSRVBAS) user profile	command	value 50
authority to console 179	authorized IBM-supplied user	Change Document Library Object
default values 283	- I I	Authority (CHGDLOAUT)
batch	profiles 290	
butti	-	command 277
restricting jobs 193	object authority required 332	command 277 Change Document Library Object Owner
	-	command 277 Change Document Library Object Owner (CHGDLOOWN) command 277
restricting jobs 193	object authority required 332 CFGSYSSEC (Configure System Security)	command 277 Change Document Library Object Owner (CHGDLOOWN) command 277 Change Document Library Object
restricting jobs 193 batch job	object authority required 332 CFGSYSSEC (Configure System Security) command	command 277 Change Document Library Object Owner (CHGDLOOWN) command 277

Change Expiration Schedule Entry (CHGEXPSCDE) command	Change Security Auditing (CHGSECAUD) command	changing (continued) document library object (DLO)
description 619 Change Job (CHGJOB) command	description 279, 621 Change Service Program (CHGSRVPGM)	authority 277 owner 277
adopted authority 130	command	primary group 277
Change Journal (CHGJRN)	specifying USEADPAUT	document library object auditing
command 260, 261 Change Library List (CHGLIBL)	parameter 131 Change Spooled File Attributes	command description 277 DST (dedicated service tools)
command 183	(CHGSPLFA) command 186	password 109
Change Library Owner (CHGLIBOWN)	change system distribution directory (SD)	DST (dedicated service tools) user
tool 217	file layout 585	ID 109
Change Menu (CHGMNU) command PRDLIB (product library)	change system distribution directory (SD) journal entry type 245	IBM-supplied user profile passwords 108
parameter 185	Change System Library List	IPC object
security risks 185	(CHGSYSLIBL) command 183, 202	audit journal (QAUDJRN)
Change Network Attributes (CHGNETA)	change to DLO object (YC) file	entry 250
Change Nada Croup Attributes (Change	layout 610	job
Change Node Group Attributes (Change Node Group Attributes) command	change to object (ZC) file layout 611 change to spooled file (SF) journal entry	adopted authority 130 audit journal (QAUDJRN)
object auditing 484	type 252	entry 243
Change Object Auditing (CHGOBJAUD)	Change User Audit (CHGUSRAUD)	job description
command	command 276	audit journal (QAUDJRN)
*AUDIT (audit) special authority 71	*AUDIT (audit) special authority 71	entry 250
description 274, 277 QAUDCTL (Auditing Control) system	description 277 QAUDCTL (Auditing Control) system	library list 183 menu
value 50	value 50	PRDLIB (product library)
Change Object Owner (CHGOBJOWN)	using 107	parameter 185
command 143, 274	Change User Audit display 107	security risks 185
Change Object Primary Group (CHGOBJPGP) command 123, 144, 274	Change User Profile (CHGUSRPRF) command 276	network attribute
change of subsystem routing entry (SE)	description 275	audit journal (QAUDJRN) entry 250
file layout 586	password composition system	security-related 189
change of subsystem routing entry (SE)	values 39	network profile
journal entry type 251	setting password equal to profile	audit journal (QAUDJRN)
change of system value (SV) journal entry type 251	name 60 using 101	entry 251 object auditing 71, 274, 277
Change Output Queue (CHGOUTQ)	changing	command description 277
command 186	access control list	object owner 143, 274
Change Owner (CHGOWN)	audit journal (QAUDJRN)	object ownership
command 143, 274	entry 251	moving application to
change ownership (IP) journal entry type 250	accounting code 82 active profile list 619	production 217 output queue 186
Change Password (CHGPWD) command	adopted authority	ownership
auditing 233	authority required 130	device description 179
description 275	audit journal receiver 260, 261	password
enforcing password system values 39	auditing	description 275 DST (dedicated service tools) 109
setting password equal to profile name 60	command description 274, 277 authority	275
Change Primary Group (CHGPGP)	audit journal (QAUDJRN)	enforcing password system
command 144, 274	entry 249	values 39
Change Profile (CHGPRF)	command description 274	IBM-supplied user profiles 108
command 101, 276 Change Program (CHGPGM) command	procedures 138 authorization list	setting password equal to profile name 60
specifying USEADPAUT	entry 273	primary group 123, 274
parameter 131	user authority 146	audit journal (QAUDJRN)
change request description	changing	entry 250
object authority required for	audit journal (QAUDJRN)	primary group during restore
commands 317 change request description (*CRQD)	entry 250 command	audit journal (QAUDJRN) entry 246
object auditing 455	ALWLMTUSR (allow limited user)	profile
Change Security Auditing	parameter 67	See changing user profile
(CHGSECAUD)	defaults 210	program
See also audit level (QAUDLVL)	current library 183, 185	specifying USEADPAUT
system value auditing	device description owner 179	parameter 131 program adopt
one-step 257	directory entry 278	audit journal (QAUDJRN) entry 250

changing (continued)	checking (continued)	CHGAUTLE (Change Authorization List
QAUDCTL (audit control) system	object integrity 623	Entry) command (continued)
value 279	auditing use 235	object auditing 453
QAUDLVL (audit level) system	description 270, 276	object authority required 316
value 279	password 107, 275	using 146
routing entry	checklist	CHGBCKUP (Change Backup Options)
audit journal (QAUDJRN)	auditing security 231	command
entry 251	planning security 231	object authority required 403
security auditing 279, 621	CHGACGCDE (Change Accounting	CHGCDEFNT (Change Coded Font)
security level (QSECURITY) system	Code) command	object authority required for
value	object authority required 369	commands 312
level 10 to level 20 10	relationship to user profile 82	CHGCFGL (Change Configuration List)
level 20 to level 30 10	CHGACTPRFL (Change Active Profile	command
level 20 to level 40 15	List) command	object auditing 454
level 20 to level 50 17	description 619	object authority required 324
level 30 to level 20 10	object authority required 443	CHGCFGLE (Change Configuration List
level 30 to level 40 15	CHGACTSCDE	Entry) command
level 30 to level 50 17	authorized IBM-supplied user	object auditing 454
level 40 to level 20 10	profiles 290	object authority required 324
level 40 to level 30 16	CHGACTSCDE (Change Activation	CHGCLNUP (Change Cleanup)
level 50 to level 30 or 40 18	Schedule Entry) command	command
server authentication entry 278	description 619	object authority required 403
spooled file	CHGACTSCDE (Change Activity	CHGCLS (Change Class) command
audit journal (QAUDJRN)	Schedule Entry) command	object auditing 456
entry 252	object authority required 443	object authority required 318
system directory	CHGAJE (Change Autostart Job Entry)	CHGCLUCFG
audit journal (QAUDJRN)	command	authorized IBM-supplied user
entry 245	object auditing 493	profiles 290
system library list 183, 202	object authority required 435	CHGCLUCFG command
system value	CHGALRACNE (Change Alert Action	object authority required 319
audit journal (QAUDJRN)	Entry) command	CHGCLUNODE
entry 251	object auditing 474	authorized IBM-supplied user
systems management	object authority required 346	profiles 290
audit journal (QAUDJRN)	CHGALRD (Change Alert Description) command	CHGCLUNODE command
entry 252		object authority required 319 CHGCLURCY
user auditing 71, 276, 277 user authority	object auditing 452 object authority required 314	authorized IBM-supplied user
authorization list 146	CHGALRSLTE (Change Alert Selection	profiles 290
user ID	Entry) command	CHGCLUVER
DST (dedicated service tools) 109	object auditing 474	authorized IBM-supplied user
user profile	object authority required 346	profiles 290
audit journal (QAUDJRN)	CHGALRTBL (Change Alert Table)	CHGCLUVER command
entry 247	command	object authority required 319
command descriptions 275, 276	object auditing 452	CHGCMD (Change Command) command
methods 101	object authority required 314	ALWLMTUSR (allow limited user)
password composition system	CHGASPA	parameter 67
values 39	authorized IBM-supplied user	object auditing 456
setting password equal to profile	profiles 290	object authority required 321
name 60	CHGASPA command 328	PRDLIB (product library)
changing access control list (VA) file	CHGATR (Change Attribute) command	parameter 185
layout 598	object auditing 460	security risks 185
characters	CHGATR (Change Attributes) command	CHGCMDCRQA (Change Command
password 40	object auditing 461	Change Request Activity) command
chart format	CHGAUD (Change Audit) command	authorized IBM-supplied user
object authority required for	using 107	profiles 290
commands 317	CHGAUD (Change Auditing) command	object auditing 455
chart format (*CHTFMT) auditing 454	description 274, 277	object authority required 317
Check Object Integrity (CHKOBJITG)	object auditing 461, 495, 500	CHGCMDDFT (Change Command
command	object authority required 350	Default) command
auditing use 235	CHGAUT (Change Authority)	object auditing 456
description 270, 276, 623	command 139	object authority required 321
Check Password (CHKPWD)	description 274	using 210
command 107, 275	object auditing 461, 495, 500	CHGCMNE (Change Communications
checking	object authority required 350	Entry) command
See also authority checking	CHGAUTLE (Change Authorization List	object auditing 493
altered objects 270	Entry) command	object authority required 435
default passwords 619	description 273	

CHGCNNL (Change Connection List) CHGCTLRTL (Change Controller CHGDEVOPT (Change Device Description (Retail)) command Description (Optical)) command object auditing 457 object authority required 325 object authority required 404 CHGCNNLE (Change Connection List CHGCTLRWS (Change Controller CHGDEVPRT (Change Device Entry) command Description (Remote Workstation)) Description (Printer)) command object auditing 457 command object authority required 329 CHGDEVRTL (Change Device CHGCOMSNMP (Change Community object authority required 325 for SNMP) command CHGCTLTAP (Change Controller Description (Retail)) command Description (TAPE)) command object authority required 329 object authority required 441 CHGCOSD (Change Class-of-Service object authority required 325 CHGDEVSNPT (Change Device CHGCTLVWS (Change Controller Description (SNPT)) command Description) command Description (Virtual Workstation)) object authority required 329 object auditing 457 object authority required 318 command CHGDEVSNUF (Change Device **CHGCRG** object authority required 325 Description (SNUF)) command authorized IBM-supplied user CHGCURDIR (Change Current Directory) object authority required 329 CHGDEVTAP (Change Device profiles 290 command CHGCRG command object auditing 462 Description (Tape)) command object authority required 319 CHGCURLIB (Change Current Library) object authority required 329 **CHGCRGDEVE** CHGDIRE (Change Directory Entry) command authorized IBM-supplied user object authority required 384 command profiles 290 restricting 185 description 278 CHGDBG (Change Debug) command CHGCRGDEVE command object authority required 331 object authority required 319 object authority required 415 CHGDIRSHD (Change Directory Shadow **CHGCRGPRI** CHGDDMF (Change Distributed Data System) command authorized IBM-supplied user Management File) command object authority required 331 object auditing 471 profiles 290 CHGDKTF (Change Diskette File) CHGCRGPRI command object authority required 339 command object authority required 319 CHGDEVAPPC (Change Device object auditing 471 CHGCRQD (Change Change Request Description (APPC)) command object authority required 339 CHGDLOAUD (Change Document object authority required 328 Description) command CHGDEVASC (Change Device Library Object Auditing command object auditing 455 object authority required 317 Description (Async)) command \*AUDIT (audit) special authority CHGCRSDMNK (Change Cross Domain object authority required 328 CHGDLOAUD (Change Document Library Object Auditing) command Key) command CHGDEVASP (Change Device Description for Auxiliary Storage Pool) authorized IBM-supplied user description 277 profiles 290 command object auditing 465 object authority required 327 object authority required 328 QAUDCTL (Auditing Control) system CHGCSI (Change Communications Side CHGDEVBSC (Change Device value 50 Description (BSC)) command CHGDLOAUT (Change Document Information) command object auditing 458 object authority required 328 Library Object Auditing) command object authority required 322 CHGDEVCRP command object authority required 333 CHGCSPPGM (Change CSP/AE object authority required 328 CHGDLOAUT (Change Document Program) command CHGDEVDKT (Change Device Library Object Authority) command object auditing 489 Description (Diskette)) command description 277 CHGCTLAPPC (Change Controller object authority required 328 object auditing 465 Description (APPC)) command CHGDEVDSP (Change Device object authority required 333 object authority required 325 Description (Display)) command CHGDLOOWN (Change Document CHGCTLASC (Change Controller object authority required 328 Library Object Owner) command CHGDEVFNC (Change Device description 277 Description (Async)) command object authority required 325 Description (Finance)) command object auditing 465 CHGCTLBSC (Change Controller object authority required 328 object authority required 334 Description (BSC)) command CHGDEVHOST (Change Device CHGDLOPGP (Change Document object authority required 325 Library Object Primary Group) Description (SNA Host)) command CHGCTLFNC (Change Controller object authority required 328 command Description (Finance)) command CHGDEVINTR (Change Device object auditing 465 object authority required 325 Description (Intrasystem)) command object authority required 334 CHGCTLHOST (Change Controller object authority required 328 CHGDLOPGP (Change Document Description (SNA Host)) command CHGDEVMLB command Library Object Primary) command 277 object authority required 325 object authority required 328 description 277 CHGCTLLWS (Change Controller CHGDEVNET (Change Device CHGDLOUAD (Change Document Description (Local Workstation)) Library Object Auditing) command Description (Network)) command object authority required 329 description 277 command object authority required 325 CHGDEVNWSH command CHGDOCD (Change Document CHGCTLNET (Change Controller object authority required 329 Description) command Description (Network)) command CHGDEVOPT (Change Device object auditing 465 object authority required 325 Description (Optical) command object authority required 334

object authority required 329

CHGDSPF (Change Display File) CHGFCTE (Change Forms Control Table CHGJOBSCDE (Change Job Schedule command Entry) command Entry) command object auditing 471 object authority required 423 object auditing 477 object authority required 339 CHGFNTTBLE (Change DBCS Font Table object authority required 373 CHGDSTD (Change Distribution **CHGJOBTRC** Description) command object authority required for authorized IBM-supplied user object auditing 465 commands 312 profiles 291 CHGFTR (Change Filter) command object authority required 333 CHGJOBTYP (Change Job Type) CHGDSTL (Change Distribution List) object auditing 474 command command object authority required 346 authorized IBM-supplied user object authority required 333 **CHGGPHFMT** profiles 291 CHGDSTPWD (Change Dedicated authorized IBM-supplied user object authority required 409 Service Tools Password) command profiles 290 CHGJRN (Change Journal) command authorized IBM-supplied user CHGGPHFMT (Change Graph Format) authorized IBM-supplied user profiles 290 command profiles 291 object authority required 409 description 275 detaching receiver 260, 261 object auditing 478, 479 object authority required 443 CHGGPHPKG (Change Graph Package) object authority required 374 CHGDSTQ (Change Distribution Queue) command authorized IBM-supplied user CHGJRNOBJ (Change Journaled Object ) command authorized IBM-supplied user profiles 290 command profiles 290 object authority required 409 object auditing 450 CHGLANADPI (Change LAN Adapter object authority required 333 CHGGRPA (Change Group Attributes) CHGDSTRTE (Change Distribution Information) command Route) command object authority required 369 object authority required 391 authorized IBM-supplied user CHGHLLPTR (Change High-Level CHGLF (Change Logical File) command object auditing 471 profiles 290 Language Pointer) command object authority required 415 object authority required 333 object authority required 340 CHGDTA (Change Data) command CHGICFDEVE (Change Intersystem CHGLFM (Change Logical File Member) object authority required 339 Communications Function Program command CHGDTAARA (Change Data Area) object auditing 471 Device Entry) command command object authority required 340 object authority required 340 object auditing 468 CHGICFF (Change Intersystem CHGLIB (Change Library) command object authority required 327 Communications Function File) object auditing 479 **CHGEMLCFGE** (Change Emulation object authority required 384 command CHGLIBL (Change Library List) Configuration Entry) command object authority required 340 object authority required 330 CHGIMGCLG command CHGENVVAR (Change Environment authorized IBM-supplied user object authority required 384 Variable) command profiles 290 using 183 CHGIMGCLG command CHGLIBOWN (Change Library Owner) object authority required 338 CHGEWCBCDE (Change Extended object authority required 348 tool 217 Wireless Controller Bar Code Entry) CHGLICINF (Change License **CHGIMGCLGE** authorized IBM-supplied user Information) command object authority required 338 profiles 291 authorized IBM-supplied user **CHGEWCM (Change Extended Wireless** CHGIMGCLGE command profiles 291 Controller Member) command object authority required 348 object authority required 389 object authority required 338 CHGIPLA command 369 CHGLINASC (Change Line Description CHGIPSIFC (Change IP over SNA CHGEWCPTCE (Change Extended (Async)) command Interface) command object authority required 389 Wireless Controller PTC Entry) command object authority required 314 CHGLINBSC (Change Line Description object authority required 338 CHGIPSLOC (Change IP over SNA (BSC)) command CHGEWLM (Change Extended Wireless Location Entry) command object authority required 389 CHGLINETH (Change Line Description Line Member) command object authority required 314 object authority required 338 CHGIPSTOS (Change IP over SNA Type (Ethernet)) command CHGEXPSCDE (Change Expiration of Service) command object authority required 389 Schedule Entry) command object authority required 314 CHGLINFAX (Change Line Description authorized IBM-supplied user CHGJOB (Change Job) command (FAX)) command profiles 290 adopted authority 130 object authority required 389 description 619 object auditing 476 CHGLINFR (Change Line Description object authority required 369 (Frame Relay Network)) command object authority required 443 **CHGFCNARA** CHGJOBD (Change Job Description) object authority required 389 authorized IBM-supplied user CHGLINIDD (Change Line Description command object auditing 476 (DDI Network)) command profiles 290 CHGFCT (Change Forms Control Table) object authority required 372 object authority required 389 command CHGJOBQE (Change Job Queue Entry) CHGLINSDLC (Change Line Description object authority required 423 command (SDLC)) command object auditing 476, 493 object authority required 389

object authority required 435

CHGLINTDLC (Change Line Description CHGNFSEXP (Change Network File CHGOBJPGP (Change Object Primary Group) command 123, 144 System Export) command (TDLC)) command object authority required 389 authorized IBM-supplied user description 274 CHGOBJPGP (Change Object Primary) CHGLINTRN (Change Line Description profiles 291 (Token-Ring Network)) command object authority required 398 object authority required 389 CHGNTBD (Change NetBIOS object authority required 306 CHGOBJUAD (Change Object Auditing) CHGLINWLS (Change Line Description Description) command object auditing 485 (Wireless)) command command object authority required 390 object authority required 397 description 277 CHGLINX25 (Change Line Description CHGNWIFR (Change Network Interface CHGOPTA (Change Optical Attributes) Description (Frame Relay Network)) (X.25)) command command command authorized IBM-supplied user object authority required 389 CHGLPDA (Change LPD Attributes) object authority required 399 profiles 291 command CHGNWIISDN (Change Network object authority required 404 object authority required 441 Interface Description for ISDN) CHGOPTVOL (Change Optical Volume) CHGMGDSYSA (Change Managed command command object auditing 485 System Attributes) command object authority required 404 authorized IBM-supplied user CHGNWSA (Change Network Server CHGOUTQ (Change Output Queue) profiles 291 Attribute) command command CHGMGRSRVA (Change Manager object authority required 401 object auditing 486 Service Attributes) command CHGNWSA (Change Network Server object authority required 407 authorized IBM-supplied user Attributes) command using 186 profiles 291 authorized IBM-supplied user CHGOWN (Change Owner) CHGMNU (Change Menu) command profiles 291 command 143 object auditing 481 CHGNWSALS (Change Network Server description 274 object authority required 392 Alias) command object auditing 461, 495, 500, 502 PRDLIB (product library) object authority required 401 object authority required 351 parameter 185 CHGNWSCFG command CHGPCST (Change Physical File security risks 185 authorized IBM-supplied user Constraint) command CHGMOD (Change Module) command object authority required 340 profiles 291 object auditing 482 object authority required 401 CHGPDGPRF (Change Print Descriptor object authority required 396 CHGNWSD (Change Network Server Group Profile) command CHGMODD (Change Mode Description) Description) command object auditing 488 object authority required 402 object authority required 413 command CHGNWSSTG (Change Network Server CHGPEXDFN (Change Performance object auditing 482 object authority required 396 Explorer Definition) command Storage Space) command CHGMSGD (Change Message object authority required 400 authorized IBM-supplied user Description) command CHGNWSVRA (Create Network Server profiles 291 object auditing 483 object authority required 409 Attribute) command object authority required 394 object authority required 400 CHGPF (Change Physical File) command CHGMSGF (Change Message File) CHGOBJAUD (Change Object Audit) object auditing 471 object authority required 340 object auditing 483 object authority required 305 CHGPFCNARA Change Functional Area) object authority required 395 CHGOBJAUD (Change Object Auditing command CHGMSGQ (Change Message Queue) object authority required 409 command \*AUDIT (audit) special authority 71 CHGPFCST (Change Physical File command object auditing 484 CHGOBJAUD (Change Object Auditing) Constraint) command object authority required 395 object auditing 472 command CHGMSTK (Change Master Key) CHGPFM (Change Physical File Member) description 274 QAUDCTL (Auditing Control) system command command authorized IBM-supplied user value 50 object auditing 472 CHGOBJCRQA (Change Object Change object authority required 340 profiles 291 object authority required 327 Request Activity) command CHGPFTRG (Change Physical File CHGMWSD (Change Network Server authorized IBM-supplied user Trigger) command Description) command profiles 291 object authority required 340 object auditing 486 object auditing 455 CHGPGM (Change Program) command object authority required 317 object auditing 489 CHGNETA (Change Network Attributes) command CHGOBJD (Change Object Description) object authority required 415 specifying USEADPAUT authorized IBM-supplied user command profiles 291 object auditing 450 parameter 131 object authority required 398 object authority required 305 CHGPGMVAR (Change Program CHGOBJOWN (Change Object Owner) Variable) command using 189 CHGNETJOBE (Change Network Job command object authority required 415 Entry) command description 274 CHGPGP (Change Primary Group) authorized IBM-supplied user command 144 object auditing 450 profiles 291 object authority required 305 description 274 object authority required 398 using 143 object auditing 461, 495, 500, 502

CHGPGP (Change Primary Group) CHGQSTDB (Change CHGSAVF (Change Save File) command command (continued) Question-and-Answer Database) object auditing 472 object authority required 351 object authority required 340 command CHGPJ (Change Prestart Job) command authorized IBM-supplied user CHGSBSD (Change Subsystem object authority required 369 profiles 291 Description) command CHGPJE (Change Prestart Job Entry) object authority required 420 object auditing 494 CHGRCYAP (Change Recovery for object authority required 435 command object auditing 494 Access Paths) command CHGSCHIDX (Change Search Index) authorized IBM-supplied user object authority required 435 command CHGPRB (Change Problem) command profiles 291 object auditing 495 authorized IBM-supplied user object auditing 452 object authority required 368 profiles 291 object authority required 312 CHGSECA (Change Security Attributes) object authority required 414 CHGRDBDIRE (Change Relational command CHGPRBACNE (Change Problem Action Database Directory Entry) command object authority required 426 Entry) command object authority required 422 CHGSECAUD (Change Security Audit) object auditing 474 CHGRJECMNE (Change RJE command object authority required 346, 414 Communications Entry) command object authority required 426 CHGPRBSLTE (Change Problem Selection object authority required 423 CHGSECAUD (Change Security CHGRJERDRE (Change RJE Reader Entry) command object auditing 474 Entry) command security auditing function 257 object authority required 346, 414 object authority required 423 CHGSECAUD (Change Security CHGPRDCRQA (Change Product Change CHGRJEWTRE (Change RJE Writer Auditing) command Request Activity) command Entry) command description 279, 621 authorized IBM-supplied user object authority required 423 CHGSHRPOOL (Change Shared Storage CHGRMTJRN (Change Remote Journal) profiles 291 Pool) command object auditing 456 command object authority required 436 object authority required 317 object auditing 478 CHGSNMPA (Change SNMP Attributes) CHGPRF (Change Profile) command CHGRPYLE (Change Reply List Entry) description 276 command object authority required 441 object auditing 504 authorized IBM-supplied user CHGSPLFA (Change Spooled File profiles 291 Attributes) command object authority required 444 using 101 object auditing 493 action auditing 497 CHGPRTF (Change Printer File) object authority required 436 DSPDTA parameter of output CHGRSCCRQA (Change Resource command queue 186 object auditing 472 Change Request Activity) command object auditing 486, 487 object authority required 340 authorized IBM-supplied user object authority required 432 CHGPSFCFG (Change Print Services profiles 291 CHGSRCPF (Change Source Physical Facility Configuration) command object auditing 456 File) command object authority required 414 object authority required 317 object authority required 340 CHGPTFCRQA (Change PTF Change CHGRTGE (Change Routing Entry) CHGSRVA (Change Service Attributes) Request Activity) command command command authorized IBM-supplied user object auditing 494 object authority required 427 profiles 291 object authority required 435 CHGSRVPGM (Change Service Program) object auditing 456 CHGS34LIBM (Change System/34 command object authority required 317 Library Members) command object auditing 499 CHGPTR (Change Pointer) command authorized IBM-supplied user object authority required 415 authorized IBM-supplied user profiles 291 specifying USEADPAUT profiles 291 object authority required 396 parameter 131 object authority required 415 CHGS36 (Change System/36) command CHGSSND (Change Session Description) CHGPWD (Change Password) command object auditing 503 command auditing 233 object authority required 437 object authority required 423 description 275 CHGS36A (Change System/36 Attributes) CHGSSNMAX (Change Session enforcing password system values 39 command Maximum) command object auditing 504 object auditing 482 object auditing 503 object authority required 444 object authority required 437 object authority required 396 setting password equal to profile CHGS36PGMA (Change System/36 CHGSVRAUTE (Change Server Program Attributes) command Authentication Entry) command name 60 CHGPWRSCD (Change Power On/Off object auditing 489 object authority required 427 Schedule) command object authority required 437 CHGSYSDIRA (Change System Directory object authority required 403 CHGS36PRCA (Change System/36 Attributes) command CHGPWRSCDE (Change Power On/Off Procedure Attributes) command object auditing 463 Schedule Entry) command object auditing 472 object authority required 331 object authority required 403 object authority required 437 CHGSYSJOB (Change System Job) CHGQRYA (Change Query Attribute) CHGS36SRCA (Change System/36 Source command command Attributes) command object authority required 369 object authority required 418 object authority required 437

CHGSYSLIBL (Change System Library	CHKCMNTRC (Check Communications	CLRDKT (Clear Diskette) command
List) command	Trace) command	object authority required 392
authorized IBM-supplied user	authorized IBM-supplied user	CLRJOBQ (Clear Job Queue) command
profiles 291	profiles 291	object auditing 476
object authority required 384	object authority required 427	object authority required 372
programming example 202	CHKDKT (Check Diskette) command	CLRLIB (Clear Library) command
using 183	object authority required 392	object auditing 480
CHGSYSVAL (Change System Value) command	CHKDLO (Check Document Library Object) command	object authority required 384 CLRMSGQ (Clear Message Queue)
authorized IBM-supplied user	object command object authority required 334	command
profiles 291	CHKDOC (Check Document) command	object auditing 484
object authority required 436	object auditing 464	object authority required 395
CHGTAPCTG (Change Tape Cartridge)	object authority required 334	CLROUTQ (Clear Output Queue)
command	CHKIGCTBL (Check DBCS Font Table)	command
object authority required 392	command	action auditing 498
CHGTAPF (Change Tape File) command	object auditing 476	object auditing 486
object auditing 472	CHKIN (Check In) command	object authority required 407
object authority required 340	object auditing 495, 500	CLRPFM (Clear Physical File Member)
CHGTCPA (Change TCP/IP Attributes)	object authority required 352	command
command	CHKOBJ (Check Object) command	object auditing 472
object authority required 441	object auditing 451	object authority required 340
CHGTCPHTE (Change TCP/IP Host	object authority required 306	CLRSAVF (Clear Save File) command
Table Entry) command	CHKOBJITG (Check Object Integrity)	object authority required 340
object authority required 441 CHGTCPIFC (Change TCP/IP Interface)	command 3 auditing use 235	CLRTRCDTA (Clear Trace Data)
command	description 270, 276, 623	command object authority required 415
object authority required 441	object authority required 306	cluster
CHGTCPRTE (Change TCP/IP Route	CHKOUT (Check Out) command	object authority required for
Entry) command	object auditing 495, 500	commands 318
object authority required 441	object authority required 352	Cluster Operations(CU) file layout 528
CHGTELNA (Change TELNET	CHKPRDOPT (Check Product Option)	CMPJRNIMG (Compare Journal Images)
Attributes) command	command	command
object authority required 441	authorized IBM-supplied user	object auditing 477
CHGTIMZON command 442	profiles 291	object authority required 375
CHGUSRAUD (Change User Audit)	object authority required 427	CNLRJERDR (Cancel RJE Reader)
command	CHKPWD (Check Password) command	command
*AUDIT (audit) special authority 71	description 275	object authority required 423
description 276, 277	object auditing 504	CNLRJEWTR (Cancel RJE Writer)
object authority required 444	object authority required 444	command
QAUDCTL (Auditing Control) system value 50	using 107	object authority required 424 CNTRYID (country or region identifier)
using 107	CHKTAP (Check Tape) command object authority required 392	parameter
CHGUSRPRF (Change User Profile)	CHRIDCTL (user options) parameter	user profile 88
command	user profile 88	CO (create object) file layout 524
description 275, 276	CL keyword (*CLKWD) user option 88,	CO (create object) journal entry
object auditing 504	89, 90	type 123, 243
object authority required 444	class	coded character set identifier
password composition system	object authority required for	CCSID user profile parameter 88
values 39	commands 318	QCCSID system value 88
setting password equal to profile	relationship to security 192	combining authorization methods
name 60	Class (*CLS) auditing 456	example 172
using 101	class files	command
CHGUSRTRC (Change User Trace)	jar files 217	auditing
command	class-of-service description	audit journal (QAUDJRN)
object authority required 370 CHGVTMAP (Change VT100 Keyboard	object authority required for commands 318	entry 243 changing
Map) command	class-of-service description (*COSD)	ALWLMTUSR (allow limited user)
object authority required 441	auditing 457	parameter 67
CHGWSE (Change Workstation Entry)	class, user	defaults 210
command	See user class (USRCLS) parameter	PRDLIB (product library)
object auditing 494	cleanup	parameter 185
object authority required 435	object authority required for	security risks 185
CHGWTR (Change Writer) command	commands 403	creating
object authority required 447	client request access (PCSACC) network	ALWLMTUSR (allow limited user)
CHKASPBAL	attribute 189	parameter 67
authorized IBM-supplied user	close of server files (VF) file layout 599	PRDLIB (product library)
profiles 291	CLP38 programs 117	parameter 185

1 / // //	1 (71 / 11 1)	1 GI ( " 1)
command (continued)	command, CL (continued)	command, CL (continued)
creating (continued)	CFGSYSSEC (Configure System	Change Password (CHGPWD)
security risks 185	Security)	(continued)
NLV (national language version)	description 280, 627	setting password equal to profile
security 210	Change Accounting Code	name 60
· ·	(CHGACGCDE) 82	
planning security 209	,	Change Profile (CHGPRF) 101, 276
revoking public authority 280, 627	Change Authorization List Entry	Change Program (CHGPGM)
System/38	(CHGAUTLE)	specifying USEADPAUT
security 210	description 273	parameter 131
command (*CMD object type)	using 146	Change Security Auditing
object authority required for	Change Command (CHGCMD)	(CHGSECAUD)
0 0 1		*
commands 321	ALWLMTUSR (allow limited user)	description 279
Command (*CMD) auditing 456	parameter 67	Change Server Authentication Entry
command capability	PRDLIB (product library)	(CHGSVRAUTE) 278
listing users 268	parameter 185	Change Service Program
command string	security risks 185	(CHGSRVPGM)
audit journal (QAUDJRN) file	Change Command Default	specifying USEADPAUT
	8	
layout 523	(CHGCMDDFT) 210	parameter 131
command string (*CMD) audit level 243	Change Current Library	Change Spooled File Attributes
command string (CD) file layout 523	(CHGCURLIB)	(CHGSPLFA) 186
command string (CD) journal entry	restricting 185	Change System Library List
type 243	Change Dedicated Service Tools	(CHGSYSLIBL) 183, 202
command, CL	Password (CHGDSTPWD) 275	Change User Audit
		S
activation schedule 619	Change Directory Entry	(CHGUSRAUD) 276
Add Authorization List Entry	(CHGDIRE) 278	*AUDIT (audit) special
(ADDAUTLE) 146, 273	Change Document Library Object	authority 71
Add Directory Entry	Auditing (CHGDLOAUD) 277	description 277
(ADDDIRE) 278	*AUDIT (audit) special	QAUDCTL (Auditing Control)
Add Document Library Object	authority 71	system value 50
0 0	0	
Authority (ADDDLOAUT) 277	description 277	using 107
Add Library List Entry	QAUDCTL (Auditing Control)	Change User Profile
(ADDLIBLE) 183, 185	system value 50	(CHGUSRPRF) 276
Add Server Authentication Entry	Change Document Library Object	description 275
(ADDSVRAUTE) 278	Authority (CHGDLOAUT) 277	password composition system
ADDAUTLE (Add Authorization List	•	values 39
	Change Document Library Object	
Entry) 146, 273	Owner (CHGDLOOWN) 277	setting password equal to profile
ADDDIRE (Add Directory	Change Document Library Object	name 60
Entry) 278	Primary (CHGDLOPGP) 277	using 101
ADDDLOAUT (Add Document	Change Job (CHGJOB)	Check Object Integrity (CHKOBJITG)
Library Object Authority) 277	adopted authority 130	auditing use 235
ADDJOBSCDE (Add Job Schedule	Change Journal (CHGJRN) 260, 261	
		description 270, 276
Entry)	Change Library List (CHGLIBL) 183	Check Password (CHKPWD) 107,
SECBATCH menu 623	Change Menu (CHGMNU)	275
ADDLIBLE (Add Library List	PRDLIB (product library)	CHGACGCDE (Change Accounting
Entry) 183, 185	parameter 185	Code) 82
ADDSVRAUTE (Add Server	security risks 185	CHGACTPRFL (Change Active Profile
Authentication Entry) 278	Change Network Attributes	List)
<b>3</b> ·		*
allowed for limit capabilities user 67	(CHGNETA) 189	description 619
ALWLMTUSR (allow limited user)	Change Object Auditing	CHGACTSCDE (Change Activation
parameter 67	(CHGOBJAUD) 274	Schedule Entry)
ANZDFTPWD (Analyze Default	*AUDIT (audit) special	description 619
Passwords)	authority 71	CHGAUTLE (Change Authorization
description 619	description 277	List Entry)
•	•	3 -
ANZPRFACT (Analyze Profile	QAUDCTL (Auditing Control)	description 273
Activity)	system value 50	using 146
creating exempt users 619	Change Object Owner	CHGCMD (Change Command)
description 619	(CHGOBJOWN) 143, 274	ALWLMTUSR (allow limited user)
authority holders, table 273, 278	Change Object Primary Group	parameter 67
authorization lists 273	(CHGOBJPGP) 123, 144, 274	PRDLIB (product library)
CALL (Call Program)	Change Output Queue	parameter 185
transferring adopted	(CHGOUTQ) 186	security risks 185
authority 128	Change Password (CHGPWD)	CHGCMDDFT (Change Command
Call Program (CALL)	auditing 233	Default) 210
transferring adopted	description 275	CHGCURLIB (Change Current
authority 128	enforcing password system	Library)
authority 120	values 39	restricting 185
	Values 59	restricting 185

command, CL (continued) command, CL (continued) command, CL (continued) CHGDIRE (Change Directory CHGSVRAUTE (Change Server CRTMNU (Create Menu) Authentication Entry) 278 PRDLIB (product library) Entry) 278 CHGDLOAUD (Change Document CHGSYSLIBL (Change System Library parameter 185 Library Object Auditing) 277 List) 183, 202 security risks 185 \*AUDIT (audit) special CHGUSRAUD (Change User CRTOUTQ (Create Output authority 71 Audit) 276 Queue) 186, 188 QAUDCTL (Auditing Control) \*AUDIT (audit) special CRTUSRPRF (Create User Profile) authority 71 description 98, 275, 276 system value 50 CHGDLOAUT (Change Document description 277 Delete Authority Holder Library Object Authority) 277 **QAUDCTL** (Auditing Control) (DLTAUTHLR) 133, 273 CHGDLOOWN (Change Document system value 50 Delete Authorization List Library Object Owner) 277 using 107 (DLTAUTL) 147, 273 CHGDLOPGP (Change Document CHGUSRPRF (Change User Delete Journal Receiver Library Object Primary) 277 Profile) 276 (DLTJRNRCV) 261 CHGDLOUAD (Change Document description 275 Delete User Profile (DLTUSRPRF) Library Object Auditing) password composition system description 276 description 277 values 39 example 102 CHGDSTPWD (Change Dedicated setting password equal to profile object ownership 122 Service Tools Password) 275 name 60 Display Audit Journal Entries using 101 CHGEXPSCDE (Change Expiration (DSPAUDJRNE) CHKOBJITG (Check Object Integrity) Schedule Entry) description 279 description 619 auditing use 235 Display Authority Holder CHGJOB (Change Job) description 270, 276, 623 (DSPAUTHLR) 132, 273 CHKPWD (Check Password) 107, adopted authority 130 Display Authorization List CHGJRN (Change Journal) 260, 261 (DSPAUTL) 273 Display Authorization List Document CHGLIBL (Change Library List) 183 Configure System Security CHGMNU (Change Menu) (CFGSYSSEC) Library Objects PRDLIB (product library) description 280 (DSPAUTLDLO) 277 Copy Spooled File (CPYSPLF) 186 Display Authorization List Objects parameter 185 security risks 185 CPYSPLF (Copy Spooled File) 186 (DSPAUTLOBJ) 147, 273 CHGNETA (Change Network Create Authority Holder Display Authorized Users Attributes) 189 (CRTAUTHLR) 132, 273, 278 (DSPAUTUSR) CHGOBJAUD (Change Object Create Authorization List auditing 268 Auditing) 274 (CRTAUTL) 145, 273 description 276 \*AUDIT (audit) special Create Command (CRTCMD) example 104 authority 71 ALWLMTUSR (allow limited user) Display Document Library Object description 277 parameter 67 Auditing (DSPDLOAUD) 256, 277 Display Document Library Object PRDLIB (product library) QAUDCTL (Auditing Control) system value 50 parameter 185 Authority (DSPDLOAUT) 277 CHGOBJOWN (Change Object security risks 185 Display Job Description (DSPJOBD) 234 Owner) 143, 274 Create Journal (CRTJRN) 258 CHGOBJPGP (Change Object Primary Create Journal Receiver Display Journal (DSPJRN) (CRTJRNRCV) 258 audit (QAUDJRN) journal Group) 123, 144, 274 CHGOUTQ (Change Output Create Library (CRTLIB) 136 example 262 Queue) 186 Create Menu (CRTMNU) auditing file activity 210, 267 CHGPGM (Change Program) creating output file 263 PRDLIB (product library) specifying USEADPAUT parameter 185 displaying QAUDJRN (audit) parameter 131 security risks 185 journal 235 CHGPRF (Change Profile) 101, 276 Create Output Queue Display Library (DSPLIB) 269 CHGPWD (Change Password) (CRTOUTQ) 186, 188 Display Library Description (DSPLIBD) auditing 233 Create User Profile (CRTUSRPRF) description 98, 275, 276 CRTAUT parameter 137 description 275 CRTAUTHLR (Create Authority enforcing password system Display Object Authority Holder) 132, 273, 278 (DSPOBJAUT) 269, 274 values 39 Display Object Description setting password equal to profile CRTAUTL (Create Authorization (DSPOBJD) 256, 274 name 60 List) 145, 273 CHGSECAUD (Change Security CRTCMD (Create Command) created by 123 ALWLMTUSR (allow limited user) object domain 12 Auditing) description 279, 621 parameter 67 program state 13 CHGSPLFA (Change Spooled File PRDLIB (product library) using output file 269 Display Program (DSPPGM) parameter 185 Attributes) 186 CHGSRVPGM (Change Service security risks 185 adopted authority 130 Program) CRTJRN (Create Journal) 258 program state 13 specifying USEADPAUT Display Programs That Adopt CRTJRNRCV (Create Journal (DSPPGMADP) parameter 131 Receiver) 258 CRTLIB (Create Library) 136 auditing 270

command, CL (continued)	command, CL (continued)	command, CL (continued)
Display Programs That Adopt	DSPJRN (Display Journal) (continued)	GRTOBJAUT (Grant Object
(DSPPGMADP) (continued)	displaying QAUDJRN (audit)	Authority) 274
description 277	journal 235	affect on previous authority 142
using 130, 210	DSPLIB (Display Library) 269	multiple objects 141
Display Security Auditing	DSPLIBD (Display Library	GRTUSRAUT (Grant User Authority)
(DSPSECAUD Values)	Description)	copying authority 101
description 279	CRTAUT parameter 137	description 276
Display Service Program	DSPOBJAUT (Display Object	recommendations 145
(DSPSRVPGM)	Authority) 269, 274	renaming profile 106
adopted authority 130	DSPOBJD (Display Object	GRTUSRPMN (Grant User
Display Spooled File (DSPSPLF) 186	Description) 256, 274	Permission) 277
Display User Profile (DSPUSRPRF)	created by 123	keywords, displaying (*CLKWD user
description 276	object domain 12	option) 88, 89, 90
using 104	program state 13	object authority, table 274
using output file 268	using output file 269	parameter names, displaying
displaying keywords (*CLKWD user	DSPPGM (Display Program)	(*CLKWD user option) 88, 89, 90
option) 88, 89, 90	adopted authority 130	passwords, table 275
DLTAUTHLR (Delete Authority	program state 13	Print Communications Security
Holder) 133, 273	DSPPGMADP (Display Programs That	Attributes (PRTCMNSEC)
DLTAUTL (Delete Authorization	Adopt)	description 280
List) 147, 273	auditing 270	Print Job Description Authority
DLTJRNRCV (Delete Journal	description 277	(PRTJOBDAUT) 279
Receiver) 261	using 130, 210	Print Private Authorities
DLTUSRPRF (Delete User Profile)	DSPSECAUD (Display Security	(PRTPVTAUT) 279
description 276 example 102	Auditing Values) description 279	Print Publicly Authorized Objects (PRTPUBAUT) 279
object ownership 122	•	Print Queue Authority (PRTQAUT)
document library object (DLO)	DSPSECAUD (Display Security Auditing)	description 279
table 277	description 621	Print Subsystem Description Authority
DSPACTPRFL (Display Active Profile	DSPSPLF (Display Spooled File) 186	(PRTSBSDAUT)
List)	DSPSRVPGM (Display Service	description 279
description 619	Program)	Print System Security Attributes
DSPACTSCD (Display Activation	adopted authority 130	(PRTSYSSECA)
Schedule)	DSPUSRPRF (Display User Profile)	description 280
description 619	description 276	Print Trigger Programs
DSPAUDJRNE (Display Audit Journal	using 104	(PRTTRGPGM)
Entries)	using output file 268	description 279
description 279, 623	Edit Authorization List	Print User Objects (PRTUSROBJ)
DSPAUTHLR (Display Authority	(EDTAUTL) 146, 273	description 279
Holder) 132, 273	Edit Document Library Object	PRTADPOBJ (Print Adopting Objects)
DSPAUTL (Display Authorization	Authority (EDTDLOAUT) 277	description 623
List) 273	Edit Library List (EDTLIBL) 183	PRTCMNSEC (Print Communications
DSPAUTLDLO (Display Authorization	Edit Object Authority	Security)
List Document Library Objects) 277	(EDTOBJAUT) 139, 274	description 280, 623
DSPAUTLOBJ (Display Authorization	EDTAUTL (Edit Authorization	PRTJOBDAUT (Print Job Description
List Objects) 147, 273	List) 146, 273	Authority) 279
DSPAUTUSR (Display Authorized	EDTDLOAUT (Edit Document Library	description 623
Users)	Object Authority) 277	PRTPUBAUT (Print Publicly
auditing 268	EDTLIBL (Edit Library List) 183	Authorized Objects) 279
description 276	EDTOBJAUT (Edit Object	description 623
example 104	Authority) 139, 274	PRTPVTAUT (Print Private
DSPDLOAUD (Display Document	End Job (ENDJOB)	Authorities) 279
Library Object Auditing) 256, 277	QINACTMSGQ system value 24	authorization list 623
DSPDLOAUT (Display Document	ENDJOB (End Job)	description 625
Library Object Authority) 277	QINACTMSGQ system value 24 Grant Object Authority	PRTQAUT (Print Queue Authority)
DSPEXPSCD (Display Expiration Schedule)	(GRTOBJAUT) 274	description 279, 625 PRTSBSDAUT (Print Subsystem
description 619	affect on previous authority 142	Description Authority)
DSPJOBD (Display Job	multiple objects 141	description 279
Description) 234	Grant User Authority (GRTUSRAUT)	PRTSBSDAUT (Print Subsystem
DSPJRN (Display Journal)	copying authority 101	Description)
audit (QAUDJRN) journal	description 276	description 623
example 262	recommendations 145	PRTSYSSECA (Print System Security
auditing file activity 210, 267	renaming profile 106	Attributes)
creating output file 263	Grant User Permission	description 280, 623
<b>U</b> 1	(GRTUSRPMN) 277	•

command, CL (continued) command, CL (continued) command, CL (continued) PRTTRGPGM (Print Trigger RSTAUT (Restore Authority) TFRCTL (Transfer Control) Programs) (continued) transferring adopted description 279, 623 using 225 authority 129 PRTUSROBJ (Print User Objects) RSTDLO (Restore Document Library TFRGRPJOB (Transfer to Group Job) description 279, 623 Object) 221 adopted authority 129 PRTUSRPRF (Print User Profile) RSTLIB (Restore Library) 221 Transfer Control (TFRCTL) description 623 RSTLICPGM (Restore Licensed transferring adopted RCLSTG (Reclaim Storage) 16, 21, authority 129 Program) 124, 229 recommendations 227 Transfer to Group Job (TFRGRPJOB) Reclaim Storage (RCLSTG) 16, 21, security risks 227 adopted authority 129 user profiles (related), table 277 124, 229 RSTOBJ (Restore Object) Remove Authorization List Entry using 221 user profiles (working with), (RMVAUTLE) 146, 273 RSTUSRPRF (Restore User table 276 Remove Directory Entry Profiles) 221, 277 Work with Authorization Lists (RMVDIRE) 278 RTVAUTLE (Retrieve Authorization (WRKAUTL) 273 List Entry) 273 Remove Document Library Object Work with Directory Authority (RMVDLOAUT) 277 RTVUSRPRF (Retrieve User (WRKDIRE) 278 Remove Library List Entry Profile) 107, 276 Work with Journal (WRKJRN) 261, (RMVLIBLE) 183 RVKOBJAUT (Revoke Object 268 Remove Server Authentication Entry Authority) 147, 274 Work with Journal Attributes RVKPUBAUT (Revoke Public (RMVSVRAUTE) 278 (WRKJRNA) 261, 268 Restore Authority (RSTAUT) Authority) Work with Objects (WRKOBJ) 274 audit journal (QAUDJRN) description 280, 627 Work with Objects by Owner (WRKOBJOWN) entry 246 details 630 RVKUSRPMN (Revoke User auditing 234 description 277 procedure 226 description 274 Permission) 277 role in restoring security 221 SAVDLO (Save Document Library using 143 Work with Objects by Primary Group using 225 Object) 221 Restore Document Library Object Save Document Library Object (WRKOBJPGP) 123, 144 (RSTDLO) 221 (SAVDLO) 221 description 274 Restore Library (RSTLIB) 221 Save Library (SAVLIB) 221 Work with Output Queue Description Restore Licensed Program Save Object (SAVOBJ) 221, 261 (WRKOUTQD) 186 Save Security Data Work with Spooled Files (RSTLICPGM) recommendations 227 (SAVSECDTA) 221, 277 (WRKSPLF) 186 security risks 227 Save System (SAVSYS) 221, 277 Work with System Status Restore Object (RSTOBJ) SAVLIB (Save Library) 221 (WRKSYSSTS) 192 using 221 SAVOBJ (Save Object) 221, 261 Work with System Values Restore User Profiles SAVSECDTA (Save Security (WRKSYSVAL) 232 (RSTUSRPRF) 221, 277 Data) 221, 277 Work with User Profiles Retrieve Authorization List Entry SAVSYS (Save System) 221, 277 (WRKUSRPRF) 97, 276 (RTVAUTLE) 273 SBMJOB (Submit Job) 176 WRKAUTL (Work with Authorization Retrieve User Profile SECBATCH menu 622 Lists) 273 WRKDIRE (Work with (RTVUSRPRF) 107, 276 security tools 279, 619 security, list 273 Revoke Object Authority Directory) 278 (RVKOBJAUT) 147, 274 Send Journal Entry (SNDJRNE) 259 WRKJRN (Work with Journal) 261, Revoke Public Authority Send Network Spooled File 268 (SNDNETSPLF) 186 (RVKPUBAUT) WRKJRNA (Work with Journal description 280 Set Attention Program Attributes) 261, 268 Revoke User Permission (SETATNPGM) 86 WRKOBJ (Work with Objects) 274 (RVKUSRPMN) 277 SETATNPGM (Set Attention WRKOBJOWN (Work with Objects by RMVAUTLE (Remove Authorization Program) 86 Owner) setting QALWUSRDMN (allow user auditing 234 List Entry) 146, 273 RMVDIRE (Remove Directory objects) system value 21 description 274 SNDJRNE (Send Journal Entry) 259 using 143 Entry) 278 WRKOBJPGP (Work with Objects by RMVDLOAUT (Remove Document SNDNETSPLF (Send Network Spooled File) 186 Primary Group) 123, 144 Library Object Authority) 277 RMVLIBLE (Remove Library List Start System/36 (STRS36) description 274 user profile, special WRKOUTQD (Work with Output Entry) 183 RMVSVRAUTE (Remove Server environment 72 Queue Description) 186 Authentication Entry) 278 STRS36 (Start System/36) WRKSPLF (Work with Spooled RSTAUT (Restore Authority) user profile, special Files) 186 WRKSYSSTS (Work with System audit journal (QAUDJRN) environment 72 entry 246 Submit Job (SBMJOB) 176 Status) 192 description 277 WRKSYSVAL (Work with System system distribution directory, procedure 226 Values) 232 table 278

role in restoring security 221

command, CL (continued)	comparison	controlling (continued)
WRKUSRPRF (Work with User	group profile and authorization	remote (continued)
Profiles) 97, 276	list 216	sign-on (QRMTSIGN system
command, generic	complete change of password 44	value) 27
Change Authority (CHGAUT) 139	complex	restore operations 191
Change Owner (CHGOWN) 143	authority	save operations 191
Change Primary Group	example 172	user library list 201
(CHGPGP) 144	confidential data	Copy Spooled File (CPYSPLF)
CHGAUT (Change Authority) 139	protecting 234	command 186
CHGOWN (Change Owner) 143	confidentiality 1	Copy User display 100
CHGPGP (Change Primary	configuration	copying
Group) 144	automatic	spooled file 186
Grant Object Authority	virtual devices (QAUTOVRT	user authority
(GRTOBJAUT) 139	system value) 31	command description 276
GRTOBJAUT (Grant Object	object authority required for	example 101
Authority) 139	commands 323	recommendations 145
Revoke Object Authority	configuration list	renaming profile 106
(RVKOBJAUT) 139	object authority required for	user profile 99
RVKOBJAUT (Revoke Object	commands 324	country or region dentifier
Authority) 139	configuration list object auditing 454	QCNTRYID system value 88
Work with Authority	Configure System Security (CFGSYSSEC)	countryor region identifier
(WRKAUT) 139	command	CNTRYID user profile parameter 88
WRKAUT (Work with	description 280, 627	CP (user profile change) file layout 525
Authority) 139	connection	CP (user profile change) journal entry
command, generic object	ending	type 247
Change Auditing (CHGAUD) 274	audit journal (QAUDJRN)	CPHDTA (Cipher Data) command
description 277	entry 244	authorized IBM-supplied user
Change Authority (CHGAUT) 274	starting	profiles 291
Change Owner (CHGOWN) 274	audit journal (QAUDJRN)	object authority required 327
Change Primary Group	entry 244	CPROBJ (Compress Object) command
(CHGPGP) 274	connection list	object auditing 451
CHGAUD (Change Auditing) 274	object authority required for	object authority required 306
description 277	commands 324	CPY (Copy Object) command
CHGAUT (Change Authority) 274	connection list (*CNNL) auditing 457	object auditing 460
CHGOWN (Change Owner) 274	connection start and end (VC) file	CPY (Copy) command
CHGPGP (Change Primary	layout 598	object auditing 461, 500, 502
Group) 274	connection start or end (VC) journal entry	object authority required 352
Display Authority (DSPAUT) 274	type 244	CPYAUDJRNE command
DSPAUT (Display Authority) 274	connection verification (CV) file	object authority required 375
Work with Authority	layout 529	CPYCFGL (Copy Configuration List)
(WRKAUT) 274	console	command
WRKAUT (Work with	authority needed to sign on 179	object auditing 454
Authority) 274	QCONSOLE system value 179	object authority required 324
command, integrated file system	QSECOFR (security officer) user	CPYCNARA (Copy Functional Area)
Change Auditing (CHGAUD)	profile 179	command
using 107	QSRV (service) user profile 179	object authority required 409
CHGAUD (Change Auditing)	QSRVBAS (basic service) user	CPYDOC (Copy Document) command
using 107	profile 179	object auditing 464, 465
commands	restricting access 232	object authority required 334
Application development 314	contents	CPYF (Copy File) command
COMMIT (Commit) command	security tools 279, 619	object auditing 470, 472
object authority required 322	controller description	object authority required 340
commitment control	object authority required for	CPYFCNARA
object authority required for	commands 325	authorized IBM-supplied user
commands 322	printing security-relevant	profiles 291
Common Criteria security	parameters 623	CPYFRMDIR (Copy from Directory)
description 5	controller description (*CTLD)	command
communications	auditing 459	object authority required 331
monitoring 235	controlling	CPYFRMDKT (Copy from Diskette)
communications entry	access	command
job description 181	DDM request (DDM) 190	object authority required 340
communications side information	iSeries Access 189	CPYFRMIMPF (Copy from Import File)
object authority required for	objects 12	command
commands 322	system programs 12	object authority required 340
communications side information (*CSI)	auditing 50	CPYFRMQRYF (Copy from Query File)
auditing 458	remote	command
	job submission 189	object authority required 341
	-	

CPYFRMSTMF (Copy from Stream File) command	CQ (change *CRQD object) journal entry type 247	creating (continued) program
object authority required 341	create (*CREATE) audit level 243	adopted authority 130
CPYFRMTAP (Copy from Tape)	create authority (CRTAUT) parameter	user profile
command	description 118	audit journal (QAUDJRN)
object authority required 341	displaying 137	entry 247
CPYGPHFMT	risks 119	
		command descriptions 275, 276
authorized IBM-supplied user	create authority (QCRTAUT) system	example 98
profiles 291	value	methods 96
CPYGPHFMT (Copy Graph Format)	description 22	creating object
command	risk of changing 22	object auditing 450
object authority required 409	using 119	cross system product map (*CSPMAP)
CPYGPHPKG	Create Authority Holder (CRTAUTHLR)	auditing 458
authorized IBM-supplied user	command 132, 273, 278	cross system product table (*CSPTBL)
profiles 291	Create Authorization List (CRTAUTL)	auditing 458
CPYGPHPKG (Copy Graph Package)	command 145, 273	CRTADMDMN command
command	Create Command (CRTCMD) command	authorized IBM-supplied user
object authority required 410	ALWLMTUSR (allow limited user)	profiles 291
CPYIGCSRT (Copy DBCS Sort Table)	parameter 67	CRTALRTBL (Create Alert Table)
command	PRDLIB (product library)	command
object auditing 475	parameter 185	object authority required 314
CPYIGCTBL (Copy DBCS Font Table)	security risks 185	CRTAUT (create authority) parameter
command	Create Journal (CRTJRN) command 258	description 118
object auditing 475	Create Journal Receiver (CRTJRNRCV)	displaying 137
object authority required 337	command 258	risks 119
CPYLIB (Copy Library) command	Create Library (CRTLIB) command 136	CRTAUTHLR (Create Authority Holder)
object authority required 385	Create Menu (CRTMNU) command	command
CPYOPT (Copy Optical) command	· · · · · · · · · · · · · · · · · · ·	
10 1	PRDLIB (product library)	authorized IBM-supplied user
object authority required 405	parameter 185	profiles 291
CPYPFRDTA	security risks 185	considerations 132
authorized IBM-supplied user	create object (CO) file layout 524	description 273, 278
profiles 291	create object (CO) journal entry	object authority required 316
CPYPFRDTA (Copy Performance Data)	type 123, 243	CRTAUTL (Create Authorization List)
command	create object auditing (CRTOBJAUD)	command
object authority required 410	value 54	description 273
CPYPTF (Copy Program Temporary Fix)	create object auditing (QCRTOBJAUD)	object authority required 316
command	system value	using 145
authorized IBM-supplied user	overview 54	CRTBESTMDL (Create BEST/1 Model)
profiles 291	Create Output Queue (CRTOUTQ)	command
object authority required 427	command 186, 188	authorized IBM-supplied user
CPYPTFGRP (Copy Program Temporary	Create User Profile (CRTUSRPRF)	profiles 291
Fix Group) 291	command	CRTBESTMDL (Create Best/1-400 Mode
CPYPTFGRP (Copy PTF Group)	description 275, 276	command
command	using 98	object authority required 410
object authority required 427	Create User Profile display 97	CRTBNDC (Create Bound C Program)
CPYSPLF (Copy Spooled File) command	Create Validation Lists (CRTVLDL) 218	command
action auditing 497	creating	object authority required 378
DSPDTA parameter of output	audit journal 258	CRTBNDCBL (Create Bound COBOL
queue 186	audit journal receiver 258	Program) command
object auditing 487	authority holder 132, 273, 278	object authority required 378
object authority required 433	authorization list 145, 273	CRTBNDCL
CPYSRCF (Copy Source File) command	command	object authority required 378
object authority required 341	ALWLMTUSR (allow limited user)	CRTBNDCPP (Create Bound CPP
CPYTODIR (Copy to Directory)	parameter 67	Program) command
command		0 ,
	PRDLIB (product library)	object authority required 378
object authority required 331	parameter 185	CRTBNDDIR (Create Binding Directory)
CPYTODKT (Copy to Diskette) command	security risks 185	command
object authority required 341	library 136	object authority required 317
CPYTOIMPF (Copy to Import File)	menu	CRTBNDRPG (Create Bound RPG
command	PRDLIB (product library)	Program) command
object authority required 341	parameter 185	object authority required 379
CPYTOSTMF (Copy to Stream File)	security risks 185	CRTBSCF (Create Bisync File) command
command	object	object auditing 470
object authority required 341	audit journal (QAUDJRN)	CRTCBLMOD (Create COBOL Module)
CPYTOTAP (Copy to Tape) command	entry 123, 243	command
object authority required 341	output queue 186, 188	object authority required 379
CQ (*CRQD change) file layout 527		

CRTCBLPGM (Create COBOL Program) command object authority required 379 CRTCFGL (Create Configuration List) command object authority required 324 CRTCLD (Create C Locale Description) command object authority required 379 **CRTCLMOD** object authority required 379 CRTCLPGM (Create Control Language Program) command object authority required 379 CRTCLS (Create Class) command authorized IBM-supplied user profiles 292 object authority required 318 authorized IBM-supplied user profiles 292 CRTCLU command object authority required 320 CRTCMD (Create Command) command ALWLMTUSR (allow limited user) parameter 67 object authority required 321 PRDLIB (product library) parameter 185 security risks 185 CRTCMNF (Create Communications File) command object auditing 470 CRTCMOD (Create C Module) command object authority required 380 CRTCOSD (Create Class-of-Service Description) command object authority required 318 CRTCPPMOD (Create Bound CPP Module) command object authority required 380 **CRTCRG** authorized IBM-supplied user profiles 292 CRTCRQD (Create Change Request Description) command object authority required 317 CRTCSI (Create Communications Side Information) command object authority required 322 CRTCTLAPPC (Create Controller Description (APPC)) command object authority required 325 CRTCTLASC (Create Controller Description (Async)) command object authority required 325 CRTCTLBSC (Create Controller Description (BSC)) command object authority required 325 CRTCTLFNC (Create Controller Description (Finance)) command object authority required 325 CRTCTLHOST (Create Controller Description (SNA Host)) command object authority required 326

**CRTCTLLWS** (Create Controller CRTDEVRTL (Create Device Description Description (Local Workstation)) (Retail)) command object authority required 329 command object authority required 326 CRTDEVSNPT (Create Device CRTCTLNET (Create Controller Description (SNPT)) command Description (Network)) command object authority required 329 CRTDEVSNUF (Create Device object authority required 326 CRTCTLRTL (Create Controller Description (SNUF)) command object authority required 330 Description (Retail)) command object authority required 326 CRTDEVTAP (Create Device Description CRTCTLRWS (Create Controller (Tape)) command Description (Remote Workstation)) object authority required 330 command CRTDIR (Create Directory) command object authority required 326 object auditing 461 CRTCTLTAP (Create Controller CRTDKTF (Create Diskette File) Description (Tape)) command command object authority required 342 object authority required 326 CRTCTLVWS (Create Controller CRTDOC (Create Document) command Description (Virtual Workstation)) object authority required 334 command CRTDSPF (Create Display File) command object authority required 326 object auditing 470 CRTDDMF (Create Distributed Data object authority required 342 Management File) command CRTDSTL (Create Distribution List) object authority required 342 command CRTDEVAPPC (Create Device object authority required 333 CRTDTAARA (Create Data Area) Description (APPC)) command object authority required 329 command CRTDEVASC (Create Device Description object authority required 327 (Async)) command CRTDTADCT (Create a Data Dictionary) object authority required 329 command CRTDEVASP (Create Device Description object authority required 367 for Auxiliary Storage Pool) command CRTDTAQ (Create Data Queue) object authority required 329 command CRTDEVBSC (Create Device Description object authority required 328 CRTDUPOBJ (Create Duplicate Object) (BSC)) command object authority required 329 command CRTDEVDKT (Create Device Description object auditing 449 (Diskette)) command object authority required 306 CRTEDTD (Create Edit Description) object authority required 329 CRTDEVDSP (Create Device Description command (Display)) command object authority required 338 object authority required 329 **CRTFCNARA** CRTDEVFNC (Create Device Description authorized IBM-supplied user (Finance)) command profiles 292 object authority required 329 CRTFCNARA (Create Functional Area) CRTDEVHOST (Create Device command Description (SNA Host)) command object authority required 410 object authority required 329 CRTFCT (Create Forms Control Table) CRTDEVINTR (Create Device Description command object authority required 424 (Intrasystem)) command object authority required 329 CRTFLR (Create Folder) command CRTDEVMLB command object auditing 465 object authority required 329 object authority required 334 CRTDEVNET (Create Device Description CRTFNTRSC (Create Font Resources) (Network)) command object authority required 329 object authority required 312 CRTDEVNWSH command CRTFNTTBL (Create DBCS Font Table) object authority required 329 object authority required for CRTDEVOPT (Create Device Description commands 313 (Optical) command **CRTFORMDF** (Create Form Definition) object authority required 329 command CRTDEVOPT (Create Device Description object authority required 313 (Optical)) command CRTFTR (Create Filter) command object authority required 405 object authority required 346 CRTDEVPRT (Create Device Description CRTGDF (Create Graphics Data File) command (Printer)) command

object auditing 455

object authority required 329

**CRTGPHFMT** authorized IBM-supplied user profiles 292 **CRTGPHPKG** authorized IBM-supplied user profiles 292 CRTGPHPKG (Create Graph Package) command object authority required 410 CRTGSS (Create Graphics Symbol Set) command object authority required 347 **CRTHSTDTA** authorized IBM-supplied user profiles 292 CRTHSTDTA (Create Historical Data) command object authority required 410 CRTICFF (Create ICF File) command object auditing 470 **CRTICFF** (Create Intersystem Communications Function File) object authority required 342 CRTIGCDCT (Create DBCS Conversion Dictionary) command object authority required 337 **CRTIMGCLG** authorized IBM-supplied user profiles 292 CRTIMGCLG command object authority required 348 CRTJOBD (Create Job Description) command authorized IBM-supplied user profiles 292 object authority required 372 CRTJOBQ (Create Job Queue) command object authority required 372 CRTJRN (Create Journal) command creating audit (QAUDJRN) journal 258 object authority required 375 CRTJRNRCV (Create Journal Receiver) command creating audit (QAUDJRN) journal receiver 258 object authority required 377 CRTLASREP (Create Local Abstract Syntax) command authorized IBM-supplied user profiles 292 CRTLF (Create Logical File) command object auditing 470, 503 object authority required 342 CRTLIB (Create Library) command 136 object authority required 385 CRTLINASC (Create Line Description (Async)) command object authority required 390 CRTLINBSC (Create Line Description (BSC)) command object authority required 390 CRTLINDDI (Create Line Description (DDI Network)) command object authority required 390

**CRTLINETH** (Create Line Description (Ethernet)) command object authority required 390 **CRTLINFAX** (Create Line Description (FAX)) command object authority required 390 CRTLINFR (Create Line Description (Frame Relay Network)) command object authority required 390 CRTLINSDLC (Create Line Description (SDLC)) command object authority required 390 CRTLINTDLC (Create Line Description (TDLC)) command object authority required 390 CRTLINTRN (Create Line Description (Token-Ring Network)) command object authority required 390 CRTLINWLS (Create Line Description (Wireless)) command object authority required 390 CRTLINX25 (Create Line Description (X.25)) command object authority required 390 CRTLOCALE (Create Locale) command object authority required 391 CRTMNU (Create Menu) command object authority required 393 PRDLIB (product library) parameter 185 security risks 185 CRTMODD (Create Mode Description) command object authority required 396 CRTMSDF (Create Mixed Device File) command object auditing 470 CRTMSGF (Create Message File) command object authority required 395 CRTMSGFMNU (Create Message File Menu) command object authority required 437 CRTMSGQ (Create Message Queue) command object authority required 395 CRTNODL (Create Node List) command object authority required 402 CRTNTBD (Create NetBIOS Description) command object authority required 397 CRTNWIFR (Create Network Interface Description (Frame Relay Network)) command object authority required 399 CRTNWSALS (Create Network Server Alias) command object authority required 401 CRTNWSCFG command authorized IBM-supplied user profiles 292 object authority required 401 CRTNWSD (Create Network Server Description) command

object authority required 402

Storage Space) command object authority required 400 CRTOBJAUD (create object auditing) value 54, 256 CRTOUTQ (Create Output Queue) command examples 188 object authority required 407 using 186 CRTOVL (Create Overlay) command object authority required 313 CRTPAGDFN (Create Page Definition) command object authority required 313 CRTPAGSEG (Create Page Segment) command object authority required 313 CRTPDG (Create Print Descriptor Group) command object authority required 413 CRTPEXDTA (Create Performance Explorer Data) command authorized IBM-supplied user profiles 292 CRTPF (Create Physical File) command object auditing 470 object authority required 342 **CRTPFRDTA** authorized IBM-supplied user profiles 292 CRTPFRDTA (Create Performance Data) command object authority required 410 CRTPGM (Create Program) command object auditing 453, 482, 489, 499 CRTPNLGRP (Create Panel Group) command object authority required 393 CRTPRTF (Create Printer File) command object auditing 470 object authority required 343 CRTPSFCFG (Create Print Services Facility Configuration) command object authority required 414 CRTQMFORM (Create Query Management Form) command object auditing 491 object authority required 419 CRTQMQRY (Create Query Management Query) command object auditing 491 CRTQSTDB (Create Question and Answer Database) command authorized IBM-supplied user profiles 292 object authority required 420 CRTQSTLOD (Create Question-and-Answer Load) command authorized IBM-supplied user profiles 292 object authority required 420 CRTRJEBSCF (Create RJE BSC File) command object authority required 424

CRTNWSSTG (Create Network Server

CRTRJECFG (Create RJE Configuration) CRTSQLPKG (Create Structured Query current library (CURLIB) parameter Language Package) command See also current library object authority required 424 object authority required 408 user profile 64 CRTRJECMNF (Create RJE CRTSQLPLI (Create Structured Query customizing Communications File) command Language PL/I) command security values 627 object authority required 424 object authority required 383 CV (connection verification) file CRTRPGMOD (Create RPG Module) CRTSQLRPG (Create Structured Query layout 529 command Language RPG) command CVTBASSTR (Convert BASIC Stream object authority required 380 object authority required 383 Files) command CRTRPGPGM (Create RPG/400 Program) CRTSQLRPGI (Create Structured Query authorized IBM-supplied user Language ILE RPG Object) command command profiles 292 object authority required 380 object authority required 383 object authority required 396 CRTRPTPGM (Create Auto Report CRTSRCPF (Create Source Physical File) CVTBASUNF (Convert BASIC Program) command command Unformatted Files) command object authority required 381 object authority required 343 authorized IBM-supplied user CRTS36CBL (Create System/36 COBOL) CRTSRVPGM (Create Service Program) profiles 292 command command object authority required 396 object authority required 381 object auditing 453, 482, 499 CVTBGUDTA (Convert BGU Data) CRTS36DSPF (Create System/36 Display object authority required 416 command File) command CRTSSND (Create Session Description) authorized IBM-supplied user object authority required 343, 437 command profiles 292 CRTS36MNU (Create System/36 Menu) object authority required 424 object authority required 396 CRTTAPF (Create Tape File) command CVTCLSRC (Convert CL Source) object authority required 393, 438 object authority required 343 command CRTS36MSGF (Create System/36 CRTTBL (Create Table) command object authority required 416 Message File) command object authority required 439 **CVTDIR** object authority required 438 CRTTIMZON command 442 authorized IBM-supplied user CRTS36RPG (Create System/36 RPG) **CRTUDFS** profiles 292 command authorized IBM-supplied user CVTDIR (Convert Directory) command object authority required 381 profiles 292 object authority required 353 CRTS36RPGR (Create System/36 RPGR) CRTUDFS (Create User-Defined File CVTEDU (Convert Education) command command System) command object authority required 403 object authority required 381 authorized IBM-supplied user CVTIPSIFC (Convert IP over SNA CRTS36RPT (Create System/36 Auto profiles 292 Interface) command Report) command object authority required 442 object authority required 314 object authority required 381 CRTUSRPRF (Create User Profile) CVTIPSLOC (Convert IP over SNA CRTSAVF (Create Save File) command Location Entry) command command object authority required 343 description 275, 276 object authority required 314 CRTSBSD (Create Subsystem Description) object authority required 444 CVTOPTBKU (Convert Optical Backup) command using 98 command CRTVLDL (Create Validation List) authorized IBM-supplied user object authority required 405 profiles 292 CVTPFRDTA command authorized IBM-supplied user object authority required 435 authorized IBM-supplied user CRTSCHIDX (Create Search Index) profiles 292 profiles 292 object authority required 446 command CVTPFRDTA (Convert Performance Data) object authority required 368 CRTWSCST (Create Workstation command CRTSPADCT (Create Spelling Aid Customizing Object) command object authority required 410 Dictionary) command object authority required 446 **CVTPFRTHD** object auditing 497 cryptographic configuration (CY) file authorized IBM-supplied user object authority required 431 profiles 292 layout 531 CRTSQLCBL (Create Structured Query cryptography CVTPFRTHD (Convert Performance Language COBOL) command object authority required for Thread Data) command object authority required 382 object authority required 410 commands 326 CRTSQLCBLI (Create Structured Query CU (Cluster Operations) file layout 528 CVTRJEDTA (Convert RJE Data) Language ILE COBOL Object) CURLIB (current library) parameter command See also current library object authority required 424 object authority required 382 user profile 64 CVTRPGSRC (Convert RPG Source) current library CRTSQLCI (Create Structured Query command Language ILE C Object) command changing object authority required 383 object authority required 381 limit capabilities 65 CVTS36CFG (Convert System/36 CRTSQLCPPI (Create SQL ILE C++ methods 183 Configuration) command authorized IBM-supplied user Object) command recommendations 185 object authority required 382 definition 64 profiles 292 CRTSQLFTN (Create Structured Query library list 183, 185 object authority required 396 Language FORTRAN) command limit capabilities 65 object authority required 382 recommendations 185

user profile 64

CVTS36FCT (Convert System/36 Forms Control Table) command	dedicated service tools (DST) <i>(continued)</i> changing passwords 109	delivery (DLVRY) parameter  See also message queue
authorized IBM-supplied user	changing user ID 109	user profile 84
profiles 292	resetting password	describing
object authority required 396	audit journal (QAUDJRN)	library security requirements 203
CVTS36JOB (Convert System/36 Job)	entry 247	menu security 207
command	command description 275	description (TEXT) parameter
authorized IBM-supplied user profiles 292	Dedicated Service Tools (DST) users 108	user profile 67 descriptor
object authority required 396	default 283	giving
CVTS36QRY (Convert System/36 Query)	*DFT delivery mode	audit journal (QAUDJRN)
command	See also message queue	entry 250
authorized IBM-supplied user	user profile 84	designing
profiles 292	job description (QDFTJOBD) 79	libraries 200
object authority required 396	object	security 195
CVTS38JOB (Convert System/38 Job)	auditing 256	detaching
command	owner (QDFTOWN) user profile	audit journal receiver 260, 261
authorized IBM-supplied user	audit journal (QAUDJRN)	journal receiver 260
profiles 292	entry 246	DEV (print device) parameter
object authority required 396	default values 283	user profile 85
CVTSQLCPP (Convert SQL C++ Source)	description 124	development commands
command	restoring programs 227	Application 314
object authority required 383	sign-on	device
CVTTCPCL (Convert TCP/IP CL)	security level 40 13	See also device description
command	subsystem description 181	authority to sign-on 177
object authority required 440	value	securing 177
CVTTCPCL (Convert TCP/IP Control	IBM-supplied user profile 281	virtual
Language) command	user profile 281	automatic configuration
authorized IBM-supplied user	delete (*DELETE) audit level 243 delete (*DLT) authority 112, 302	(QAUTOVRT system value) 31
profiles 292 CVTTOFLR (Convert to Folder)	Delete Authority Holder (DLTAUTHLR)	definition 31 device description
command	command 133, 273, 278	See also device
object auditing 466	Delete Authorization List (DLTAUTL)	authority to use 177
CY(cryptographic configuration) file	command 147, 273	creating
layout 531	Delete Journal Receiver (DLTJRNRCV)	public authority 119
ayout our	command 261	QCRTAUT (create authority)
	delete operation (DO) file layout 536	system value 119
D	delete operation (DO) journal entry	definition 177
_	type 243	object authority required for
damaged audit journal 260	Delete User Profile (DLTUSRPRF)	commands 328
damaged authorization list	command	ownership
recovering 228 data area	description 276	changing 179
object authority required for	example 102	default owner 179
commands 327	object ownership 122	owned by QPGMR (programmer)
data authority	Delete User Profile display 102	profile 179
definition 112	Delete Validation Lists (DLTVLDL) 218	owned by QSECOFR (security
data queue	deleting	officer) user profile 179
object authority required for	audit journal receiver 261	printing security-relevant
commands 328	authority for user 140	parameters 623
database share (QDBSHR) user	authority holder 133, 273	securing 177
profile 283	authorization list 147, 273 object	device description (*DEVD) auditing 459
DCEADM (QDCEADM) user profile 283	audit journal (QAUDJRN)	device recovery action (QDEVRCYACN)
DCPOBJ (Decompress Object) command	entry 243	system value 32
object auditing 451	object owner profile 122	value set by CFGSYSSEC
object authority required 306	user profile	command 628
DDM (distributed data management)	command description 276	device session
security 190	directory entry 101	limiting
DDM request access (DDMACC) network	distribution lists 101	LMTDEVSSN user profile
attribute 190	message queue 101	parameter 75
DDMACC (DDM request access) network	owned objects 101	QLMTDEVSSN system value 24
attribute 190 DDMACC (distributed data management	primary group 101	DI(Directory Server) file layout 532
access) network attribute 235	spooled files 103	digital ID
debug functions	user's authority 140	if private authorization is not
adopted authority 129	deleting object	found. 96
dedicated service tools (DST)	object auditing 450	directory
auditing passwords 232		authority 5

directory (continued)	Display Document Library Object	display station pass-through (continued)
new objects 119	Auditing (DSPDLOAUD) command	target profile change
object authority required for	(continued)	audit journal (QAUDJRN)
commands 318, 331, 348, 349	using 256	entry 250
security 117 working with 278	Display Document Library Object Authority (DSPDLOAUT)	Display User Profile (DSPUSRPRF) command
directory (*DIR) auditing 460	command 277	description 276
directory entry	Display Expiration Schedule	using 104
adding 278	(DSPEXPSCD) command	using output file 268
changing 278	description 619	displaying
deleting user profile 101	Display Job Description (DSPJOBD)	adopted authority
removing 278	command 234	command description 277
directory server	Display Journal (DSPJRN) command	critical files 210
auditing 463	audit (QAUDJRN) journal	programs that adopt a profile 130
directory server (DI) file layout 532	example 262	USRPRF parameter 130
directory, system distribution	auditing file activity 210, 267	all user profiles 104
commands for working with 278	creating output file 263	audit (QAUDJRN) journal entries 235, 262
disabled (*DISABLED) user profile status description 62	displaying QAUDJRN (audit) journal 235	audit journal entries 279
QSECOFR (security officer) user	Display Library (DSPLIB) command 269	authority 133, 274
profile 62	Display Library Description (DSPLIBD)	authority holders 132
disabling	command	command description 273
audit function 261	CRTAUT parameter 137	authorization list
security level 40 16	Display Object Authority (DSPOBJAUT)	document library objects
security level 50 18	command 269, 274	(DLO) 277
user profile 62	Display Object Authority display	users 273
automatically 619	displaying detail (*EXPERT user	authorization list objects 147, 273
disconnected job time-out interval	option) 88, 89, 90	authorized users 268, 276
(QDSCJOBITV) system value 33	example 137, 138	CRTAUT (create authority)
value set by CFGSYSSEC	Display Object Description (DSPOBJD)	parameter 137
command 628 disk	command 274 created by 123	document library object authority 277
limiting use (MAXSTG)	object domain 12	job description 234
parameter 76	program state 13	journal
diskette	using 256	auditing file activity 210, 267
object authority required for	using output file 269	object
commands 391	Display Program (DSPPGM) command	originator 123
Display Activation Schedule	adopted authority 130	object auditing 256
(DSPACTSCD) command	program state 13	object authority 269, 274
description 619	Display Programs That Adopt	object description 274
Display Audit Journal Entries	(DSPPGMADP) command	object domain 12
(DSPAUDJRNE) command	auditing 270	path name 144
description 279, 623	description 277	program adopt 130
Display Authority (DSPAUT) command 274	using 130, 210 Display Security Auditing (DSPSECAUD)	program state 13 Display Program (DSPPGM)
Display Authority Holder (DSPAUTHLR)	command	command 13
command 132, 273	description 621	programs that adopt 130, 270
Display Authorization List (DSPAUTL)	Display Security Auditing	QAUDCTL (audit control) system
command 273	Values(DSPSECAUD) command	value 279, 621
Display Authorization List display	description 279	QAUDLVL (audit level) system
displaying detail (*EXPERT user	display service function	value 279, 621
option) 88, 89, 90	*SERVICE (service) special	security auditing 279, 621
Display Authorization List Document	authority 70	sign-on information
Library Objects (DSPAUTLDLO)	Display Service Program (DSPSRVPGM) command	DSPSGNINF user profile
command 277 Display Authorization List Objects	adopted authority 130	parameter 73 QDSPSGNINF system value 22
(DSPAUTLOBJ) command 147, 273	display sign-on information	recommendations 74
Display Authorized Users (DSPAUTUSR)	(QDSPSGNINF) system value	spooled file 186
command	value set by CFGSYSSEC	user profile
auditing 268	command 628	activation schedule 619
description 276	Display Spooled File (DSPSPLF)	active profile list 619
example 104	command 186	command description 276
Display Authorized Users (DSPAUTUSR)	display station pass-through	expiration schedule 619
display 104, 268	object authority required for	individual 104
Display Document Library Object	commands 332	summary list 104
Auditing (DSPDLOAUD)		distributed data management access
command 277		(DDMACC) network attribute 235

distributed systems node executive DLTCLU DLTEXPSPLF (QDSNX) user profile 283 authorized IBM-supplied user authorized IBM-supplied user profiles 292 profiles 292 distribution object authority required for DLTCLU command DLTF (Delete File) command commands 332 object authority required 320 object authority required 343 distribution directory DLTCMD (Delete Command) command **DLTFCNARA** authorized IBM-supplied user object authority required 321 changing audit journal (QAUDJRN) **DLTCMNTRC** (Delete Communications profiles 292 DLTFCNARA (Delete Functional Area) entry 245 Trace) command distribution directory, system authorized IBM-supplied user command object authority required 411 commands for working with 278 profiles 292 object authority required 427 **DLTFCT** (Delete Forms Control Table) distribution list deleting user profile 101 **DLTCNNL** (Delete Connection List) command object authority required for command object authority required 425 commands 333 object authority required 324 DLTFNTRSC (Delete Font Resources) DLCOBJ (Deallocate Object) command DLTCOSD (Delete Class-of Service command object auditing 451 Description) command object authority required 313 DLTFNTTBL (Delete DBCS Font Table) object authority required 306 object authority required 318 DLO (document library object) DLTCRGCLU object authority required for authority authorized IBM-supplied user commands 313 DLTFORMDF (Delete Form Definition) profiles 292 command descriptions 277 DLTCRQD (Delete Change Request DLTADMDMN command command authorized IBM-supplied user Description) command object authority required 313 profiles 292 object authority required 317 DLTFTR (Delete Filter) command DLTALR (Delete Alert) command **DLTCSI** (Delete Communications Side object authority required 346 object authority required 314 Information) command DLTGPHFMT DLTALRTBL (Delete Alert Table) object authority required 322 authorized IBM-supplied user DLTCTLD (Delete Controller Description) profiles 292 command object authority required 314 command **DLTGPHFMT** (Delete Graph Format) DLTAPARDTA (Delete APAR Data) object authority required 326 command **DLTDEVD** (Delete Device Description) object authority required 411 command authorized IBM-supplied user command DLTGPHPKG profiles 292 object auditing 503 authorized IBM-supplied user object authority required 427 object authority required 330 profiles 293 DLTAUTHLR (Delete Authority Holder) DLTDFUPGM (Delete DFU Program) DLTGPHPKG (Delete Graph Package) command command command description 273, 278 object authority required 416 object authority required 411 object authority required 316 DLTDKTLBL (Delete Diskette Label) **DLTGSS (Delete Graphics Symbol Set)** command using 133 command **DLTAUTL** (Delete Authorization List) object authority required 392 object authority required 347 **DLTDLO** (Delete Document Library command DLTHSTDTA description 273 Object) command authorized IBM-supplied user object authority required 316 object auditing 466 profiles 293 DLTHSTDTA (Delete Historical Data) object authority required 334 using 147 DLTBESTMDL (Delete BEST/1 Model) DLTDOCL (Delete Document List) command command object authority required 411 command authorized IBM-supplied user object auditing 466 DLTIGCDCT (Delete DBCS Conversion profiles 292 object authority required 334 Dictionary) command DLTBESTMDL (Delete Best/1-400 Model) DLTDST (Delete Distribution) command object authority required 337 DLTIGCSRT (Delete IGC Sort) command command object auditing 466 object authority required 411 object authority required 333 object authority required 337 DLTBNDDIR (Delete Binding Directory) DLTIGCTBL (Delete DBCS Font Table) DLTDSTL (Delete Distribution List) command command command object authority required 317 object authority required 333 object authority required 337 DLTCFGL (Delete Configuration List) DLTDTAARA (Delete Data Area) DLTIMGCLG authorized IBM-supplied user object authority required 324 object authority required 327 profiles 293 **DLTCHTFMT** (Delete Chart Format) DLTDTADCT (Delete Data Dictionary) DLTIMGCLG command command object authority required 348 object authority required 317 object authority required 367 DLTIPXD command 368 DLTCLD (Delete C Locale Description) DLTDTAQ (Delete Data Queue) DLTJOBD (Delete Job Description) command command command object authority required 372 object authority required 384 object authority required 328 DLTCLS (Delete Class) command **DLTEDTD** (Delete Edit Description) DLTJOBQ (Delete Job Queue) command object authority required 318 command object authority required 372 DLTJRN (Delete Journal) command object authority required 338 object authority required 375

DLTJRNRCV (Delete Journal Receiver) command object authority required 377 stopping auditing function 261 DLTLIB (Delete Library) command object authority required 385 **DLTLICPGM** (Delete Licensed Program) command authorized IBM-supplied user profiles 293 object authority required 389 DLTLIND (Delete Line Description) command object authority required 391 DLTLOCALE (Create Locale) command object authority required 391 DLTMNU (Delete Menu) command object authority required 393 DLTMOD (Delete Module) command object authority required 396 DLTMODD (Delete Mode Description) command object authority required 396 DLTMSGF (Delete Message File) command object authority required 395 DLTMSGQ (Delete Message Queue) command object authority required 395 **DLTNETF** (Delete Network File) command object authority required 398 DLTNODL (Delete Node List) command object authority required 402 **DLTNTBD** (Delete NetBIOS Description) command object authority required 397 DLTNWID (Delete Network Interface Description) command object authority required 399 **DLTNWSALS** (Delete Network Server Alias) command object authority required 401 DLTNWSCFG command authorized IBM-supplied user profiles 293 object authority required 401 DLTNWSD (Delete Network Server Description) command object authority required 402 DLTNWSSTG (Delete Network Server Storage Space) command object authority required 400 DLTOUTQ (Delete Output Queue) object authority required 407 DLTOVL (Delete Overlay) command object authority required 313 **DLTPAGDFN** (Delete Page Definition) command object authority required 313

DLTPEXDTA authorized IBM-supplied user profiles 293 **DLTPEXDTA** (Delete Performance Explorer Data) command object authority required 411 **DLTPFRDTA** authorized IBM-supplied user profiles 293 DLTPFRDTA (Delete Performance Data) command object authority required 411 DLTPGM (Delete Program) command object authority required 416 DLTPNLGRP (Delete Panel Group) command object authority required 393 DLTPRB (Delete Problem) command authorized IBM-supplied user profiles 293 object authority required 414 **DLTPSFCFG** (Delete Print Services Facility Configuration) command object authority required 414 DLTPTF (Delete PTF) command authorized IBM-supplied user profiles 293 object authority required 427 DLTQMFORM (Delete Query Management Form) command object authority required 419 DLTQMQRY (Delete Query Management Query) command object authority required 419 DLTQRY (Delete Query) command object auditing 492 object authority required 419 DLTQST (Delete Question) command authorized IBM-supplied user profiles 293 object authority required 420 DLTQSTDB (Delete Question-and-Answer Database) command authorized IBM-supplied user profiles 293 object authority required 420 DLTRJECFG (Delete RJE Configuration) command object authority required 425 DLTRMTPTF (Delete Remote PTF) command authorized IBM-supplied user profiles 293 DLTSBSD (Delete Subsystem Description) object authority required 435 DLTSCHIDX (Delete Search Index) command object authority required 368 DLTSHF (Delete Bookshelf) command object auditing 466 DLTSMGOBJ (Delete Systems Management Object) command authorized IBM-supplied user profiles 293

DLTSPADCT (Delete Spelling Aid Dictionary) command object authority required 431 DLTSPLF (Delete Spooled File) command action auditing 498 object auditing 486 object authority required 433 DLTSQLPKG (Delete Structured Query Language Package) command object authority required 408 DLTSRVPGM (Delete Service Program) command object authority required 416 DLTSSND (Delete Session Description) command object authority required 425 DLTTBL (Delete Table) command object authority required 440 DLTTIMZON command 442 DLTTRC (Delete Trace) command object authority required 428 DLTUDFS (Delete User-Defined File System) command authorized IBM-supplied user profiles 293 object authority required 442 DLTUSRIDX (Delete User Index) command object authority required 442 DLTUSRPRF (Delete User Profile) command description 276 example 102 object auditing 504 object authority required 444 object ownership 122 DLTUSRQ (Delete User Queue) command object authority required 442 DLTUSRSPC (Delete User Space) command object authority required 442 DLTUSRTRC (Delete User Trace) command object authority required 370 DLTVLDL (Delete Validation List) command authorized IBM-supplied user profiles 293 object authority required 446 **DLTWNTSVR** command authorized IBM-supplied user profiles 293 **DLTWSCST** (Delete Workstation Customizing Object) command object authority required 446 DLVRY (message queue delivery) parameter See also message queue user profile 84 DLYJOB (Delay Job) command object authority required 370 DMPCLPGM (Dump CL Program) command object auditing 489 object authority required 416

command

command

**DLTPAGSEG** (Delete Page Segment)

object authority required 313

object authority required 413

DLTPDG (Delete Print Descriptor Group)

DMPDLO (Dump Document Library	document library object (DLO)	DSPAUTL (Display Authorization List)
Object) command	(continued)	command (continued)
authorized IBM-supplied user	displaying authority 277	object authority required 316
profiles 293 object auditing 464	displaying authorization list 277 editing authority 277	DSPAUTLDLO (Display Authorization List Document Library Objects)
object authority required 334	object authority required for	command
DMPJOB (Dump Job) command	commands 333	description 277
authorized IBM-supplied user	removing authority 277	object auditing 453
profiles 293	document library object auditing	object authority required 316, 334
object authority required 428	changing	DSPAUTLOBJ (Display Authorization List
DMPJOBINT (Dump Job Internal)	command description 277	Objects) command
command	domain attribute, object	description 273
authorized IBM-supplied user profiles 293	description 12 displaying 12	object auditing 453
object authority required 428	double byte-character set dictionary	object authority required 316 using 147
DMPJVM	(*IGCDCT) object auditing 475	DSPAUTUSR (Display Authorized Users)
authorized IBM-supplied user	double byte-character set sort (*IGCSRT)	command
profiles 293	object auditing 475	auditing 268
DMPMEMINF	double byte-character set table (*IGCTBL)	description 276
authorized IBM-supplied user	object auditing 475	example 104
profiles 293	double-byte character set (DBCS)	object authority required 444
DMPOBJ (Dump Object) command	object authority required for commands 337	DSPBCKSTS (Display Backup Status)
authorized IBM-supplied user profiles 293	DS (DST password reset) journal entry	command object authority required 403
object auditing 449	type 247	DSPBCKUP (Display Backup Options)
object authority required 306	DS (IBM-Supplied Service Tools User ID	command
DMPSYSOBJ (Dump System Object)	Reset) file layout 538	object authority required 403
command	DSCJOB (Disconnect Job) command	DSPBCKUPL (Display Backup List)
authorized IBM-supplied user	object authority required 370	command
profiles 293	DSPACC (Display Access Code)	object authority required 403
object auditing 449	command	DSPBKP (Display Breakpoints) command
object authority required 306 DMPTAP (Dump Tape) command	object auditing 467 object authority required 402	object authority required 416 DSPBNDDIR (Display Binding Directory)
object authority required 392	DSPACCAUT (Display Access Code	command
DMPTRC (Dump Trace) command	Authority) command	object authority required 317
authorized IBM-supplied user	object authority required 402	DSPBNDDIRE (Display Binding
profiles 293	DSPACTPJ (Display Active Prestart Jobs)	Directory) command
object authority required 411	command	object auditing 454
DMPUSRTRC (Dump User Trace)	object authority required 370	DSPCDEFNT (Display Coded Font)
command	DSPACTPRFL (Display Active Profile	object authority required for
object authority required 370 DO (delete operation) file layout 536	List) command	commands 313
DO (delete operation) journal entry	description 619 object authority required 444	DSPCFGL (Display Configuration List) command
type 243	DSPACTSCD (Display Activation	object auditing 454
DOCPWD (document password)	Schedule) command	object authority required 324
parameter	description 619	DSPCHT (Display Chart) command
user profile 83	object authority required 444	object auditing 454
document	DSPASPSTS command	object authority required 317
library object (DLO) 221	object authority required 330	DSPCLS (Display Class) command
object authority required for commands 333	DSPAUDJRNE (Display Audit Journal Entries) command	object auditing 456 object authority required 318
password	description 279, 623	DSPCMD (Display Command) command
changes when restoring	object authority required 375	object auditing 456
profile 223	DSPAUT (Display Authority) command	object authority required 321
password (DOCPWD user profile	description 274	DSPCNNL (Display Connection List)
parameter) 83	object auditing 462, 496, 501	command
QDOC profile 283	object authority required 353	object auditing 457
restoring 221	DSPAUTHLR (Display Authority Holder)	object authority required 324
saving 221	command	DSPCNNSTS (Display Connection Status)
document library object object auditing 464	description 273 object auditing 453	command
document library object (DLO)	object auditing 453 object authority required 316	object authority required 330 DSPCOSD (Display Class-of-Service
adding authority 277	using 132	Description) command
changing authority 277	DSPAUTL (Display Authorization List)	object auditing 458
changing owner 277	command	object authority required 318
changing primary group 277	description 273	-
commands 277	object auditing 453	

DSPCPCST (Display Check Pending Constraint) command object authority required 343 DSPCPCST (Display Check Pending Constraints) command object auditing 473 DSPCSI (Display Communications Side Information) command object auditing 458 object authority required 323 DSPCSPOBJ (Display CSP/AE Object) command object auditing 458, 489 DSPCTLD (Display Controller Description) command object auditing 459 object authority required 326 DSPCURDIR (Display Current Directory) command object auditing 460 object authority required 354 DSPDBG (Display Debug) command object authority required 416 DSPDBGWCH (Display Debug Watches) command object authority required 416 DSPDBR (Display Database Relations) command object auditing 473 object authority required 343 DSPDDMF (Display Distributed Data Management File) command object authority required 343 DSPDEVD (Display Device Description) command object auditing 460 object authority required 330 DSPDIRE (Display Directory Entry) command object authority required 331 DSPDKT (Display Diskette) command object authority required 392 DSPDLOAUD (Display Document Library Object Auditing) command description 277 object auditing 464 object authority required 334 using 256 DSPDLOAUT (Display Document Library Object Authority) command description 277 object auditing 464 object authority required 334 DSPDLONAM (Display Document Library Object Name) command object authority required 334 DSPDOC (Display Document) command object auditing 464 object authority required 334 DSPDSTL (Display Distribution List) command object authority required 333 DSPDSTLOG (Display Distribution Log) command authorized IBM-supplied user profiles 293 object authority required 333

DSPDSTSRV (Display Distribution Services) command object authority required 333 DSPDTA (Display Data) command object authority required 343 DSPDTA (display data) parameter 186 DSPDTAARA (Display Data Area) command object auditing 468 object authority required 327 DSPDTADCT (Display Data Dictionary) command object authority required 367 DSPEDTD (Display Edit Description) command object auditing 469 object authority required 338 DSPEWCBCDE (Display Extended Wireless Controller Bar Code Entry) command object authority required 338 DSPEWCM (Display Extended Wireless Controller Member) command object authority required 338 DSPEWCPTCE (Display Extended Wireless Controller PTC Entry) command object authority required 338 DSPEWLM (Display Extended Wireless Line Member) command object authority required 338 DSPEXPSCD (Display Expiration Schedule) command description 619 object authority required 444 DSPF (Display File) command 354 DSPFD (Display File Description) command object auditing 473 object authority required 343 DSPFFD (Display File Field Description) object auditing 473 object authority required 343 DSPFLR (Display Folder) command object authority required 334 DSPFNTRSCA (Display Font Resource Attributes) command object authority required 313 DSPFNTTBL (Display DBCS Font Table) object authority required for commands 313 DSPGDF (Display Graphics Data File) command object authority required 318 DSPHDWRSC (Display Hardware Resources) command object authority required 422 DSPHLPDOC (Display Help Document) command object auditing 464 **DSPHSTGPH** authorized IBM-supplied user profiles 293 DSPHSTGPH (Display Historical Graph)

object authority required 372 using 234 DSPJOBLOG (Display Job Log) command object authority required 370 DSPJRN (Display Journal) command audit (QAUDJRN) journal example 262 auditing file activity 210, 267 creating output file 263 displaying QAUDJRN (audit) journal 235 object auditing 477, 479 object authority required 375 DSPJRNA (S/38E) Work with Journal Attributes object auditing 479 DSPJRNMNU (S/38E) Work with Journal object auditing 479 DSPJRNRCVA (Display Journal Receiver Attributes) command object auditing 479 object authority required 377 DSPLANADPP (Display LAN Adapter Profile) command object authority required 391 DSPLANSTS (Display LAN Status) object authority required 391 DSPLIB (Display Library) command object auditing 479 object authority required 385 using 269 DSPLIBD (Display Library Description) command CRTAUT parameter 137 object authority required 385 DSPLICKEY (Display License Key) command object authority required 388 DSPLIND (Display Line Description) command object auditing 480 object authority required 391 DSPLNK object authority required 354 DSPLNK (Display Links) command object auditing 460, 495, 500, 502 DSPLOG (Display Log) command object auditing 483 object authority required 395 DSPMFSINF (Display Mounted File System Information) command authorized IBM-supplied user profiles 293 object authority required 398

DSPIGCDCT (Display DBCS Conversion

object authority required 337

object authority required 370

DSPJOBD (Display Job Description)

DSPJOB (Display Job) command

Dictionary) command object auditing 475

DSPIPXD command 368

object auditing 476

command

command

object authority required 411

DSPMGDSYSA (Display Managed System DSPNWSUSRA (Display Network Server DSPPRB (Display Problem) command Attributes) command User Attribute) command object authority required 414 authorized IBM-supplied user object authority required 401 DSPPTF (Display Program Temporary profiles 293 DSPOBJAUT (Display Object Authority) Fix) command DSPMNUA (Display Menu Attributes) command authorized IBM-supplied user command description 274 profiles 293 object auditing 481 object auditing 451 object authority required 428 object authority required 393 object authority required 306 DSPPWRSCD (Display Power On/Off DSPMOD (Display Module) command using 269 Schedule) command object auditing 482 DSPOBJD (Display Object Description) object authority required 403 DSPRCYAP (Display Recovery for Access object authority required 396 command DSPMODD (Display Mode Description) created by 123 Paths) command command description 274 object auditing 452 object auditing 482 object auditing 451 object authority required 312 DSPRDBDIRE (Display Relational object authority required 396 object authority required 306 DSPMODSRC (Display Module Source) Database Directory Entry) command using 256 command using output file 269 object authority required 422 DSPOPT (Display Optical) command DSPRJECFG (Display RJE Configuration) object auditing 470 object authority required 416 object authority required 405 DSPMODSTS (Display Mode Status) DSPOPTLCK (Display Optical Lock) object authority required 425 DSPS36 (Display System/36) command command command object auditing 503 object auditing 460 object authority required 405 object authority required 396 DSPOPTSVR (Display Optical Server) object authority required 438 DSPMSG (Display Messages) command command DSPSAVF (Display Save File) command object auditing 483 object authority required 406 object authority required 343 object authority required 394 DSPPDGPRF (Display Print Descriptor DSPSBSD (Display Subsystem DSPMSGD (Display Message Group Profile) command Description) command Descriptions) command object authority required 413 object auditing 494 object auditing 482 DSPPFM (Display Physical File Member) object authority required 435 DSPSECA (Display Security Attributes) object authority required 394 command DSPNETA (Display Network Attributes) object auditing 470 command command object authority required 343 object authority required 426 object authority required 398 **DSPPFRDTA** DSPSECAUD (Display Security Auditing DSPNTBD (Display NetBIOS Description) authorized IBM-supplied user Values) command command profiles 293 description 279 object auditing 485 DSPPFRDTA (Display Performance Data) object authority required 426 object authority required 397 command DSPSECAUD (Display Security Auditing) DSPNWID (Display Network Interface object authority required 411 command description 621 Description) command **DSPPFRGPH** object auditing 485 authorized IBM-supplied user DSPSFWRSC (Display Software object authority required 399 profiles 293 Resources) command DSPNWSA (Display Network Server DSPPFRGPH (Display Performance object authority required 422 Graph) command Attribute) command DSPSGNINF (display sign-on object authority required 411 object authority required 401 information) parameter DSPNWSALS (Display Network Server DSPPGM (Display Program) command user profile 73 Alias) command adopted authority DSPSOCSTS (Display Sphere of Control object authority required 401 object auditing 489 Status) command DSPNWSCFG command object authority required 416 object authority required 432 authorized IBM-supplied user program state 13 DSPSPLF (Display Spooled File) DSPPGMADP (Display Program Adopt) profiles 293 command object authority required 401 command action auditing 497 DSPNWSD (Display Network Server object authority required 445 DSPDTA parameter of output Description) command DSPPGMADP (Display Programs that queue 186 object auditing 486 Adopt) command object auditing 487 object authority required 402 object auditing 504 object authority required 433 DSPPGMADP (Display Programs That DSPNWSSSN (Display Network Server DSPSRVA (Display Service Attributes) Adopt) command Session) command command object authority required 401 auditing 270 object authority required 428 DSPNWSSTC (Display Network Server description 277 DSPSRVPGM (Display Service Program) Statistics) command using 130, 210 command object authority required 401 DSPPGMREF (Display Program adopted authority 130 object auditing 499 DSPNWSSTG (Display Network Server References) command Storage Space) command object auditing 473 object authority required 416 object authority required 400 object authority required 416 DSPSRVSTS (Display Service Status) DSPNWSUSR (Display Network Server DSPPGMVAR (Display Program Variable) command authorized IBM-supplied user User) command command object authority required 401 object authority required 416 profiles 293

DSPSRVSTS (Display Service Status)	edit description	EDTRCYAP (Edit Recovery for Access
command (continued)	object authority required for	Paths) command
object authority required 428	commands 338	authorized IBM-supplied user
DSPSYSSTS (Display System Status)	Edit Document Library Object Authority	profiles 293
command	(EDTDLOAUT) command 277	object auditing 452
object authority required 436	Edit Library List (EDTLIBL)	object authority required 312
DSPSYSVAL (Display System Value)	command 183	EDTS36PGMA (Edit System/36 Program
command		· · · · · ·
	Edit Object Authority (EDTOBJAUT)	Attributes) command
object authority required 436	command 139, 274	object auditing 489
DSPTAP (Display Tape) command	Edit Object Authority display	object authority required 438
object authority required 392	displaying detail (*EXPERT user	EDTS36PRCA (Edit System/36 Procedure
DSPTAPCTG (Display Tape Cartridge)	option) 88, 89, 90	Attributes) command
command	editing	object auditing 472
object authority required 392	authorization list 146, 273	object authority required 438
DSPTRC (Display Trace) command	document library object (DLO)	EDTS36SRCA (Edit System/36 Source
object authority required 416	authority 277	Attributes) command
DSPTRCDTA (Display Trace Data)	library list 183	object auditing 472
command	object authority 139, 274	object authority required 438
object authority required 416	EDTAUTL (Edit Authorization List)	EDTWSOAUT (Edit Workstation Object
DSPUDFS (Display User-Defined File	command	Authority) command
System) command	description 273	object authority required 347
authorized IBM-supplied user	object auditing 453	eim association (EIMASSOC) parameter
profiles 293	object authority required 316	user profile 92
object authority required 442	using 146	EIMASSOC (eim association) parameter
DSPUSRPMN (Display User Permission)	EDTBCKUPL (Edit Backup List)	user profile 92
command	command	EJTEMLOUT (Eject Emulation Output)
object auditing 467	object authority required 403	command
object authority required 402	EDTCPCST (Edit Check Pending	object authority required 330
DSPUSRPRF (Display User Profile)	Constraints) command	EML3270 (Emulate 3270 Display)
command	authorized IBM-supplied user	command
description 276	profiles 293	object authority required 331
	•	0 0 1
object auditing 505	object auditing 473	EMLPRTKEY (Emulate Printer Key)
object authority required 445	object authority required 344	command
using 104	EDTDEVRSC (Edit Device Resources)	object authority required 331
using output file 268	command	emulation
DSPVTMAP (Display VT100 Keyboard	object authority required 422	object authority required for
Map) command	EDTDLOAUT (Edit Document Library	commands 330
object authority required 441	Object Authority) command	enabled (*ENABLED) user profile
DST (dedicated service tools)	description 277	status 62
auditing passwords 232	object auditing 464, 466	enabling
changing passwords 109	object authority required 334	QSECOFR (security officer) user
changing user ID 109	EDTDOC (Edit Document) command	profile 62
resetting password	object auditing 466	user profile
audit journal (QAUDJRN)	object authority required 334	automatically 619
entry 247	EDTF (Edit file) command 357	sample program 104
command description 275	EDTIGCDCT (Edit DBCS Conversion	ENCCPHK (Encipher Cipher Key)
DST password reset (DS) journal entry	Dictionary) command	command
type 247	object auditing 475	authorized IBM-supplied user
dump function	object authority required 337	profiles 293
*SERVICE (service) special	EDTLIBL (Edit Library List) command	object authority required 327
authority 70	object authority required 385	ENCFRMMSTK (Encipher from Master
DUPDKT (Duplicate Diskette) command	using 183	Key) command
object authority required 392	EDTOBJAUT (Edit Object Authority)	authorized IBM-supplied user
duplicate password (QPWDRQDDIF)	command	profiles 293
system value 42	description 274	object authority required 327
DUPOPT (Duplicate Optical) command	object auditing 451	
	· ·	encrypting
object authority required 406	object authority required 306	password 60 ENCTOMSTK (Engineer to Master Key)
DUPTAP (Duplicate Tape) command	using 139	ENCTOMSTK (Encipher to Master Key)
object authority required 392	EDTQST (Edit Questions and Answers)	command
	command	authorized IBM-supplied user
_	authorized IBM-supplied user	profiles 294
E	profiles 293	object authority required 327
Edit Authorization List (EDTAUTL)	object authority required 420	End Job (ENDJOB) command
command 146, 273	EDTRBDAP (Edit Rebuild Of Access	QINACTMSGQ system value 24
Edit Authorization List display	Paths) command	ENDASPBAL
displaying detail (*EXPERT user	authorized IBM-supplied user	authorized IBM-supplied user
option) 88, 89, 90	profiles 293	profiles 294
± // // // // // // // // // // // // //		

ENDASPBAL command 330 ending **ENDNWIRCY** (End Network Interface ENDCBLDBG (End COBOL Debug) audit function 261 Recovery) command object auditing 485 command auditing 50 ENDPASTHR (End Pass-Through) object authority required 384, 417 connection **ENDCHTSVR** audit journal (QAUDJRN) authorized IBM-supplied user entry 244 object authority required 332 profiles 294 disconnected job 33, 34 **ENDPEX (End Performance Explorer)** inactive job 23 ENDCLNUP (End Cleanup) command command object authority required 403 ENDIPSIFC (End IP over SNA Interface) authorized IBM-supplied user **ENDCLUNOD** command profiles 294 authorized IBM-supplied user authorized IBM-supplied user object authority required 411 profiles 294 profiles 294 **ENDPFRMON (End Performance** ENDCLUNOD command object authority required 314 Monitor) command object authority required 320 ENDJOB (End Job) command object authority required 413 **ENDCMNTRC** action auditing 498 ENDPFRTRC (End Performance Trace) object authority required 370 authorized IBM-supplied user command profiles 294 QINACTMSGQ system value 24 authorized IBM-supplied user **ENDCMNTRC** (End Communications ENDJOBABN (End Job Abnormal) profiles 294 ENDPJ (End Prestart Jobs) command Trace) command object authority required 428 authorized IBM-supplied user action auditing 498 ENDCMTCTL (End Commitment profiles 294 object authority required 370 ENDPRTEML (End Printer Emulation) Control) command object authority required 370 object authority required 322 **ENDJOBTRC** ENDCPYSCN (End Copy Screen) authorized IBM-supplied user object authority required 331 ENDRDR (End Reader) command profiles 294 command ENDJOBTRC (End Job Trace) command object authority required 428 object authority required 421 object authority required 411 ENDRJESSN (End RJE Session) command **ENDCRG** authorized IBM-supplied user ENDJRN (End Journal) command object authority required 425 profiles 294 object authority required 357, 375 ENDRQS (End Request) command object authority required 417 **ENDCTLRCY (End Controller Recovery)** ENDJRN (End Journaling) command object auditing 450 ENDS36 (End System/36) command command object auditing 459 ENDJRNAP (End Journal Access Path) object auditing 503 object authority required 326 ENDSBS (End Subsystem) command command ENDDBG (End Debug) command object authority required 375 object auditing 493 object authority required 435 ENDJRNPF (End Journal Physical File object authority required 417 ENDDBGSVR (End Debug Server) Changes) command ENDSRVJOB (End Service Job) command command object authority required 375 authorized IBM-supplied user authorized IBM-supplied user ENDJRNxxx (End Journaling) command profiles 294 object authority required 428 profiles 294 object auditing 478 ENDDBMON (End Database Monitor) ENDLINRCY (End Line Recovery) ENDSYS (End System) command object authority required 436 command command object authority required 413 object auditing 480 ENDSYSMGR (End System Manager) ENDDEVRCY (End Device Recovery) object authority required 391 command ENDLOGSVR (End Job Log Server) command authorized IBM-supplied user object auditing 460 command profiles 294 object authority required 330 object authority required 370 ENDTCP (End TCP/IP) command ENDDIRSHD (End Directory Shadow ENDMGDSYS (End Managed System) authorized IBM-supplied user System) command profiles 294 command authorized IBM-supplied user object authority required 331 object authority required 440 ENDDIRSHD (End Directory Shadowing) ENDTCPCNN (End TCP/IP Connection) profiles 294 **ENDMGRSRV** (End Manager Services) command command authorized IBM-supplied user object auditing 464 command ENDDSKRGZ (End Disk Reorganization) authorized IBM-supplied user profiles 294 profiles 294 object authority required 441 command object authority required 332 ENDMOD (End Mode) command **ENDTCPIFC** ENDGRPJOB (End Group Job) command object auditing 482 authorized IBM-supplied user object authority required 396 object authority required 370 profiles 294 **ENDHOSTSVR** ENDMSF (End Mail Server Framework) ENDTCPIFC (End TCP/IP Interface) authorized IBM-supplied user command profiles 294 authorized IBM-supplied user object authority required 440 ENDHOSTSVR (End Host Server) ENDTCPPTP (End Point-to-Point profiles 294 object authority required 391 command TCP/IP) command object authority required 348 ENDNFSSVR (End Network File System object authority required 440 ENDIDXMON (End Index Monitor) Server) command ENDTCPSRV (End TCP/IP Service) command authorized IBM-supplied user command authorized IBM-supplied user profiles 294 object authority required 440

object authority required 398

profiles 294

ENDTCPSVR (End TCP/IP Server)	example (continued)	file layout 512
command	restricting save and restore	file security
authorized IBM-supplied user	commands 191	SQL 213
profiles 294	RSTLICPGM (Restore Licensed	file transfer
ENDTRC (End Trace) command	Program) command 227	securing 190 filter
object authority required 428 ENDWCH (End Watch) command	securing output queues 188 exceeding	object authority required for
authorized IBM-supplied user	account limit	commands 346
profiles 294	audit journal (QAUDJRN)	filter (*FTR) object auditing 474
ENDWCH command	entry 252	finance
object authority required 428	exclude (*EXCLUDE) authority 113	object authority required for
ENDWTR (End Writer) command	execute (*EXECUTE) authority 112, 302	commands 346
object authority required 447	existence (*OBJEXIST) authority 112, 301	finance (QFNC) user profile 283
enhanced hardware storage protection	exit 46	flowchart
audit journal (QAUDJRN) entry 246	exit points	authority checking 148
security level 40 14	user profile 107	determining special environment 72
enrolling	expert (*EXPERT) user option 88, 89, 90,	device description authority 177
users 98	139	FNDSTRPDM (Find String Using PDM)
ENTCBLDBG (Enter COBOL Debug)	expiration	command
command	password (QPWDEXPITV system	object authority required 314
object authority required 384, 417	value) 39	folder
Entries	user profile	security shared 190
journal entries	displaying schedule 619	font resource (*FNTRSC) object
auditing 241	setting schedule 619	auditing 473
security 241 EV (Environment variable) file	extended wireless LAN configuration object authority required for	force conversion on restore (QFRCCVNRST)
layout 539	commands 338	system value 36
example	EXTPGMINF (Extract Program	force level
adopted authority	Information) command	audit records 51
application design 204, 207	object authority required 417	form definition (*FORMDF) object
authority checking process 167,	object administry required 11.	auditing 473
169		forms control table
assistance level	F	object authority required for
changing 64	-	commands 422
authority checking	faccessx (Determine file accessibility for a	FTP (File Transfer Protocol) command
adopted authority 167, 169	class of users by descriptor) command	object authority required 440
authorization list 170	object auditing 460 failure	full
group authority 164	sign-on	audit (QAUDJRN) journal
ignoring group authority 168	*ALLOBJ (all object) special	receiver 260
primary group 165	authority 177	full-screen help (*HLPFULL) user
public authority 166, 168	*SERVICE (service) special	option 90
changing	authority 177	
assistance levels 64	QSECOFR (security officer) user	•
system portion of library list 202	profile 177	G
controlling user library list 201	field authorities 115	GENCAT (Merge Message Catalog)
describing	field authority	command
library security 203	definition 112	object authority required 344
menu security 207	field-level security 210	GENCMDDOC (Generate Command
enabling user profile 104	FILDOC (File Document) command	Documentation) command
ignoring adopted authority 206	object auditing 466	object authority required 322
JKL Toy Company applications 195	object authority required 334	GENCPHK (Generate Cipher Key)
library list	file	command
changing system portion 202	journaling	authorized IBM-supplied user
controlling user portion 201	security tool 210 object authority required for	profiles 294 object authority required 327
program 201	commands 339	GENCRSDMNK (Generate Cross Domain
security risk 183	planning security 210	Key) command
library security	program-described	authorized IBM-supplied user
describing 203	holding authority when	profiles 294
planning 200	deleted 132	object authority required 327
menu security	securing	generic name
describing 207	critical 210	example 142
password validation exit program 46	fields 210	generic record(GR) file layout 540
password validation program 46 public authority	records 210	GENMAC (Generate Message
creating new objects 118	source	Authentication Code) command
creaming new objects 110	securing 217	authorized IBM-supplied user
	file (*FILE) object auditing 470	profiles 294

GENMAC (Generate Message	group (continued)	GRTOBJAUT (Grant Object Authority)
Authentication Code) command	primary (continued)	command 139
(continued)	introduction 5	affect on previous authority 142
object authority required 327	group (*GROUP) authority 135	description 274
GENPIN (Generate Personal	group authority	multiple objects 141
Identification Number) command	adopted authority 128	object auditing 450
authorized IBM-supplied user	authority checking example 164, 168	object authority required 307
profiles 294 object authority required 327	description 111 GRPAUT user profile parameter 80,	GRTUSRAUT (Grant User Authority) command
GENS36RPT (Generate System/36	122, 124	copying authority 101
Report) command	GRPAUTTYP user profile	description 276
authorized IBM-supplied user	parameter 81, 124	object auditing 504, 505
profiles 294	group authority type	object authority required 445
object authority required 396	GRPAUTTYP user profile	recommendations 145
GENS38RPT (Generate System/38	parameter 81	renaming profile 106
Report) command	group identification number (gid))	GRTUSRPMN (Grant User Permission)
authorized IBM-supplied user	restoring 224	command
profiles 294	group job	description 277
object authority required 396	adopted authority 129	object auditing 466
gid (group identification number)	group profile	object authority required 402
restoring 224	auditing	GRTWSOAUT (Grant Workstation Object
give descriptor (GS) file layout 544	*ALLOBJ special authority 233	Authority) command
give descriptor (GS) journal entry	membership 233	object authority required 347
type 250	password 233	GS (give descriptor) file layout 544
giving	authorization list	GS (give descriptor) journal entry
descriptor	comparison 216	type 250
audit journal (QAUDJRN) entry 250	comparison authorization list 216	
socket	GRPPRF user profile parameter	Н
audit journal (QAUDJRN)	changes when restoring	<del></del>
entry 250	profile 223	hardware
GO (Go to Menu) command	description 79	enhanced storage protection 14
object authority required 393	introduction 4, 57	object authority required for
GR (generic record) file layout 540	multiple	commands 422
Grant Object Authority (GRTOBJAUT)	planning 215	help full screen (*HLPFULL) user
command 139, 274	naming 59	option 90 help information
affect on previous authority 142	object ownership 122	displaying full screen (*HLPFULL
multiple objects 141	password 60	user option) 90
Grant User Authority (GRTUSRAUT)	planning 214	history (QHST) log
command	primary 123	using to monitor security 266
copying authority 101	planning 215	HLDCMNDEV (Hold Communications
description 276 recommendations 145	resource security 4, 111	Device) command
	supplemental SUPGRPPRF (supplemental	authorized IBM-supplied user
renaming profile 106 Grant User Permission (GRTUSRPMN)	groups) parameter 81	profiles 294
command 277	user profile	object auditing 460
granting	description 79	object authority required 330
authority using referenced object 145	user profile parameter	HLDDSTQ (Hold Distribution Queue)
object authority 274	changes when restoring	command
affect on previous authority 142	profile 223	authorized IBM-supplied user
multiple objects 141	GRPAUT (group authority) parameter	profiles 294 object authority required 333
user authority	user profile 80, 122, 124	HLDJOB (Hold Job) command
command description 276	GRPAUTTYP (group authority type)	object authority required 370
user permission 277	parameter	HLDJOBQ (Hold Job Queue) command
graphic symbols set (*GSS) object	user profile 81, 124	object auditing 476
auditing 475	GRPPRF (group profile) parameter	object authority required 373
graphical operations	See also group profile	HLDJOBSCDE (Hold Job Schedule Entry)
object authority required for	user profile	command
commands 347	description 79	object auditing 477
graphics symbol set	example 124	object authority required 373
object authority required for commands 347	GRTACCAUT (Grant Access Code Authority) command	HLDOUTQ (Hold Output Queue)
group	authorized IBM-supplied user	command
authority	profiles 294	object auditing 486
displaying 135	object auditing 466	object authority required 407
primary	object authority required 402	HLDRDR (Hold Reader) command
See also primary group	,	object authority required 421

HLDSPLF (Hold Spooled File) command	IBM-supplied user profile (continued)	inactive job message queue
action auditing 498	QDFTOWN (default owner)	(QINACTMSGQ) system value
object auditing 487	(continued)	value set by CFGSYSSEC
object authority required 433	description 124	command 628
HLDWTR (Hold Writer) command	QDOC (document) 283	inactive job time-out interval
object authority required 447	QDSNX (distributed systems node	(QINACTITV) system value
hold (*HOLD) delivery mode	executive) 283	value set by CFGSYSSEC
See also message queue	QFNC (finance) 283	command 628
user profile 84	QGATE (VM/MVS bridge) 283	incorrect password
home directory (HOMEDIR) parameter	QLPAUTO (licensed program	audit journal (QAUDJRN) entry 242,
user profile 91	automatic install) 283	243
HOMEDIR (home directory) parameter	QLPINSTALL (licensed program	incorrect user ID
user profile 91	install) 283	audit journal (QAUDJRN) entry 242
host server	QMSF (mail server framework) 283	information search index
object authority required for commands 348	QNFSANON (NFS user profile) 283	object authority required 368
commands 546	QPGMR (programmer) 283 QRJE (remote job entry) 283	initial library list  See also library list
	QSECOFR (security officer) 283	current library 65
1	QSNADS (Systems Network	job description (JOBD)
I	Architecture distribution	user profile 78
IBM-supplied objects	services) 283	recommendations 185
securing with authorization list 118	QSPL (spool) 283	relationship to library list for job 183
IBM-Supplied Service Tools User ID Reset	QSPLJOB (spool job) 283	risks 185
(DS) file layout 538	QSRV (service) 283	initial menu
IBM-supplied user profile	QSRVBAS (service basic) 283	*SIGNOFF 66
See also specific profiles	QSYS (system) 283	changing 66
ADSM (QADSM) 283	QSYSOPR (system operator) 283	preventing display 66
AFDFTUSR (QAFDFTUSR) 283	QTCP (TCP/IP) 283	recommendation 67
AFOWN (QAFOWN) 283	QTMPLPD (TCP/IP printing	user profile 66
AFUSR (QAFUSR) 283	support) 283	initial menu (INLMNU) parameter
auditing 232	QTSTRQS (test request) 283	See also initial menu
authority profile (QAUTPROF) 283	QUSER (workstation user) 283	user profile 66
automatic install (QLPAUTO) 283	remote job entry (QRJE) 283	initial program (INLPGM) parameter
basic service (QSRVBAS) 283	restoring 224	changing 65
BRM (QBRMS) 283 BRM user profile (QBRMS) 283	restricted commands 289	user profile 65
BRM user profile (QBRMS) 283 changing password 108	security officer (QSECOFR) 283	initial program load (IPL)
database share (QDBSHR) 283	service (QSRV) 283	*JOBCTL (job control) special
DCEADM (QDCEADM) 283	service basic (QSRVBAS) 283	authority 69
default owner (QDFTOWN)	SNA distribution services	INLMNU (initial menu) parameter
default values 283	(QSNADS) 283	See also initial menu
description 124	spool (QSPL) 283	user profile 66
default values table 281	spool job (QSPLJOB) 283	INLPGM (initial program) parameter
distributed systems node executive	system (QSYS) 283	changing 65
(QDSNX) 283	system operator (QSYSOPR) 283	user profile 65
document (QDOC) 283	TCP/IP (QTCP) 283	INSPTF (Install Program Temporary Fix)
finance (QFNC) 283	TCP/IP printing support	command
IBM authority profile	(QTMPLPD) 283	authorized IBM-supplied user
(QAUTPROF) 283	test request (QTSTRQS) 283	profiles 294
install licensed programs	VM/MVS bridge (QGATE) 283 workstation user (QUSER) 283	object authority required 428 INSRMTPRD (Install Remote Product)
(QLPINSTALL) 283	ignoring	command
mail server framework (QMSF) 283	adopted authority 131	authorized IBM-supplied user
NFS user profile (QNFSANON) 283	image	profiles 294
programmer (QPGMR) 283	object authority required for	install licensed program (QLPINSTALL)
purpose 108	commands 348	user profile
QADSM (ADSM) 283	inactive	default values 283
QAFDFTUSR (AFDFTUSR) 283	job	restoring 224
QAFOWN (AFOWN) 283	message queue (QINACTMSGQ)	install licensed program automatic
QAFUSR (AFUSR) 283	system value 24	(QLPAUTO) user profile
QAUTPROF (database share) 283	time-out interval (QINACTITV)	restoring 224
QAUTPROF (IBM authority	system value 23	installing
profile) 283	user	operating system 229
QBRMS (BRM user profile) 283	listing 269	INSWNTSVR command
QBRMS (BRM) 283	inactive job	authorized IBM-supplied user
QDBSHR (database share) 283	message (CPI1126) 24	profiles 294
QDCEADM (DCEADM) 283 QDFTOWN (default owner)		
QDITOWIN (actault OWHEL)		

default values 283

integrated file system object authority required for commands 349	IPL (initial program load)  *JOBCTL (job control) special authority 69	job description <i>(continued)</i> object authority required for commands 372
integrity 1	IR (IP rules actions) file layout 547	printing security-relevant
checking	IS (Internet security management) file	parameters 623
auditing use 235	layout 548	protecting 13
description 270, 276	iSeries Access	protecting 13 protecting system resources 192
interactive data definition	controlling sign-on 27	QDFTJOBD (default) 79
object authority required for	file transfer security 190	recommendations 79
commands 367	message function security 190	restoring
interactive data definition utility (IDDU)	shared folder security 190	audit journal (QAUDJRN)
object auditing 468	virtual printer security 190	entry 246
interactive job	virtual printer security 100	security issues 182
routing		security issues 102 security level 40 13
SPCENV (special environment)	J	USER parameter 181
parameter 72	•	user profile 78
security when starting 175	jar files	workstation entry 181
intermediate assistance level 58, 64	class files 217	job description (*JOBD) object
internal control block	Java	auditing 476
preventing modification 17	object authority required for	job description (JOBD) parameter
	commands 369	
Internet security management (GS) file	JD (job description change) file	See also job description
layout 548 Internet user	layout 550	user profile 78
	JD (job description change) journal entry	job description change (JD) file
validation lists 218	type 250	layout 550
interprocess communication actions (IP)	JKL Toy Company	job description change (JD) journal entry
file layout 546	diagram of applications 195	type 250
interprocess communications	job	job description violation
incorrect	*JOBCTL (job control) special	audit journal (QAUDJRN) entry 13
audit journal (QAUDJRN)	authority 69	job initiation
entry 242	automatic cancelation 33, 34	adopted authority 176
interprocess communications (IP) journal	changing	Attention-key-handling program 176
entry type 242	adopted authority 130	job queue
INZDKT (Initialize Diskette) command	audit journal (QAUDJRN)	*JOBCTL (job control) special
object authority required 392	entry 243	authority 69
INZDSTQ (Initialize Distribution Queue)	disconnected job interval	*OPRCTL (operator control)
command	(QDSCJOBITV) system value 33	parameter 69
authorized IBM-supplied user	inactive	*SPLCTL (spool control) special
profiles 294	time-out interval (QINACTITV)	authority 69
object authority required 333 INZNWSCFG command	system value 23	object authority required for commands 372
	object authority required for	
authorized IBM-supplied user	commands 369	printing security-relevant
profiles 294	restricting to batch 193	parameters 279, 625 job queue (*JOBQ) auditing 476
object authority required 401	scheduling 192	
INZOPT (Initialize Optical) command	security when starting 175	job schedule
object authority required 406 INZPFM (Initialize Physical File Member)	verify object on restore	object authority required for commands 373
command	(QVFYOBJRST) system value 34	job scheduler (*JOBSCD) auditing 477
object auditing 472	job accounting	JOBACN (job action) network
object auditing 472 object authority required 344	user profile 82	attribute 189, 235
INZSYS (Initialize System) command	job action (JOBACN) network	JOBD (job description) parameter
authorized IBM-supplied user	attribute 189, 235	See also job description
profiles 294	job change (*JOBDTA) audit level 243	user profile 78
object authority required 389	job change (JS) file layout 550	journal
INZTAP (Initialize Tape) command	job change (JS) journal entry type 243	audit (QAUDJRN)
object authority required 392	job control (*JOBCTL) special authority	introduction 235
IP (change ownership) journal entry	functions allowed 69	displaying
type 250	output queue parameters 187	auditing file activity 210, 267
IP (interprocess communication actions)	priority limit (PTYLMT) 78	managing 260
file layout 546	risks 69	object authority required for
IP (interprocess communications) journal	job description	commands 374
	changing	
entry type 242 IP rules actions (IR) file layout 547	audit journal (QAUDJRN)	using to monitor security 267 working with 268
IPC object	entry 250	journal (*JRN) auditing 477
changing	communications entry 181	journal attributes
audit journal (QAUDJRN)	default (QDFTJOBD) 79	working with 268
entry 250	displaying 234	Journal Entries
	monitoring 234	security auditing 241

journal entry	length of password 41, 42	library (continued)
sending 259	level 10	public authority
journal receiver	QSECURITY (security level) system	specifying 136
changing 261	value 9	QRETSVRSEC (retain server security)
deleting 261	level 20	value 26
detaching 260, 261	QSECURITY (security level) system	QTEMP (temporary)
managing 260	value 10	security level 50 16
maximum storage (MAXSTG) 77	level 30	restoring 221
object authority required for	QSECURITY (security level) system	retain server security (QRETSVRSEC)
commands 377	value 10	value 26
storage needed 77	level 40	saving 221
journal receiver (*JRNRCV) auditing 479	internal control blocks 17	security
journal receiver, audit	QSECURITY (security level) system	adopted authority 115
creating 258	value 11	description 115
naming 258	level 50	designing 200
saving 261	internal control blocks 17	example 200
storage threshold 260	message handling 16	guidelines 200
journal, audit	QSECURITY (security level) system	risks 114
See also audit (QAUDJRN) journal	value 16	library (*LIB) auditing 479
working with 261	QTEMP (temporary) library 16	library list
journaling	validating parameters 14	adding entries 183, 185
security tool 210	level of security (QSECURITY) system	adopted authority 115
JRNAP (Journal Access Path) command	value	changing 183
object authority required 375	comparison of levels 7	current library
JRNAP (Start Journal Access Path)	level 20 10	description 183
command	level 30 10	recommendations 185
object auditing 478	level 40 11	user profile 65
JRNPF (Journal Physical File) command	level 50 16	definition 183
object authority required 375	overview 7	editing 183
JRNPF (Start Journal Physical File)	recommendations 9	job description (JOBD)
command	special authority 8	user profile 78
object auditing 478	user class 8	monitoring 234
JS (job change) file layout 550	library	product library
JS (job change) journal entry type 243	authority	description 183
	definition 5	recommendations 184
17	description 115	recommendations 184
K	new objects 118	removing entries 183
kerberos authentication (X0) file	AUTOCFG (automatic device	security risks 183
layout 605	configuration) value 31	system portion
keyboard buffering	automatic device configuration	changing 202
KBDBUF user profile parameter 76	(AUTOCFG) value 31	description 183
QKBDBUF system value 76	create authority (CRTAUT) parameter	recommendations 184
keylock security 2	description 118	user portion
keylock switch	example 124	controlling 201
auditing 232	risks 119	description 183
KF (key ring file) file layout 554	specifying 136	recommendations 185
	create object auditing (CRTOBJAUD)	licensed program
	value 54	automatic install (QLPAUTO) user
L	creating 136	profile
	CRTAUT (create authority) parameter	description 283
LANGID (language identifier) parameter	description 118	install (QLPINSTALL) user profile
SRTSEQ user profile parameter 87	example 124	default values 283
user profile 87	risks 119	object authority required for
language identifier	specifying 136	commands 389
LANGID user profile parameter 87	CRTOBJAUD (create object auditing)	restoring
QLANGID system value 87	value 54	recommendations 227
SRTSEQ user profile parameter 87	current 64	security risks 227
language, programming	designing 200	licensed program automatic install
object authority required for	listing	(QLPAUTO) user profile
commands 378	all libraries 269	restoring 224
large profiles	contents 269	licensed program install (QLPINSTALL)
planning applications 201	object authority required for	user profile
large user profile 269	commands 384	restoring 224
LCLPWDMGT (local password	object ownership 217	limit capabilities (LMTCPB) parameter
management) parameter 75	planning 200	See also limiting capabilities
LD (link, unlink, search directory) file	printing list of subsystem	user profile 66
layout 557	descriptions 279	

limit characters (QPWDLMTCHR) system	Lists, Delete Validation 218	management (*OBJMGT) authority
value 43	LMTDEVSSN (limit device sessions)	object 112, 301
limit repeated characters	parameter	managing
(QPWDLMTREP) system value 43	See also limiting device sessions	audit journal 259
		•
limit security officer (QLMTSECOFR)	user profile 75	maximum
system value	LNKDTADFN (Link Data Definition)	auditing 232
value set by CFGSYSSEC	command	length of password (QPWDMAXLEN
command 628	object auditing 468	system value) 42
	·	
limiting	object authority required 367	sign-on attempts (QMAXSIGN)
capabilities 66	local socket (*SOCKET) auditing 495	system value 232
changing Attention-key-handling	locale	description 25
program 86	object authority required for	size
changing current library 65, 185	commands 391	audit (QAUDJRN) journal
changing initial menu 66	LOCALE (user options) parameter	receiver 260
changing initial program 65	user profile 89	storage (MAXSTG) parameter
commands allowed 67	LODIMGCLG	authority holder 124
functions allowed 67	authorized IBM-supplied user	group ownership of objects 122
listing users 268	profiles 295	journal receiver 76
LMTCPB user profile	LODIMGCLG command	restore operation 76
•		
parameter 66	object authority required 348	user profile 76
command line use 66	LODIMGCLGE command	maximum sign-on attempts
device sessions	object authority required 348	(QMAXSIGN) system value
auditing 233	LODOPTFMW	value set by CFGSYSSEC
e		command 628
LMTDEVSSN user profile	authorized IBM-supplied user	
parameter 75	profiles 295	maximum storage (MAXSTG) parameter
recommendations 76	LODOPTFMW command	authority holder
device sessions (QLMTDEVSSN)	object authority required 406	transferred to QDFTOWN (default
system value	LODPTF (Load Program Temporary Fix)	owner) 124
description 24	command	group ownership of objects 122
•		
disk usage (MAXSTG) 76	authorized IBM-supplied user	journal receiver 76
security officer (QLMTSECOFR)	profiles 295	restore operation 76
changing security levels 11	object authority required 428	user profile 76
security officer (QLMTSECOFR)	LODQSTDB (Load Question-and-Answer	MAXSTG (maximum storage) parameter
system value	Database) command	authority holder
0		· ·
auditing 232	authorized IBM-supplied user	transferred to QDFTOWN (default
authority to device	profiles 295	owner) 124
descriptions 177	object authority required 420	group ownership of objects 122
description 25	logging off	journal receiver 76
sign-on process 179	network	restore operation 76
· .		•
sign-on	audit journal (QAUDJRN)	user profile 76
attempts (QMAXSGNACN) system	entry 244	media
value 26	logging on	object authority required for
attempts (QMAXSIGN) system	network	commands 391
value 25	audit journal (QAUDJRN)	memory
		· ·
multiple devices 24	entry 244	sharing control
sign-on attempts	logical file	QSHRMEMCTL (share memory
auditing 232, 235	securing	control) system value 29
use of system resources	fields 210	menu
priority limit (PTYLMT)	records 210	See also initial menu
parameter 77	LPR (Line Printer Requester) command	changing
line description	object authority required 440	PRDLIB (product library)
object authority required for		parameter 185
commands 389		security risks 185
line description (*LIND) auditing 480	M	creating
link	IVI	PRDLIB (product library)
	mail	
object authority required for	handling	parameter 185
commands 318, 349	audit journal (QAUDJRN)	security risks 185
listing		designing for security 203
all libraries 269	entry 245	initial 66
authority holders 132	mail actions (ML) file layout 559	object authority required for
library contents 269	mail actions (ML) journal entry type 245	commands 392
	mail server framework	
selected user profiles 268	object authority required for	security tools 619
system values 232	commands 391	user profile 66
user profile		menu (*MENU) auditing 481
individual 104	mail server framework (QMSF) user	Merge Source (Merge Source) command
summary list 104	profile 283	object authority required 344
Lists, Create Validation 218	mail services	jj required off
LISES, CICATE VARIABION &10	action auditing 481	

message	MGRS36DSPF	module (*MODULE) auditing 482
inactive timer (CPI1126) 24	authorized IBM-supplied user	monitoring
object authority required for	profiles 295	*ALLOBJ (all object) special
commands 394	MGRS36ITM (Migrate System/36 Item)	authority 233
print notification (*PRTMSG user	command	See also auditing
option) 90	authorized IBM-supplied user	adopted authority 234
printing completion (*PRTMSG user	profiles 295	authority
option) 90	object authority required 396	user profiles 234
restricting content 16	MGRS36LIB	authorization 234
security	authorized IBM-supplied user	checklist for 231
monitoring 266	profiles 295	communications 235
status	MGRS36MNU	encryption of sensitive data 235
displaying (*STSMSG user	authorized IBM-supplied user	group profile
option) 90	profiles 295	membership 233
not displaying (*NOSTSMSG user	MGRS36MSGF	password 233
option) 90	authorized IBM-supplied user	IBM-supplied user profiles 232
message description	profiles 295	inactive users 233
object authority required for	MGRS36QRY	job descriptions 234
commands 394	authorized IBM-supplied user	library lists 234
message file	profiles 295	limit capabilities 233
object authority required for	MGRS36RPG	message
commands 395	authorized IBM-supplied user	security 266
message file (*MSGF) auditing 482	profiles 295	methods 266
message function (iSeries Access)	MGRS36SEC	network attributes 235
securing 190	authorized IBM-supplied user	object authority 269
message queue	profiles 295	object integrity 270
*BREAK (break) delivery mode 84	MGRS38OBJ (Migrate System/38 Objects)	overview 231
*DFT (default) delivery mode 84	command	password controls 233
*HOLD (hold) delivery mode 84	authorized IBM-supplied user	physical security 232
*NOTIFY (notify) delivery mode 84	profiles 295	program failure 270
automatic creation 83	object authority required 396	programmer authorities 233
default responses 84	MGRTCPHT (Merge TCP/IP Host Table)	remote sign-on 235
inactive job (QINACTMSGQ) system	command	security officer 271
value 24	object authority required 441	sensitive data
object authority required for	MIGRATE	authority 234
commands 395	authorized IBM-supplied user	encrypting 235
QSYSMSG 266	profiles 295	sign-on without user ID and
QMAXSGNACN (action when	migrating	password 234
attempts reached) system	security level (QSECURITY) system	system values 232
value 26	value	unauthorized access 235
QMAXSIGN (maximum sign-on	level 10 to level 20 10	unauthorized programs 235
attempts) system value 25	level 20 to level 30 10	unsupported interfaces 235
recommendation	level 20 to level 30 10	user profile
	level 20 to level 40 13	administration 233
MSGQ user profile parameter 84	level 30 to level 30 17	using
restricting 182 severity (SEV) parameter 84	level 30 to level 40 15	journals 267
	level 30 to level 40 13	
user profile	level 40 to level 20 10	QHST (history) log 266
deleting 101 delivery (DLVRY) parameter 84	migration	QSYSMSG message queue 235 MOUNT (Add Mounted File System)
recommendations 84	0	command
	object authority required for commands 395	
severity (SEV) parameter 84		object authority required 442
message queue (*MSGQ) auditing 483	minimum length of password	MOUNT (Add Mounted File System)
message queue (MSGQ) parameter	(QPWDMINLEN) system value 41	command) command
See also message queue	ML (mail actions) file layout 559	object authority required 399
user profile 83	ML (mail actions) journal entry type 245	MOV
MGRS36 (Migrate System/36) command	mode description	object authority required 358
authorized IBM-supplied user	object authority required for	MOV (Move) command
profiles 295	commands 396	object auditing 461, 500, 502
MGRS36APF	mode description (*MODD)	MOVDOC (Move Document) command
authorized IBM-supplied user	auditing 482	object auditing 466
profiles 295	mode of access	object authority required 334
MGRS36CBL	See also authority	moving
authorized IBM-supplied user	definition 112	object
profiles 295	module	audit journal (QAUDJRN)
MGRS36DFU	binding directory 396	entry 245
authorized IBM-supplied user	object authority required for	spooled file 186
profiles 295	commands 396	

MOVOBJ (Move Object) command object auditing 450, 480 object authority required 307 MRGDOC (Merge Document) command object auditing 464, 466 object authority required 335 MRGFORMD (Merge Form Description) command object authority required 314 MRGMSGF (Merge Message File) command object auditing 483 object authority required 395 MSGQ (message queue) parameter See also message queue user profile 83 multiple group example 171 planning 215	network attribute (continued) JOBACN (job action) 189, 235 object authority required for commands 397 PC Support (PCSACC) 235 PCSACC (client request access) 189 PCSACC (PC Support access) 235 printing security-relevant 623 network attribute change (NA) file layout 559 network attribute change (NA) journal entry type 250 network attributes printing security- communications 280 printing security-relevant 280 network interface (*NWID) auditing 485 network interface description object authority required for commands 399	node group (*NODGRP) auditing 484 node list object authority required for commands 402 node list (*NODL) auditing 484 notification, message DLVRY (message queue delivery) parameter user profile 84 no status message (*NOSTSMSG) user option 90 notify (*NOTIFY) delivery mode See also message queue user profile 84 number required in password 44 numeric character required in password 44 numeric password 60 numeric user ID 59
NI	network log on and off (VN) file	
N	layout 600 network log on or off (VN) journal entry	0
NA (network attribute change) file	type 244	OBJAUD (object auditing) parameter
layout 559 NA (network attribute change) journal	network password error (VP) file	user profile 93 object
entry type 250	layout 602	(*Mgt) authority 112
naming	network password error (VP) journal entry type 243	(*Ref) authority 112
audit journal receiver 258	network profile	add (*ADD) authority 112, 302
group profile 59 user profile 59	changing	altered checking 270
national language version (NLV)	audit journal (QAUDJRN)	assigning authority and
command security 210	entry 251	ownership 124
ND (APPN directory) file layout 559	network profile change (VU) file layout 604	auditing
NE (APPN end point) file layout 560	network profile change (VU) journal	changing 71
NetBIOS description object authority required for	entry type 251	default 256 authority
commands 397	network resource access (VR) file	*ALL (all) 113, 302
NetBIOS description (*NTBD)	layout 603 Network Server	*CHANGE (change) 113, 302
auditing 485	object authority required for	*USE (use) 113, 302
NETSTAT (Network Status) command	commands 400	changing 138
object authority required 441 network	network server configuration	commonly used subsets 113 new 119
logging off	object authority required for	new object 118
audit journal (QAUDJRN)	commands 401 network server description	storing 222
entry 244	object authority required for	system-defined subsets 113
logging on audit journal (QAUDJRN)	commands 402	using referenced 145 authority required for
entry 244	network server description (*NWSD)	commands 305
password	auditing 486	controlling access 12
audit journal (QAUDJRN)	network spooled file sending 186	default owner (QDFTOWN) user
entry 243	new object	profile 124
network attribute *SECADM (security administrator)	authority	delete (*DLT) authority 112, 302
special authority 69	CRTAUT (create authority)	displaying originator 123
changing	parameter 118, 136	domain attribute 12
audit journal (QAUDJRN)	GRPAUT (group authority) parameter 80, 122	execute (*EXECUTE) authority 112,
entry 250	GRPAUTTYP (group authority	302
command 189 client request access (PCSACC) 189	type) parameter 81	existence (*OBJEXIST) authority 112, 301
command for setting 280, 627	authority (QCRTAUT system	failure of unsupported interface 12
DDM request access (DDMACC) 190	value) 22 authority (QUSEADPAUT system	management (*OBJMGT)
DDMACC (DDM request access) 190	value) 30	authority 112, 301
DDMACC (distributed data	authority example 124	non-IBM
management access) 235 distributed data management access	ownership example 124	printing list 279 operational (*OBJOPR) authority 112,
(DDMACC) 235	NLV (national language version)	301
job action (JOBACN) 189, 235	command security 210	

object (continued)	object auditing (continued)	object auditing (continued)
ownership	*GSS (graphic symbols set)	*SVRSTG (server storage space)
See also object ownership	object 475	object 499
introduction 4	*IGCDCT (double-byte character set	*SYMLNK (symbolic link) object 502
primary group 101, 123	dictionary) object 475	*TBL (table) object 503
printing	*IGCSRT (double-byte character set	*USRIDX (user index) object 504
adopted authority 623	sort) object 475	*USRPRF (user profile) object 504
authority source 623	*IGCTBL (double-byte character set	*USRQ (user queue) object 505
non-IBM 623	table) object 475	*USRSPC (user space) object 505 *VLDL (validation list) object 506
read (*READ) authority 112, 302 restoring 221, 224	*JOBD (job description) object 476 *JOBQ (job queue) object 476	alert table (*ALRTBL) object 452
saving 221	*JOBSCD (job scheduler) object 477	authority holder (*AUTHLR)
securing with authorization list 147	*JRN (journal) object 477	object 453
state attribute 12	*JRNRCV (journal receiver)	authorization list (*AUTL) object 453
storing	object 479	binding directory (*BDNDIR)
authority 222	*LIB (library) object 479	object 453
update (*UPD) authority 112, 302	*LIND (line description) object 480	C locale description (*CLD)
user domain	*MENU (menu) object 481	object 455
restricting 16	*MODD (mode description)	change request description (*CRQD)
security exposure 16	object 482	object 455
working with 274	*MODULE (module) object 482	changing
object alter (*OBJALTER) authority 112,	*MSGF (message file) object 482	command description 274, 277
301	*MSGQ (message queue) object 483	chart format (*CHTFMT) object 454
object auditing	*NODGRP (node group) object 484	Class (*CLS) object 456
*ALRTBL (alert table) object 452	*NODL (node list) object 484	class-of-service description (*COSD)
*AUTHLR (authority holder)	*NTBD (NetBIOS description)	object 457
object 453	object 485	Command (*CMD) object 456
*AUTL (authorization list) object 453 *BNDDIR (binding directory)	*NWID (network interface) object 485	common operations 449 communications side information
object 453	*NWSD (network server description)	(*CSI) object 458
*CFGL (configuration list) object 454	object 486	configuration list (*CFGL) object 454
*CHTFMT (chart format) object 454	*OUTQ (output queue) object 486	connection list (*CNNL) object 457
*CLD (C locale description)	*OVL (overlay) object 487	controller description (*CTLD)
object 455	*PAGDFN (page definition)	object 459
*CLS (Class) object 456	object 487	cross system product map (*CSPMAP)
*CMD (Command) object 456	*PAGSEG (page segment) object 488	object 458
*CNNL (connection list) object 457	*PDG (print descriptor group)	cross system product table (*CSPTBL)
*COSD (class-of-service description)	object 488	object 458
object 457	*PGM (program) object 488	data area (*DTAARA) object 467
*CRQD (change request description)	*PNLGRP (panel group) object 489	data dictionary (*DTADCT)
object 455	*PRDAVL (product availability) object 490	object 468
*CSI (communications side information) object 458	*PRDDFN (product definition)	data queue (*DTAQ) object 468 definition 254
*CSPMAP (cross system product map)	object 490	device description (*DEVD)
object 458	*PRDLOD (product load) object 490	object 459
*CSPTBL (cross system product table)	*QMFORM (query manager form)	directory (*DIR) object 460
object 458	object 490	displaying 256
*CTLD (controller description)	*QMQRY (query manager query)	document (*DOC) object 464
object 459	object 491	double byte-character set dictionary
*DEVD (device description)	*QRYDFN (query definition)	(*IGCDCT) object 475
object 459	object 491	double byte-character set sort
*DIR (directory) object 460	*RCT (reference code table)	(*IGCSRT) object 475
*DOC (document) object 464	object 492	double byte-character set table
*DTAARA (data area) object 467	*S36 (S/36 machine description)	(*IGCTBL) object 475
*DTADCT (data dictionary) object 468	object 503 *SBSD (subsystem description)	edit description (*EDTD) object 469 exit registration (*EXITRG) object 469
*DTAQ (data queue) object 468	object 493	file (*FILE) object 470
*EDTD (edit description) object 469	*SCHIDX (search index) object 494	filter (*FTR) object 474
*EXITRG (exit registration) object 469	*SOCKET (local socket) object 495	folder (*FLR) object 464
*FCT (forms control table) object 470	*SPADCT (spelling aid dictionary)	font resource (*FNTRSC) object 473
*FILE (file) object 470	object 497	form definition (*FORMDF)
*FLR (folder) object 464	*SQLPKG (SQL package) object 498	object 473
*FNTRSC (font resource) object 473	*SRVPGM (service program)	forms control table (*FCT) object 470
*FORMDF (form definition)	object 499	graphic symbols set (*GSS)
object 473	*SSND (session description)	object 475
*FTR (filter) object 474	object 499	job description (*JOBD) object 476
	*STMF (stream file) object 499	job queue (*JOBQ) object 476

object auditing (continued) object auditing (OBJAUD) parameter object authority (continued) job scheduler (\*JOBSCD) object 477 user profile 93 finance commands 346 journal (\*JRN) object 477 object authority format on save media 222 \*ALLOBJ (all object) special journal receiver (\*JRNRCV) forms control table commands 422 object 479 authority 68 granting 274 library (\*LIB) object 479 \*SAVSYS (save system) special affect on previous authority 142 line description (\*LIND) object 480 multiple objects 141 authority 70 local socket (\*SOCKET) object 495 access code commands 402 graphical operations 347 menu (\*MENU) object 481 access path recovery 312 graphics symbol set commands 347 message file (\*MSGF) object 482 Advanced Function Printing hardware commands 422 message queue (\*MSGQ) object 483 commands 312 host server 348 information search index AF\_INET sockets over SNA 313 mode description (\*MODD) object 482 alert commands 314 commands 368 module (\*MODULE) object 482 alert description commands 314 interactive data definition 367 NetBIOS description (\*NTBD) alert table commands 314 job commands 369 job description commands 372 object 485 analyzing 269 authority holder commands 316 network interface (\*NWID) job queue commands 372 object 485 authorization list commands 316 job schedule commands 373 network server description (\*NWSD) backup commands 403 journal commands 374 object 486 binding directory 317 journal receiver commands 377 node group (\*NODGRP) object 484 change request description language commands 378 node list (\*NODL) object 484 commands 317 library commands 384 output queue (\*OUTQ) object 486 changing licensed program commands 389 overlay (\*OVL) object 487 audit journal (QAUDJRN) line description commands 389 page definition (\*PAGDFN) entry 249 locale commands 391 object 487 procedures 138 mail server framework page segment (\*PAGSEG) object 488 chart format commands 317 commands 391 panel group (\*PNLGRP) object 489 class commands 318 media commands planning 254 class-of-service description menu commands 392 print descriptor group (\*PDG) message commands 394 commands 318 object 488 cleanup commands 403 message description commands 394 product availability (\*PRDAVL) commands 274 message file commands 395 object 490 commitment control commands 322 message queue commands 395 product definition (\*PRDDFN) common object commands 305 migration commands 395 communications side information object 490 mode description commands 396 product load (\*PRDLOD) object 490 commands 322 NetBIOS description commands 397 program (\*PGM) object 488 configuration commands 323 network attribute commands 397 query definition (\*QRYDFN) configuration list commands 324 network interface description object 491 connection list commands 324 commands 399 query manager form (\*QMFORM) controller description commands 325 Network Server commands 400 object 490 cryptography commands 326 network server configuration query manager query (\*QMQRY) data area commands 327 commands 401 object 491 data queue commands 328 network server description reference code table (\*RCT) definition 112 commands 402 detail, displaying (\*EXPERT user object 492 node list commands 402 S/36 machine description (\*S36) option) 88, 89, 90 online education commands 403 object 503 device description commands 328 Operational Assistant commands 403 search index (\*SCHIDX) object 494 directory commands 331 optical commands 404 display station pass-through server storage space (\*SVRSTG) output queue commands object 499 commands 332 package commands 408 service program (\*SRVPGM) displaying 269, 274 panel group commands 392 displaying detail (\*EXPERT user object 499 performance commands 408 session description (\*SSND) option) 88, 89, 90 printer output commands 432 object 499 distribution commands 332 printer writer commands 447 spelling aid dictionary (\*SPADCT) distribution list commands 333 problem commands 414 object 497 document commands 333 program commands 415 SQL package (\*SQLPCK) object 498 document library object (DLO) program temporary fix (PTF) stream file (\*STMF) object 499 commands 333 commands 427 subsystem description (\*SBSD) double-byte character set programming language object 493 commands 337 commands 378 symbolic link (\*SYMLNK) object 502 edit description commands 338 PTF (program temporary fix) table (\*TBL) object 503 editing 139, 274 commands 427 user index (\*USRIDX) object 504 emulation commands 330 Query Management/400 user profile (\*USRPRF) object 504 extended wireless LAN configuration commands 418 user queue (\*USRQ) object 505 commands 338 question and answer commands 420 user space (\*USRSPC) object 505 file commands 339 reader commands 421 validation list (\*VLDL) object 506 filter commands 346

object authority (continued)	object ownership (continued)	output queue (continued)
relational database directory	deleting	*SPLCTL (spool control) special
commands 421	owner profile 101, 122	authority 69
reply list commands 436	description 122	AUTCHK (authority to check)
required for *CMD commands 321	flowchart 153	parameter 187
resource commands 422	group profile 122	authority to check (AUTCHK)
revoking 274	managing	parameter 187
RJE (remote job entry)	owner profile size 122	changing 186
commands 422	private authority 111	creating 186, 188
search index commands 368	responsibilities 234	display data (DSPDTA)
security attributes commands 426	restoring 221, 224	parameter 186
security audit commands 426	saving 221	DSPDTA (display data)
server authentication 427	working with 143, 274	parameter 186
service commands 427	object reference (*OBJREF)	object authority required for
session commands 422	authority 112, 302	commands 407
spelling aid dictionary	object restore (OR) journal entry	operator control (OPRCTL)
commands 431	type 246	parameter 187
sphere of control commands 432	object signing 3	OPRCTL (operator control)
spooled file commands 432	objective	parameter 187
storing 222	availability 1	•
S .	•	printing security-relevant parameters 279, 625
subsystem commands 434	confidentiality 1	*
system commands 436	integrity 1	securing 186, 188
system reply list commands 436	objects by primary group	user profile 85
system value commands 436	working with 123	working with description 186
System/36 environment	office services	output queue (*OUTQ) auditing 486
commands 437	action auditing 481	output queue (OUTQ) parameter
table commands 439	office services (*OFCSRV) audit	See also output queue
TCP/IP (Transmission Control	level 245, 463, 481	user profile 85
Protocol/Internet Protocol)	OM (object management) journal entry	OUTQ (output queue) parameter
commands 440	type 245	See also output queue
text index commands 402	on behalf	user profile 85
token-ring commands 391	auditing 481	overlay (*OVL) auditing 487
upgrade order information	online education	Override commands 213
commands 442	object authority required for	OVRMSGF (Override with Message File)
user index, queue, and space	commands 403	command
commands 442	online help information	object auditing 483
user permission commands 402	displaying full screen (*HLPFULL	OW (ownership change) file layout 566
user profile commands 442, 443	user option) 90	OW (ownership change) journal entry
validation list 446	operating system	type 250
workstation customizing object	security installation 229	owner
commands 446	operational (*OBJOPR) authority 112,	See also object ownership
writer commands 447	301	See also ownership
object description	Operational Assistant Attention Program	OWNER user profile parameter
displaying 274	Attention-key-handling program 86	description 122
object domain	Operational Assistant commands	OWNER (owner) parameter
definition 12	object authority required for	user profile 124
displaying 12	commands 403	owner authority
object integrity	OPNDBF (Open Database File) command	flowchart 153
auditing 270	object authority required 344	ownership
e e e e e e e e e e e e e e e e e e e	0 0 1	•
object management (*OBJMGT) audit level 245	OPNQRYF (Open Query File) command	See also object ownership
	object authority required 344	adopted authority 130
object management (OM) journal entry	OPRCTL (operator control)	ALWOBJDIF (allow object differences)
type 245	parameter 187	parameter 224
object ownership	optical	assigning to new object 124
adopted authority 130	object authority required for	change when restoring
ALWOBJDIF (allow object differences)	commands 404	audit journal (QAUDJRN)
parameter 224	OR (object restore) journal entry	entry 246
changes when restoring 224	type 246	changes when restoring 224
changing	output	changing
audit journal (QAUDJRN)	object authority required for	audit journal (QAUDJRN)
entry 250	commands 432	entry 250
authority required 122	output priority 192	authority required 122
command description 274	output queue	methods 143
methods 143	*JOBCTL (job control) special	default (QDFTOWN) user profile 124
moving application to	authority 69	deleting
production 217	*OPRCTL (operator control)	owner profile 101, 122
	parameter 69	description 122

ownership (continued)	password (continued)	password (continued)
device description 179	approval program (continued)	minimum length (QPWDMINLEN)
flowchart 153	security risk 46	system value
group profile 122	auditing	value set by CFGSYSSEC
introduction 4	DST (dedicated service tools) 232	command 628
managing	user 233	network
owner profile size 122	changes when restoring profile 223	audit journal (QAUDJRN)
new object 124	changing	entry 243
object	description 275	position characters (QPWDPOSDIF)
managing 217	DST (dedicated service tools) 275	system value 44
private authority 111	enforcing password system	possible values 60
OWNER user profile parameter	values 39	preventing
description 80	setting password equal to profile	adjacent digits (QPWDLMTAJC
printer output 186	name 60	system value) 43
restoring 221, 224	checking 107, 275	repeated characters 43
saving 221	checking for default 619	trivial 38, 233
spooled file 186	commands for working with 275	use of words 43
working with 143	communications 42	PWDEXP (set password to
workstation 179	document	expired) 61
ownership change (OW) file layout 566	DOCPWD user profile	QPGMR (programmer) user
ownership change (OW) journal entry	parameter 83	profile 629
type 250	DST (dedicated service tools)	QSRV (service) user profile 629
ownership change for restored object	auditing 232	QSRVBAS (basic service) user
(RO) file layout 580	changing 109	profile 629
ownership change for restored object	encrypting 60	QSYSOPR (system operator) user
(RO) journal entry type 246	equal to user profile name 39, 60	profile 629
ownership, object	expiration interval	QUSER (user) user profile 629
responsibilities 234	auditing 233	recommendations 61, 62
•	PWDEXPITV user profile	require numeric character
	parameter 74	(QPWDRQDDGT) system value
P	QPWDEXPITV system value 39	value set by CFGSYSSEC
-	expiration interval (QPWDEXPITV)	command 628
PA (program adopt) file layout 570	system value	require position difference
PA (program adopt) journal entry	value set by CFGSYSSEC	(QPWDPOSDIF) system value
type 250	command 628	value set by CFGSYSSEC
package	expired (PWDEXP) parameter 61	command 628
object authority required for	IBM-supplied user profile	required difference (QPWDRQDDIF)
commands 408	auditing 232	system value
PAGDOC (Paginate Document) command	changing 108	value set by CFGSYSSEC
object auditing 466	immediate expiration 39	command 628
object authority required 335	incorrect	requiring
page definition (*PAGDFN) auditing 487	audit journal (QAUDJRN)	change (PWDEXPITV
page down key	entry 242	parameter) 74
reversing (*ROLLKEY user	length	change (QPWDEXPITV system
option) 90	maximum (QPWDMAXLEN)	value) 39
page segment (*PAGSEG) auditing 488	system value 42	complete change 44
page up key	minimum (QPWDMINLEN)	different (QPWDRQDDIF system
reversing (*ROLLKEY user	system value 41	value) 42
option) 90	limit repeated characters	numeric character 44
panel group	(QPWDLMTREP) system value	resetting
object authority required for	value set by CFGSYSSEC	DST (dedicated service tools) 247
commands 392	command 628	user 60
panel group (*PNLGRP) auditing 489	local password management	restrict adjacent characters
parameter	LCLPWDMGT user profile	(QPWDLMTAJC) system value
validating 14	parameter 75	value set by CFGSYSSEC
partial (*PARTIAL) limit capabilities 67	lost 60	command 628
pass-through		restrict characters (QPWDLMTCHR)
controlling sign-on 27	maximum length (QPWDMAXLEN system value) 42	
target profile change	3	system value
audit journal (QAUDJRN)	maximum length (QPWDMAXLEN)	value set by CFGSYSSEC
entry 250	system value	command 628
password	value set by CFGSYSSEC	restricting
all-numeric 60	command 628	adjacent digits (QPWDLMTAJC
allowing users to change 233	minimum length (QPWDMINLEN	system value) 43
approval program	system value) 41	characters 43
example 46		repeated characters 43
QPWDVLDPGM system value 44		rules 60
requirements 45		setting to expired (PWDEXP) 61

password (continued)	performance (continued)	PO (printer output) file layout 575
system 110	routing entry 192	PO (printer output) journal entry
system values	run priority 192	type 246
overview 38	storage	pool 192
trivial	pool 192	position characters (QPWDPOSDIF)
preventing 38, 233	subsystem description 192	system value 44
user profile 60	time slice 192	preventing
validation exit program	performance tuning	access
example 46	security 192	DDM request (DDM) 190
validation program	permission definition 114	iSeries Access 189 modification of internal control
example 46 QPWDVLDPGM system value 44	PG (primary group change) file	blocks 17
requirements 45	layout 572	performance abuses 192
security risk 46	PG (primary group change) journal entry	remote job submission 189
validation program (QPWDVLDPGM)	type 250	sign-on without user ID and
system value	physical security 2	password 234
value set by CFGSYSSEC	auditing 232	trivial passwords 38, 233
command 628	planning 232	unauthorized access 235
password (PW) journal entry type 242	PING (Verify TCP/IP Connection)	unauthorized programs 235
password characters 40	command	preventing large profiles
password expiration interval	object authority required 441	planning applications 201
(PWDEXPITV)	PKGPRDDST (Package Product	primary group
recommendations 74	Distribution) command	changes when restoring 224
password expiration interval	authorized IBM-supplied user	changing 123
(QPWDEXPITV) system value	profiles 295	audit journal (QAUDJRN)
auditing 233	planning	entry 250
Password Level (QPWDLVL)	application programmer security 216	command description 274
description 40	audit	changing during restore
Password Level (QPWDLVL) system	system values 256	audit journal (QAUDJRN)
value	auditing	entry 246
description 40	actions 236	definition 111
password required difference	objects 254	deleting
(QPWDRQDDIF) system value	overview 236	profile 101
value set by CFGSYSSEC	checklist for 231	description 123
command 628	command security 209	introduction 5
password validation program (QPWDVLDPGM) system value 44	file security 210 group profiles 214	new object 124 planning 215
passwords	library design 200	restoring 221, 224
password levels 269	menu security 203	saving 221
Passwords 40	multiple groups 215	working with 104, 144
path name	password controls 233	working with objects 274
displaying 144	physical security 232	primary group authority
PC (personal computer)	primary group 215	authority checking example 165
preventing access 189	security 1	primary group change (PG) file
PC Organizer	system programmer security 218	layout 572
allowing for limit capabilities user 67	planning password level changes	primary group change (PG) journal entr
disconnecting (QINACTMSGQ system	changing assword levels (0 to 1) 197	type 250
value) 24	changing assword levels (0 to 2) 197	primary group change for restored object
PC Support access (PCSACC) network	changing assword levels (1 to 2) 197	(RZ) file layout 583
attribute 235	changing assword levels (2 to 3) 198	primary group change for restored object
PC text-assist function (PCTA)	changing password level from 1to	(RZ) journal entry type 246
disconnecting (QINACTMSGQ system	0 200	Print Adopting Objects (PRTADPOBJ)
value) 24	changing password level from 2 to	command
PCSACC (client request access) network	1 199	description 623
attribute 189	changing password level from 2to	Print Communications Security (PRTCMNSEC) command
PCSACC (PC Support access) network attribute 235	0 199	description 280, 623
performance	changing password level from 3 to 0 199	print descriptor group (*PDG)
class 192	changing password level from 3 to	auditing 488
job description 192	1 199	print device (DEV) parameter
job scheduling 192	changing password level from 3 to	user profile 85
object authority required for	2 199	Print Job Description Authority
commands 408	changing password levels	(PRTJOBDAUT) command 279
output priority 192	planning level changes 196, 197	description 623
pool 192	decreasing password levels 199, 200	Print Private Authorities (PRTPVTAUT)
priority limit 192	increasing password level 197	command 279
restricting jobs to batch 193	QPWDLVL changes 196, 197	authorization list 623

Print Private Authorities (PRTPVTAUT) command (continued)	printing (continued) security-relevant output queue	profile <i>(continued)</i> IBM-supplied
description 625	parameters 279, 625	auditing 232
Print Publicly Authorized Objects	security-relevant subsystem	authority profile
(PRTPUBAUT) command 279	description values 623	(QAUTPROF) 283
description 625	sending message (*PRTMSG user	automatic install (QLPAUTO) 283
Print Queue Authority (PRTQAUT)	option) 90	basic service (QSRVBAS) 283
command	system values 232, 280, 623	BRM user profile (QBRMS) 283
description 279, 625	trigger programs 279, 623	database share (QDBSHR) 283
Print Subsystem Description	printing message (*PRTMSG) user	default owner (QDFTOWN) 283
(PRTSBSDAUT) command	option 90	distributed systems node executive
description 623	priority 192	(QDSNX) 283
Print Subsystem Description Authority	priority limit (PTYLMT) parameter	document (QDOC) 283
(PRTSBSDAUT) command	recommendations 78	finance (QFNC) 283
description 279 Print System Security Attributes	user profile 77 private authorities	IBM authority profile (QAUTPROF) 283
(PRTSYSSECA) command	authority cache 174	install licensed programs
description 280, 623	private authority	(QLPINSTALL) 283
Print Trigger Programs (PRTTRGPGM)	definition 111	mail server framework
command	flowchart 152	(QMSF) 283
description 279, 623	object ownership 111	network file system (QNFS) 283
Print User Objects (PRTUSROBJ)	planning applications 201	programmer (QPGMR) 283
command	restoring 221, 225	QAUTPROF (IBM authority
description 279, 623	saving 221	profile) 283
Print User Profile (PRTUSRPRF)	privilege	QBRMS (BRM user profile) 283
command	See also authority	QDBSHR (database share) 283
description 623	definition 111	QDFTOWN (default owner) 283
printed output (*PRTDTA) audit	problem	QDOC (document) 283
level 246	object authority required for	QDSNX (distributed systems node
printer	commands 414	executive) 283
user profile 85	problem analysis	QFNC (finance) 283
virtual	remote service attribute (QRMTSRVATR) system value 33	QGATE (VM/MVS bridge) 283 QLPAUTO (licensed program
securing 190 printer output	processor keylock 232	automatic install) 283
*JOBCTL (job control) special	processor password 110	QLPINSTALL (licensed program
authority 69	product availability (*PRDAVL)	install) 283
*SPLCTL (spool control) special	auditing 490	QMSF (mail server
authority 69	product definition (*PRDDFN)	framework) 283
object authority required for	auditing 490	QNFSANON (network file
commands 432	product library	system) 283
owner 186	library list 184	QPGMR (programmer) 283
securing 186	description 183	QRJE (remote job entry) 283
printer output (PO) file layout 575	recommendations 184	QSECOFR (security officer) 283
printer output (PO) journal entry	product load (*PRDLOD) auditing 490	QSNADS (Systems Network
type 246	profile	Architecture distribution
printer writer	action auditing (AUDLVL) 94	services) 283
object authority required for commands 447	analyzing with query 268	QSPL (spool) 283 QSPLJOB (spool job) 283
printing 447	auditing *ALLOBJ special authority 233	QSRV (service) 283
See also printer output	authority to use 234	QSRVBAS (service basic) 283
adopted object information 623	auditing membership 233	QSYS (system) 283
audit journal (QAUDJRN) entry 246	auditing password 233	QSYSOPR (system operator) 283
audit journal entries 623	AUDLVL (action auditing) 94	QTCP (TCP/IP) 283
authority holder 279	changing 276	QTMPLPD (TCP/IP printing
authorization list information 623	default values table 281	support) 283
communications 280	group 233	QTSTRQS (test request) 283
list of non-IBM objects 279, 623	See also group profile	QUSER (workstation user) 283
list of subsystem descriptions 279	auditing 233	remote job entry (QRJE) 283
network attributes 280, 623	introduction 4, 57	restricted commands 289
notification (*PRTMSG user	naming 59	security officer (QSECOFR) 283
option) 90	object ownership 122	service (QSRV) 283
publicly authorized objects 625	password 60	service basic (QSRVBAS) 283
security 186 security-relevant communications	planning 214 resource security 4	SNA distribution services (QSNADS) 283
settings 623	handle	spool (QSPL) 283
security-relevant job queue	audit journal (QAUDJRN)	spool job (QSPLJOB) 283
parameters 279, 625	entry 250	system (QSYS) 283

profile (continued)	profile (continued)	profile (continued)
IBM-supplied (continued)	user (continued)	user (continued)
system operator (QSYSOPR) 283	IBM-supplied 108	SPCENV (special
TCP/IP (QTCP) 283	initial menu (INLMNU) 66	environment) 72
TCP/IP printing support	initial program (INLPGM) 65	special authority (SPCAUT) 68
(QTMPLPD) 283	INLMNU (initial menu) 66	special environment
test request (QTSTRQS) 283	INLPGM (initial program) 65	(SPCENV) 72
VM/MVS bridge (QGATE) 283	introduction 4	SRTSEQ (sort sequence) 87
workstation user (QUSER) 283	job description (JOBD) 78	status (STATUS) 62
OBJAUD (object auditing) 93	JOBD (job description) 78	SUPGRPPRF (supplemental
object auditing (OBJAUD) 93	KBDBUF (keyboard buffering) 76	groups) 81
QDFTOWN (default owner)	keyboard buffering (KBDBUF) 76	supplemental groups
restoring programs 227	LANGID (language identifier) 87	(SUPGRPPRF) 81
swap	language identifier (LANGID) 87	System/36 environment 72
audit journal (QAUDJRN)	large, examining 269	text (TEXT) 67
entry 250	LCLPWDMGT (local password	user class (USRCLS) 63
user 93, 94, 268	management) 75	user identification number() 90
accounting code (ACGCDE) 82	limit capabilities 66, 233	user options (CHRIDCTL) 88
ACGCDE (accounting code) 82	limit device sessions	user options (LOCALE) 89
assistance level (ASTLVL) 63	(LMTDEVSSN) 75	user options (SETJOBATR) 89
ASTLVL (assistance level) 63	listing inactive 269	user options (USROPT) 88, 89, 90
ATNPGM (Attention-key-handling	listing selected 268	USRCLS (user class) 63
program) 86	listing users with command	USROPT (user options) 88, 89, 90
Attention-key-handling program	capability 268	USRPRF (name) 59
(ATNPGM) 86	listing users with special	profile swap (PS) file layout 576
auditing 233	authorities 268	profile swap (PS) journal entry type 250
authority (AUT) 93	LMTCPB (limit capabilities) 66	program
automatic creation 57	LMTDEVSSN (limit device	adopt authority function
CCSID (coded character set	sessions) 75	auditing 270
identifier) 88	local password management	adopted authority
changing 101	(LCLPWDMGT) 75	audit journal (QAUDJRN)
CHRIDCTL (user options) 88	LOCALE (user options) 89	entry 250
CNTRYID (country or region	maximum storage (MAXSTG) 76	auditing 234
identifier) 88	MAXSTG (maximum storage) 76	creating 130
coded character set identifier	message queue (MSGQ) 83	displaying 130
(CCSID) 88	message queue delivery	ignoring 131
country or region identifier	(DLVRY) 84	purpose 128
(CNTRYID) 88	message queue severity (SEV) 84	restoring 227
CURLIB (current library) 64	MSGQ (message queue) 83	transferring 128, 129
current library (CURLIB) 64	name (USRPRF) 59	bound
delivery (DLVRY) 84	naming 59	adopted authority 130
description (TEXT) 67	output queue (OUTQ) 85	changing
DEV (print device) 85	OUTQ (output queue) 85	specifying USEADPAUT
display sign-on information	owner of objects created	parameter 131
(DSPSGNINF) 73	(OWNER) 80, 122	creating
DLVRY (message queue	password 60	adopted authority 130
delivery) 84	password expiration interval	displaying
DOCPWD (document	(PWDEXPITV) 74	adopted authority 130
password) 83	print device (DEV) 85	ignoring
document password	priority limit (PTYLMT) 77	adopted authority 131
(DOCPWD) 83	PTYLMT (priority limit) 77	object authority required for
DSPSGNINF (display sign-on	public authority (AUT) 93	commands 415
information) 73	PWDEXP (set password to	password validation
eim association (EIMASSOC) 92	expired) 61	example 46
group (GRPPRF) 79	PWDEXPITV (password expiration	QPWDVLDPGM system value 44
group authority (GRPAUT) 80, 122	interval) 74	requirements 45
	renaming 106 retrieving 107	password validation exit
group authority type	e e	example 46
(GRPAUTTYP) 81 group identification number(gid	roles 57 set password to expired	preventing unauthorized 235
0 1		
) 91 GRPAUT (group authority) 80,	(PWDEXP) 61 SETIORATE (usor options) 80	program failure
122	SETJOBATR (user options) 89 SEV (message queue severity) 84	audit journal (QAUDJRN) entry 250
	severity (SEV) 84	restoring
GRPAUTTYP (group authority type) 81	sort sequence (SRTSEQ) 87	adopted authority 227
GRPPRF (group) 79	SPCAUT (special authority) 68	risks 227
home directory (HOMEDIR) 91	of CACT (special additionity) 00	validation value 14
nome uncetory (FromEDIR) 31		vanuautti valut 14

program (continued)	PRTCMDUSG (Print Command Usage)	PRTLCKRPT (Print Lock Report)
service	command (continued)	command
adopted authority 130 transferring	object authority required 417 PRTCMNSEC (Print Communication	object authority required 412 PRTPEXRPT (Print Performance Explorer
adopted authority 128, 129	Security) command	Report) command
translation 14	object authority required 326	object authority required 412
trigger	PRTCMNSEC (Print Communications	PRTPOLRPT
listing all 279	Security) command	authorized IBM-supplied user
unauthorized 235	description 280, 623	profiles 295
working with user profiles 107	object authority required 330, 391	PRTPOLRPT (Print Pool Report)
program (*PGM) auditing 488	PRTCMNTRC (Print Communications	command
program adopt (PA) file layout 570	Trace) command	object authority required 412
program adopt (PA) journal entry	authorized IBM-supplied user	PRTPRFINT (Print Profile Internals)
type 250	profiles 295	command
program adopt function	object authority required 428	authorized IBM-supplied user
See adopted authority	PRTCPTRPT	profiles 295
program failure	authorized IBM-supplied user	PRTPUBAUT (Print Public Authorities)
auditing 270	profiles 295	command
restoring programs	PRTCPTRPT (Print Component Report)	object authority required 307
audit journal (QAUDJRN)	command	PRTPUBAUT (Print Publicly Authorized
entry 246	object authority required 412	Objects) command
program failure (*PGMFAIL) audit	PRTCSPAPP (Print CSP/AE Application)	description 279, 623
level 246	command	PRTPVTAUT (Print Private Authorities)
program state	object auditing 489	command
definition 13	PRTDEVADR (Print Device Addresses)	authorization list 623
displaying 13	command	description 279, 625
program temporary fix (PTF)	object auditing 459	object authority required 307
object authority required for	object authority required 323	PRTQAUT (Print Queue Authorities)
commands 427	PRTDOC (Print Document) command	command
program validation	object auditing 464	object authority required 373, 407
definition 14	PRTDSKINF	PRTQAUT (Print Queue Authority)
program-described file	authorized IBM-supplied user	command
holding authority when deleted 132	profiles 295	description 279, 625
programmer	PRTDSKINF (Print Disk Activity	PRTRSCRPT
application	Information) command	authorized IBM-supplied user
planning security 216	object authority required 403	profiles 295
auditing access to production	PRTERRLOG	PRTRSCRPT (Print Resource Report)
libraries 233	authorized IBM-supplied user	command
system	profiles 295	object authority required 412
planning security 218	PRTERRLOG (Print Error Log) command	PRTSBSDAUT (Print Subsystem
programmer (QPGMR) user profile	object authority required 428	Description Authority) command
default values 283	PRTINTDTA	description 279
device description owner 179	authorized IBM-supplied user	object authority required 435
programming language	profiles 295	PRTSBSDAUT (Print Subsystem
object authority required for	PRTINTDTA (Print Internal Data)	Description) command
commands 378	command	description 623
programs that adopt	object authority required 428	PRTSQLINF (Print SQL Information)
displaying 270	PRTIPSCFG (Print IP over SNA	command
protecting	Configuration) command	object auditing 489, 499
backup media 232	object authority required 314	PRTSQLINF (Print Structured Query
protection	PRTJOBDAUT (Print Job Description	Language Information) command
enhanced hardware storage 14	Authority) command	object authority required 408
PRTACTRPT	description 279, 623	PRTSYSRPT
authorized IBM-supplied user	object authority required 372	authorized IBM-supplied user
profiles 295	PRTJOBRPT	profiles 295
PRTACTRPT (Print Activity Report)	authorized IBM-supplied user	PRTSYSRPT (Print System Report)
command	profiles 295	command
object authority required 411	PRTJOBRPT (Print Job Report) command	object authority required 412
PRTADPOBJ (Print Adopted Object)	object authority required 412	PRTSYSSECA (Print System Security
command	PRTJOBTRC	Attribute) command
object authority required 307	authorized IBM-supplied user	object authority required 426
PRTADPOBJ (Print Adopting Objects)	profiles 295	PRTSYSSECA (Print System Security
command	PRTJOBTRC (Print Job Trace) command	Attributes) command
description 623	object authority required 412	description 280, 623
PRTCMDUSG (Print Command Usage) command	PRTLCKRPT	PRTTNSRPT
	outhorized IDM over-lind over-	authorized IDM complied com
object auditing 456, 489	authorized IBM-supplied user profiles 295	authorized IBM-supplied user profiles 295

PRTTNSRPT (Print Transaction Report) command	QALWOBJRST (allow object restore option) system value 37	QASYOMJE (object management) file layout 560
object authority required 412 PRTTRC (Print Trace) command	QALWOBJRST (allow object restore) system value	QASYORJE (object restore) file layout 563
object authority required 428	value set by CFGSYSSEC	QASYOWJE (ownership change) file
PRTTRCRPT	command 628	layout 566
authorized IBM-supplied user	QALWUSRDMN (allow user objects)	QASYPAJE (program adopt) file
profiles 295	system value 16, 21	layout 570
PRTTRGPGM (Print Trigger Program)	QASYADJE (auditing change) file	QASYPGJE (primary group change) file
command	layout 512	layout 572
object authority required 344	QASYAFJE (authority failure) file	QASYPOJE (printer output) file
PRTTRGPGM (Print Trigger Programs)	layout 514	layout 575
command	QASYAPJE (adopted authority) file	QASYPSJE (profile swap) file layout 576
description 279, 623 PRTUSROBJ (Print User Object)	layout 519 QASYAUJ5 (attribute change) file	QASYPWJE (password) file layout 577 QASYRAJE (authority change for restored
command	layout 520	object) file layout 578
object authority required 307	QASYCAJE (authority change) file	QASYRJJE (restoring job description) file
PRTUSROBJ (Print User Objects)	layout 520	layout 579
command	QASYCDJE (command string) file	QASYROJE (ownership change for object
description 279, 623	layout 523	program) file layout 580
PRTUSRPRF (Print User Profile)	QASYCOJE (create object) file	QASYRPJE (restoring programs that
command	layout 524	adopt authority) file layout 581
description 623	QASYCPJE (user profile change) file	QASYRQJE (restoring *CRQD that adopts
object authority required 445	layout 525	authority) file layout 583
PS (profile swap) file layout 576	QASYCQJE (*CRQD change) file	QASYRUJE (restore authority for user
PS (profile swap) journal entry type 250 PTF (program temporary fix)	layout 527 QASYCUJ4 (Cluster Operations) file	profile) file layout 583 QASYRZJE (primary group change for
object authority required for	layout 528	restored object) file layout 583
commands 427	QASYCVJ4 (connection verification) file	QASYSDJE (change system distribution
PTYLMT (priority limit) parameter	layout 529	directory) file layout 585
recommendations 78	QASYCYJ4 (cryptographic configuration)	QASYSEJE (change of subsystem routing
user profile 77	file layout 531	entry) file layout 586
public authority	QASYCYJ4 (Directory Server) file	QASYSFJE (action to spooled file) file
authority checking example 166, 168	layout 532	layout 587
definition 111	QASYDOJE (delete operation) file	QASYSGJ4() file layout 590, 591
flowchart 159	layout 536	QASYSMJE (systems management
library 136	QASYDSJE (IBM-Supplied Service Tools	change) file layout 592
new objects description 118	User ID Reset) file layout 538 QASYEVJE (EV) file layout 539	QASYSOJ4 (server security user information actions) file layout 593
specifying 136	QASYGRJ4 (generic record) file	QASYSTJE (service tools action) file
printing 625	layout 540	layout 594
restoring 221, 225	QASYGSJE (give descriptor) file	QASYSVJE (action to system value) file
revoking 280, 627	layout 544	layout 597
revoking with RVKPUBAUT	QASYGSJE (Internet security	QASYVAJE (changing access control list)
command 630	management) file layout 548	file layout 598
saving 221	QASYGSJE (interprocess communication	QASYVCJE (connection start and end)
user profile	actions) file layout 546	file layout 598
recommendation 93	QASYIRJ4 (IP rules actions) file	QASYVFJE (close of server files) file
PW (password) journal entry type 242 PWDEXP (set password to expired)	layout 547 QASYJDJE (job description change) file	layout 599 QASYVLJE (account limit exceeded) file
parameter 61	layout 550	layout 599
PWDEXPITV (password expiration	QASYJSJE (job change) file layout 550	QASYVNJE (network log on and off) file
interval) parameter 74	QASYKFJ4 (key ring file) file layout 554	layout 600
PWRDWNSYS (Power Down System)	QASYLDJE (link, unlink, search	QASYVOJ4 (validation list) file
command	directory) file layout 557	layout 601
authorized IBM-supplied user	QASYMLJE (mail actions) file	QASYVPJE (network password error) file
profiles 295	layout 559	layout 602
object authority required 436	QASYNAJE (network attribute change)	QASYVRJE (network resource access) file
	file layout 559	layout 603
0	QASYNDJE (APPN directory) file layout 559	QASYVSJE (server session) file
Q	QASYNEJE (APPN end point) file	layout 603 QASYVUJE (network profile change) file
QADSM (ADSM) user profile 283	layout 560	layout 604
QAFDFTUSR (AFDFTUSR) user	QASYO1JE (optical access) file	QASYVVJE (service status change) file
profile 283	layout 568, 569	layout 605
QAFOWN (AFOWN) user profile 283 QAFUSR (AFUSR) user profile 283	QASYO3JE (optical access) file	QASYX0JE (kerberos authentication) file
A T COIL (TI COIL) MOU PROUNT 400	layout 570	layout 605

QASYYCJE (change to DLO object) file QAUDJRN (audit) journal (continued) QAUDJRN (audit) journal (continued) layout 610 CY(cryptographic configuration) file PS (profile swap) entry type 250 layout 531 QASYYRJE (read of DLO object) file PS (profile swap) file layout 576 layout 611 damaged 260 PW (password) entry type 242 QASYZCJE (change to object) file detaching receiver 260, 261 PW (password) file layout 577 layout 611 DI(Directory Server) file layout 532 RA (authority change for restored QASYZRJE (read of object) file displaying entries 235, 262 object) entry type 246 layout 614 DO (delete operation) entry type 243 RA (authority change for restored QATNPGM (Attention-key-handling DO (delete operation) file layout 536 object) file layout 578 program) system value 86 DS (DST password reset) entry receiver storage threshold 260 QAUDCTL (audit control) system value type 247 RJ (restoring job description) entry changing 279, 621 DS (IBM-Supplied Service Tools User type 246 displaying 279, 621 ID Reset) file layout 538 RJ (restoring job description) file QAUDCTL (auditing control) system error conditions 50 layout 579 EV (Environment variable) file RO (ownership change for restored overview 50 layout 539 object) entry type 246 RO (ownership change for restored QAUDENDACN (auditing end action) force level 51 system value 50, 256 GR(generic record) file layout 540 object) file layout 580 QAUDFRCLVL (auditing force level) GS (give descriptor) file layout 544 RP (restoring programs that adopt system value 51, 256 introduction 235 authority) entry type 246 IP (Interprocess Communication QAUDJRN (audit) journal 250, 252 RP (restoring programs that adopt See also object auditing actions) file layout 546 authority) file layout 581 See also QAUDLVL (audit level) IP (interprocess communications) RQ (restoring \*CRQD object that system value entry type 242 adopts authority) file layout 583 AD (auditing change) entry type 249 IR(IP rules actions) file layout 547 RQ (restoring \*CRQD object) entry type 246 AD (auditing change) file layout 512 IS (Internet security management) file AF (authority failure) entry type RU (restore authority for user profile) layout 548 default sign-on violation 13 JD (job description change) entry entry type 246 description 242 type 250 RU (restore authority for user profile) JD (job description change) file hardware protection violation 14 file layout 583 layout 550 RZ (primary group change for job description violation 13 program validation 15 JS (job change) entry type 243 restored object) entry type 246 restricted instruction 15 JS (job change) file layout 550 RZ (primary group change for KF (key ring file) file layout 554 restored object) file layout 583 unsupported interface 13, 15 AF (authority failure) file layout 514 LD (link, unlink, search directory) file SD (change system distribution layout 557 directory) entry type 245 analyzing with query 263 managing 259 SD (change system distribution directory) file layout 585 AP (adopted authority) entry methods for analyzing 262 type 245 ML (mail actions) entry type 245 SE (change of subsystem routing AP (adopted authority) file ML (mail actions) file layout 559 entry) entry type 251 layout 519 NA (network attribute change) entry SE (change of subsystem routing AU (attribute change) file layout 520 entry) file layout 586 SF (action to spooled file) file auditing level (QAUDLVL) system NA (network attribute change) file value 51 lavout 559 layout 587 ND (APPN directory) file layout 559 auditing level extension (QAUDLVL2) SF (change to spooled file) entry NE (APPN end point) file layout 560 type 252 system value 53 automatic cleanup 260 O1 (optical access) file layout 568, SG file layout 590, 591 CA (authority change) entry type 249 SM (systems management change) CA (authority change) file layout 520 O3 (optical access) file layout 570 entry type 252 SM (systems management change) file CD (command string) entry type OM (object management) entry type 245 CD (command string) file layout 523 layout 592 SO (server security user information changing receiver 261 OM (object management) file CO (create object) entry type 123, layout 560 actions) file layout 593 OR (object restore) entry type 246 ST (service tools action) entry CO (create object) file layout 524 OR (object restore) file layout 563 type 252 CP (user profile change) entry OW (ownership change) entry ST (service tools action) file type 247 type 250 layout 594 CP (user profile change) file OW (ownership change) file stopping 261 layout 525 layout 566 SV (action to system value) entry type 251 CQ (\*CRQD change) file layout 527 PA (program adopt) entry type 250 CQ (change \*CRQD object) entry PA (program adopt) file layout 570 SV (action to system value) file PG (primary group change) entry type 247 layout 597 type 250 creating 258 system entries 259 CU(Cluster Operations) file PG (primary group change) file VA (access control list change) entry layout 528 layout 572 type 251 CV(connection verification) file PO (printer output) entry type 246 VA (changing access control list) file layout 529 PO (printer output) file layout 575 layout 598

QAUDJRN (audit) journal (continued) QAUDLVL2 (auditing level extension) QINACTITY (inactive job time-out VC (connection start and end) file interval) system value (continued) system value layout 598 value set by CFGSYSSEC overview 53 QAUTOCFG (automatic configuration) VC (connection start or end) entry command 628 type 244 system value QINACTMSGQ (inactive job message value set by CFGSYSSEC VF (close of server files) file queue) system value 24 layout 599 value set by CFGSYSSEC command 628 VL (account limit exceeded) file QAUTOCFG (automatic device command 628 layout 599 QjoAddRemoteJournal (Add Remote configuration) system value 31 VN (network log on and off) file QAUTOVRT (automatic configuration of Journal) API object auditing 478 layout 600 virtual devices) system value 31 VN (network log on or off) entry QAUTOVRT (automatic virtual-device QjoChangeJournal State(Change Journal configuration) system value State) API type 244 VO (validation list) file layout 601 value set by CFGSYSSEC object auditing 478 QjoEndJournal (End journaling) API VP (network password error) entry command 628 QAUTPROF (authority profile) user type 243 object auditing 450 VP (network password error) file profile 283 QjoEndJournal (End Journaling) API layout 602 QBRMS (BRM) user profile 283 object auditing 478 VR (network resource access) file QCCSID (coded character set identifier) QJORDJE2 record format 507 layout 603 system value 88 QjoRemoveRemoteJournal (Remove VS (server session) entry type 244 QCL program 117 Remote Journal) API VS (server session) file layout 603 QCMD command processor object auditing 478 VU (network profile change) entry QjoRetrieveJournalEntries (Retrieve Attention-key-handling program 86 type 251 special environment (SPCENV) 72 Journal Entries) API VU (network profile change) file QCNTRYID (country or region identifier) object auditing 478 layout 604 system value 88 QjoRetrieveJournalInformation (Retrieve VV (service status change) entry QCONSOLE (console) system value 179 Journal Information) API QCRTAUT (create authority) system object auditing 479 type 252 VV (service status change) file QJORJIDI (Retrieve Journal Identifier description 22 (JID) Information) API layout 605 X0 (kerberos authentication) file risk of changing 22 object auditing 477 layout 605 using 119 QjoSJRNE (Send Journal Entry) API YC (change to DLO object) file QCRTOBJAUD (create object auditing) object auditing 478 QjoStartJournal (Start Journaling) API layout 610 system value 54 YR (read of DLO object) file QDBSHRDO (database share) user object auditing 450, 478 layout 611 profile 283 QKBDBUF (keyboard buffering) system ZC (change to object) file layout 611 QDCEADM (DCEADM) user profile 283 value 76 QLANGID (language identifier) system ZR (read of object) file layout 614 QDEVRCYACN (device recovery action) system value 32 QAUDLVL (audit level) system value value 87 \*AUTFAIL value 242 value set by CFGSYSSEC QlgAccess command (Detremine File Accessibility) \*CREATE (create) value 243 command 628 \*DELETE (delete) value 243 QDFTJOBD (default) job description 79 object auditing 460 \*JOBDTA (job change) value 243 QDFTOWN (default owner) user profile QlgAccessx command (Determine File \*OBJMGT (object management) audit journal (QAUDJRN) entry 246 Accessibility) value 245 default values 283 object auditing 460 \*OFCSRV (office services) value 245 description 124 QLMTDEVSSN (limit device sessions) \*PGMADP (adopted authority) restoring programs 227 system value QDOC (document) user profile 283 auditing 233 value 245 QDSCJOBITV (disconnected job time-out description 24 \*PGMFAIL (program failure) LMTDEVSSN user profile value 246 interval) system value 33 \*PRTDTA (printer output) value 246 value set by CFGSYSSEC parameter 75 QLMTSECOFR (limit security officer) \*SAVRST (save/restore) value 246 command 628 \*SECURITY (security) value 249 QDSNX (distributed systems node system value \*SERVICE (service tools) value 252 executive) user profile 283 auditing 232 \*SPLFDTA (spooled file changes) QDSPSGNINF (display sign-on authority to device descriptions 177 value 252 information) system value 22, 74 changing security levels 11 \*SYSMGT (systems management) value set by CFGSYSSEC description 25 value 252 command 628 sign-on process 179 value set by CFGSYSSEC See also QAUDJRN (audit) journal QEZMAIN program 86 changing 259, 279, 621 QFNC (finance) user profile 283 command 628 displaying 279, 621 QGATE (VM/MVS bridge) user QLPAUTO (licensed program automatic profile 283 purpose 236 install) user profile user profile 94 QHST (history) log default values 283 QAUDLVL (auditing level) system value using to monitor security 266 restoring 224 overview 51 QINACTITY (inactive job time-out QLPINSTALL (licensed program install) interval) system value 23 user profile default values 283

QLPINSTALL (licensed program install)	QPWDMINLEN (password minimum	QSECURITY (security level) system
user profile (continued)	length) system value 41	value (continued)
restoring 224 QMAXSGNACN (action when sign-on	value set by CFGSYSSEC command 628	automatic user profile creation 57 changing, 20 from higher level 10
attempts reached) system value	QPWDPOSDIF (password require	changing, level 10 to level 20 10
description 26	position difference) system value	changing, level 20 to 30 10
user profile status 62	value set by CFGSYSSEC	changing, to level 40 15
value set by CFGSYSSEC	command 628	changing, to level 50 17
command 628	QPWDPOSDIF (position characters)	comparison of levels 7
QMAXSIGN (maximum sign-on	system value 44	disabling level 40 16
attempts) system value	QPWDRQDDGT (password require	disabling level 50 18
auditing 232, 235	numeric character) system value	enforcing QLMTSECOFR system
description 25	value set by CFGSYSSEC	value 179
user profile status 62	command 628	internal control blocks 17
value set by CFGSYSSEC	QPWDRQDDGT (required password	introduction 2
command 628	digits) system value 44	level 10 9
QMSF (mail server framework) user	QPWDRQDDIF (duplicate password)	level 20 10
profile 283	system value 42	level 30 10
QPGMR (programmer) user profile	QPWDRQDDIF (password required	level 40 11
default values 283	difference) system value	level 50 16
device description owner 179	value set by CFGSYSSEC	message handling 16
password set by CFGSYSSEC	command 628	validating parameters 14
command 629	QPWDVLDPGM (password validation	overview 7
QPRTDEV (print device) system	program) system value 44	recommendations 9
value 85	value set by CFGSYSSEC	special authority 8
QPWDEXPITV (password expiration	command 628	user class 8
interval) system value	QRCL (reclaim storage) library	value set by CFGSYSSEC
auditing 233	setting QALWUSRDMN (allow user	command 628
description 39	objects) system value 21	QSH (Start QSH) command
PWDEXPITV user profile	QRCLAUTL (reclaim storage)	alias for STRQSH 418
parameter 74 value set by CFGSYSSEC	authorization list 229 QRETSVRSEC (retain server security)	QSHRMEMCTL (share memory control) system value
command 628	system value 26	description 29
QPWDLMTAJC (password limit adjacent)	QRETSVRSEC (retain server security)	possible values 29
system value 43	value 26	QSNADS (Systems Network Architecture
QPWDLMTAJC (password restrict	QRJE (remote job entry) user profile 283	distribution services) user profile 283
adjacent characters) system value	QRMTSIGN (allow remote sign-on)	QSPCENV (special environment) system
value set by CFGSYSSEC	system value	value 72
command 628	value set by CFGSYSSEC	QSPL (spool) user profile 283
QPWDLMTCHR (limit characters) system	command 628	QSPLJOB (spool job) user profile 283
value 43	QRMTSIGN (remote sign-on) system	QSPRJOBQ (Retrieve job queue
QPWDLMTCHR (password restrict	value 27, 235	information) API
characters) system value	QRMTSRVATR (remote service attribute)	object auditing 477
value set by CFGSYSSEC	system value 2, 33	QsrRestore
command 628	QRYDOCLIB (Query Document Library)	object auditing 450
QPWDLMTCHR command 61	command	QSRRSTO (Restore Object) API
QPWDLMTREP (limit repeated	object auditing 466	object auditing 450
characters) system value 43	object authority required 335	QsrSave
QPWDLVL	QRYDST (Query Distribution) command	object auditing 449
case sensitive passwords 44, 60	object authority required 333	QSRSAVO
Password levels (maximum	QRYPRBSTS (Query Problem Status)	object auditing 449
length) 42	command	QSRTSEQ (sort sequence) system
Password levels (minimum	object authority required 414	value 87
length) 41 Password levels (QPWDLVL) 41, 42,	QSCANFS (Scan File Systems) system	QSRV (service) user profile
43	value 28 QSCANFSCTL (Scan File Systems	authority to console 179 default values 283
QPWDLVL (case sensitive)	Control) system value 28	password set by CFGSYSSEC
case sensitive passwords	QSECOFR (security officer) user profile	command 629
QPWDLVL case sensitive 43	See also security officer	QSRVBAS (basic service) user profile
Password levels (case sensitive) 43	authority to console 179	authority to console 179
QPWDLVL (current or pending value)	default values 283	default values 283
and program name 44	device description owner 179	password set by CFGSYSSEC
QPWDMAXLEN (password maximum	disabled status 62	command 629
length) system value 42	enabling 62	QSYS (system) library
value set by CFGSYSSEC	restoring 224	authorization lists 118
command 628	QSECURITY (security level) system value	QSYS (system) user profile
	auditing 232	default values 283

QSYS (system) user profile (continued)	RCLDLO (Reclaim Document Library	reclaim storage (QRCL) library
restoring 224	Object) command	setting QALWUSRDMN (allow user
QSYSLIBL (system library list) system	object auditing 467	objects) system value 21
value 183	object authority required 335	reclaim storage (QRCLAUTL)
QSYSMSG message queue	RCLLNK (Reclaim Object Links)	authorization list 229
auditing 235, 266	command	Reclaim Storage (RCLSTG)
QMAXSGNACN (action when	object authority required 359	command 16, 124, 229
· ·		
attempts reached) system value 26	RCLOBJOWN (Reclaim Objects by	setting QALWUSRDMN (allow user
QMAXSIGN (maximum sign-on	Owner) command	objects) system value 21
attempts) system value 25	authorized IBM-supplied user	reclaiming
QSYSOPR (system operator) message	profiles 295	storage 16, 124, 229
	1	
queue	object authority required 307	setting QALWUSRDMN (allow
restricting 182	RCLOPT (Reclaim Optical) command	user objects) system value 21
QSYSOPR (system operator) user	authorized IBM-supplied user	recommendation
profile 283	profiles 295	adopted authority 131
•	1	
password set by CFGSYSSEC	object authority required 406	application design 201
command 629	RCLRSC (Reclaim Resources) command	display sign-on information
QTCP (TCP/IP) user profile 283	object authority required 436	(DSPSGNINF) 74
QTEMP (temporary) library	RCLSPLSTG (Reclaim Spool Storage)	initial library list 79
security level 50 16	command	initial menu (INLMNU) 67
QTMPLPD (TCP/IP printing support)	authorized IBM-supplied user	initial program (INLPGM) 67
user profile 283	profiles 295	job descriptions 79
QTSTRQS (test request) user profile 283	object authority required 433	library design 200
•		
query	RCLSTG (Reclaim Storage) command	library list
analyzing audit journal entries 263	authorized IBM-supplied user	current library 185
query definition (*QRYDFN)	profiles 295	product library portion 184
auditing 491	damaged authorization list 229	system portion 184
S .		
Query Management/400	object auditing 450	user portion 185
object authority required for	object authority required 307	limit capabilities (LMTCPB) 67
commands 418	QDFTOWN (default owner)	limiting
query manager form (*QMFORM)	profile 124	device sessions 76
auditing 490	security level 50 16	
S .	•	message queue 84
query manager query (*QMQRY)	setting QALWUSRDMN (allow user	naming
auditing 491	objects) system value 21	group profile 59
question and answer	RCLTMPSTG (Reclaim Temporary	user profiles 59
object authority required for		password expiration interval
0 0 1	Storage) command	
commands 420	authorized IBM-supplied user	(PWDEXPITV) 74
QUSEADPAUT (use adopted authority)	profiles 296	passwords 61
system value	object auditing 452	priority limit (PTYLMT)
description 30	object authority required 307	parameter 78
•		•
risk of changing 30	RCVDST (Receive Distribution) command	public authority
QUSER (user) user profile	object auditing 466	user profiles 93
password set by CFGSYSSEC	object authority required 333	QUSRLIBL system value 79
command 629	RCVJRNE (Receive Journal Entry)	RSTLICPGM (Restore Licensed
QUSER (workstation user) user	command	Program) command 227
profile 283	object auditing 478	security design 196
QUSER38 library 117	object authority required 376	security level (QSECURITY) system
QUSRLIBL (user library list) system	RCVMGRDTA (Receive Migration Data)	value 9
	_	
value 79	command	set password to expired
QVFYOBJRST (verify object on restore)	object authority required 395	(PWDEXP) 62
system value 34	RCVMSG (Receive Message) command	special authority (SPCAUT) 72
QVFYOBJRST (Verify Object Restore)	object auditing 483, 484	special environment (SPCENV) 72
system value 3	•	•
	object authority required 394	summary 196
QWCLSCDE (List job schedule entry) API	RCVNETF (Receive Network File)	user class (USRCLS) 63
object auditing 477	command	record-level security 210
	object authority required 398	recovering
	read (*READ) authority 112, 302	
D	•	authority holder 221
R	read of DLO object (YR) file layout 611	authorization list 221
RA (authority change for rectored object)	read of object (ZR) file layout 614	damaged audit journal 260
RA (authority change for restored object)	reader	damaged authorization list 228
journal entry type 246	object authority required for	object ownership 221
RCLACTGRP (Reclaim Activation Group)		•
command	commands 421	private authority 221
object authority required 436	receiver	public authority 221
0 0 1	changing 261	security information 221
RCLDBXREF command	deleting 261	user profiles 221
object authority required 307		•
	detaching 260, 261	reference code table (*RCT) auditing 492
	saving 261	referenced object 145

rejecting	required password digits	restoring (continued)
access	(QPWDRQDDGT) system value 44	authority
DDM request (DDM) 190	resetting	audit journal (QAUDJRN)
iSeries Access access 189	DST (dedicated service tools)	entry 246
remote job submission 189	password	command description 277
relational database directory	audit journal (QAUDJRN)	description of process 226
object authority required for	entry 247	overview of commands 221
commands 421	RESMGRNAM (Resolve Duplicate and	procedure 225
remote job entry (QRJE) user profile 283	Incorrect Office Object Names)	authority changed by system
remote job entry (RJE)	command	audit journal (QAUDJRN)
object authority required for	authorized IBM-supplied user	entry 246
commands 422	profiles 296	authority holder 221
remote job submission	object authority required 396	authorization list
securing 189	resource	association with object 225
remote service attribute (QRMTSRVATR)	object authority required for	description of process 228
system value 33	commands 422	overview of commands 221
remote sign-on	resource security	document library object (DLO) 221
QRMTSIGN system value 27	definition 111	gid (group identification
remote sign-on (QRMTSIGN) system	introduction 4	number) 224
value 27, 235	limit access 218	job description
Remove Authorization List Entry	restore	audit journal (QAUDJRN)
(RMVAUTLE) command 146, 273	security risks 191	entry 246
	Restore Authority (RSTAUT) command	library 221
Remove Directory Entry (RMVDIRE)	3 1	•
command 278	audit journal (QAUDJRN) entry 246	licensed program recommendations 227
Remove Document Library Object	description 277	_
Authority (RMVDLOAUT)	procedure 226	security risks 227
command 277	role in restoring security 221	maximum storage (MAXSTG) 77
Remove Library List Entry (RMVLIBLE)	using 225	object
command 183	restore authority for user profile (RU) file	audit journal (QAUDJRN)
Remove User display 102, 103	layout 583	entry 246
removing	restore authority for user profile (RU)	commands 221
authority for user 140	journal entry type 246	ownership 221, 224
authorization list	Restore Document Library Object	security issues 224
object 147	(RSTDLO) command 221	operating system 229
user authority 146, 273	Restore Library (RSTLIB) command 221	ownership change
directory entry 278	Restore Licensed Program (RSTLICPGM)	audit journal (QAUDJRN)
document library object	command	entry 246
authority 277	recommendations 227	primary group 221, 224
employees who no longer need	security risks 227	private authority 221, 225
access 233	Restore Object (RSTOBJ) command	program failure
library list entry 183	using 221	audit journal (QAUDJRN)
security level 40 16	restore operation	entry 246
security level 50 18	maximum storage (MAXSTG) 77	program validation 14
server authentication entry 278	storage needed 77	programs 227
user authority	restore system value	public authority 221, 225
authorization list 146	security-related	QDFTOWN (default) owner
object 140	overview 33	audit journal (QAUDJRN)
user profile	Restore User Profiles (RSTUSRPRF)	entry 246
automatically 619	command 221, 277	restricting 191
directory entry 101	restoring	security information 221
distribution lists 101	*ALLOBJ (all object) special authority	storage needed 77
message queue 101	all object (*ALLOBJ) special	uid (user identification number) 224
owned objects 101	authority 224	user profile
primary group 101	*CRQD object	audit journal (QAUDJRN)
renaming	audit journal (QAUDJRN)	entry 247
object	entry 246	command description 277
audit journal (QAUDJRN)	*CRQD object that adopts authority	procedures 221, 223
entry 245	(RQ) file layout 583	restoring *CRQD (RQ) file layout 583
user profile 106	adopted authority	restoring *CRQD object (RQ) journal
repeated characters (QPWDLMTREP)	changes to ownership and	entry type 246
system value 43	authority 227	restoring job description (RJ) file
repeating passwords 42	allow object differences (ALWOBJDIF)	layout 579
reply list	parameter 225	restoring job description (RJ) journal
action auditing 493	ALWOBJDIF (allow object differences)	entry type 246
object authority required for	parameter 224, 225	restoring programs that adopt authority
commands 436	*	(RP) file layout 581

restoring programs that adopt authority	risk	RLSRDR (Release Reader) command
(RP) journal entry type 246	*ALLOBJ (all object) special	object authority required 421
restricted instruction	authority 68	RLSRMTPHS (Release Remote Phase)
audit journal (QAUDJRN) entry 246	*AUDIT (audit) special authority 71	command
restricting	*IOSYSCFG (system configuration)	authorized IBM-supplied user
access	special authority 72	profiles 296
console 232	*JOBCTL (job control) special	RLSSPLF (Release Spooled File)
workstations 232	authority 69	command
adjacent digits in passwords	*SAVSYS (save system) special	object auditing 487
(QPWDLMTAJC system value) 43	authority 70	object authority required 433
capabilities 66	*SERVICE (service) special	RLSWTR (Release Writer) command
characters in passwords 43	authority 70	object authority required 447
command line use 66	*SPLCTL (spool control) special	RMVACC (Remove Access Code)
commands (ALWLMTUSR) 67	authority 70	command
consecutive digits in passwords	adopted authority 131	authorized IBM-supplied user
(QPWDLMTAJC system value) 43	authority holder 133	profiles 296
messages 16	create authority (CRTAUT)	object auditing 466
QSYSOPR (system operator) message	parameter 119	object authority required 402
queue 182	library list 183	RMVAJE (Remove Autostart Job Entry)
repeated characters in passwords 43	password validation program 46	command
restore operations 191	restore commands 191	object auditing 494
save operations 191	restoring programs that adopt	object authority required 435
security officer (QLMTSECOFR	authority 227	RMVALRD (Remove Alert Description)
system value) 232	restoring programs with restricted	command
retain server security (QRETSVRSEC)	instructions 227	object auditing 452
system value	RSTLICPGM (Restore Licensed	object authority required 314
overview 26	Program) command 227	RMVAUTLE (Remove Authorization List
retain server security (QRETSVRSEC)	save commands 191	Entry) command
value 26	special authorities 68	description 273
Retrieve Authorization List Entry	RJ (restoring job description) file	object auditing 453
(RTVAUTLE) command 273	layout 579	object authority required 316
Retrieve Journal Receiver Information	RJ (restoring job description) journal	using 146
API	entry type 246	RMVBKP (Remove Breakpoint) command
object auditing 479	RJE (remote job entry)	object authority required 417
Retrieve User Profile (RTVUSRPRF)	object authority required for	RMVBNDDIRE (Remove Binding
command 107, 276	commands 422	Directory Entry) command
retrieving	RLSCMNDEV (Release Communications	object auditing 454
authorization list entry 273	Device) command	object authority required 317
user profile 107, 276	authorized IBM-supplied user	RMVCFGLE (Remove Configuration List
RETURN (Return) command	profiles 296	Entries) command
object authority required 436	object auditing 460, 480	object authority required 324
reversing	object authority required 330	RMVCFGLE (Remove Configuration List
page down (*ROLLKEY user	RLSDSTQ (Release Distribution Queue)	Entry) command
option) 90	command	object auditing 454
page up (*ROLLKEY user option) 90	authorized IBM-supplied user	RMVCLUNODE
Revoke Object Authority (RVKOBJAUT)	profiles 296	authorized IBM-supplied user
command 139, 147, 274	object authority required 333	profiles 296
Revoke Public Authority (RVKPUBAUT)	RLSIFSLCK (Release IFS Lock) command	RMVCLUNODE command
command	authorized IBM-supplied user	object authority required 320
description 280, 627	profiles 296	RMVCMNE (Remove Communications
details 630	RLSIFSLCK (Release IFS Lock) command)	Entry) command
Revoke User Permission (RVKUSRPMN)	command	object auditing 494
command 277	object authority required 399	object authority required 435
revoking	RLSJOB (Release Job) command	RMVCNNLE (Remove Connection List
object authority 274	object authority required 370	Entry) command
public authority 280, 627	RLSJOBQ (Release Job Queue) command	object auditing 457
user permission 277	object auditing 476	RMVCOMSNMP (Remove Community
RGZDLO (Reorganize Document Library	object authority required 373	for SNMP) command
Object) command	RLSJOBSCDE (Release Job Schedule	object authority required 441
object auditing 466	Entry) command	RMVCRGDEVE
object authority required 335	object auditing 477	authorized IBM-supplied user
RGZPFM (Reorganize Physical File	object authority required 373	profiles 296
Member) command	RLSOUTQ (Release Output Queue)	RMVCRGNODE
object auditing 472	command	authorized IBM-supplied user
object authority required 344	object auditing 487	profiles 296
	object authority required 407	

RMVCRQD (Remove Change Request RMVEXITPGM (Remove Exit Program) RMVLICKEY (Remove License Key) Description Activity) command command object auditing 456 authorized IBM-supplied user object authority required 388 RMVCRQDA (Remove Change Request profiles 296 RMVLNK (Remove Link) command Description Activity) command object authority required 421 object auditing 496, 501, 502 object authority required 317 RMVFCTE (Remove Forms Control Table object authority required 360 RMVCRSDMNK (Remove Cross Domain Entry) command RMVM (Remove Member) command object auditing 472 Key) command object authority required 425 authorized IBM-supplied user RMVFNTTBLE (Remove DBCS Font object authority required 344 profiles 296 Table Entry) RMVMFS (Remove Mounted File System) object authority required 327 object authority required for object authority required 442 RMVMFS (Remove Mounted File System) RMVDEVDMNE commands 313 authorized IBM-supplied user RMVFTRACNE (Remove Filter Action command profiles 296 Entry) command authorized IBM-supplied user RMVDEVDMNE command object auditing 474 profiles 296 object authority required 346 object authority required 321 object authority required 399 RMVDIR (Remove Directory) command RMVFTRSLTE (Remove Filter Selection RMVMSG (Remove Message) command object auditing 462 Entry) command object auditing 484 object authority required 359 object auditing 474 object authority required 394 RMVDIRE (Remove Directory Entry) object authority required 346 RMVMSGD (Remove Message command RMVICFDEVE (Remove Intersystem Description) command description 278 **Communications Function Program** object auditing 483 object authority required 331 Device Entry) command object authority required 394 RMVDIRSHD (Remove Directory Shadow object authority required 344 RMVNETJOBE (Remove Network Job RMVIMGCLGE Entry) command System) command authorized IBM-supplied user object authority required 331 authorized IBM-supplied user RMVDLOAUT (Remove Document profiles 296 profiles 296 Library Object Authority) command RMVIMGCLGE command object authority required 398 description 277 object authority required 349 RMVNETTBLE (Remove Network Table RMVIPSIFC (Remove IP over SNA object auditing 466 Entry) command object authority required 335 Interface) command object authority required 441 RMVDSTLE (Remove Distribution List object authority required 314 RMVNODLE (Remove Node List Entry) Entry) command RMVIPSLOC (Remove IP over SNA command object auditing 485 object authority required 333 Location Entry) command RMVDSTQ (Remove Distribution Queue) object authority required 314 object authority required 402 command RMVIPSRTE (Remove IP over SNA RMVNWSSTGL (Remove Network Server authorized IBM-supplied user Route) command Storage Link) command profiles 296 object authority required 314 object authority required 400 RMVJOBQE (Remove Job Queue Entry) object authority required 333 RMVOPTCTG (Remove Optical RMVDSTRTE (Remove Distribution command Cartridge) command object auditing 477, 494 authorized IBM-supplied user Route) command authorized IBM-supplied user object authority required 435 profiles 296 profiles 296 RMVJOBSCDE (Remove Job Schedule object authority required 406 RMVOPTSVR (Remove Optical Server) object authority required 333 Entry) command RMVDSTSYSN (Remove Distribution object auditing 477 command Secondary System Name) command object authority required 373 authorized IBM-supplied user authorized IBM-supplied user RMVJRNCHG (Remove Journaled profiles 296 profiles 296 object authority required 406 Changes) command object authority required 333 authorized IBM-supplied user RMVPEXDFN (Remove Performance RMVEMLCFGE (Remove Emulation Explorer Definition) command profiles 296 Configuration Entry) command object auditing 450, 478 authorized IBM-supplied user object authority required 331 object authority required 376 profiles 296 RMVENVVAR (Remove Environment RMVLANADP (Remove LAN Adapter) object authority required 412 Variable) command RMVPEXFTR command command object authority required 338 authorized IBM-supplied user authorized IBM-supplied user RMVEWCBCDE (Remove Extended profiles 296 profiles 296 RMVLANADPI (Remove LAN Adapter RMVPFCST (Remove Physical File Wireless Controller Bar Code Entry) command Information) command Constraint) command object auditing 472 object authority required 338 object authority required 391 RMVEWCPTCE (Remove Extended RMVLANADPT (Remove LAN Adapter) object authority required 344 Wireless Controller PTC Entry) RMVPFTGR (Remove Physical File command command object authority required 391 Trigger) command object authority required 339 RMVLIBLE (Remove Library List Entry) object auditing 472 RMVEXITPGM (Add Exit Program) command RMVPFTRG (Remove Physical File command using 183 Trigger) command object auditing 470 object authority required 344

RMVPGM (Remove Program) command RMVTCPRTE (Remove TCP/IP Route) RSMCTLRCY (Resume Controller object authority required 417 Recovery) command RMVPJE (Remove Prestart Job Entry) object authority required 441 object auditing 459 command RMVTRC (Remove Trace) command object authority required 326 object auditing 494 object authority required 417 RSMDEVRCY (Resume Device Recovery) object authority required 435 RMVTRCFTR RMVPTF (Remove Program Temporary authorized IBM-supplied user object auditing 460 Fix) command profiles 296 object authority required 330 authorized IBM-supplied user RMVWSE (Remove Workstation Entry) RSMLINRCY (Resume Line Recovery) profiles 296 command command object authority required 428 object auditing 494 object auditing 480 object authority required 391 RMVRDBDIRE (Remove Relational object authority required 435 Database Directory Entry) command RNM (Rename) command RSMNWIRCY (Resume Network object authority required 422 object auditing 462, 496, 501, 502 Interface Recovery) command RMVRJECMNE (Remove RJE object authority required 360 object auditing 485 Communications Entry) command RST (Restore) command RNMCNNLE (Rename Connection List object authority required 425 Entry) command authorized IBM-supplied user RMVRJERDRE (Remove RJE Reader object auditing 457 profiles 296 RNMDIRE (Rename Directory Entry) object auditing 451, 462, 496, 501, Entry) command object authority required 425 command RMVRJEWTRE (Remove RJE Writer object authority required 331 object authority required 360 Entry) command RNMDKT (Rename Diskette) command RSTAUT (Restore Authority) command object authority required 425 object authority required 392 audit journal (QAUDJRN) entry 246 RMVRMTJRN (Remove Remote Journal) RNMDLO (Rename Document Library authorized IBM-supplied user Object) command profiles 296 command object auditing 478 object auditing 467 description 277 RMVRMTPTF (Remove Remote Program object authority required 335 object authority required 445 Temporary Fix) command RNMDSTL (Rename Distribution List) procedure 226 authorized IBM-supplied user command role in restoring security 221 profiles 296 object authority required 333 using 225 RMVRPYLE (Remove Reply List Entry) RNMM (Rename Member) command RSTCFG (Restore Configuration) command object auditing 473 command authorized IBM-supplied user object authority required 344 authorized IBM-supplied user RNMOBJ (Rename Object) command profiles 296 profiles 296 object auditing 451 object auditing 493 object auditing 451, 480, 503 object authority required 307 object authority required 436 object authority required 323 RMVRTGE (Remove Routing Entry) RNMTCPHTE (Rename TCP/IP Host RSTDLO (Restore Document Library Object) command 221 command Table Entry) command object auditing 494 object authority required 441 authorized IBM-supplied user object authority required 435 RO (ownership change for restored profiles 296 RMVSCHIDXE (Remove Search Index object) file layout 580 object auditing 467 RO (ownership change for restored object authority required 335 Entry) command object auditing 495 object) journal entry type 246 RSTLIB (Restore Library) command 221 object authority required 368 roll key (\*ROLLKEY) user option 90 authorized IBM-supplied user RMVSOCE (Remove Sphere of Control ROLLBACK (Rollback) command profiles 296 object authority required 322 object auditing 451 Entry) command object authority required 432 routing entry object authority required 386 RMVSVRAUTE (Remove Server RSTLICPGM (Restore Licensed Program) authority to program 176 Authentication Entry) command changing command audit journal (QAUDJRN) authorized IBM-supplied user object authority required 427 RMVTAPCTG (Remove Tape Cartridge) entry 251 profiles 296 command performance 192 object auditing 451 object authority required 392 RP (restoring programs that adopt object authority required 389 recommendations 227 RMVTCPHTE (Remove TCP/IP Host authority) file layout 581 Table Entry) command RP (restoring programs that adopt security risks 227 object authority required 441 authority) journal entry type 246 RSTOBJ (Restore Object) command authorized IBM-supplied user RMVTCPIFC (Remove TCP/IP Interface) RPLDOC (Replace Document) command command object auditing 467 profiles 296 object authority required 335 object auditing 451 object authority required 441 RQ (restoring \*CRQD object that adopts RMVTCPPORT (Remove TCP/IP Port object authority required 307 authority) file layout 583 Entry) command using 221 object authority required 441 RQ (restoring \*CRQD object) journal RSTS36F (Restore System/36 File) RMVTCPRSI (Remove TCP/IP Remote entry type 246 command System Information) command RRTJOB (Reroute Job) command authorized IBM-supplied user object authority required 441 object authority required 370 profiles 296

RSMBKP (Resume Breakpoint) command

object authority required 417

object authority required 344, 439

RSTS36FLR (Restore System/36 Folder) RTVCURDIR (Retrieve Current Directory) RTVQMQRY (Retrieve Query Management Query) command command command (continued) authorized IBM-supplied user object authority required 361 (continued) profiles 296 RTVDLONAM (Retrieve Document object authority required 419 object authority required 336, 439 Library Object Name) command RTVS36A (Retrieve System/36 Attributes) RSTS36LIBM (Restore System/36 Library object authority required 336 command Members) command RTVDOC (Retrieve Document) command object auditing 503 authorized IBM-supplied user object auditing 465, 467 object authority required 439 object authority required 336 RTVSMGOBJ (Retrieve Systems profiles 296 object authority required 386, 439 RTVDSKINF (Retrieve Disk Activity Management Object) command RSTS38AUT (Restore System/38 authorized IBM-supplied user Information) command Authority) command profiles 297 authorized IBM-supplied user RTVSYSVAL (Retrieve System Value) authorized IBM-supplied user profiles 297 profiles 296 object authority required 404 command object authority required 396 RTVDTAARA (Retrieve Data Area) object authority required 436 RSTSHF (Restore Bookshelf) command RTVUSRPRF (Retrieve User Profile) command object auditing 467 object auditing 468 command object authority required 327 RSTSYSINF description 276 object authority required 308 RTVGRPA (Retrieve Group Attributes) object auditing 505 RSTUSFCNR (Restore USF Container) command object authority required 445 using 107 command object authority required 436 RTVWSCST (Retrieve Workstation authorized IBM-supplied user RTVIMGCLG command profiles 297 authorized IBM-supplied user Customizing Object) command RSTUSRPRF (Restore User Profiles) profiles 297 object auditing 506 object authority required 349 object authority required 446 command RU (restore authority for user profile) file authorized IBM-supplied user RTVJOBA (Retrieve Job Attributes) profiles 297 command layout 583 description 221, 277 object authority required 370 RU (restore authority for user profile) object auditing 504 RTVJRNE (Retrieve Journal Entry) journal entry type 246 object authority required 445 run priority 192 command RTVAUTLE (Retrieve Authorization List object auditing 478 RUNBCKUP (Run Backup) command Entry) command object authority required 376 object authority required 404 description 273 RTVLIBD (Retrieve Library Description) RUNLPDA (Run LPDA-2) command authorized IBM-supplied user object auditing 453 command profiles 297 object authority required 316 object authority required 386 RTVBCKUP (Retrieve Backup Options) RTVMBRD (Retrieve Member object auditing 480 Description) command object authority required 428 object authority required 404 object auditing 473 RUNQRY (Run Query) command object auditing 492 RTVBNDSRC (Retrieve Binder Source) object authority required 344 RTVMSG (Retrieve Message) command object authority required 419 command \*SRVPGM, retrieving exports object auditing 483 RUNSMGCMD (Run Systems from 397 RTVNETA (Retrieve Network Attributes) Management Command) command object auditing 453, 482, 499 command authorized IBM-supplied user object authority required 397 profiles 297 object authority required 398 RTVCFGSRC (Retrieve Configuration RTVOBJD (Retrieve Object Description) RUNSMGOBJ (Run Systems Management Source) command Object) command command object auditing 457, 458, 459, 460, object auditing 452 authorized IBM-supplied user 480, 485, 486 object authority required 308 profiles 297 object authority required 323 RTVPDGPRF (Retrieve Print Descriptor RUNSQLSTM (Run Structured Query RTVCFGSTS (Retrieve Configuration Group Profile) command Language Statement) command Status) command object authority required 413 object authority required 384 object auditing 459, 460, 480, 485, RTVPRD (Retrieve Product) command RVKACCAUT (Revoke Access Code authorized IBM-supplied user Authority) command profiles 297 object authority required 323 object auditing 467 RTVCLDSRC (Retrieve C Locale Source) RTVPTF (Retrieve PTF) command object authority required 402 authorized IBM-supplied user RVKOBJAUT (Revoke Object Authority) profiles 297 object auditing 455 command 139 RTVCLNUP (Retrieve Cleanup) RTVPWRSCDE (Retrieve Power On/Off description 274 command Schedule Entry) command object auditing 451 object authority required 404 object authority required 404 object authority required 308 RTVCLSRC (Retrieve CL Source) RTVQMFORM (Retrieve Query using 147 Management Form) command RVKPUBAUT (Revoke Public Authority) command object auditing 488 object auditing 492 command object authority required 417 object authority required 419 authorized IBM-supplied user RTVCURDIR (Retrieve Current Directory) RTVQMQRY (Retrieve Query profiles 297 Management Query) command description 280, 627 command object auditing 461 object auditing 491, 492 details 630

RVKPUBAUT (Revoke Public Authority)	saving (continued)	SAVSTG (Save Storage) command
command (continued)	private authority 221	(continued)
object authority required 308	public authority 221	object authority required 309
RVKUSRPMN (Revoke User Permission)	restricting 191	SAVSYS (Save System) command
command	security data 221, 277	description 277
description 277	security information 221	object authority required 309
object auditing 467	security risks 191	using 221
object authority required 402	system 221, 277	SAVSYSINF
RVKWSOAUT (Revoke Workstation	user profile	object authority required 310
Object Authority) command	commands 221	SBMCRQ (Submit Change Request)
object authority required 347	SAVLIB (Save Library) command	command
RZ (primary group change for restored	object auditing 449	object auditing 455
object) file layout 583	object authority required 387	SBMDBJOB (Submit Database Jobs)
RZ (primary group change for restored	using 221	command
object) journal entry type 246	SAVLICPGM (Save Licensed Program)	object authority required 370
	command authorized IBM-supplied user	SBMDKTJOB (Submit Diskette Jobs) command
S	profiles 297	object authority required 370
	object auditing 449	SBMFNCJOB (Submit Finance Job)
S/36 machine description (*S36)	object authority required 389	command
auditing 503	SAVOBJ (Save Object) command	authorized IBM-supplied user
SAV (Save) command	object auditing 449	profiles 297
object auditing 449, 461, 500, 502	object authority required 309	object authority required 346
object authority required 362	saving audit journal receiver 261	SBMJOB (Submit Job) command
SAVAPARDTA (Save APAR Data)	using 221	authority checking 176
command authorized IBM-supplied user	SAVRSOBJ (Save Restore Object)	object authority required 370
profiles 297	command	SECBATCH menu 622
object authority required 428	object authority required 310	SBMNETJOB (Submit Network Job)
SAVCFG (Save Configuration) command	SAVRSTCFG (Save Restore	command
object auditing 459, 480, 485, 486	Configuration) command	object authority required 370
object authority required 323	object authority required 323	SBMNWSCMD (Submit Network Server
SAVCHGOBJ (Save Changed Object)	SAVRSTCHG	Command) command
command	authorized IBM-supplied user profiles 297	authorized IBM-supplied user profiles 297
object auditing 449	SAVRSTCHG (Save Restore Change)	object authority required 401
object authority required 308	command	SBMRJEJOB (Submit RJE Job) command
SAVDLO (Save Document Library Object)	object authority required 310	object authority required 425
command	SAVRSTDLO (Save Restore Document	SBMRMTCMD (Submit Remote
object auditing 449, 465	Library Object) command	Command) command
object authority required 336 using 221	object authority required 336	object authority required 322
Save Document Library Object (SAVDLO)	SAVRSTLIB	scan
command 221	authorized IBM-supplied user	object alterations 235, 270, 276
Save Library (SAVLIB) command 221	profiles 297	scan file systems (QSCANFS) system
Save Object (SAVOBJ) command 221,	SAVRSTLIB (Save Restore Library)	value 28
261	command	scan file systems control (QSCANFSCTL)
Save Security Data (SAVSECDTA)	object authority required 387 SAVRSTOBJ	system value 28 scheduling
command 221, 277	authorized IBM-supplied user	security reports 622
save system (*SAVSYS) special authority	profiles 297	user profile
*OBJEXIST authority 112, 302	SAVS36F (Save System/36 File) command	activation 619
description 230	object authority required 345, 439	expiration 619
functions allowed 70	SAVS36LIBM (Save System/36 Library	scheduling priority
removed by system changing security levels 10	Members) command	limiting 77
risks 70	object authority required 345, 387	scrolling
Save System (SAVSYS) command 221,	SAVSAVFDTA (Save Save File Data)	reversing (*ROLLKEY user
277	command	option) 90
save/restore (*SAVRST) audit level 246	object auditing 449	SD (change system distribution directory)
saving	object authority required 345	file layout 585
audit journal receiver 261	SAVSECDTA (Save Security Data)	SD (change system distribution directory)
auditing 230	command description 277	journal entry type 245 SE (change of subsystem routing entry)
authority holder 221	object authority required 445	file layout 586
authorization list 221	using 221	SE (change of subsystem routing entry)
document library object (DLO) 221	SAVSHF (Save Bookshelf) command	journal entry type 251
library 221	object auditing 449, 465	search index
object 221 object ownership 221	SAVSTG (Save Storage) command	object authority required 368
primary group 221	object auditing 452	search index (*SCHIDX) auditing 494
. JUT		

SECBATCH (Submit Batch Reports) menu scheduling reports 622	security level (QSECURITY) system value (continued)	server authentication object authority required for		
submitting reports 622	automatic user profile creation 57 commands 427			
SECTOOLS (Security Tools) menu 619	changing server authentication entry			
security	level 10 to level 20 10	adding 278		
Common Criteria	level 20 to level 30 10	changing 278		
description 5	level 20 to level 40 15	removing 278		
critical files 210	level 20 to level 50 17	server security user information actions		
designing 195	level 30 to 20 10	(SO) file layout 593		
job description 182	level 30 to level 40 15	server session		
keylock 2	level 30 to level 50 17	audit journal (QAUDJRN) entry 244		
library lists 183	level 40 to 20 10	server session (VS) file layout 603		
objective	level 40 to level 30 16	server session VS) journal entry		
availability 1	level 50 to level 30 or 40 18	type 244		
confidentiality 1	comparison of levels 7	server storage space (*SVRSTG)		
integrity 1 output queue 186	disabling level 40 16 disabling level 50 18	object 499 service		
overall recommendations 196	enforcing QLMTSECOFR system	object authority required for		
physical 2	value 179	commands 427		
planning 1	internal control blocks 17	service (*SERVICE) special authority		
printer output 186	introduction 2	failed sign-on 177		
source files 217	level 10 9	functions allowed 70		
spooled file 186	level 20 10	risks 70		
starting	level 30 10	service (QSRV) user profile		
batch job 176	level 40 11	authority to console 179		
interactive job 175	level 50	default values 283		
jobs 175	message handling 16	service basic (QSRVBAS) user		
subsystem description 181	overview 16	profile 283		
system values 3	QTEMP (temporary) library 16	service program		
tools 279	validating parameters 14	adopted authority 130		
why needed 1	overview 7	service program (*SRVPGM)		
security (*SECURITY) audit level 249	recommendations 9	auditing 499		
security administrator (*SECADM)	special authority 8	service status change (VV) file		
special authority	user class 8	layout 605		
functions allowed 69	value set by CFGSYSSEC command 628	service status change (VV) journal entry		
security attribute object authority required for	security officer	type 252 service tools (*SERVICE) audit level 252		
commands 426	See also security officer (QSECOFR)	service tools (SERVICE) audit rever 232 service tools action (ST) file layout 594		
security audit	user profile	service tools action (ST) journal entry		
object authority required for	limiting workstation access 25	type 252		
commands 426	monitoring actions 271	session		
security audit journal	restricting to certain	object authority required for		
displaying entries 279	workstations 232	commands 422		
printing entries 623	security officer (QSECOFR) user profile	session description (*SSND)		
security auditing	authority to console 179	auditing 499		
displaying 279, 621	default values 283	Set Attention Program (SETATNPGM)		
setting up 279, 621	device description owner 179	command 86		
security auditing function	disabled status 62	set password to expired (PWDEXP)		
activating 258	enabling 62	parameter 61		
CHGSECAUD 257	restoring 224	SETATNPGM (Set Attention Program)		
stopping 261	security tools	command		
Security Auditing Journal Entries 241 security command	commands 279, 619	job initiation 86 object authority required 417		
list 273	contents 279, 619 menus 619	SETCSTDTA (Set Customization Data)		
security data	Security Tools (SECTOOLS) menu 619	command		
saving 221, 277	security value	object authority required 347		
security information	setting 627	SETJOBATR (user options) parameter		
backup 221				
Dackup 221	e e	user profile 89		
•	Send Journal Entry (SNDJRNE) command 259	user profile 89 SETMSTK (Set Master Key) command		
format on save media 222 format on system 222	Send Journal Entry (SNDJRNE)	user profile 89 SETMSTK (Set Master Key) command authorized IBM-supplied user		
format on save media 222	Send Journal Entry (SNDJRNE) command 259	SETMSTK (Set Master Key) command		
format on save media 222 format on system 222	Send Journal Entry (SNDJRNE) command 259 Send Network Spooled File	SETMSTK (Set Master Key) command authorized IBM-supplied user		
format on save media 222 format on system 222 recovery 221 restoring 221 saving 221	Send Journal Entry (SNDJRNE) command 259 Send Network Spooled File (SNDNETSPLF) command 186 sending journal entry 259	SETMSTK (Set Master Key) command authorized IBM-supplied user profiles 297		
format on save media 222 format on system 222 recovery 221 restoring 221 saving 221 stored on save media 222	Send Journal Entry (SNDJRNE) command 259 Send Network Spooled File (SNDNETSPLF) command 186 sending journal entry 259 network spooled file 186	SETMSTK (Set Master Key) command authorized IBM-supplied user profiles 297 object authority required 327 SETOBJACC (Set Object Access) command		
format on save media 222 format on system 222 recovery 221 restoring 221 saving 221 stored on save media 222 stored on system 222	Send Journal Entry (SNDJRNE) command 259 Send Network Spooled File (SNDNETSPLF) command 186 sending journal entry 259 network spooled file 186 sensitive data	SETMSTK (Set Master Key) command authorized IBM-supplied user profiles 297 object authority required 327 SETOBJACC (Set Object Access)		
format on save media 222 format on system 222 recovery 221 restoring 221 saving 221 stored on save media 222	Send Journal Entry (SNDJRNE) command 259 Send Network Spooled File (SNDNETSPLF) command 186 sending journal entry 259 network spooled file 186	SETMSTK (Set Master Key) command authorized IBM-supplied user profiles 297 object authority required 327 SETOBJACC (Set Object Access) command		

SETPGMINF (Set Program Information) command	sign-on information (continued) displaying (continued)	SNDNETSPLF (Send Network Spooled File) command
object authority required 417	QDSPSGNINF system value 22	action auditing 497
SETTAPCGY (Set Tape Category)	Sign-on Information display	object auditing 487
command	DSPSGNINF user profile	object authority required 433
object authority required 392	parameter 74	output queue parameters 186
setting	example 22	SNDNWSMSG (Send Network Server
Attention-key-handling program	expired password message 39, 61	Message) command
(ATNPGM) 86 network attributes 280, 627	signing	object authority required 401
	integrity 3 object 3	SNDPGMMSG (Send Program Message)
security values 627 system values 280, 627	SIGNOFF (Sign Off) command	command object authority required 394
setting up	object authority required 436	SNDPRD (Send Product) command
auditing function 258	Signon screen	authorized IBM-supplied user
security auditing 279, 621	changing 180	profiles 297
SETVTMAP (Set VT100 Keyboard Map)	displaying source for 180	SNDPTF (Send PTF) command
command	Signon screen display file 180	authorized IBM-supplied user
object authority required 441	size of password 41, 42	profiles 297
SETVTTBL (Set VT Translation Tables)	SLTCMD (Select Command) command	SNDPTFORD (Send Program Temporary
command	object authority required 322	Fix Order) command
object authority required 440	SM (systems management change) file	authorized IBM-supplied user
SEV (message queue severity) parameter	layout 592	profiles 297
See also message queue	SM (systems management change)	object authority required 428
user profile 84	journal entry type 252	SNDRJECMD (Send RJE Command)
severity (SEV) parameter	SNA distribution services (QSNADS) user	command
See also message queue	profile 283	object authority required 425
user profile 84	SNADS (Systems Network Architecture	SNDRJECMD (Send RJE) command
SF (action to spooled file) file layout 587	distribution services)	object authority required 425
SF (change to spooled file) journal entry	QSNADS user profile 283	SNDRPY (Send Reply) command
type 252	SNDBRKMSG (Send Break Message)	object auditing 484
share memory control (QSHRMEMCTL)	command	object authority required 394
system value	object authority required 394	SNDSMGOBJ (Send Systems
description 29	SNDDOC (Send Document) command	Management Object) command
possible values 29 shared folder	object auditing 465 SNDDST (Send Distribution) command	authorized IBM-supplied user profiles 297
securing 190	object auditing 465	SNDSRVRQS (Send Service Request)
sign-on	object authority required 333	command
action when attempts reached	SNDDSTQ (Send Distribution Queue)	authorized IBM-supplied user
(QMAXSGNACN system value) 26	command	profiles 297
authorities required 175	authorized IBM-supplied user	object authority required 429
authority failures 175	profiles 297	SNDTCPSPLF (Send TCP Spooled File)
console 179	object authority required 333	command
incorrect password	SNDDTAARA (Send Data Area)	object authority required 434
audit journal (QAUDJRN)	command	SNDTCPSPLF (Send TCP/IP Spooled
entry 242	object auditing 468	File) command
incorrect user ID	SNDEMLIGC (Send DBCS 3270PC	action auditing 497
audit journal (QAUDJRN)	Emulation Code) command	object auditing 506
entry 242	object authority required 331	object authority required 440
limiting attempts 25	SNDFNCIMG (Send Finance Diskette	SNDUSRMSG (Send User Message)
preventing default 234	Image) command	command
remote (QRMTSIGN system	object authority required 346	object authority required 394
value) 27	SNDJRNE (Send Journal Entry)	SO (server security user information
restricting security officer 177 security checking 175	command 259 object auditing 478	actions) file layout 593 socket
security effecting 173	object authority required 376	giving
service user fails 177	SNDMGRDTA (Send Migration Data)	audit journal (QAUDJRN)
user with *ALLOBJ special authority	command	entry 250
fails 177	object authority required 395	sockets
user with *SERVICE special authority	SNDMSG (Send Message) command	object authority required for
fails 177	object authority required 394	commands 313
without user ID 181	SNDNETF (Send Network File) command	sort sequence
without user ID and password 13	object authority required 398	QSRTSEQ system value 87
workstation authority needed 177	SNDNETMSG (Send Network Message)	shared weight 87
sign-on information	command	unique weight 87
displaying	object authority required 398	user profile 87
DSPSGNINF user profile		source file
parameter 73		securing 217

SPCAUT (special authority) parameter See also special authority recommendations 72	Special Files (*CHRSF) auditing 454 spelling aid dictionary object authority required for	status (STATUS) parameter user profile 62 status message
user profile 68 SPCENV (special environment) parameter recommendations 72	commands 431 spelling aid dictionary (*SPADCT) auditing 497	displaying (*STSMSG user option) 90 not displaying (*NOSTSMSG user option) 90
routing interactive job 72	sphere of control	stopping
Special Authorities	object authority required for	audit function 261
authorities, special 215	commands 432	auditing 50
Special Authorities, Accumulating 215	spool (QSPL) user profile 283	storage
special authority	spool control (*SPLCTL) special authority	enhanced hardware protection 14
*ALLOBJ (all object)	functions allowed 69	maximum (MAXSTG) parameter 76
auditing 233	output queue parameters 187	reclaiming 16, 124, 229
automatically added 10	risks 70	setting QALWUSRDMN (allow
automatically removed 10	spool job (QSPLJOB) user profile 283	user objects) system value 21
failed sign-on 177	spooled file	threshold
functions allowed 68	*JOBCTL (job control) special	audit (QAUDJRN) journal
risks 68	authority 69	receiver 260
*AUDIT (audit)	*SPLCTL (spool control) special	user profile 76
functions allowed 71	authority 69	storage pool 192
risks 71	action auditing 497	STRAPF (Start Advanced Printer
*IOSYSCFG (system configuration)	changing	Function) command
functions allowed 71	audit journal (QAUDJRN)	object authority required 314, 345
risks 72	entry 252	STRASPBAL
*JOBCTL (job control)	copying 186	authorized IBM-supplied user
functions allowed 69	deleting user profile 103	profiles 297
output queue parameters 187	displaying 186	STRASPBAL command 330
priority limit (PTYLMT)	moving 186	STRBEST (Start Best/1-400 Capacity
parameter 78	object authority required for	Planner) command
risks 69	commands 432	object authority required 412
*SAVSYS (save system)	owner 186	STRBEST (Start BEST/1) command
*OBJEXIST authority 112, 302	securing 186	authorized IBM-supplied user
automatically removed 10	working with 186	profiles 297
description 230	spooled file changes (*SPLFDTA) audit	STRBGU (Start Business Graphics Utility)
functions allowed 70	level 252, 497	command
risks 70	SQL	object authority required 314
*SECADM (security administrator)	file security 213	STRCBLDBG (Start COBOL Debug)
functions allowed 69	SQL catalog 213	command
*SERVICE (service)	SQL package (*SQLPKG) auditing 498	object authority required 384, 417
failed sign-on 177	SRC (system reference code)	STRCGU (Start CGU) command
functions allowed 70	B900 3D10 (auditing error) 51	object authority required 337 STRCHTSVR (Start Clustered Hash Table
risks 70	SRTSEQ (sort sequence) parameter	Server Server
*SPLCTL (spool control) functions allowed 69	user profile 87 ST (service tools action) file layout 594	
output queue parameters 187	ST (service tools action) ine layout 554 ST (service tools action) journal entry	authorized IBM-supplied user profiles 297
risks 70	type 252	STRCLNUP (Start Cleanup) command
added by system	Start QSH (STRQSH) command	object authority required 404
changing security level 10	object authority required	STRCLUNOD
adopted authority 128	alias, QSH 418	authorized IBM-supplied user
analyzing assignment 623	Start System/36 (STRS36) command	profiles 297
changing security level 10	user profile	STRCLUNOD command
definition 68	special environment 72	object authority required 321
listing users 268	starting	STRCMNTRC (Start Communications
recommendations 72	auditing function 258	Trace) command
removed by system	connection	authorized IBM-supplied user
automatically removed 224	audit journal (QAUDJRN)	profiles 297
changing security level 10	entry 244	object authority required 429
user profile 68	state	STRCMTCTL (Start Commitment Control)
special authority (SPCAUT) parameter	program 13	command
See also special authority	state attribute	object authority required 322
recommendations 72	object 12	STRCPYSCN (Start Copy Screen)
user profile 68	state attribute, program	command
special environment (QSPCENV) system	displaying 13	object authority required 429
value 72	STATFS (Display Mounted File System	STRCRG
special environment (SPCENV) parameter recommendations 72	Information) command object authority required 399	authorized IBM-supplied user profiles 297
routing interactive job 72	object audiority required 355	promes 231

STRCSP (Start CSP/AE Utilities) command object auditing 489 STRDBG (Start Debug) command authorized IBM-supplied user profiles 297 object auditing 470, 488 object authority required 417 STRDBGSVR (Start Debug Server) command authorized IBM-supplied user profiles 297 STRDBMON (Start Database Monitor) command object authority required 412 STRDBRDR (Start Database Reader) command object authority required 421 STRDFU (Start DFU) command object authority required 315, 345 STRDIRSHD (Start Directory Shadow System) command object authority required 331 STRDIRSHD (Start Directory Shadowing) command object auditing 464 STRDKTRDR (Start Diskette Reader) command object authority required 421 STRDKTWTR (Start Diskette Writer) command object authority required 447 STRDSKRGZ (Start Disk Reorganization) command object authority required 332 stream file (\*STMF) auditing 499 STREDU (Start Education) command object authority required 403 STREML3270 (Start 3270 Display Emulation) command object authority required 331 STRFMA (Start Font Management Aid) command object auditing 476 object authority required 338 STRHOSTSVR authorized IBM-supplied user profiles 297 STRHOSTSVR (Start Host Server) command object authority required 348 STRIDD (Start Interactive Data Definition Utility) command object authority required 367 STRIDXMON (Start Index Monitor) command authorized IBM-supplied user profiles 297 STRIPSIFC (Start IP over SNA Interface) command authorized IBM-supplied user profiles 297 object authority required 314 STRJOBTRC (Start Job Trace) command authorized IBM-supplied user profiles 297 object authority required 412

STRJRN (Start Journal) command object authority required 363, 376 STRJRN (Start Journaling) command object auditing 451 STRJRNAP (Start Journal Access Path) command object authority required 376 STRJRNOBJ (Start Journal Object) command object authority required 376 STRJRNPF (Start Journal Physical File) command object authority required 376 STRJRNxxx (Start Journaling) command object auditing 478 STRLOGSVR (Start Job Log Server) command object authority required 370 STRMGDSYS (Start Managed System) command authorized IBM-supplied user profiles 297 STRMGRSRV (Start Manager Services) command authorized IBM-supplied user profiles 297 STRMOD (Start Mode) command object auditing 482 object authority required 396 STRMSF (Start Mail Server Framework) command authorized IBM-supplied user profiles 297 object authority required 391 STRNFSSVR (Start Network File System Server) command authorized IBM-supplied user profiles 298 STRNFSSVR (Start Network File System Server) command) command object authority required 399 STROBJCVN authorized IBM-supplied user profiles 298 STROBJCVN command 310 STRPASTHR (Start Pass-Through) command object auditing 459 object authority required 332 STRPDM (Start Programming Development Manager) command object authority required 315 STRPEX (Start Performance Explorer) command authorized IBM-supplied user profiles 298 object authority required 412 STRPFRG authorized IBM-supplied user profiles 298 STRPFRG (Start Performance Graphics) command object authority required 412 authorized IBM-supplied user

profiles 298

STRPFRT (Start Performance Tools) command object authority required 413 STRPFRTRC (Start Performance Trace) command authorized IBM-supplied user profiles 298 object authority required 413 STRPJ (Start Prestart Jobs) command object authority required 371 STRPRTEML (Start Printer Emulation) command object authority required 331 STRPRTWTR (Start Printer Writer) command object auditing 486, 506 object authority required 448 STRQMQRY (Start Query Management Query) command object auditing 490, 491, 492 object authority required 419 STRQRY (Start Query) command object authority required 420 STRQSH (Start QSH) command object authority required alias, QSH 418 STRQST (Start Question and Answer) command object authority required 420 STRREXPRC (Start REXX Procedure) command object authority required 384 STRRGZIDX (Start Reorganization of Index) command authorized IBM-supplied user profiles 298 STRRJECSL (Start RJE Console) command object authority required 425 STRRJERDR (Start RJE Reader) command object authority required 425 STRRJESSN (Start RJE Session) command object authority required 425 STRRJEWTR (Start RJE Writer) command object authority required 426 STRRLU (Start Report Layout Utility) command object authority required 315 STRRMTWTR (Start Remote Writer) command action auditing 497, 506 object auditing 486 object authority required 448 STRS36 (Start System/36) command object auditing 503 user profile special environment 72 STRS36MGR (Start System/36 Migration) command authorized IBM-supplied user profiles 298 object authority required 396 STRS38MGR (Start System/38 Migration) command authorized IBM-supplied user profiles 298 object authority required 396

STRSBS (Start Subsystem) command	subsystem	system distribution directory (continued)
object auditing 493	*JOBCTL (job control) special	deleting user profile 101
object authority required 436	authority 69	system library list
STRSCHIDX (Start Search Index)	See also subsystem description	changing 183, 202
command	object authority required for	QSYSLIBL system value 183
object auditing 494	commands 434	system operations
object authority required 368	sign on without user ID and	special authority (SPCAUT)
3 1	_	
STRSDA (Start SDA) command	password 13	parameter 68
object authority required 315	subsystem description	system operator (QSYSOPR) user
STRSEU (Start SEU) command	authority 279	profile 283
object authority required 315	communications entry 181	system password 110
STRSQL (Start Structured Query	default user 279	system portion
Language) command	entry 279	library list
object authority required 384, 408	performance 192	changing 202
STRSRVJOB (Start Service Job) command	printing list of descriptions 279	description 183
authorized IBM-supplied user	printing security-relevant	recommendations 184
profiles 298	parameters 623	system program
object authority required 429	routing entry change	calling directly 12
STRSST (Start System Service Tools)	audit journal (QAUDJRN)	system reference code (SRC)
command	entry 251	B900 3D10 (auditing error) 51
authorized IBM-supplied user	security 181	system reply list
profiles 298	subsystem description (*SBSD)	object authority required for
object authority required 429	auditing 493	commands 436
STRSSYSMGR (Start System Manager)	SUPGRPPRF (supplemental groups)	system request function
command	parameter	adopted authority 129
authorized IBM-supplied user	user profile 81	System request menu
profiles 298	supplemental group	options and commands 208
STRTCP (Start TCP/IP) command	planning 215	using 208
· · · · · · · · · · · · · · · · · · ·	1 0	System Request menu
authorized IBM-supplied user	supplemental groups	y 1
profiles 298	SUPGRPPRF user profile	limit device sessions
object authority required 440	parameter 81	(LMTDEVSSN) 75
STRTCPFTP (Start TCP/IP File Transfer	SV (action to system value) file	system resources
Protocol) command	layout 597	limiting use
object authority required 440	SV (action to system value) journal entry	priority limit (PTYLMT)
STRTCPIFC (Start TCP/IP Interface)	type 251	parameter 77
command	symbolic link (*SYMLNK) auditing 502	preventing abuse 192
authorized IBM-supplied user	system	system signing 3
profiles 298	object authority required for	system status
object authority required 441	commands 436	working with 192
STRTCPPTP (Start Point-to-Point TCP/IP)	saving 221, 277	system value
command	system (*SYSTEM) domain 12	action when sign-on attempts reached
object authority required 441	system (*SYSTEM) state 13	(QMAXSGNACN)
STRTCPSVR (Start TCP/IP Server)	system (QSYS) library	description 26
command	authorization lists 118	user profile status 62
authorized IBM-supplied user	system (QSYS) user profile	allow object restore option
profiles 298	default values 283	(QALWOBJRST) 37
object authority required 441	restoring 224	allow user objects
STRTCPTELN (Start TCP/IP TELNET)	system change-journal management	(QALWUSRDMN) 16, 21
command	support 260	Attention-key-handling program
object authority required 441	system configuration	(QATNPGM) 86
STRTRC (Start Trace) command	*IOSYSCFG (system configuration)	audit
object authority required 429	special authority 71	planning 256
STRUPDIDX (Start Update of Index)	system configuration (*IOSYSCFG)	audit control (QAUDCTL)
command	special authority	changing 279
authorized IBM-supplied user	functions allowed 71	displaying 279
	risks 72	1 3 0
profiles 298	_	audit level (QAUDLVL)
STRWCH (Start Watch) command	system console	*AUTFAIL (authority failure)
authorized IBM-supplied user	See also console	description 242
profiles 298	QCONSOLE system value 179	*CREATE (create) value 243
STRWCH command	system directory	*DELETE (delete) value 243
object authority required 429	changing	*JOBDTA (job change) value 243
Submit Job (SBMJOB) command 176	audit journal (QAUDJRN)	*OBJMGT (object management)
SECBATCH menu 622	entry 245	value 245
submitting	system distribution directory	*OFCSRV (office services)
security reports 622	*SECADM (security administrator)	value 245
subset	special authority 69	*PGMADP (adopted authority)
authority 113	commands for working with 278	value 245

audit level (QAUDINT) (continued) **PCMFAIL (porgram failure) value 246 **PRITTY (printer output) value 246 **SEVURIT (security) value 249 **SEVURIT (security) value 249 **SEVURIT (severite tools) **SEVURIT (severite) value 249 **SEVURIT (systems management) value 252 **Changing 259, 279 displaying 279 purpose 236 user profile 91 auditing 232 coverview 49 auditing 232 **SEVURIT (systems management) value 252 changing 259, 279 displaying 279 purpose 236 user profile 91 auditing 232 coverview 49 auditing 232 coverview 49 auditing control (QAUDINT) coverview 50 auditing control (QAUDINT) coverview 51 auditing control (QAUDINT) coverview 53 auditing interest evide (QAUDINT) coverview 51 auditing interest control (systems management) value 248 **CREATE (create) value 243 **CREATE (create) value 245 **CREATE (create) value 246 **CREATE (create) value 246 **CREATE (create) value 246 **CREATE (create) value 247 **CREATE (create) value 248 **CREATE (create) value 248 **CREATE (create) value 248 **CREATE (create) value 2	system value (continued)	system value (continued)	system value (continued)		
scan (QSCANES) 28 PERIDIA (printer output) value 246 PERIDIA (printer output) value 246 SECURIT (security) value 249 SERVICE (service tools) value 252 SPLPIDA (apoeled file changes) purpose 236 Langing 259, 279 displaying 279 displ	•		•		
PRIDITA (printer output) value 246		scan (QSCANFSCTL) 28			
value 246 *SECURITY (security) value 249 *SEEVICE (service tools) value 232 *SELURITY (security) value 249 *SEEVICE (service tools) value 232 *SYSMGT (systems management) value 232 *Systems *Systems (systems management) value 232 *SYSMGT (systems management) value 232 *Systems *SYSMGT (systems management) value 232 *Systems *SYSMGT (systems management) value 232 *SYSMGT (systems management) value 232 *Systems *Systems (systems management) *Systems (systems profile parameter 75 *Suthfile (systems profile parameter 75 *Systems (systems profile parameter 75 *Systems (systems profile parameter 75 *Systems (systems profile parameter 75 *Suthf	value 246	keyboard buffering (QKBDBUF) 76	QAUDCTL (audit control)		
value 246 *SECURITY (security) value 249 *SEEVICE (service tools) value 232 *SELURITY (security) value 249 *SEEVICE (service tools) value 232 *SYSMGT (systems management) value 232 *Systems *Systems (systems management) value 232 *SYSMGT (systems management) value 232 *Systems *SYSMGT (systems management) value 232 *Systems *SYSMGT (systems management) value 232 *SYSMGT (systems management) value 232 *Systems *Systems (systems management) *Systems (systems profile parameter 75 *Suthfile (systems profile parameter 75 *Systems (systems profile parameter 75 *Systems (systems profile parameter 75 *Systems (systems profile parameter 75 *Suthf	*PRTDTA (printer output)	language identifier (QLANGID) 87			
*SECURITY (security) value 249 *SERVICE (service tools) value 252 *SPIFDTA (spooled file changes) value 252 *SYSMGT (systems management) value 252 changing 259, 279 displaying 279 purpose 236 user profile 94 auditing 232 overview 49 auditing 232 overview 50 auditing rortol (QAUDCTL) overview 50 auditing rortol (QAUDCTL) overview 50 auditing rorte elvel (QALDENDACN) 50, 256 auditing force level (QALDENDACN) 50, 256 auditing force level (QALDENCALY) 31, 256 auditing three level (QALDENCALY) 51, 256 auditing three level (QALDENCALY) 31 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCCC) 31 color for esting 280, 827 composite (QCONSOLID) 179 country or region identifier (QCYNTBYLD) 88 create authority 98 audit (purnal (QAUDRN) entry 25; disk of changing 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing (QCRTOBIAUD) 54 description 22 using 119 reate object auditing reader audition riverval (QPWDESPTI'V) second auditing reader audition riverval (QPWDESPTI'V) preventing trivial 233 required file systems scan (QSCANEST) 28 printing security-relevant 280, 623 QALWOSERIM (allow object restore) option) 37 qualdition provalesting security co		limit device sessions (QLMTDEVSSN)	displaying 279, 621		
**SERVICE* (service tools) value 252  **SPLFDTA (spooled file changes) value 252  **SYSMCT (systems management) value 252  changing 259, 279  displaying 279  purpose 236  user profile 94  auditing 232  overview 49  auditing 232  overview 49  auditing control (QAUDENDACN) 50, 256  auditing force level (QAUDECLU) 50, 256  auditing force level (QAUDECLU) 50, 256  auditing force level (QAUDECLU) 51, 256  auditing level (QAUDECLU) 52, 254  changing 528, 278, 251  auditing level (QAUDECLU) 52, 254  changing 528, 278, 274  changing 529, 278  changing on attempts 10  changing 628, 279  changing 628, 279  changing 628, 279	*SAVRST (save/restore) value 246	auditing 233	QAUDCTL (auditing control)		
value 252  VSPMETTA Gooded file changes) value 252  Value 252  VSPMETTA Gooded file changes) value 252  changing 259, 279  displaying 279  purpose 236  user profile 94  auditing 232  overview 49  auditing 232  overview 49  auditing 232  overview 49  auditing 232  overview 50  auditing action (QAUDCIL)  overview 50  auditing action (QAUDCIL)  overview 51  auditing 102  daybe extension (QAUDLVL)  overview 51  auditing evel extension (QAUDLVL)  overview 52  automatic configuration (QAUDINN)  culting explication 123  daturnatic device originarition (QAUTOCFG) 31  changing  QALTOCFG 31  changing  CONTENTID 88  curan authority 68  curan authority 68  curan authority 68  curan authority 68  curan authority of consecutive digits (QPWDLATICR) 43  proved or region identifier (QCMTENTD) 88  curan authority (QCKTAUT)  description 22  raise of changing 22  using 119  create object auditing (QCMTOBIALD) 34  disconnected job time-out interval (QDSCORTY) 33  display sign on information (QPWDEAPTIV) uses profile authority of the consecutive digits (QPWDLATICR) 85  printing 232  rinting out interval (QPWDEAPTIV) 85  rinting 232  rinting security selvels 11  description 25  sign on process 179  sign on process 179  sign on process 179  changing security selvels 11  description 25  sign on process 179  sing on process 179  sign of process 179  sign of pr	*SECURITY (security) value 249	description 24	overview 50		
value 252  VSPMETTA Gooded file changes) value 252  Value 252  VSPMETTA Gooded file changes) value 252  changing 259, 279  displaying 279  purpose 236  user profile 94  auditing 232  overview 49  auditing 232  overview 49  auditing 232  overview 49  auditing 232  overview 50  auditing action (QAUDCIL)  overview 50  auditing action (QAUDCIL)  overview 51  auditing 102  daybe extension (QAUDLVL)  overview 51  auditing evel extension (QAUDLVL)  overview 52  automatic configuration (QAUDINN)  culting explication 123  daturnatic device originarition (QAUTOCFG) 31  changing  QALTOCFG 31  changing  CONTENTID 88  curan authority 68  curan authority 68  curan authority 68  curan authority 68  curan authority of consecutive digits (QPWDLATICR) 43  proved or region identifier (QCMTENTD) 88  curan authority (QCKTAUT)  description 22  raise of changing 22  using 119  create object auditing (QCMTOBIALD) 34  disconnected job time-out interval (QDSCORTY) 33  display sign on information (QPWDEAPTIV) uses profile authority of the consecutive digits (QPWDLATICR) 85  printing 232  rinting out interval (QPWDEAPTIV) 85  rinting 232  rinting security selvels 11  description 25  sign on process 179  sign on process 179  sign on process 179  changing security selvels 11  description 25  sign on process 179  sing on process 179  sign of process 179  sign of pr	*SERVICE (service tools)		QAUDENDACN (auditing end		
value 252	value 252				
value 252		limit security officer (QLMTSECOFR)	QAUDFRCLVL (auditing force		
changing 259, 779 displaying 279 purpose 236 user profile 94 auditing 232 overview 49 auditing control (QAUDCTI) overview 50 auditing end action (QAUDEDACN) 50, 256 auditing force level (QAUDERCIVI) 51, 256 auditing level extension (QAUDLVI2) overview 51 auditing level extension (QAUDLVI2) overview 53 automatic configuration of virtual devices (QAUDVIX) 31 automatic device configuration (QAUTOCFG 31 changing "SECADM (security administrator) special authority 69 autit journal (QAUDIRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNID) 88 create authority (QCRTAUT) description 22 risk of changing 22 using 119 create object auditing (QCRTOSINT) 23 display sign-on information (QDSPGSONIN) 22, 74 file systems scan (QSCANFS) 28 file systems	value 252	authority to device	level) 51, 256		
changing 259, 779 displaying 279 purpose 236 user profile 94 auditing 232 overview 49 auditing control (QAUDCTI) overview 50 auditing end action (QAUDEDACN) 50, 256 auditing force level (QAUDERCIVI) 51, 256 auditing level extension (QAUDLVI2) overview 51 auditing level extension (QAUDLVI2) overview 53 automatic configuration of virtual devices (QAUDVIX) 31 automatic device configuration (QAUTOCFG 31 changing "SECADM (security administrator) special authority 69 autit journal (QAUDIRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNID) 88 create authority (QCRTAUT) description 22 risk of changing 22 using 119 create object auditing (QCRTOSINT) 23 display sign-on information (QDSPGSONIN) 22, 74 file systems scan (QSCANFS) 28 file systems	*SYSMGT (systems management)	descriptions 177	QAUDLVL (audit level)		
changing 259, 279 displaying 279 purpose 236 user profile 94 auditing 232 overview 49 auditing enter level (QALDECTL) overview 50 auditing force level (QALDENDACN) 50, 256 auditing force level (QALDENDACN) 50, 256 auditing level (QALDIVL) overview 51 auditing level extension (QAUDIVL) overview 51 auditing level extension (QAUDIVL) overview 51 automatic device configuration of virtual devices (QALTIOVRT) 31 automatic device configuration (QAUTOCFC) 31 clanging *SECADM (security administrator) special authority of 99 audit journal (QALDIRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCTIDD 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCTISD 88 create authority (QCKTAUT) description 22 risk of changing 22 using 19 create object auditing (QCECORSOLE) 27 risk of changing 22 using 19 create object auditing (QCECORSOLE) 27 risk of changing 22 risk of chang		changing security levels 11	*AUTFAIL (authority failure)		
purpose 236 user profile 94 auditing 232 overview 49 auditing control (QAUDCTL) overview 50 auditing entrol (QAUDCTL) overview 50 auditing entrol (QAUDCTL) overview 50 auditing control (QAUDCTL) overview 50 auditing control (QAUDCTL) overview 51 auditing level (QAUDIVL) overview 51 auditing level (QAUDIVL) overview 53 auditing level (QAUDIVL) overview 54 auditing level (QAUDIVL) overview 53 auditing level (QAUDIVL) overview 54 sauditing level (QAUDIVL) overview 54 southers	changing 259, 279				
user profile 94 auditing 232 23 overview 49 auditing control (OAUDCTL) overview 50 auditing end action (QAUDENDACN) 50, 256 auditing force level (QAUDERDACN) 50, 256 auditing force level (QAUDERDEVIL) 51, 256 auditing level (QAUDIXL) overview 51 auditing evel (QAUDIXL) overview 53 automatic configuration of virtual devices (QAUDIVI) 31 automatic device configuration (QAUTOVRT) 40 control 40 coverview 53 auditing level extension (QAUTOVRT) 85 (QPWDIMTALEN) 42 minimum length (QPWDEMPTIV) 93, 74 displaying 729, 621 displaying 729, 621 displaying 729, 621 displaying 729, 621 purpose 235 user profile 94 QAUDLVL (auditing level) value 245 "PGMADIR (adopted authority) value 245 "PCMFAIL (program failure) value 245 "PCMFAIL (program failure) value 245 "SAVRRT (save/restory value 246 "SECURITY (security) value 249 "SERVICE (service tools) value 252 "SPLFDTA (spooled file changes) value 252 "SPLFDTA	displaying 279	sign-on process 179	*CREATE (create) value 243		
audtling 232 overview 49 audtling control (QAUDCTL) overview 50 audting end action (QAUDENDACN) 50, 256 audtling free level (QAUDENDACN) 50, 256 audtling free level (QAUDENDACN) 50, 256 audtling evel (QAUDLYL) overview 51 audtling level (QAUDLYL) overview 53 audtomatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 changing 'SECADM (security administrator) special authority 69 audtling level devices of limit repeated characters (QPWDLMTCHR) 43 limit repeated characters (QPWDLMTR) 43 limit repeated characters (	purpose 236	listing 232	*DELETE (delete) value 243		
auditing control (QAUDCTL) overview 50 auditing end action (QAUDENDACN) 50, 256 auditing force level (QAUDER(IVL) 51, 256 auditing fere level (QAUDLRCIVL) overview 51 auditing level (QAUDLVL) overview 51 auditing level extension (QAUDLVL) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 clhanging "SECADM (security administrator) special authority 69 audit journal (QAUDLRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console QCONSOLE) 179 country or region identifier (QCCTOBLOED) 58 create authority (QCRTALT) description 22 risk of changing 22 using 119 create object auditing (QCRTOBIAUD) 54 disconnected job time-out interval (QDSCORINF) 22, 74 file systems scan (QSCANFCI) 28 inactive job message queue (QINACTIMSQ) 24 time-out interval (QINACTIMSQ) 24 time-out interval (QINACTIMSQ) 24 time-out interval (QINACTIMSQ) 28 interpreted for command 628 QALMOBIRST (allow object restore) value 245 'PGMADP (adopted authority) value 246 'PRIDTA (printed output) value 246 'PSCURTALL (program failure) value 246 'SECURIC (services) value 245 'PGMADP (adopted authority) value 246 'SECURIC (service tous) value 246 'SECURITY (security) value 249 'SERVICE (services) value 246 'SECURITY (security) value 249 'SERVICE (service tools) value 252 'SYBMGT (systems management) value 245 'SECURITY (scourity) value 249 'SERVICE (service tools) value 252 'SYBMGT (systems management) value 252 'SYBMGT (sy	user profile 94	maximum sign-on attempts	*JOBDTA (job change) value 243		
auditing control (QAUDCTL) overview 50 auditing end action (QAUDENDACN) 50, 256 auditing force level (QAUDFRCIAL) 51, 256 auditing force level (QAUDFRCIAL) 51, 256 auditing evel (QAUDLVL) overview 51 auditing evel extension (QAUDLVL) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 (QPWDLMFCHR) 43 imit adjacent (QPWDLMFCHR) 43 imit adjacent (QPWDLMFCHR) 43 imit adjacent (QPWDLMFCHR) 43 imit adjacent (QPWDLMFRPP) 43 auditing expiration tinterval (QAUTOVRT) 31 automatic device configuration (QAUTOVRT) 83 (QPWDMINLEN) 42 maximum length (QPWDMINLEN) 41 auditing expiration tinterval (QCONSOLE) 179 connic device department of the value 252 changing 259, 279, 621 displaying 279		(QMAXSIGN)	*OBJMGT (object management)		
overview 50 auditing end action (QAUDENDACN) 50, 256 commands 436 password queries (QAUDERCLY) 51, 256 auditing force level (QAUDERCLY) 51, 256 auditing fevel (QAUDLYL) overview 51 auditing expiration 233 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 clear (QPWDLMTAIC) 43 limit adjacent (QPWDLMTAIC) 43 limit reparted characters (QPWDIAMTER) 43 limit reparted characters (QPWDIAMTER) 43 auditi journal (QAUDIRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 create authority (QCRTOBIAUD) 54 disconnected job time out interval (QDSCJOBITV) 33 display sign-on information (QDSCSONNF) 22 file systems scan (QSCANFCT) 28 inactive job message queue (QINACTIMSCQ) 24 time-out interval (QINACTIMSCQ) 28 integrated file systems scan (QCANES) 28 integrated file systems scan (QCANES) 28 integrated file systems scan (QCANES) 28 integrated file systems scan (QSCANES) 28 integrated file systems scan (QSCANES) 28 integrated file systems scan (QSCANES) 28 integrated file systems scan (QCANES) 28 integrated file systems	overview 49	auditing 232, 235	value 245		
auditing end action (QAUDENDACN) 50, 256 auditing force level (QAUDFRCLYL) 51, 256 auditing level (QAUDIVL) overview 51 auditing level extension (QAUDIVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 changing "SECADM (security administrator) special authority 69 audit journal (QAUDINN) entry 251 coded character set identifier (QCCSTOB) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNSOLE) 179 country or region identifier (QCCNTSUDB) 88 create authority (QCRTAUT) description 22 risk of changing 22 using 119 create object auditing (QCRTOBIAUD) 54 disconnected job time-out interval (QDSCIOBITV) 33 display sign-on information (QDSCIOBITV) 33 display sign-on information (QDSCSONET) 28 file systems can (QSCANFST) 28 file systems control scan (QSCANFST) 28 fine-out interval (QINACTMSCQ) 24 (QINACTMSCQ) 24 (QINACTMSCQ) 24 (QINACTMSCQ) 24 (QINACTMSCQ) 25 inactive job message queue (QINACTTTY) 23 integrated file systems scan (QSCANFST) 28 inactive job message queue (QINACTMSCQ) 24 (QINACTMSCQ) 24 (QINACTMSCQ) 25 integrated file systems scan (QSCANFST) 28 inactive job message queue (QINACTTTY) 23 integrated file systems scan (QSCANFST) 28 inactive job message queue (QINACTTTY) 23 integrated file systems scan (QSCANFST) 28 inactive job message queue (QINACTTTY) 23 integrated file systems scan (QSCANFST) 28 integrated file s	auditing control (QAUDCTL)	description 25	*OFCSRV (office services)		
(QAUDENDACN) 50, 256 auditing force level (QAUDFRCLVL) 51, 256 auditing level (QAUDLVL) overview 51 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 changling "SECADM (security administrator) special authority 69 audit journal (QAUDJRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 create authority (QCRTAUT) description 22 risk of changing 25 reate authority (QCRTAUT) description 22 risk of changing 25 reate authority (QCRTAUT) description 22 risk of changing 25 reate authority (QCRTAUT) description 22 risk of changing 25 reate authority (QCRTAUT) description 22 risk of changing 25 reate object auditing (QCRTOBJAUD) 54 disconnected job time-out interval (QDSCJOBITV) 33 display sign on information (QCRTOBJAUD) 54 disconnected job time-out interval (QDSPSGNINF) 22, 74 file systems scan (QSCANFCTLS) 28 inactive job message queue (QINACTMSGQ) 24 rime-out interval (QINACTMSGQ) 24 rime-out interval (QINACTMSGQ) 24 rime-out interval (QINACTMSGQ) 24 rime-out interval (QINACTTIV) 23 integrated file systems scan (QSCANFCTLS) 28 inactive job message queue (QINACTTIV) 23 integrated file systems scan (QSCANFS) 28 QALWOSRBMS (allow object restore) value 245 *SAVRST (saver/restore) value 246 *SAVRST (saver/restore) value 249 *SERVICE (service tools) value 252 *SYSMCT (systems management) value 252 *SYSMCT (sy	overview 50	user profile status 62	value 245		
auditing force level (QAUDFRCLVL) 51, 256 auditing level (QAUDIVL) overview 51 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic configuration of (QAUDCCFG) 31 (QAUTOCCFG) 31 (QCATTOCCFG) 31 (QCAT	auditing end action	object authority required for	*PGMADP (adopted authority)		
QAUDYRCLVI J. 51, 256 auditing level (QAUDLVL) overview 51 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 changing "SECADM (security administrator) special authority 69 audit journal (QAUDIRN) entry 251 coded character set identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 create authority (QCRTAUT) description 22 risk of changing 22 risk of changing 22 restee object auditing (QCCTGIBAUD) 54 disconnected job time-out interval (QDSCGBITV) 33 display sign-on information (QCSCSID Sa) sean (QSCANFS) 28 file systems sean (QSCANFS) 28 file systems sean (QSCANFS) 28 file systems sean (QSCANFS) 28 inactive job message queue (QINACTITV) 23 integrated file systems sean (QSCANFS) 28 integrated file systems sean (QSCANFS) 28 QALWSKDMN (allow user  value 246 "PRTDTA (printed output) value 246 "SANEST (save restore) value 246 "SANEST (save restore) value 249 "SEECUERTY (security) value 249 "SEECUERTY (security) value 252 "SPLFDTA (printed output) value 249 "SEECUERTY (security value 249 "SEECUERTY (security value 249 "SEECUERTY (security value 252 "SPLFDTA (prointed output) value 249 "SEECUERTY (security value 252 "SPLFDTA (prointed output) value 249 "SEECUERTY (security value 252 "SPLFDTA (prointed output) value 249 "SEECUERTY (security value 252 "SPLFDTA (prointed output) value 249 "SEECUER (service tools) value 252 "SPLFDTA (prointed output) value 249 "SEEVICE (service tools) value 252 "SPLFDTA (prointed output) value 249 "SEEVICE (service tools) value 252 "SPLFDTA (prointed output) value 249 "SEEVICE (service tools) value 252 "SPLFDTA (prointed output) value 249 "SEEVICE (service tools) value 252 "SPLFDTA (prointed output) value 252 "SP	(QAUDENDACN) 50, 256	commands 436	value 245		
auditing level (QAUDLVL) overview 51 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOVRT) 46 auditing evel 249 *SECURITY (security) value 252 *SPLFDTA (spooled file changes) value 252 *SYSMGT (systems management) value 252 *AUTOVR (automatic value 252 *AUTOVR (automatic value 252 *AUTOVR (automatic value 252 *AUTOVR (automatic value 252 *AUTOVR (autom	auditing force level	password	*PGMFAIL (program failure)		
overview 51 auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic configuration (QAUTOCFC) 31 changing 'SECADM (security administrator) special authority 69 audit journal (QAUDJRN) entry 251 code character st identifier (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCCNTRYD) 88 create authority (QCRTAUT) description 22 risk of changing 22 risk of changing 22 risk of changing 22 restriction of consecutive digits (QPWDLMTALC) 43 limit repeated characters (QPWDRMNLEN) 41 (QPWDRMNLEN) 42 restriction of consecutive digits (QPWDRMDNLEN) 44 disconnected job time-out interval (QNCSIGNITY) 23 display sign-on information (QCRTOBJAUD) 54 disconnected job time-out interval (QNCSCORITY) 28 file systems scan (QSCANFS) 28 printing security- communications 280 printing security- restore option) 37 QALWOBIRST (allow object restore) (QINACTTIV) 23 integrated file systems scan (QSCANFS) 28 QALWUSRDMN (allow user  automatic device configuration of virtual device to option) 37 duplicate (QPWDRCDGT) 44 cyperting trivial 233 cyalue 248 *SAVRST (save/restore) value 246 *SAVRST (save/restore) value 248 *SECUCITY (security) value 252 *SPLFDTA (spooled file changes) value 252 *CANGT (spooled file changes) value 252 *CANGT (spooled file changes) value 252 *CANGT (spooled file changes) value 252 *CANGTOBLAUL (auditing level extension) overview 51 QALTOCFG (automatic configuration) value set by CFGSYSSEC configuration) value set by CFGSYSSEC configuration) value set by CFGSYSSEC configuration value set by CFGSYSSEC configuration value set by CFGSYSSEC con	(QAUDFRCLVL) 51, 256	approval program	value 246		
auditing level extension (QAUDLVL2) overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 automatic device configuration (QAUTOCFG) 31 changing  "SECADM (security administrator) special authority 69 audit journal (QAUDIRN) entry 251 coded character set identifier (QCCSID) 88 (QPWDMAXLEN) 42 minimum length (QCCNSOLE) 179 country or region identifier (QCCSID) 88 (QPWDMRQDDGT) 44 create authority (QCRTAUT) description 22 risk of changing 22 restriction of consecutive digits (QCWDLATTAC) 43 disconnected job time-out interval (QDSPSGNINF) 22, 74 file systems scan (QSCANFS) 28 inactive job message queue (QINACTITV) 23 integrated file systems scan (QSCANFS) 28 inactive job message queue (QINACTITV) 23 integrated file systems scan (QSCANFS) 28 integrated file systems scan (QSCANFS) 28 inactive job restriction of consecutive digits (QRMDEXPITV user profile parameter 74 QALWOBIRST (allow object restore) value 252 changing 259, 279, 621 displaying 279, 621 purpose 236 user profile 9 QUEDIVLI (auditing level) overview 51 QAUDIVLI (auditing level) overview 51 QAUDIVLI (auditing level extension) overview 53 QAUTOCFG (automatic device configuration) value set by CFGSYSSEC command 628 QAUTOCRG (automatic device configuration) 31 QAUTOVRT (automatic virtual-device) configuration) value set by CFGSYSSEC command 628 QCCSID (coded character set identifier) 88 QCCSID (coded character set identifier) 88 QCONSOLE (console) 179 QCRTAUT (create authority) description 22 using 119 QCRTOBAUD (create object auditing) 54	auditing level (QAUDLVL)	(QPWDVLDPGM) 44	*PRTDTA (printed output)		
overview 53 automatic configuration of virtual devices (QAUTOVRT) 31 limit adjacent (QAWDEXPITV) 39, 74 limit adjacent (QAWDEOFIG) 31 limit characters (QAWDLMTCHR) 43 limit characters (QPWDLMTCHR) 43 limit characters (QPWDLMTCHR) 43 limit characters changing  "SECADM (security administrator) special authority 69 audit journal (QAUDJRN) entry 251 coded character set identifier (QCCSID) 88 (QPWDMAXLEN) 42 minimum length (QCCSID) 88 (QPWDMINLEN) 41 (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 create authority (QCRTAUT) description 22 risk of changing 22 risk of changing 22 risk of changing 22 reate authority (QCRTOBIAUD) 54 (QCRTOBISONSOLE) 28 file systems scan (QSCANFS) 28 file systems control scan (QSCANFS) 28 file systems control scan (QSCANFS) 28 inactive job message queue (QINACTINSQQ) 24 time-out interval (QINACTINSQQ) 25 command 628 QALWOSIBST (allow object restore) value 252 sSPLFDTA (spoted shanges) value 252 sSPLFDTA (spoted systems management) value 252 sysymc value 252 sysymc value 252 sysymc value 252 changing 25, 279, 621 displaying 279, 621 displayi	overview 51	auditing expiration 233	value 246		
automatic configuration of virtual devices (QAUTOVRT) 31 limit adjacent (QPWDEMTAIC) 43 limit adjacent (QPWDLMTAIC) 43 schanging (QPWDLMTAIC) 43 limit repeated characters (QPWDLMTGEP) 43 maximum length (QPWDLMTREP) 43 maximum length (QPWDLMTREP) 43 maximum length (QPWDLMTLEN) 41 displaying 279, 621 displaying 279, 621 displaying 279, 621 overview 38 command for setting 280, 627 overview 38 position characters (QCCNSOLE) 179 conded characters (QPWDEMTAIC) 43 preventing trivial 233 create authority (QCRTAUT) required password digits using 119 (QPWDRAICA) 44 disconnected job time-out interval (QDSCIOBITV) 33 display sign-on information (QDSCIOBITV) 33 display sign-on information (QDSCIOBITV) 28 file systems scan (QSCANFS) 28 file systems control scan (QSCANFS) 28 file systems control scan (QSCANFS) 28 file systems control scan (QSCANFS) 24 (QINACTITV) 25 (QINACTITV)	auditing level extension (QAUDLVL2)	duplicate (QPWDRQDDIF) 42	*SAVRST (save/restore) value 246		
devices (QAUTOVRT) 31 limit adjacent (QPWDLMTAJC) 43 syspensis configuration (QAUTOCFG) 31 limit characters (QPWDLMTCHR) 43 special authority 69 (QPWDLMTCHR) 43 special authority 69 audit journal (QAUDIRN) amaximum length (QPWDLMTREP) 43 maximum length (QPWDLMTREP) 43 maximum length (QPWDLMTREP) 45 special authority 69 audit journal (QAUDIRN) amaximum length (QPWDMINLEN) 41 special overview 38 (QPWDMINLEN) 41 sposition characters (QPWDMINLEN) 41 sposition characters (QPWDMINLEN) 41 sposition characters (QPWDRINDEN) 41 sposition characters (QPWDRINDEN) 41 sposition characters (QPWDRINDEN) 41 sposition characters (QPWDRINDEN) 42 sposition characters (QPWDRINDEN) 41 sposition characters (QPWDRINDEN) 42 sposition characters (QPWDRINDEN) 43 sposition characters (QPWDRINDEN) 44 preventing trivial 233 required password digits (QPWDRINDEN) 45 sposition program (QPWDRINDEN) 41 sposition program (QPWDRINDEN) 42 sposition program (QPWDRINDEN) 43 sposition program (QPWDRINDEN) 44 password expiration interval (QDSCIOBITV) 33 (QPWDRINDEN) 44 password expiration interval (QDSCIOBITV) 35 (QPWDRINDEN) 45 printing security communications 280 printing security expirating security spointing security-relevant 280, 623 (CCSID (coded character set identifier) 88 (CONSOLE (console) 179 (CONSOLE) 21 sintegrated file systems control sport and care set of the program of the p	overview 53	expiration interval	*SECURITY (security) value 249		
automatic device configuration (QAUTOCFG) 31 (QAUTOCFG) 31 (QPWDLMTCHR) 43 (SECADM (security administrator) special authority 69 (QPWDLMTCHR) 43 (QPWDLMTCHR) 43 (Autility 69 (QPWDLMTCHR) 43 (Autility 69 (QPWDLMTCHR) 43 (Autility 69 (QPWDLMTCHR) 43 (Autility 69 (Aut	automatic configuration of virtual	(QPWDEXPITV) 39, 74	*SERVICE (service tools)		
(QAUTOCFG) 31 changing (QPWDLMTCHR) 43 "SECADM (security administrator) special authority 69 audit journal (QAUDJRN) maximum length entry 251 coded character set identifier minimum length (QCCSID) 88 (QPWDMAXLEN) 42 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QPWDDNDIE) 44 (QCCSID) 88 create authority (QCRTAUT) required password digits description 22 risk of changing 22 restriction of consecutive digits (QPWDLMTAIC) 43 disconnected job time-out interval (QDSCJOBITV) 33 display sign-on information (QCRTOBJAUD) 54 file systems scan (QSCANFC) 28 file systems scan (QSCANFCTLS) 28 maximum length (QPWDRVDLDPCM) 44 parameter 74 print device (QPRTDEV) 85 file systems control scan (QSCANFCTLS) 28 maximum length (QPWDRVDLDPCM) 45 printing security-relevant 280, 623 message queue (QINACTITV) 23 integrated file systems scan (QSCANFS) 28 QALWOSBRST (allow object restore (QINACTITV) 23 integrated file systems scan (QSCANFS) 28 QALWOSBRST (allow object restore) qQRNACTITV) 23 integrated file systems maximum length (QPWDLMTCHC) 43 user profile 94 QAUDIVL (auditing level) overview 51 QAUDIVL2 (auditing level) overview 53 QAUTOCFG (automatic configuration) value set by CFGSYSSEC command 628 QAUTOVRT (automatic configuration of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC command 628 QCCSID (coded characters identifier) 88 QCNTRYID (country or region identifier) 88 QCNTRYID (country or region identifier) 88 QCNTRYID (country or region identifier) 89 QCNTRYID (country or region iden	devices (QAUTOVRT) 31	limit adjacent	value 252		
changing  "SECADM (security administrator) special authority 69 audit journal (QAUDJRN) entry 251 (QPWDLMTREP) 43 audit journal (QAUDJRN) entry 251 (QPWDMAXLEN) 42 minimum length (QCCSID) 88 (QPWDMINLEN) 41 (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 create authority (QCRTAUT) description 22 risk of changing 22 restriction of consecutive digits using 119 create object auditing (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCSCOBJETV) 33 (QSCANFS) 28 file systems scan (QSCANFS) 28 inactive job message queue (QINACTITIV) 23 integrated file systems scan (QCANFS) 28 pare verification for consecutive digits communications 280 printing security-relevant 280, 623 qALWOSRDEN (allow object restore) value set by CFGSYSSEC command 628 QCCSID (coded character set identifier) 88 QCONSOLE (console) 179 QCRTOBJAUD (coded character set identifier) 88 QCONSOLE (console) 179 QCRTRYID (country or region identifier) 88 inactive job message queue (QINACTITIV) 23 value set by CFGSYSSEC command 628 QALWOSBRST (allow object restore) value set by CFGSYSSEC value at 252 risk of changing 22 risk of changing 25 risk of changing 22 risk of changing 23 risk of changing 24 ruse 252 rhogical displaying 279, 621 purpose 236 radisplaying 279, 621 purpose 236 rad	automatic device configuration	(QPWDLMTAJC) 43	*SPLFDTA (spooled file changes)		
*SECADM (security administrator) special authority 69 (QPWDLMTREP) 43 changing 259, 279, 621 displaying 279, 621 displaying 279, 621 displaying 279, 621 entry 251 (QPWDMAXLEN) 42 purpose 236 user profile 94 (QCCSID) 88 (QPWDMINLEN) 41 QAUDLUL (auditing level) overview 38 position characters (QCNTRYID) 88 position characters (QPWDPOSDIF) 44 (QCNTRYID) 88 preventing trivial 233 (QAUTOCFG (automatic configuration) overview 53 (QPWDLMTALC) 43 command 628 (QPWDLMTALC) 43 command 628 (QPWDLMTALC) 43 command 628 (QPWDLMTALC) 43 command 628 (QPWDLMTALC) 43 configuration) 31 create object auditing (QPWDVLDPGM) 44 (QPSCOBITV) 33 (QPWDVLDPGM) 44 password expiration interval (QDSCOBITV) 33 (QPWDEAPTIV) (QPWDEAPTIV) (QPWDEAPTIV) ser profile parameter 74 paramete	(QAUTOCFG) 31		value 252		
special authority 69 audit journal (QAUDIRN) entry 251 coded character set identifier (QPWDMAXLEN) 42 purpose 236 coded character set identifier (QCCSID) 88 (QPWDMINLEN) 41 QAUDLVL (auditing level) command for setting 280, 627 console (QCONSOLE) 179 country or region identifier (QCNTRYID) 88 (QPWDPOSDIF) 44 (QCNTRYID) 88 preventing trivial 233 (CREATE authority (QCRTAUT) description 22 (QPWDRQDDGT) 44 risk of changing 22 restriction of consecutive digits using 119 (QCRTOBIAUD) 54 (QCRTOBIAUD) 54 (QCRTOBIAUD) 54 (QCRTOBIAUD) 54 (QPWDEXPITV) (QDSPGNINF) 22, 74 (QDSPGNINF) 22, 74 file systems scan (QSCANFS) 28 printing security- communications 280 printing security- relevant (QPNACTINGQ) 24 time-out interval (QINACTINGQ) 24 qALWOBIRST (allow object restore (QINACTINGQ) 24 time-out interval (QINACTITIV) 23 integrated file systems scan (QSCANFS) 28 QALWUSRDMN (allow user  QALWOSRDMN (allow user  changing 259, 279, 621 displaying 28 user profile purpose 236 user profile QAUTOCFG (automatic configuration) value set by CFGSYSSEC configuration) 31 QAUTOVRT (automatic configuration of virtual device) configuration of virtual device) configuration of virtual device) 24 CVESTORICHE QAUTOVRT (automatic virtual-device configuration) of virtual device) 31 QAUTOVRT (automatic virtual-device configuration) of virtual devi	changing	(QPWDLMTCHR) 43	*SYSMGT (systems management)		
audit journal (QAUDJRN) entry 251 (QPWDMAXLEN) 42 minimum length (QCCSID) 88 (QPWDMINLEN) 41 QAUDLVL (auditing level) overview 51 QAUDLVL (auditing level) overview 53 QAUDLVL (auditing level extension) country or region identifier (QCNTRYID) 88 (QPWDPOSDIF) 44 (QCNTRYID) 88 preventing trivial 233 create authority (QCRTAUT) description 22 risk of changing 22 restriction of consecutive digits using 119 create object auditing (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QCRTOBJAUD) 54 (QDSPCSGNIF) 23 (QPWDEXPITV) QSCJOBITV) 33 (QPWDEXPITV) QSCSCONFF) 28 print device (QPRTDEV) 85 scan (QSCANFS) 28 printing 232 printing security- communications 280 printing security- quive set by CFGSYSSEC command 628 printing security- relative object auditing optiming security- quive set by CFGSYSSEC command 628 qCCNISOLORITY) 23 integrated file systems control QALWOBJRST (allow object restore) (QINACTITNS Q) quive set by CFGSYSSEC command 628 QALWUSRDMN (allow user addisplay sign-on information QALWOSRSD (allow object restore) QRINACTITIV) 23 integrated file systems scan (QSCANFS) 28 QALWUSRDMN (allow user		•			
entry 251 coded character set identifier minimum length (QCCSID) 88 command for setting 280, 627 console (QCONSOLE) 179 position characters console (QCONSOLE) 179 position characters contry or region identifier (QCNTRYID) 88 preventing trivial 233 create authority (QCRTAUT) description 22 risk of changing 22 risk of changing 22 restriction of consecutive digits using 119 create object auditing (QCRTOBJAUD) 54 disconnected job time-out interval (QDSCIOBITV) 33 display sign-on information (QDSCSORITY) 33 display sign-on information (QDSCSORITY) 28 file systems scan (QSCANFS) 28 piniting security- scan (QSCANFCTLS) 28 inactive job message queue (QINACTIMSGQ) 24 purpose 236 user profile 94 QAUDIVI. (auditing level extension) overview 51 QAUDIOCFG (automatic configuration) value set by CFGSYSSEC command 628 QAUTOCFG (automatic device configuration) 31 create object auditing validation program (QCRTOBJAUD) 54 QPWDVLDPGM) 44 qof virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) qQPWDEXPITV command 628 qCONSOLE (configuration) value set by CFGSYSSEC command 628 qCONSOLE (console) 179 message queue (QINACTIMSGQ) 24 qolivolation printing security-relevant 280, 623 qCONSOLE (console) 179 message queue (QINACTITY) 23 value set by CFGSYSSEC command 628 QALWOBJRST (allow object restore) qCRTOBJAUD (create authority) description 22 risk of changing 22 using 119 integrated file systems scan (QSCANFS) 28 QALWUSRDMN (allow user					
coded character set identifier (QCCSID) 88 (QPWDMINLEN) 41 QAUDLVL (auditing level) overview 38 command for setting 280, 627 console (QCONSOLE) 179 position characters (QPWDPOSDIF) 44 QAUDLVL (auditing level) overview 51 QAUDLVL2 (auditing level extension) overview 53 (QCNTRYID) 88 preventing trivial 233 QAUTOCFG (automatic configuration) create authority (QCRTAUT) description 22 (QPWDRQDDGT) 44 risk of changing 22 restriction of consecutive digits using 119 (QCRTABIAUD) 54 disconnected job time-out interval (QCRTOBJAUD) 54 (QPWDVLDPGM) 44 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) display sign-on information PWDEXPITV user profile scan (QSCANFS) 28 file systems scan (QSCANFS) 28 printing 232 printing security- QAUTOVET QCRTAUT) scan (QSCANFCTLS) 28 inactive job message queue (QINACTIMSGQ) 24 quit of the continer		maximum length			
command for setting 280, 627 overview 38 overview 51 console (QCONSOLE) 179 position characters country or region identifier (QPWDPOSDIF) 44 (QCNTRYID) 88 preventing trivial 233 create authority (QCRTAUT) required password digits description 22 (QPWDRQDDGT) 44 risk of changing 22 restriction of consecutive digits using 119 (QPWDRUDIMTAIC) 43 create object auditing (QCRTOBIAUD) 54 (QPWDLMTAIC) 43 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) display sign-on information (QDSPSGNINF) 22, 74 file systems scan (QSCANFS) 28 inactive job message queu (QINACTMSGQ) 24 quired password digits (QPWDEXPTV user profile scan (QSCANFS) 28 inactive job message queu (QINACTMSGQ) 24 quired password expiration interval (QINACTMSGQ) 24 time-out interval (QINACTMSGQ) 24 quired password digits (QPWDEXPTV user profile scan (QSCANFS) 28 quired password expiration interval (QINACTMSGQ) 24 quired password digits (QPWDEXPTV user profile scan (QSCANFS) 28 quired password digits (QPWDEXPTV user profile scan (QSCANFS) 28 quired password digits (QPWDEXPTV user profile scan (QSCANFCTLS) 28 quired password digits (QPWDEXPTV user profile scan (QSCANFCTLS) 28 quired password digits quired password digits (QPWDEXPTV user profile password expiration interval (QPWDEXPTV user profile scan (QSCANFS) 28 quired password digits quired pasword password digits quired password digits quired pasword digits quired pasword password digits quired pasword password password passwor		,			
command for setting 280, 627 overview 38 overview 51 console (QCONSOLE) 179 position characters (QPWDPOSDIF) 44 overview 53 (QCNTRYID) 88 preventing trivial 233 QAUTOCFG (automatic configuration) create authority (QCRTAUT) required password digits description 22 (QPWDRQDDGT) 44 command 628 command 628 risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 configuration) 31 create object auditing (QCRTBAUD) 54 (QPWDLMTAIC) 43 configuration) 31 create object auditing (QCRTBAUD) 54 (QPWDLMTAIC) 43 configuration) 31 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) configuration information (QDSCJOBITV) 33 (QPWDEXPITV) ser profile (QDSPSCNINF) 22, 74 parameter 74 parameter 74 command 628 file systems control scan (QSCANFS) 28 printing security-scan (QSCANFCTLS) 28 communications 280 rinting security-scan (QSCANFCTLS) 28 communications 280 identifier) 88 inactive job printing security-relevant 280, 623 (QNSOLE (console) 179 message queue QALWOBIRST (allow object restore (QINACTIMSQ) 24 option) 37 time-out interval (QINACTIMSQ) 24 option) 37 time-out interval (QINACTITV) 23 value set by CFGSYSSEC (QRECSID) (cortent object auditing) 54 command 628 command 628 QCRTOBIAUD) (create object sauditing) 54 command 628 QCRTOBIAUD) (create object auditing) 54 command 628 QCR		0			
console (QCONSOLE) 179 position characters country or region identifier (QPWDPOSDIF) 44 overview 53 (QCNTRYID) 88 preventing trivial 233 QAUTOCFG (automatic configuration) cerate authority (QCRTAUT) required password digits description 22 (QPWDRQDDGT) 44 command 628 risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 configuration) 54 (QPWDEXPITV) configuration) 65 (QDSCJOBITV) 33 (QPWDEXPITV) seer profile (QDSPSGNINF) 22, 74 parameter 74 parameter 74 command 628 (QPWDEXPITV) 85 (QDSPSGNINF) 22, 74 parameter 74 parameter 74 parameter 74 parameter 74 parameter 74 parameter 74 printing security-command 628 (QCSID (coded character set identifier) 88 inactive job printing security-relevant 280, 623 inactive job printing security-relevant 280, 623 printing 29 (QINACTMSGQ) 24 option) 37 description 22 risk of changing 21 using 119 integrated file systems command 628 QALWOBIRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QALWOBIRST (allow object restore) command 628 QCRTOBJAUD (create object sauditing) 54	, ,	, ,			
country or region identifier (QCNTRYID) 88 preventing trivial 233 QAUTOCFG (automatic configuration) create authority (QCRTAUT) description 22 (QPWDRQDDGT) 44 risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 create object auditing (QCRTOBJAUD) 54 (QPWDLMTAIC) 43 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) (QDSCJOBITV) 33 (QPWDEXPITV) display sign-on information (QDSPGNINF) 22, 74 parameter 74 file systems scan (QSCANFS) 28 file systems ontrol scan (QSCANFCTLS) 28 inactive job message queue QALWOBJRST (allow object restore (QINACTITV) 23 integrated file systems command 628 QAUTOCFG (automatic device configuration) 31 create object auditing validation program QAUTOVRT (automatic configuration of virtual devices) 31 configuration) qAUTOVRT (automatic configuration of virtual devices) 31 configuration) value set by CFGSYSSEC configuration) value set by CFGSYSSEC command 628 qCCSID (coded character set identifier) 88 gCCNTRYID (country or region identifier) 88 qCONSOLE (console) 179 description 22 risk of changing 22 using 119 integrated file systems command 628 QAUTOCFG (automatic configuration) value set by CFGSYSSEC configuration) of virtual device configuration) value set by CFGSYSSEC command 628 QCONTRYID (country or region identifier) 88 QCONSOLE (console) 179 description 22 risk of changing 22 using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user					
create authority (QCRTAUT) crequired password digits description 22 risk of changing 22 risk of changing 22 risk of changing 21 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 create object auditing (QPWDLMTAIC) 43 create object auditing (QCRTOBJAUD) 54 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) (QDSPSGNINF) 22, 74 file systems scan (QSCANFS) 28 printing 232 file systems control scan (QSCANFCTLS) 28 inactive job message queue (QINACTMSGQ) 24 (QINACTITV) 23 integrated file systems scan (QSCANFS) 28 QALWOSRDMN (allow user  preventing trivial 233 QAUTOCFG (automatic configuration) value set by CFGSYSSEC command 628 QAUTOVRT (automatic configuration) of virtual devices 31 QAUTOVRT (automatic virtual-device configuration) of virtual devices 31 OAUTOVRT (automatic virtual-device confi		•	_		
create authority (QCRTAUT) description 22 (QPWDRQDDGT) 44 risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 create object auditing (QCRTOBJAUD) 54 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) (QDSPSGNINF) 22, 74 file systems scan (QSCANFS) 28 file systems control scan (QSCANFCTLS) 28 inactive job message queue (QINACTITV) 23 (QAUTOVRT (automatic device configuration) 44 of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC configuration) 45 configuration of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC configuration of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC configuration of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC configuration of virtual devices) 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC command 628 QCCSID (coded character set identifier) 88 printing security- qCNTRYID (country or region identifier) 88 QCNTRYID (country or region identifier) 88 QCNTRYID (country or region identifier) 88 QCNNSOLE (console) 179 QCRTAUT (create authority) description 22 risk of changing 119 integrated file systems command 628 QALWUSRDMN (allow user					
description 22 risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAIC) 43 create object auditing (QCRTOBJAUD) 54 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) display sign-on information (QDSPSGNINF) 22, 74 file systems scan (QSCANFS) 28 file systems control scan (QSCANFCTLS) 28 inactive job message queue (QINACTITV) 23 (QINACTITV) 23 value set by CFGSYSSEC (QINACTITV) 23 value set by CFGSYSSEC value set by CFGSYSSEC (QINACTITV) 23 value set by CFGSYSSEC value set by CFGSYSSEC (QINACTITV) 23 value set by CFGSYSSEC value set by CF					
risk of changing 22 restriction of consecutive digits using 119 (QPWDLMTAJC) 43 configuration) 31 create object auditing validation program QAUTOVRT (automatic configuration (QCRTOBJAUD) 54 (QPWDVLDPGM) 44 of virtual devices) 31 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) configuration) display sign-on information (QDSPGNINF) 22, 74 parameter 74 parameter 74 command 628 file systems print device (QPRTDEV) 85 QCCSID (coded character set identifier) 88 file systems control printing security-scan (QSCANFCTLS) 28 communications 280 printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QALWUSRDMN (allow user auditing) 54			· ·		
using 119 create object auditing create object auditing (QCRTOBJAUD) 54 (QPWDVLDPGM) 44 (QPWDVLDPGM) 44 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) display sign-on information (QDSPSGNINF) 22, 74 parameter 74 parameter 74 pirit device (QPRTDEV) 85 scan (QSCANFS) 28 print device (QPRTDEV) 85 printing 232 printing 232 printing security-scan (QSCANFCTLS) 28 printing security-relevant 280, 623 printing sequerity (QINACTMSGQ) 24 poption 37 quick and be a configuration of virtual devices 31 QAUTOVRT (automatic virtual-device configuration) value set by CFGSYSSEC command 628 QCCSID (coded character set identifier) 88 QCNTRYID (country or region identifier) 88 inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QALWUSRDMN (allow user auditing) 54	•				
create object auditing validation program (QCRTOBJAUD) 54 (QPWDVLDPGM) 44 of virtual devices) 31 disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) configuration) value set by CFGSYSSEC (QDSPSGNINF) 22, 74 parameter 74 command 628 file systems print device (QPRTDEV) 85 QCCSID (coded character set identifier) 88 file systems control printing security-scan (QSCANFS) 28 printing 232 identifier) 88 inactive job printing security-relevant 280, 623 qCONSOLE (console) 179 qSLWOBJRST (allow object restore (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QALWOSRDMN (allow user auditing) 54	0 0	_			
(QCRTOBJAUD)54(QPWDVLDPGM)44of virtual devices)31disconnected job time-out interval (QDSCJOBITV)password expiration interval (QPWDEXPITV)QAUTOVRT (automatic virtual-device configuration)display sign-on information (QDSPSGNINF)PWDEXPITV user profile parametervalue set by CFGSYSSEC command(QDSPSGNINF)22, 74parameter74command628file systemsprint device (QPRTDEV)85QCCSID (coded character set identifier)88file systems control scan (QSCANFCTLS)printing security- communicationsQCNTRYID (country or region identifier)88inactive jobprinting security-relevant (QINACTMSGQ)28QCONSOLE (console)179(QINACTMSGQ)24option)37description description22time-out interval (QINACTITV)QALWOBJRST (allow object restore) value set by CFGSYSSEC value set by CFGSYSSEC usingrisk of changing value set object using22integrated file systems scan (QSCANFS)QALWUSRDMN (allow userQCRTOBJAUD (create object auditing)			e ·		
disconnected job time-out interval (QDSCJOBITV) 33 (QPWDEXPITV) configuration)  display sign-on information PWDEXPITV user profile (QDSPSGNINF) 22, 74 parameter 74 command 628  file systems print device (QPRTDEV) 85 QCCSID (coded character set identifier) 88  file systems control scan (QSCANFS) 28 printing 232 printing security- scan (QSCANFCTLS) 28 printing security-relevant 280, 623 message queue QALWOBJRST (allow object restore (QINACTMSGQ) 24 time-out interval (QINACTITV) 23 value set by CFGSYSSEC using 119 QCRTOBJAUD (create object starting) 54		. 0			
(QDSCJOBITV) 33 (QPWDEXPITV) configuration)  display sign-on information PWDEXPITV user profile value set by CFGSYSSEC (QDSPSGNINF) 22, 74 parameter 74 command 628  file systems print device (QPRTDEV) 85 QCCSID (coded character set identifier) 88  file systems control printing 232 identifier) 88  file systems control printing security- scan (QSCANFCTLS) 28 communications 280 identifier) 88  inactive job printing security-relevant 280, 623 QCONSOLE (console) 179  message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22  time-out interval QALWOBJRST (allow object restore) risk of changing 22  (QINACTITV) 23 value set by CFGSYSSEC using 119  integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		,			
display sign-on information (QDSPSGNINF) 22, 74 parameter 74 parameter 74 parameter 74 command 628  file systems print device (QPRTDEV) 85 QCCSID (coded character set identifier) 88 file systems control scan (QSCANFS) 28 printing 232 gCNTRYID (country or region identifier) 88 inactive job printing security-relevant 280, 623 printing security-relevant 280, 623 QCONSOLE (console) 179 QALWOBJRST (allow object restore QINACTMSGQ) 24 time-out interval QALWOBJRST (allow object restore) QCRTAUT (create authority) description 22 time-out interval QALWOBJRST (allow object restore) QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	•				
(QDSPSGNINF) 22, 74 parameter 74 command 628  file systems print device (QPRTDEV) 85 QCCSID (coded character set scan (QSCANFS) 28 printing 232 identifier) 88  file systems control printing security- scan (QSCANFCTLS) 28 communications 280 identifier) 88  inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	,	, •	8		
file systems print device (QPRTDEV) 85 QCCSID (coded character set scan (QSCANFS) 28 printing 232 identifier) 88 file systems control printing security- scan (QSCANFCTLS) 28 communications 280 identifier) 88 inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) risk of changing 22 (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		•	•		
scan (QSCANFS) 28 printing 232 identifier) 88  file systems control printing security- scan (QSCANFCTLS) 28 communications 280 identifier) 88  inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		•			
file systems control printing security- QCNTRYID (country or region scan (QSCANFCTLS) 28 communications 280 identifier) 88 inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	0	*			
scan (QSCANFCTLS) 28 communications 280 identifier) 88 inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) risk of changing 22 (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		1 0	· · · · · · · · · · · · · · · · · · ·		
inactive job printing security-relevant 280, 623 QCONSOLE (console) 179 message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) risk of changing 22 (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	· ·				
message queue QALWOBJRST (allow object restore QCRTAUT (create authority) (QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) risk of changing 22 (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	The state of the s				
(QINACTMSGQ) 24 option) 37 description 22 time-out interval QALWOBJRST (allow object restore) risk of changing 22 (QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	ū				
time-out interval QALWOBJRST (allow object restore) risk of changing 22  (QINACTITV) 23 value set by CFGSYSSEC using 119  integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54	9 -	•	*		
(QINACTITV) 23 value set by CFGSYSSEC using 119 integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		•	•		
integrated file systems command 628 QCRTOBJAUD (create object scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54					
scan (QSCANFS) 28 QALWUSRDMN (allow user auditing) 54		· ·			
	e v		·		
	(420.11.10)	objects) 16, 21			

system value (continued)	system value (continued)	system value (continued)	
QDEVRCYACN (device recovery	QPWDLMTCHR (limit characters) 43	QSECURITY (security level)	
action)	QPWDLMTCHR (password restrict	(continued)	
value set by CFGSYSSEC	characters)	introduction 2	
command 628	value set by CFGSYSSEC	level 10 9	
QDSCJOBITV (disconnected job	command 628	level 20 10	
time-out interval) 33	QPWDLMTREP (limit repeated	level 30 10 level 40 11	
value set by CFGSYSSEC command 628	characters) 43 QPWDLMTREP (password limit	level 50 16	
QDSPSGNINF (display sign-on	repeated characters)	message handling 16	
information) 22, 74	value set by CFGSYSSEC	overview 7	
value set by CFGSYSSEC	command 628	recommendations 9	
command 628	QPWDLMTREP (password require	special authority 8	
QFRCCVNRST (force conversion on	position difference)	user class 8	
restore) 36	value set by CFGSYSSEC	validating parameters 14	
QINACTITY (inactive job time-out	command 628	value set by CFGSYSSEC	
interval) 23	QPWDMAXLEN (password maximum	command 628	
value set by CFGSYSSEC	length) 42	QSHRMEMCTL (share memory	
command 628	value set by CFGSYSSEC	control)	
QINACTMSGQ (inactive job message	command 628	description 29	
queue) 24	QPWDMINLEN (password minimum	possible values 29	
value set by CFGSYSSEC	length) 41	QSPCENV (special environment) 72	
command 628	value set by CFGSYSSEC	QSRTSEQ (sort sequence) 87	
QKBDBUF (keyboard buffering) 76	command 628	QSYSLIBL (system library list) 183	
QLANGID (language identifier) 87	QPWDPOSDIF (position	QUSEADPAUT (use adopted	
QLMTDEVSSN (limit device sessions)	characters) 44	authority)	
auditing 233	QPWDRQDDGT (password require	description 30	
description 24	numeric character)	risk of changing 30	
LMTDEVSSN user profile	value set by CFGSYSSEC	QUSRLIBL (user library list) 79	
parameter 75	command 628	QVFYOBJRST (verify object on	
QLMTSECOFR (limit security officer)	QPWDRQDDGT (required password	restore) 34	
auditing 232	digits) 44	remote service attribute	
authority to device	QPWDRQDDIF (duplicate	(QRMTSRVATR) 33	
descriptions 177	password) 42	remote sign-on (QRMTSIGN) 27, 235	
changing security levels 11	QPWDRQDDIF (password required	retain server security	
description 25	difference)	(QRETSVRSEC) 26	
sign-on process 179	value set by CFGSYSSEC	Scan File Systems (QSCANFS) 28	
value set by CFGSYSSEC	command 628	Scan File Systems	
command 628	QPWDVLDPGM (password validation	(QSCANFSCTL) 28	
QMAXSGNACN (action when sign-on	program) 44	security introduction 3	
attempts reached)	value set by CFGSYSSEC		
description 26 user profile status 62	command 628 QRETSVRSEC (retain server	overview 20 setting 627	
value set by CFGSYSSEC		security level (QSECURITY)	
command 628	security) 26 QRMTSIGN (allow remote sign-on)	auditing 232	
QMAXSIGN (maximum sign-on	value set by CFGSYSSEC	automatic user profile creation 57	
attempts)	command 628	changing, 20 from higher level 10	
auditing 232, 235	QRMTSIGN (remote sign-on) 27, 235	changing, level 10 to level 20 10	
description 25	QRMTSRVATR (remote service	changing, level 20 to 30 10	
user profile status 62	attribute) 33	changing, to level 40 15	
value set by CFGSYSSEC	QSCANFS (scan file systems) 28	changing, to level 50 17	
command 628	QSCANFSCTL (scan file systems	comparison of levels 7	
QPRTDEV (print device) 85	control) 28	disabling level 40 16	
QPWDEXPITV (password expiration	QSECURITY (security level)	disabling level 50 18	
interval)	auditing 232	enforcing QLMTSECOFR system	
auditing 233	automatic user profile creation 57	value 179	
description 39	changing, 20 from higher level 10	introduction 2	
PWDEXPITV user profile	changing, level 10 to level 20 10	level 10 9	
parameter 74	changing, level 20 to 30 10	level 20 10	
value set by CFGSYSSEC	changing, to level 40 15	level 30 10	
command 628	changing, to level 50 17	level 40 11	
QPWDLMTAJC (password limit	comparison of levels 7	level 50 16	
adjacent) 43	disabling level 40 16	overview 7	
QPWDLMTAJC (password restrict	disabling level 50 18	recommendations 9	
adjacent characters)	enforcing QLMTSECOFR system	special authority 8	
value set by CFGSYSSEC	value 179	user class 8	
command 628	internal control blocks 17		

system value (continued)	TCP/IP (QTCP) user profile 283	TRCCNN (Trace Connection) command
security-related	TCP/IP (Transmission Control	object authority required 429
overview 30	Protocol/Internet Protocol)	TRCCPIC (Trace CPI Communications)
share memory control	object authority required for	command
(QSHRMEMCTL)	commands 440	authorized IBM-supplied user
description 29	TCP/IP printing support (QTMPLPD)	profiles 298
possible values 29	user profile 283	object authority required 429
sign-on 40	TELNET (Start TCP/IP TELNET)	TRCCSP (Trace CSP/AE Application)
action when attempts reached	command	command
(QMAXSGNACN) 26, 62	object authority required 441	object auditing 489
maximum attempts	temporary (QTEMP) library	TRCICF (Trace ICF) command
(QMAXSIGN) 25, 62, 232, 235	security level 50 16	authorized IBM-supplied user
remote (QRMTSIGN) 27, 235	test request (QTSTRQS) user profile 283	profiles 298
sort sequence (QSRTSEQ) 87	text (TEXT) parameter	object authority required 429 TRCINT (Trace Internal) command
special environment (QSPCENV) 72 system library list (QSYSLIBL) 183	user profile 67 text index	authorized IBM-supplied user
use adopted authority	object authority required for	profiles 298
(QUSEADPAUT)	commands 402	object authority required 429
description 30	TFRBCHJOB (Transfer Batch Job)	TRCJOB (Trace Job) command
risk of changing 30	command	authorized IBM-supplied user
user library list (QUSRLIBL) 79	object auditing 477	profiles 298
verify object on restore	object authority required 371	object authority required 429
(QVFYOBJRST) 34	TFRCTL (Transfer Control) command	TRCTCPAPP
working with 232	object authority required 417	authorized IBM-supplied user
system-defined authority 113	transferring adopted authority 129	profiles 298
System/36	TFRGRPJOB (Transfer to Group Job)	TRCTCPAPP command
authority for deleted files 132	command	object authority required 429
migration	adopted authority 129	trigger program
authority holders 133	object authority required 371	listing all 279, 623
System/36 environment	TFRJOB (Transfer Job) command	trivial password
object authority required for	object auditing 477	preventing 38, 233
commands 437	object authority required 371	TRMPRTEML (Terminate Printer
user profile 72	TFRPASTHR (Transfer Pass-Through)	Emulation) command
System/38	command	object authority required 331
command security 210	object authority required 332	TRNPIN (Translate Personal Identification
System/38 environment 72	TFRSECJOB (Transfer Secondary Job)	Number) command
System/38 Environment 117	command	authorized IBM-supplied user
systems management	object authority required 371	profiles 298
changing	time slice 192	object authority required 327
audit journal (QAUDJRN)	time zone description commands 441	type-ahead (*TYPEAHEAD) keyboard
entry 252	time-out interval	buffering 76
systems management (*SYSMGT) audit	inactive jobs (QINACTITV) system	
level 252	value 23	
systems management change (SM) file	message queue (QINACTMSGQ)	U
layout 592	system value 24	uid (user identification number)
systems management change (SM)	token-ring	restoring 224
journal entry type 252	object authority required for	unauthorized
Systems Network Architecture (SNA)	commands 391	programs 235
distribution services (QSNADS) user	total change of password 44	UNMOUNT (Remove Mounted File
profile 283	Transfer Control (TFRCTL) command	System)
Systems Network Architecture	transferring adopted authority 129	object authority required 443
distribution services (SNADS) QSNADS user profile 283	Transfer to Group Job (TFRGRPJOB) command	UNMOUNT (Remove Mounted File
QSNADS user profile 285		System) command
	adopted authority 129 transferring	object authority required 399
Т	adopted authority 129	unsupported interface
<del>-</del>	to group job 129	audit journal (QAUDJRN) entry 13,
table	translation of programs 14	246
object authority required for	Transmission Control Protocol/Internet	update (*UPD) authority 112, 302
commands 439	Protocol (TCP/IP)	UPDDTA (Update Data) command
table (*TBL) auditing 503	object authority required for	object authority required 345
tape	commands 440	UPDPGM (Update Program) command
object authority required for	TRCASPBAL	object auditing 454, 482, 489
commands 391	authorized IBM-supplied user	object authority required 417
protecting 232	profiles 298	UPDPTFINF (Update PTF Information)
tape cartridge object authority required for	TRCASPBAL command 330	command
commands 391		authorized IBM-supplied user profiles 298
COMMINIOS JUL		Promiss 200

LIDDCDVDCM (Const. Const. Don tons)	(LICDODT)	
UPDSRVPGM (Create Service Program)	user option (USROPT) parameter	user profile (continued)
command	(continued)	authority
object auditing 482	*EXPERT (expert) 88, 89, 90, 139	storing 223
UPDSRVPGM (Update Service Program)	*HLPFULL (help full screen) 90	authority (AUT) 93
command	*NOSTSMSG (no status message) 90	automatic creation 57
object auditing 454, 499	*PRTMSG (printing message) 90	CCSID (coded character set
object authority required 418	*ROLLKEY (roll key) 90	identifier) 88
upgrade order information	*STSMSG (status message) 90	changes when restoring 223
object authority required for	0	
	user profile 88, 89, 90	changing
commands 442	USER parameter on job description 181	audit journal (QAUDJRN)
use (*USE) authority 113, 302	user permission	entry 247
use adopted authority (QUSEADPAUT)	granting 277	command descriptions 276
system value	object authority required for	methods 101
description 30	commands 402	password 275
risk of changing 30	revoking 277	password composition system
use adopted authority (USEADPAUT)	user portion	values 39
parameter 131	library list	setting password equal to profile
-		
USEADPAUT (use adopted authority)	controlling 201	name 60
parameter 131	description 183	checking for default password 619
user	recommendations 185	CNTRYID (country or region
adding 98	user profile	identifier) 88
auditing	(gid) group identification number 91	coded character set identifier
changing 71	(user identification number) 90	(CCSID) 88
working with 107	*ALLOBJ (all object) special	commands for working with 276
enrolling 98	authority 68	copying 99
user (*USER) domain 12	*AUDIT (audit) special authority 71	100
,		countryor region identifier
user (*USER) state 13	*IOSYSCFG (system configuration)	(CNTRYID) 88
user auditing	special authority 71	creating
changing	*JOBCTL (job control) special	audit journal (QAUDJRN)
command description 277	authority 69	entry 247
command descriptions 276	*SAVSYS (save system) special	command descriptions 275, 276
user authority	authority 70	example description 98
adding 140	*SECADM (security administrator)	methods 96
. ~	special authority 69	CURLIB (current library) 64
copying		•
command description 276	*SERVICE (service) special	current library (CURLIB) 64
example 101	authority 70	default values table 281
recommendations 145	*SPLCTL (spool control) special	deleting
renaming profile 106	authority 69	command description 276
user class	accounting code (ACGCDE) 82	directory entry 101
analyzing assignment 623	ACGCDE (accounting code) 82	distribution lists 101
user class (USRCLS) parameter	action auditing (AUDLVL) 94	message queue 101
description 63	all numeric user ID 59	spooled files 103
recommendations 63		•
	all object (*ALLOBJ) special	delivery (DLVRY) 84
USER DEF (user-defined) authority 139	authority 68	description (TEXT) 67
user domain object	analyzing	DEV (print device) 85
restricting 16	by special authorities 623	displaying
security exposure 16	by user class 623	command description 276
user ID	analyzing with query 268	individual 104
DST (dedicated service tools)	assistance level (ASTLVL) 63	programs that adopt 130
changing 109	ASTLVL (assistance level) 63	sign-on information
incorrect	ATNPGM (Attention-key-handling	(DSPSGNINF) 73
	program) 86	DLVRY (message queue delivery) 84
audit journal (QAUDJRN)	1 0	
entry 242	Attention-key-handling program	DOCPWD (document password) 83
user identification number (uid)	(ATNPGM) 86	document password (DOCPWD) 83
restoring 224	audit (*AUDIT) special authority 71	DSPSGNINF (display sign-on
user identification number() parameter	audit level (AUDLVL)	information) 73
user profile 90	*CMD (command string)	eim association (EIMASSOC) 92
user index (*USRIDX) auditing 504	value 243	EIMASSOC (eim association) 92
user index (*USRIDX) object 16	auditing	enabling
user option (CHRIDCTL) parameter	*ALLOBJ special authority 233	sample program 104
user profile 88	authority to use 234	exit points 107
•	•	-
user option (LOCALE) parameter	authorized users 268	group authority (GRPAUT) 80, 122,
user profile 89	AUDLVL (action auditing) 94	124
user option (SETJOBATR) parameter	AUDLVL (audit level)	group authority type
user profile 89	*CMD (command string)	(GRPAUTTYP) 81, 124
user option (USROPT) parameter	value 243	group identification number (gid
*CLKWD (CL keyword) 88, 89, 90	AUT (authority) 93	) 91

user profile (continued)	user profile (continued)	user profile (continued)		
group profile (GRPPRF) 124	MSGQ (message queue) 83	spool control (*SPLCTL) special		
changes when restoring	name (USRPRF) 59	authority 69		
profile 223	naming 59	SRTSEQ (sort sequence) 87		
description 79	OBJAUD (object auditing) 93	status (STATUS) 62		
GRPAUT (group authority) 80, 122,	object auditing (OBJAUD) 93	storing		
124	object authority required for	authority 222, 223		
GRPAUTTYP (group authority	commands 442, 443	SUPGRPPRF (supplemental		
type) 81, 124	object owner	groups) 81		
GRPPRF (group profile) 124	deleting 122	supplemental groups		
changes when restoring	output queue (OUTQ) 85	(SUPGRPPRF) 81		
profile 223	OUTQ (output queue) 85	system configuration (*IOSYSCFG)		
description 79	owned object information 95	special authority 71		
home directory (HOMEDIR) 91	OWNER (owner of objects	System/36 environment 72		
HOMEDIR (home directory) 91	created) 80, 122	text (TEXT) 67		
IBM-supplied	owner (OWNER) 124	types of displays 105		
auditing 232	OWNER (owner) 124	types of reports 105		
default values table 281	owner of objects created	used in job description 13		
purpose 108	(OWNER) 80, 122	user class (USRCLS) 63		
initial menu (INLMNU) 66	password 60	user identification number() 90		
initial program (INLPGM) 65	password expiration interval	user options (CHRIDCTL) 88		
INLMNU (initial menu) 66	(PWDEXPITV) 74	user options (LOCALE) 89		
INLPGM (initial program) 65	performance	user options (SETJOBATR) 89		
introduction 4	save and restore 95	user options (USROPT) 88, 89, 90		
job control (*JOBCTL) special	primary group 104	USRCLS (user class) 63		
authority 69	print device (DEV) 85	USROPT (user options) 88, 89, 90		
job description (JOBD) 78	printing	USRPRF (name) 59		
JOBD (job description) 78	See listing	working with 97, 276		
KBDBUF (keyboard buffering) 76	priority limit (PTYLMT) 77	user profile (*USRPRF) auditing 504		
keyboard buffering (KBDBUF) 76	private authorities 95	user profile change (CP) file layout 525		
LANGID (language identifier) 87	PTYLMT (priority limit) 77	user profile change (CP) journal entry		
language identifier (LANGID) 87	public authority (AUT) 93	type 247		
large, examining 269	PWDEXP (set password to	user profile parameter		
LCLPWDMGT (local password	expired) 61	group identification number(gid) 91		
management) 75	PWDEXPITV (password expiration	user queue (*USRQ) auditing 505		
limit capabilities	interval) 74	user queue (*USRQ) object 16		
auditing 233	related commands for working	user space (*USRSPC) auditing 505		
description 66	with 277	user space (*USRSPC) object 16		
library list 185	renaming 106	user-defined (USER DEF) authority 139		
limit device sessions	restoring	USRCLS (user class) parameter		
(LMTDEVSSN) 75	audit journal (QAUDJRN)	description 63		
list of permanently active	entry 247	recommendations 63		
changing 619	command description 277	USROPT (user option) parameter		
listing	commands 221	*CLKWD (CL keyword) 88, 89, 90		
all users 104	procedures 223	*EXPERT (expert) 88, 89, 90, 139		
inactive 269	restoring authority	*HLPFULL (help full screen) 90		
selected 268	audit journal (QAUDJRN)	*NOSTSMSG (no status message) 90		
users with command	entry 246	*PRTMSG (printing message) 90		
capability 268	retrieving 107, 276	*ROLLKEY (roll key) 90		
users with special authorities 268	roles 57	*STSMSG (status message) 90		
listing all 104	save system (*SAVSYS) special	USROPT (user options) parameter		
LMTCPB (limit capabilities) 66, 185	authority 70	user profile 88, 89, 90		
LMTDEVSSN (limit device	saving 221	USRPRF (name) parameter 59		
sessions) 75	security administrator (*SECADM)	con in (name) parameter ou		
local password management	special authority 69			
(LCLPWDMGT) 75	service (*SERVICE) special	V		
LOCALE (locale) 89	authority 70	<del>-</del>		
LOCALE (user options) 89	set job attribute (user options) 88, 89	VA (access control list change) journal		
maximum storage (MAXSTG)	set password to expired	entry type 251		
description 76	(PWDEXP) 61	VA (changing access control list) file		
group ownership of objects 122	SEV (message queue severity) 84	layout 598		
MAXSTG (maximum storage)	severity (SEV) 84	validating		
description 76	sort sequence (SRTSEQ) 87	restored programs 14		
group ownership of objects 122	SPCAUT (special authority) 68	validating parameters 14		
message queue (MSGQ) 83	SPCENV (special environment) 72	validating password 44		
message queue delivery (DLVRY) 84	special authority (SPCAUT) 68	validation list		
message queue severity (SEV) 84	special authority (SPCAOT) 68 special environment (SPCENV) 72	object authority required for		
message queue severity (SEV) 04	special chynolinicht (of CEIVV) 12	commands 446		

validation lists Uniternet user 218 Validation Lists, Create 218 Validation Lists, Create 218 Validation lists, Delete 218 Validation program, password 45, 46 VC (connection start and end) file layout 509 VC (connection start and end) file layout 509 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 249 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 245 VC (connection start or end) journal entry type 245 VC (connection start or end) journal entry type 245 VC (connection start or end) journal entry type 247 VC (connection start or end) journal entry type 248 VC (connection start or end) journal entry type 249 VC (connection start or end) journal entry type 240 VC (connection start or end) journal entry type 241 VC (connection start or end) journal entry type 241 VC (connection start or end) journal entry type 241 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection start or end) journal entry type 244 VC (connection star	validation list (*VLDL) auditing 506	VL (account limit exceeded) file	Work with System Status (WRKSYSSTS)
Internet user 218 Validation Lists, Create 218 Validation Lists, Delete 218 Validation Lists, University Lists, Delete 218 Validation Lists, University Lists, Delete 218 Validation Lists, University Lists, Delete 218 Validation Lists, University Lists, Delete 218 Validation Lists, Delete 218 Validation Lists, Delete 218 Validation Lists, University Lists, Sand Lists, Delete 218 Validation L	validation list (VO) file layout 601	layout 599 VI. (account limit exceeded) journal entry	command 192 Work with System Values (WRKSYSVAL)
Validation program, password 45, 46 validation value audit journal (QAUDJRN) entry 246 definition 14 Vork (connection start and end) file layout 598 Very Connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 244 Very (connection start or end) journal entry type 245 Very (connection start or end) journal entry type 245 Very (connection start or end) journal entry type 245 Very (connection start or end) journal entry type 245 Very (connection start or end) journal entry type 247 Very (connection start or end) journal entry type 247 Very (connection start or end) journal entry type 248 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 249 Very (connection start or end) journal entry type 240 Very (co		•	
validation yalus audit journal (QAUJURN) entry 246 definition 14  VC (connection start and end) file layout 601  VC (connection start or end) journal entry type 244  VF (close of server files) file layout 598  VF (connection start or end) journal entry type 244  VF (close of server files) file layout 599  VFVEMN (Verify Communications) command authorized IBM-supplied user profiles 298  VFYPMCGLG command object authority required 349  VFYINKLPDA (Verify Link supporting JepDA-2) command authorized IBM-supplied user profiles 298  VFYINKLPO, Verify Link Supporting JepDA-2) command authorized IBM-supplied user profiles 298  VFYYMKCCLCN (Verify Link Supporting JepDA-2) command authorized IBM-supplied user profiles 298  VFYYMKCLY (Verify Master Key) command authorized IBM-supplied user profiles 298  VFYYMKIPPA (Verify Inthe Supporting JepDA-2) command authorized IBM-supplied user profiles 298  VFYYMKIPPA (Verify Inthe Supporting JepDA-2) command 277  VFYPKIN (Verify Master Key) command authorized IBM-supplied user profiles 298  VFYMKIPPA (Verify Inthe Supporting JepDA-2) command authorized IBM-supplied user profiles 298  VFYMKIPPA (Verify Inthe Supporting JepDA-2) command 277  VFYPKIN (Verify Fersonal Identification Number) command authorized IBM-supplied user profiles 298  VFYMKIPPA (Verify Time) command authorized IBM-supplied user profiles 298  VFYMKIPPA (Verify Time) command authorized IBM-supplied user profiles 298  VFYMKIPPA (Verify Time) command authorized IBM-supplied user profiles 298  VFYPKIN (Verify Tope) command authorized IBM-supplied user profiles 298  VFYPKIN (Verify Time) command 277  VeryRT (Verify Tape) command 277  VeryRT (Verify Tape) command 278  Very Wry Charlon (Verify Time) command 279  Very Charlon (Verify Time) command 279  Very RT (Verify Time) command 270  Very RT (Verify Time) command 271  Very RT (Verify Time) command 272  Very RT (Verify Time) command 273  Very RT (Verify Time) command 274  Very RT (Verify Time) command 274  Very RT (Verify Time) command 274  Very RT (Verify Time) comman		=	1 0
validation value audit journal (QAUDJRN) entry 24d definition 14 VC (connection start and end) file layout 598 VC (connection start or end) journal entry type 244 verify object on restore (QVFYORJRST) system value 34 VEVINCRIV (close of severe files) file layout 599 VFYCMN (Verify Communications) command authorized IBM supplied user profiles 298 object auditing 459, 480 object auditority required 414, 430 VFYINCCLC authority required 414, 430 VFYINCLC command object authority required 430 VFYINCLE (Command object authority required 430 VFYINCLE (DAV (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINCLE (DAV (Verify Link supporting LPDA-2) command object authority required 430 VFYINCLE (DAV (Verify Link supporting LPDA-2) command object authority required 430 VFYINCLE (DAV (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (PVF) Presonal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Master key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (PVF) Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Fase) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Presonal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENTRY (Verify Tape) command 237 Work with Dispets (Verification Command 328 Verification Command 328 Verification Command 328 Verification Command 328 Verification Command 328 V		•	_
audit journal (QAUDINN) entry 246 definition 14  VC (connection start and end) file layout 598 VC (connection start or end) journal entry type 244 VO (validation list) file layout 601 VO (validation list) file layout 601 VO (validation list) file layout 601 VO (validation list) file layout 602 VV (validation list) file layout 602 VV (validation list) file layout 602 VV (validation list) file layout 603 VV (validati			
VC (connection start and end) file layout 501 VC (connection start or end) journal entry type 241 verify object on restore (QVFYOBIRST) yet wature 34 VF (close of server files) file layout 509 VFYCMN (Verify Communications) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYINKEPIA (Verify Link supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINKIPDA (Verify Link Supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINKIPPO (Verify Link Supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTPN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTPN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTPN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTPN (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTPN (Verify Printer) command object authority required 414, 430 VFYTPN (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) command object authority required 414, 430 VFYTPN (Verify Tape) c			working on behalf
VP (connection start or end) journal entry type 244 verify object an restore (QVPYORIRST) system value 34 VFYCMN (Verify Communications) command object authority required 14, 430 object authority required 349 VFYINKLPDA (Verify Link supporting LPDA-2) command object authority required 327 VFYINKLPDA (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 289 object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 327 VFYINKLPOR (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 289 object authority required 327 VFYINK (Verify Personal Identification Number) command authority required 327 VFYINK (Verify Personal Identification Number) command authority required 327 VFYINK (Verify Personal Identification Number) command object authority required 327 VFYINK (Verify Personal Identification Number) command object authority required 327 VFYINK (Verify Personal Identification Number) command object authority required 327 VFYINK (Verify Personal Identification Number) command 237 wireless LAN configuration object authority required 327 VFYINK (Verify Personal Identification Number) command object authority required 327 VFYINK (Verify Personal Identification Number) command 237 vFYINK (Verify Personal Identification Number) command 238 vFYINK (Verify Personal Identification Number) command 238 vFYINK (Verify Personal Identification Number) com			
VC (connection start or end) journal entry type 241 verify object on restore (QVFYOBIRST) yestem value 34 VF (close of server files) file layout 599 VFYCMN (Verify Communications) command authorized IBM supplied user profiles 298 object authority required 414, 430 VFYLNECDE (Verify Link supporting LPDA-2) command object authority required 349 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 327 VFYPIN (Verify Master Rey) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command object authority required 414, 430 VFYLNKLPDA (verify Fink) (Verify Link Supporting LPDA-2) command 327 VFYPIN (Verify Master Rey) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYLPN (Verify Printer) command object authority required 414, 430 VFYLPN (Verify Printer) command object authority required 414, 430 VFYLPN (Verify Ispecial Verify Printer) command 273 Work with Objects Wirk (WRK) (WR	- `		
verify object on restore (QVFYORJRST) system value 34 VF (close of server files) file layout 599 VFYCMN (Verify Communications) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 439 VFYLNKLPDA (Verify Inster) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYPRT (Verify Pintier) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYPRT (Verify Pintier) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYPRT (Verify Pintier) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYPRT (Verify Pintier) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYPRT (Verify Pintier) command object authority required 327 VFYPRT (Verify Pintier) command object authority required 414 viewing audit journal entries 262 view with Journal Authorized IBM-supplied user profiles 298 object authority required 414 vork with Journal (WRKAIRN) command 274 work with Journal (WRKOBINOW) command object authority required 371 Work with Objects by Owner (WRKOBINE) command object authority required 371 work with Objects by Owner (WRKOBINE) command 274 work with Objects by Owner (WRKAIRD) (WRKAIRD) (WRKAIRD) (WRKAIRD) (WRKAIRD) (WRKAIRD) (WRKAIRD) (WRKAIRD) (W	•	-	3
system value 34 VFC (close of server files) file layout 599 VFYCMN (Verify Communications) command authorized IBM-supplied user profiles 298 VFYIMS (ClG authority required 414, 430 VFYINKLPDA (Verify Link supporting 12D-A-2) command object authority required 430 VFYINKLPDA (Verify Link supplied user profiles 298 object authority required 430 VFYINKLPDA (Verify Link supporting 12D-A-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINKLPDA (Verify Link Supporting 12D-A-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINKLPDA (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 Work with Duration 1274 Work with Journal 273 Work with Duration 274 Work with Journal 273 Work with Journal 281, 288 Work with Directory (WRKDIRE) command 273 Work with Objects worker 274 objects by primary group 123, 274 object subtority required 327 vviscation user profiles 328 viscation authority required 327 vviscation 127 user profiles 328 object authority required 327 vviscation 272 voint 328 vviscation 274 voint 329 vviscation 274 voiptet 329 vviscation 27			
VFYCMN (Verify Communications) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYINGCLG command object authority required 414, 430 VFYINGCLG command object authority required 414, 430 VFYINGCLG command object authority required 419 VFYINGCLG command object authority required 419 VFYINGCLG command object authority required 410 VFYINGCLG command object authority required 430 VFYINGLPDA (verify Link Supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYINGLPDA (verify Ink supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 410 VFYINGCLG (verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYITAP (Verify Pinter) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Pinter) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Pinter) command authorized IBM-supplied user profiles 298 object authority required 414 viewing authority or profile 288 volet authority required 414 viewing authority or profile 288 volet authority required 414 viewing authority or profile 288 volet authority required 414 viewing authority or profile 288 volet authority required 414 viewing authority or profile 389 volet authority required 414 viewing authority or profile 389 view 341 viewing authority or profile 380 volet authority required 414 vi			
VFYCNK (Verify Communications) command authorized IBM-supplied user profiles 298 VFYIMGCIG authority required 414, 430 VFYLNKLPDA (Verify Link supporting 12DA 2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting 12DA 2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting 12DA 2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting 12DA 2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting 12DA 2) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 340 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 341 Work with Durated 141, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 341 Work with Objects WFKORD) command 278 Work with Divertory (WRKDIRC) command 251, 268 Work with Objects (WRKORD) command authority required for commands authority required 411 work with Objects by Owner (WRKAGIRO) command 251, 268 Work with Objects (WRKORD) command authority required for command authority required 341 Work with Objects by Owner (WRKAGIRO) command 274 Work with Objects by Owner (WRKAGIRO) command 274 Work with Objects by Owner (WRKAGIRO) command 275 Work with Objects by Owner (WRKAGIRO) command 276 Work with Objects by Owner (WRKAGIRO) command 276 Wo	•	_	
authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYLNKLPDA (Verify Link supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 327 VFYPNTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTPN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command anuthorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command anuthorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command anuthorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command anuthorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 o			•
object authority required 414, 430 VFYIMCCLG command object authority required 349 VFYIMCCLG command object authority required 349 VFYIMCLOR (Command object authority required 340 VFYINKLPA (Verify Link Supporting LPDA-2) command authorized IBM-supplied user profiles 298 VFYINKLPA (Verify Link Supporting LPDA-2) command object authority required 430 VFYINKLPA (Verify Link Supporting LPDA-2) command object authority required 327 VFYINKLPA (Verify Link Supporting LPDA-2) command object authority required 327 VFYPRIN (Verify Presonal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRIN (Verify Presonal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VF		· C	· ·
object authority required 414, 430 VFYLNGCLG authorized IBM-supplied user profiles 298 VFYIMGCLG command object authority required 349 VFYLNKLPDA (Verify Link supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object authority required 327 VFYPNSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPNTYPCNNC (Ommand authorized IBM-supplied user profiles 298 object authority required 37 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terple) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terple) command 278 Work with Directory (WRKDIRE) command 278 Work with Objects WRKCOB) command 274 Work with Objects WRKCOB) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group output queue description 186 password 275 primary group 142, 274 output eue description 186 password 275 primary group 123, 274 output euer description 186 password 275 primary group 144 volv (service status change) journal entry type 252 user auditing 459 user auditing 450 user profiles 286 work with Directory (WRKDIRE) command 274			•
VFYIMCCLG command object authority required 349 VFYLNKLPDA (Verify Link supporting authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting authorized IBM-supplied user profiles 298 object authority required 327 VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTPCNN (Derify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tepic command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Terpliced 414, 430 VFYTCPCNN (Ver	•		· ·
authorized IBM-supplied user profiles 298 object authority required 349 VFYINKLPDA (Verify Inthe Supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 340 VFYENKLPDA (Verify Inthe Supporting LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 327 VFYENK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Fersonal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Priner) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command 261, 268 Work with Journal (WRKJIRN) command 274 Work with Objects (WRKOBI) command 274 Work with Objects by Owner (WRKOBIOWN) command 274 Work with Objects by Owner (will object authority required 371 WRALIR (Work with Alert Description) 274 using 143 Work with Objects by Owner (will object solution) 274 viewing audit journal entries 262 virtual device authority required 414 viewing audit journal entries 262 virtual device authority required 414 viewing 143 work with Objects by Owner (with Objects by Owner display 102, 143 work with Objects by Owner (with Objects by Owner display 102, 143 work with Objects by Owner (with Objects by Owner display 102, 143 work with Output Queue Description 274 work with Output Queue Description 274 work with Output Queue Description 274 work with Output Queue Description 275 workstation user 275 workstation 275 work		VS (server session) journal entry	
Pyrofiles 298 VFYLNKLPDA (Verify Link supporting 1PDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting 1PDA-2) command authorized IBM-supplied user profiles 298 object authority required 307 VFYLNKLPDA (Verify Link Supporting 1PDA-2) command object authority required 327 VFYPIN (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tapp) command object authority required 414, 430 VFYTAP (Verify Tapp) command object authority required 414, 430 VFYTAP (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 414, 430 VFYTCPCNN (Verify Tapp) command object authority required 514 Viewing audit journal entries 262 virtual device authority requi			
VFVI.NKLPDA (Verify Link supporting LPDA-2) command authority required 430 VFVI.NKLPDA (Verify Link supporting LPDA-2) command authority required 430 VFVI.NKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFVI.NKLPDA (Verify Link Supporting LPDA-2) command object authority required 430 VFVI.NKLPDA (Verify Link Supporting LPDA-2) command object authority required 380 VFVMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFVPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFVPTR (Verify Trinter) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFVTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFVTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required 414, 430 VFVTCONN (Verify Top-/IP Connection) command object authority required for command 274 Work with Objects (WRKOBB) command 274 Work with Objects (WRKOBB) command 274 Work with Objects by Owner (WRKOBJOWN) command object authority required 314 WrkALR (Work with Alert) command object authority required 314 WrkALRD (Work with Alert) command object authority required 314 WrkALRD (Work with Alert) command object authority required 314 WrkALRD (Work with Alert) command object authority required 314 WrkALRD (Work with Alert) command object authority required 314 WrkALRD (Work with Alert) command object authority re			•
VY (service status change) file layout 605 VV (service status change) journal entry profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480 VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tapp) command authorized IBM-supplied user profiles 298 object authority required 4	•	VU (network profile change) journal	
LPDA-2) command authorized IBM-supplied user profiles 298 object authority required 430 VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480 VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTR (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTTAP (Verify Tape) command object authority required 414, 430 VFYTTAP (Verify Tape) command object authority required 414, 430 VFYTTCPCNN (Verify TCP/P Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 vive vist Authority (verice status change) journal entry type 252 vV (service status change) journal entry type 252 vV (service status change) journal entry user profiles 298 vork with Authority (WRKAUT) command 139, 274 work with Authority (WRKAUT) command 273 Work with Durnal (WRKIRN) command 261, 268 Work with Objects (WRKOB) command 274 work with Objects by Owner (WRKOBIPWN) command object authority required for commands 46. vorkstation customizing object object authority required for commands 486 workstation user (QUSER) user profiles 298 object authority required 414, 430 Vork with Objects (WRKOB) command 273 Work with Journal Attributes (WRKOBIPWN) command 261, 268 Work with Objects (WRKOB) command 274 work with Objects by Owner (WRKAUTD) (WRKAUTD) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKAUTP) (Work with	0 0		· ·
authorized IBM-supplied user profiles 298 object authority required 327 VFYINKLPDA (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 virtual printer securing 190 virtual printer where the profiles 298 object authority required 414 description 274 workstation authority to sign-on 177 limiting authority to sign-on 177 limiting authority to sign-on 177 limiting authority required for commands 338 workstation user to one at a time 24 restricting access 232 securing 177 security officer access 25 workstation customizing object object authority required for command 273 work with Durnal (WRKDBIPD) command 273 work with Directory (WRKDIRE) command 278 work with Journal (WRKJIRN) command 261, 268 Work with Journal (WRKJIRN) command 261, 268 Work with Objects by Owner (WRKOBIJOWN) command 274 work with Alert Description) command object authority required 314 WRKALRT (Work with Alert Description) command object authority required 314 work with Objects by Primary Group (WRKOBIJOW) command 123, 144 description 274 workstation cannot a time 24 restricting access 232 securing 177 security officer access 25 workstation user to			3
object authority required 430  VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480  VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327  VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327  VFYPTRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430  VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430  VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430  VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430  VFYTCPCNN (Verify TCP/IP Connection) command object authority required 411 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  wireless LAN configuration object authority required for command 273 Work with Authorization List (WRKAUTL) command 273 Work with Database Files Using IDDU ((WRKDIR) command 278 Work with Directory (WRKDIR) command 261, 268 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKJRN) command 274 Work with Objects (WRKOBI) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBIPC)) command 123, 144 description 274 description 31 virtual printer securing 190  wireless LAN configuration object authority required for command 273 work with Authorization Lists (WRKAUTL) command 273 work with Database Files Using IDDU ((WRKDIR) command 268, Work with Journal Attributes (WRKJRN) command 261, 268 Work with Journal Attributes (WRKAUTO) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBIPC) command 123, 144 description 274 description 274 description 274		·	
VFYLNKLPDA (Verify Link Supporting LPDA-2) command object auditing 480 VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPTRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command 261, 268 Work with Journal Attributes (WRKJRN) command 261, 268 Work with Doigets (WRKOBI) command 274 Work with Objects (WRKOBI) command 274 Work with Objects by Owner (WRKOBI) command 274 work with Objects by Owner (WRKALTR) (Work with Alert) Description) command object authority required 311 virtual printer securing 190  Wireless LAN configuration object authority required for command 233 workstation customizing object object authority required for command 273 workstation user (WRKALTR) (WRKAURN) powers and 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKALTR) (Work with Alert) Description) command object authority required 371 WrKALRD (Work with Alert) Description) command object authority required 314 Work with Objects by Primary Group (WRKOBIPCP) command 123, 144 description 274 using 149 Work with Objects by Primary Group (WRKOBIPCP) command 123, 144 description 274 with Durnal Attributes (WRKAURD) command 274 Work with Objects by Primary Group (WRKOBIPCP) command 123, 144 description 274 with Durnal Attributes (WRKAURD) command 274 Work with Objects by Owner displayed to the command object authority required 371 WRKALRD (Work with Alert) Description command object authority required 314 WRKALRTBL (Work with Alert) Descripti	•	type 252	
LPDA-2) command object auditing 480  VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327  VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327  VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327  VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tequired 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 411 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  WWA With Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBIPGP) command 123, 144 description 274 work with Output Queue Description  Wireless LAN configuration object authority required for command 338 work with Authority (WRKAUT) command 273 work with Database Files Using IDDU (WRKDBIFIDD) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKAUT) command 261, 268 Work with Objects (WRKOBJ) command 274 work with Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBIPGP) command 123, 144 description 274 work with Output Queue Description  WRKALTIDE (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Alert Table) command object authority required 314 WRKALTIBL (Work with Ale			
object auditing 480  VFYMSTK (Verify Master Key) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual printer security officer access 25 workstation customizing object object authority required for command 273 work with Authoritz (WRKAUT) command 273 Work with Database Files Using IDDU (WRKDIRE) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command authority required 441 viewing audit journal entries 262 virtual device authority required 441 viewing audit journal entries 262 virtual printer security officer access 25 workstation customizing object object authority required for command 273 work with Database Files Using IDDU (WRKDIRE) command 261, 268 Work with Journal (WRKJRN) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command 274 using 143 Work with Objects by Owner (WRKOBJOWN) command object authority required 371 Work with O		W	
object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 virtual printer securing 190 virtual viewing 190 virtual printer securing 190 virtual printer securing 190 virtual viewing 190 virtual viewing 190 virtual printer securing 190 virtual viewing 190 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 virtual viewing 190 virtual viewing 190 virtual printer securing 190 virtual viewing 190 virtual view	object auditing 480	<del></del>	securing 177
object authority required 327 VFYPIN (Verify Personal Identification Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAPP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAPP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 414 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  virtual printer securing 190  virtual device authority required 327 VFYROR (Verify Tape) command 139, 274 Work with Authorization Lists (WRKAUTL) command 273 Work with Database Files Using IDDU (WRKDIRE) command 278 Work with Directory (WRKDIRE) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKOBI) command 274 Work with Objects (WRKOBI) command 261, 268 Work with Journal Attributes (WRKAURN) command 261, 268 Work with Objects (WRKOBI) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRIBL (Work with Alert Table) command 278 Work with Output Queue Description		· ·	· ·
object authority required 327 VFYPIN (Verify Personal Identification Number) command 139, 274 work with Authorization Lists (WRKAUTL) command 273 authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Authorization Lists (WRKAUTL) command 273 work with Database Files Using IDDU (WRKDBFIDD) command 273 work with Directory (WRKDIRE) command 278 work with Directory (WRKDIRE) command 261, 268 work with Journal Attributes (WRKJRNA) command 261, 268 work with Objects (WRKOBI) command 274 work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 work with Objects by Owner display 102, 143 work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 description 274 description 274 description 274 work with Output Queue Description workstation entry is devicted in the victory (WRKDIRE) work with output user ID and password 13 workstation entry is description 181 sign on without user ID and password 13 workstation entry is description 181 sign on without user ID and password 13 workstation entry is description 273 workstation entry is description 273 workstation entry is description 273 workstation entry is description 181 sign on without user ID and password 13 workstation entry is description 274 work with Directory (WRKDIRE) command 278 Work with Objects (WRKOBI) command 274 WRKALTID (Work with Alert Description) object authority required 371 WRKALRD (Work with Alert Description) object authority required 314 WRKALR			
Number) command authorized IBM-supplied user profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Authorization Lists (WRKAUTL) command 273 Work with Database Files Using IDDU (WRKDBFIDD) command 268 Work WRKDIRE) command 278 Work WRKJIRN) command 261, 268 Work with Journal Attributes (WRKOBJOWN) command 261, 268 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 description 274 description 274 work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 work with Output Queue Description object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 371 WRKALRD (Work with Alert Table) command object authority required 371 WRKALRD (Work with Alert Table) command object authority required 371 WRKALRTBL (Work with Alert Table) command object authority required 371 WRKALRTBL (Work with Alert Table) command object authority required 371 WRKALRTBL (Work with Alert Table) object authority required 371 WRKALRTBL (Work with Alert Table) object authority required 371 WRKALRTBL (Work with Alert Table)			3 3 1
authorized IBM-supplied user profiles 298     object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298     object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298     object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298     object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31     definition 31 virtual printer securing 190  authority required 368 Work with Directory (WRKDIRE) command 261, 268 Work with Journal Attributes (WRKOBJPCP) command 261, 268 Work with Objects by Owner (WRKOBJPCWN) command auditing 234 description 274 using 143 Work with Objects by Primary Group (WRKOBJPCP) command 123, 144 description 274 Work with Output Queue Description object authority required 314 WRKALRTBL (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 371 WRKALRTBL (Work w	· ·		
profiles 298 object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 411 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Directory (WRKDIRE) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command object authority required 371 WRKALRD (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 371 WRKALRD (Work with Alert Description) command object authority required 371 WRKALRD (Work with Alert Description) command object authority required 371 WRKALRD (Work with Alert Description) command object authority required 371 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table)	· · · · · · · · · · · · · · · · · · ·		
object authority required 327 VFYPRT (Verify Printer) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  object authority required 368 Work with Directory (WRKDIRE) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKJBNA) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  object authority required 368 Work with Journal (WRKJRN) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description		8	
authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command 261, 268 Work with Journal (WRKJRN) command 261, 268 Work with Objects (WRKOBJ) command 274 Vork with Objects by Owner (WRKOBJOWN) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 work with Directory (WRKDIRE) command 278 Work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKOBJ) command 261, 268 Work with Objects (WRKOBJ) command object authority required 371 WRKALRO (Work with Alerts) command object authority required 314 WRKALRO (Work with Alert Description) command object authority required 314 WRKALRO (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 371 WRKALR (Work with Alert Table) command object authority required 371 WRKALR (Work with Alert Description) object authority required 371 WRKALR (Work with Alert Description) object authority required 371 WRKALR (Work with Alert Description) object authority required 371 WRKALR (Work with Alert Description) object authority required 371 WRKALR (Work with Alert De	object authority required 327	· ·	
profiles 298 object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Journal (WRKJRN) command 261, 268 Work with Journal (WRKOBJOWN) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  *JOBCTL (job control) special authority 69 object authority required for commands 447 WRKACTJOB (Work with Active Jobs) command 274 WRKALRUD (Work with Alerts) command object authority required 371 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRIBL (Work with Alert Table) command	•		1
object authority required 414, 430 VFYTAP (Verify Tape) command authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Journal (WRKJRN) command 261, 268 Work with Journal Attributes (WRKJRNA) command 261, 268 Work with Journal Attributes (WRKOBJ) command 261, 268 Work with Journal Attributes (WRKOBJ) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  authority 69 object authority required for command 447 WRKACTJOB (Work with Active Jobs) command object authority required 371 WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Table) command 261, 268 Work with Journal Attributes (WRKJRNA) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description			
authorized IBM-supplied user profiles 298 object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190 work with Journal Attributes (WRKJRNA) command 261, 268 Work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description object authority required 371 WRKACTJOB (Work with Active Jobs) command object authority required 371 WRKALR (Work with Alerts) command object authority required 371 WRKALR (Work with Alerts) command object authority required 371 WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 371 WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 371 WRKALRD (Work with Alert) Descriptions) command object authority required 371 WRKALR (Work with Alert) Descriptions) command object authority required 371 WRKALR (Work with Alert) Descriptions command object authority required 371 WRKALR (Work with Alert) Description 274 Work With Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143	object authority required 414, 430		authority 69
authorized IBM-supplied user profiles 298  object authority required 414, 430  VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  work with Objects (WRKOBJ) command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Alert Descriptions) command object authority required 371 WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRD (Work with Alert) Descriptions) command object authority required 314 WRKALRD (Work with Alert) Descriptions command object authority required 314 WRKALRD (Work with Alert) Descriptions command object authority required 314 WRKALRD (Work with Alert) Descriptions command object authority required 314 WRKALRD (Work with Alert)			
object authority required 414, 430 VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 Viewing audit journal entries 262 Virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 Virtual printer securing 190 Vork with Objects (WRKOBJ) Command 274 Work with Objects by Owner (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  virtual printer securing 190 Vork with Objects (WRKOBJ) Command object authority required 371 WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) object authority required 314 WRKALRD (Work with Alert Description) object authority required 314 WRKALRD (Work with Alert Description) object authority required 314 WRKALRD (Work with Alert Description) object authority required 314 WRKALRD (Work with Alert Description)		(WRKJRNA) command 261, 268	
VFYTCPCNN (Verify TCP/IP Connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  virtual evice securing 190  virtual evice automatic configuration (QAUTOVRT system value) 31 virtual printer securing 190  virtual evice securing 190  virtual printer securing 190  virtual evice securing 190  virtual printer securing 190  virtual evice securing 190  virtual printer securing 190  virtual printer securing 190  virtual evice securing 190  virtual printer securing 190  virtual evice securing 190  virtual printer securing 190  virtual evice suthority required 371  WRKALR (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  WRKALRO (Work with Alert Description) command object authority required 314  Vork with Objects by Owner  display 102, 143  Work with Objects by Primary Group  (WRKOBJPGP) command 123, 144  WRKALRO (Work with Alert Description) command	1	•	
connection) command object authority required 441 viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  (WRKOBJOWN) command auditing 234 description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  WRKALR (Work with Alerts) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert Description) command object authority required 314 WRKALRD (Work with Alert) Description 274 Work WITH Alert Tobelow	VFYTCPCNN (Verify TCP/IP		
viewing audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  wind description 274 description 274 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  wind description 274 Work with Output Queue Description  wind description 274 WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Description) command object auditing 452 writing 452 writing 452	,	3 3	,
audit journal entries 262 virtual device automatic configuration (QAUTOVRT system value) 31 definition 31 virtual printer securing 190  description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  description 274 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description  abject auditing 452  WRKALRD (Work with Alert Descriptions) command object auditing 452  WRKALRTBL (Work with Alert Table) command object auditing 452  WRKALRTBL (Work with Alert Table) command object auditing 452  WRKALRTBL (Work with Alert Table) command object auditing 452			opieci autionity reduited 314
automatic configuration (QAUTOVRT system value) 31  definition 31  virtual printer securing 190  Work with Objects by Owner display 102, 143  Work with Objects by Primary Group (WRKOBJPGP) command 123, 144  description 274  Work with Objects by Owner display 102, 143  Work with Objects by Primary Group (WRKOBJPGP) command 123, 144  description 274  Work with Output Queue Description object auditing 452  WRKALRD (Work with Alert Descriptions) command object auditing 452  WRKALRD (Work with Alert Descriptions) command object auditing 452  WRKALRD (Work with Alert Descriptions) object auditing 452  WRKALRD (Work with Alert Descriptions) command object auditing 452  WRKALRD (Work with Alert Descriptions) object auditing 452	audit journal entries 262	· ·	
display 102, 143  Work with Objects by Primary Group definition 31  Virtual printer securing 190  Wirtual printer Work with Output Queue Description  display 102, 143  Work with Objects by Primary Group (WRKOBJPGP) command 123, 144  WRKALRD (Work with Alert Descriptions) command object authority required 314  WRKALRD (Work with Alert Command Object authority required 314  WRKALRD (Work with Alert Object authority requi		description 274	WRKALRD (Work with Alert
definition 31  virtual printer securing 190  work with Objects by Primary Group (WRKOBJPGP) command 123, 144 WRKALRTBL (Work with Alert Table) command work with Objects by Primary Group object authority required 314 WRKALRTBL (Work with Alert Table) command object authority required 314 WRKALRTBL (work with Alert Table) command object authority required 314 WRKALRTBL (work with Alert Table) command object authority required 314 WRKALRTBL (work with Alert Table)	_	description 274 using 143	WRKALRD (Work with Alert Description) command object auditing 452
virtual printer securing 190  WRKOBPGP command 123, 144  description 274  WRKALRTBL (Work with Alert Table) command work with Output Queue Description		description 274 using 143 Work with Objects by Owner display 102, 143	WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert
Securing 190 Work with Output Queue Description command object auditing 452		description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group	WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Descriptions) command
	definition 31 virtual printer	description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144	WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Table)
detecting 235 270 276 (WRKOUTQD) command 186	definition 31 virtual printer securing 190	description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description	WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Table) command
scanning 270 Work with Spooled Files (WRKSPLF) command 186	definition 31 virtual printer	description 274 using 143 Work with Objects by Owner display 102, 143 Work with Objects by Primary Group (WRKOBJPGP) command 123, 144 description 274 Work with Output Queue Description (WRKOUTQD) command 186	WRKALRD (Work with Alert Description) command object auditing 452 WRKALRD (Work with Alert Descriptions) command object authority required 314 WRKALRTBL (Work with Alert Table)

WRKALRTBL (Work with Alert Tables) WRKCOSD (Work with Class-of-Service WRKDSTL (Work with Distribution Lists) Descriptions) command command object authority required 314 object auditing 458 object authority required 333 WRKASPJOB command WRKDSTQ (Work with Distribution object authority required 318 object authority required 371 WRKCRQD (Work with Change Request Queue) command WRKAUT (Work with Authority Description) command authorized IBM-supplied user object authority required 317 Directory) command profiles 298 object authority required 363 WRKCRQD (Work with Change Request object authority required 333 WRKAUT (Work with Authority) Descriptions) command WRKDTAARA (Work with Data Areas) command 139 object auditing 456 command WRKCSI (Work with Communications object auditing 468 description 274 object authority required 327 object auditing 462, 496, 501 Side Information) command WRKAUTL (Work with Authorization object auditing 458 WRKDTADCT (Work with Data List) command object authority required 323 Dictionaries) command WRKCTLD (Work with Controller object auditing 453 object authority required 367 Descriptions) command WRKDTADFN (Work with Data WRKAUTL (Work with Authorization Lists) command object auditing 459 Definitions) command object authority required 326 description 273 object authority required 368 object authority required 316 WRKDBFIDD (Work with Database Files WRKDTAQ (Work with Data Queues) WRKBNDDIR (Work with Binding Using IDDU) command command object authority required 368 Directory) command object auditing 469 WRKDDMF (Work with Distributed Data object auditing 454 object authority required 328 object authority required 317 Management Files) command WRKEDTD (Work with Edit WRKBNDDIRE (Work with Binding object authority required 345 Descriptions) command WRKDEVD (Work with Device Directory Entry) command object auditing 469 object auditing 454 Descriptions) command object authority required 338 object authority required 317 object auditing 460 WRKENVVAR (Work with Environment WRKCFGL (Work with Configuration object authority required 330 Variable) command List) command WRKDEVTBL (Work with Device Tables) object authority required 338 WRKF (Work with Files) command object auditing 454 command WRKCFGL (Work with Configuration authorized IBM-supplied user object auditing 473 profiles 298 Lists) command object authority required 345 object authority required 324 object authority required 347 WRKFCNARA WRKCFGSTS (Work with Configuration WRKDIRE (Work with Directory Entry) authorized IBM-supplied user Status) command command profiles 298 object auditing 460, 481, 486 object authority required 331 WRKFCNARA (Work with Functional object authority required 323 WRKDIRE (Work with Directory) Areas) command WRKCHTFMT (Work with Chart command object authority required 413 Formats) command description 278 WRKFCT (Work with Forms Control object authority required 318 WRKDIRLOC (Work with Directory Table) command WRKCLS (Work with Class) command object authority required 426 Locations) command object auditing 456 object authority required 331 WRKFLR (Work with Folders) command WRKCLS (Work with Classes) command WRKDIRSHD (Work with Directory object authority required 336 WRKFNTRSC (Work with Font object authority required 318 Shadow Systems) command WRKCMD (Work with Command) object authority required 331 Resources) command WRKDOC (Work with Documents) object auditing 473 command object authority required 313 object auditing 457 command WRKCMD (Work with Commands) object auditing 465 WRKFORMDF (Work with Form command object authority required 336 Definitions) command object authority required 322 WRKDOCLIB (Work with Document object auditing 474 WRKCMTDFN (Work with Commitment Libraries) command object authority required 313 WRKFSTAF (Work with FFST Alert Definition) command object auditing 467 object authority required 402 object authority required 322 Feature) command WRKDOCPRTQ (Work with Document WRKCNNL (Work with Connection Lists) object authority required 430 Print Queue) command WRKFSTPCT (Work with FFST Probe object auditing 457 object auditing 467 Control Table) command object authority required 402 object authority required 430 object authority required 324 WRKCNNLE (Work with Connection List WRKDPCQ (Work with DSNX/PC WRKFTR (Work with Filters) command Distribution Queues) command object auditing 474 Entries) command object auditing 457 authorized IBM-supplied user object authority required 346 WRKCNTINF (Work with Contact profiles 298 WRKFTRACNE (Work with Filter Action object authority required 333 Information) command Entries) command authorized IBM-supplied user WRKDSKSTS (Work with Disk Status) object auditing 474 profiles 298 command object authority required 346 object authority required 420, 430 WRKFTRSLTE (Work with Filter Selection object authority required 332

Entries) command object auditing 474

WRKFTRSLTE (Work with Filter Selection WRKLICINF (Work with License WRKNTBD (Work with NetBIOS Entries) command (continued) Description) command (continued) Information) command object authority required 346 authorized IBM-supplied user object authority required 397 WRKGSS (Work with Graphics Symbol profiles 299 WRKNWID (Work with Network Sets) command WRKLIND (Work with Line Descriptions) Interface Description Command) object auditing 475 command command object authority required 347 object auditing 480 object authority required 399 WRKHDWRSC (Work with Hardware object authority required 391 WRKNWID (Work with Network WRKLNK (Work with Links) command Interface Description) command Resources) command object authority required 422 object auditing 461, 462, 495, 496, object auditing 486 WRKNWSALS (Work with Network WRKHLDOPTF (Work with Help Optical 500, 501, 502, 503 Files) command Server Alias) command object authority required 363 object authority required 406 WRKMBRPDM (Work with Members object authority required 401 WRKIMGCLG command Using PDM) command WRKNWSCFG command object authority required 349 object authority required 315 authorized IBM-supplied user WRKIMGCLGE WRKMNU (Work with Menus) command profiles 299 authorized IBM-supplied user object auditing 482 object authority required 401 object authority required 393 WRKNWSD (Work with Network Server profiles 298 WRKIMGCLGE command WRKMOD (Work with Module) Description) command object authority required 349 command object auditing 486 WRKIPXD command 368 object authority required 397 object authority required 402 WRKNWSENR (Work with Network WRKJOB (Work with Job) command WRKMOD (Work with Modules) object authority required 371 command Server User Enrollment) command WRKJOBD (Work with Job Descriptions) object auditing 482 object authority required 401 WRKMODD (Work with Mode WRKNWSSSN (Work with Network command object auditing 476 Descriptions) command Server Session) command object authority required 372 object auditing 482 object authority required 401 WRKJOBLOG (Work with Job Logs) object authority required 396 WRKNWSSTG (Work with Network command WRKMSG (Work with Messages) Server Storage Space) command object authority required 371 object authority required 400 command WRKJOBQ (Work with Job Queue) object auditing 484 WRKNWSSTS (Work with Network command object authority required 394 Server Status) command object auditing 477 WRKMSGD (Work with Message object authority required 401 object authority required 373 Descriptions) command WRKOBJ (Work with Objects) command WRKJOBSCDE (Work with Job Schedule object auditing 483 description 274 Entries) command object authority required 394 object authority required 310 object auditing 477 WRKMSGF (Work with Message Files) WRKOBJCSP (Work with Objects for object authority required 373 command CSP/AE) command object auditing 458, 489 WRKJRN (Work with Journal) command object auditing 483 authorized IBM-supplied user object authority required 395 WRKOBJLCK (Work with Object Lock) profiles 298 WRKMSGQ (Work with Message command object auditing 479 Queues) command object auditing 452 object authority required 377 object auditing 484 WRKOBJLCK (Work with Object Locks) using 261, 268 object authority required 395 command WRKJRNA (Work with Journal WRKNAMSMTP (Work with Names for object authority required 310 Attributes) command WRKOBJOWN (Work with Objects by SMTP) command object auditing 479 object authority required 441 Owner) command object authority required 377 WRKNETF (Work with Network Files) auditing 234 using 261, 268 description 274 command WRKJRNRCV (Work with Journal object authority required 398 object auditing 452, 505 Receivers) command WRKNETJOBE (Work with Network Job object authority required 310 object auditing 479 Entries) command using 143 object authority required 377 object authority required 398 WRKOBJPDM (Work with Objects Using WRKLANADPT (Work with LAN WRKNETTBLE (Work with Network PDM) command Adapters) command Table Entries) command object authority required 315 WRKOBJPGP (Work with Objects by object authority required 391 object authority required 441 Primary Group) command 123, 144 WRKLIB WRKNODL (Work with Node List) authorized IBM-supplied user command object authority required 310 WRKOBJPGP (Work with Objects by profiles 298 object auditing 485 WRKLIB (Work with Libraries) command object authority required 402 Primary) command object authority required 387 WRKNODLE (Work with Node List description 274 WRKOPTDIR (Work with Optical WRKLIBPDM Entries) command authorized IBM-supplied user object auditing 485 Directories) command profiles 299 object authority required 402 object authority required 406 WRKNTBD (Work with NetBIOS WRKLIBPDM (Work with Libraries Using WRKOPTF (Work with Optical Files) PDM) command Description) command command object authority required 315 object auditing 485 object authority required 406

WRKOPTVOL (Work with Optical WRKQMFORM (Work with Query WRKSOC (Work with Sphere of Control) Management Form) command Volumes) command command object authority required 406 object auditing 491 object authority required 432 object authority required 420 WRKSPADCT (Work with Spelling Aid WRKORDINF (Work with Order Information) command WRKQMQRY (Work with Query Dictionaries) command authorized IBM-supplied user Management Query) command object authority required 431 WRKSPLF (Work with Spooled Files) profiles 299 object authority required 420 object authority required 442 WRKQRY (Work with Query) command command 186 WRKOUTQ (Work with Output Queue) object authority required 420 object auditing 487 command WRKQST (Work with Questions) object authority required 434 object auditing 487 WRKSPLFA (Work with Spooled File command object authority required 407 object authority required 420 Attributes) command WRKOUTQD (Work with Output Queue WRKRDBDIRE (Work with Relational object auditing 487 Description) command Database Directory Entries) command WRKSPTPRD (Work with Supported object auditing 487 object authority required 422 Products) command WRKREGINF (Work with Registration object authority required 407 object auditing 490 security parameters 186 Information) command WRKSRVPGM (Work with Service WRKOVL (Work with Overlays) object auditing 470 Programs) command WRKREGINF (Work with Registration) object auditing 499 command object auditing 487 command object authority required 418 WRKSRVPVD (Work with Service object authority required 313 object authority required 421 WRKPAGDFN (Work with Page WRKRJESSN (Work with RJE Session) Providers) command Definitions) command authorized IBM-supplied user object auditing 488 object authority required 426 profiles 299 WRKRPYLE (Work with System Reply object authority required 313 object authority required 430 WRKPAGSEG (Work with Page List Entries) command WRKSRVTBLE (Work with Service Table object auditing 493 Segments) command Entries) command object auditing 488 object authority required 436 object authority required 441 object authority required 313 WRKS36PGMA (Work with System/36 WRKSSND (Work with Session WRKPCLTBLE (Work with Protocol Table Program Attributes) command Description) command Entries) command object auditing 489 object authority required 426 object authority required 441 object authority required 439 WRKSYSACT WRKPDG (Work with Print Descriptor WRKS36PRCA (Work with System/36 authorized IBM-supplied user Procedure Attributes) command Group) command profiles 299 object auditing 473 object auditing 488 WRKSYSACT (Work with System object authority required 439 WRKPEXDFN command Activity) command authorized IBM-supplied user WRKS36SRCA (Work with System/36 object authority required 413 profiles 299 Source Attributes) command WRKSYSSTS (Work with System Status) WRKPEXFTR command object auditing 473 command 192 authorized IBM-supplied user object authority required 439 object authority required 436 WRKSBMJOB (Work with Submitted WRKSYSVAL (Work with System Values) profiles 299 WRKPFCST (Work with Physical File Jobs) command Constraints) command object authority required 371 object authority required 436 WRKSBS (Work with Subsystems) object auditing 473 using 232 WRKTAPCTG (Work with Tape object authority required 345 command WRKPGM (Work with Programs) object auditing 494 Cartridge) command object authority required 436 object authority required 392 command object auditing 489 WRKSBSD (Work with Subsystem WRKTBL (Work with Tables) command object authority required 418 Descriptions) command object auditing 504 WRKPGMTBL (Work with Program object auditing 494 object authority required 440 Tables) command object authority required 436 WRKTCPSTS (Work with TCP/IP authorized IBM-supplied user WRKSBSJOB (Work with Subsystem Jobs) Network Status) command object authority required 441 profiles 299 command object authority required 347 object auditing 494 WRKTIMZON command 442 WRKPNLGRP (Work with Panel Groups) object authority required 371 WRKTRC command WRKSCHIDX (Work with Search command authorized IBM-supplied user object auditing 490 profiles 299 Indexes) command object authority required 393 object auditing 495 WRKTXTIDX (Work with Text Index) WRKPRB (Work with Problem) command object authority required 368 command authorized IBM-supplied user WRKSCHIDXE (Work with Search Index authorized IBM-supplied user profiles 299 Entries) command profiles 299 object auditing 494 object authority required 414, 430 WRKUSRJOB (Work with User Jobs) WRKPTFGRP (Work with Program object authority required 368 command Temporary Fix Groups) 299 WRKSHRPOOL (Work with Shared object authority required 371 WRKPTFGRP (Work with PTF Group) WRKUSRPRF (Work with User Profiles) Storage Pools) command object authority required 436 command command object authority required 430 description 276

WRKUSRPRF (Work with User Profiles)
command (continued)
object auditing 505
object authority required 445
using 97
WRKUSRTBL (Work with User Tables)
command
authorized IBM-supplied user
profiles 299
object authority required 347
WRKWCH command
authorized IBM-supplied user
profiles 299
WRKWTR (Work with Writers) command
object authority required 448

## X

 $\begin{array}{cc} X0 \ (kerberos \ authentication) \ file \\ layout \quad 605 \end{array}$ 

## Y

YC (change to DLO object) file layout 610 YR (read of DLO object) file layout 611

## Z

ZC (change to object) file layout 611 ZR (read of object) file layout 614

## Readers' Comments — We'd Like to Hear from You

IBM Systems - iSeries Security Reference Version 5 Release 4

Publication No. SC41-530	02-09				
Overall, how satisfied are	you with the info	ormation in this	book?		
	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very
Overall satisfaction					Dissatisfied
How satisfied are you that	at the information	in this book is:			
	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate Complete Easy to find Easy to understand Well organized Applicable to your tasks Please tell us how we can	□ □ □ □ n improve this boo	                 			
Thank you for your respon	nses. May we conta	act you? □ Ye	s 🗌 No		
When you send comments way it believes appropriat		g any obligation	to you.	or distribute your c	omments in any
Name		Ac	ldress		
Company or Organization					
Phone No.					

Readers' Comments — We'd Like to Hear from You SC41-5302-09



Cut or Fold Along Line

Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

## **BUSINESS REPLY MAIL**

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM CORPORATION ATTN DEPT 542 IDCLERK 3605 HWY 52 N ROCHESTER MN 55901-7829



Fold and Tape

Please do not staple

Fold and Tape

# 

Printed in USA

SC41-5302-09

