

Smart Security Administrator

User Guide

Release 1.4

Publication information

June 2016

Information in this publication is subject to change. Changes will be published in new editions or technical newsletters.

Trademarks

The following are trademarks or registered trademarks of UNICOM Systems, Inc. in the United States and/or other jurisdictions worldwide: UNICOM, UNICOM Systems.

Copyright notice

Smart Security Administrator (the Programs and associated materials) is a proprietary product of UNICOM Systems, Inc. – a division of UNICOM Global. The Programs have been provided pursuant to License Agreement containing restrictions on their use. The programs and associated materials contain valuable trade secrets and proprietary information of UNICOM Systems, Inc. and are protected by United States Federal and non-United States copyright laws. The Programs and associated materials may not be reproduced, copied, changed, stored, disclosed to third parties, and distributed in any form or media (including but not limited to copies on magnetic media) without the express prior written permission of UNICOM Systems, Inc., UNICOM Plaza Suite 310, 15535 San Fernando Mission Blvd., Mission Hills, CA 91345 USA.

Smart Security Administrator

© Copyright 1988-2016 All Rights Reserved. UNICOM Systems, Inc. – a Division of UNICOM Global.

No part of this Program may be reproduced in any form or by electronic means, including the use of information storage and retrieval systems, without the express prior written consent and authorization of UNICOM Systems, Inc.

No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, without prior written permission from UNICOM Systems, Inc.

Disclaimer

We cannot guarantee freedom from, or assume any responsibility or liability for technical inaccuracies or typographical errors. The information herein is furnished for informational use only and should not be construed as a commitment by UNICOM Systems, Inc. – a division of UNICOM Global.

Trademark acknowledgements

IBM:

IBM[®], AIX[®], CICS[®], CICS/ESA[®], CICS TS[®] CMAC[®], DB2[®], DFSMS/MVS[®], Domino[®], ESCON[®], IMS[™], Internet Explorer[®], iSeries[®], Language Environment[®], LE[®], Lotus[®], MQSeries[®], MVS[™], MVS/ESA[®], OMEGAMON[®], OS/390[®], OS/400[®], Power[®], POWER[®], pSeries[®], RACF[®], RMF[™], S/370[®], S/390[®], SMF[®], System/390[®], System i[®], System p[®], System z[®], VisualAge[®], VM/ESA[®], VSE/ESA[®], VTAM[®], WebSphere[®], z/OS[®], z/VM[®], z/VSE[®], zSeries[®], z Systems[®] and the IBM logo are trademarks or registered trademarks of IBM Corporation in the United States or other countries or both.

Microsoft:

Active Directory, Excel, Microsoft, Notepad, PowerPoint, Visual Basic, Windows, Windows 2000, Windows NT, Windows Server 2003, Windows Server 2007, Windows Vista, Windows XP, WordPad and/or other Microsoft products referenced are either trademarks or registered trademarks of Microsoft Corporation.

Adobe Systems Incorporated:

Adobe[®] and Acrobat[®] are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Apache Software Foundation:

Apache, Apache Tomcat and Tomcat are trademarks of the Apache Software Foundation.

Apple Inc.:

AirPrint, iPad and Safari are trademarks or registered trademarks of Apple Inc. registered in the United States and other countries.

BEA Systems, Inc.:

JRockit and WebLogic are registered trademarks of BEA Systems, Inc.

BMC Software Inc.:

Boole & Babbage, Data Packer, Optimizer and Super Optimizer are trademarks or registered trademarks of BMC Software, Inc., or its affiliates or subsidiaries (collectively, "BMC Software").

BSD:

PostgreSQL is distributed under the classic BSD license. (Portions Copyright © 1996-2006, PostgreSQL Global Development Group; Portions Copyright © 1994-1996 Regents of the University of California.)

CA, Inc.:

CA ACF2, CA Datacom, CA Endevor, CA IDMS, CA InterTest, CA NetMaster, CA Optimizer, CA Panexec, CA Panvalet, CA Ramis, CA Telon and CA Top Secret are registered trademarks of CA, Inc.

Candescent SoftBase LLC:

SoftBase[®] is a registered trademark of Candescent SoftBase LLC.

Canonical Ltd:

Ubuntu is a registered trademark of Canonical Ltd.

Chicago-Soft, Ltd.:

QuickRef is a trademark of Chicago-Soft, Ltd.

Cincom Systems, Inc.:

MANTIS is a registered trademark of Cincom Systems, Inc.

Computer Sciences Corporation:

Hogan and Hogan Umbrella are trademarks or registered trademarks of Computer Sciences Corporation.

Compuware Corporation:

Abend-AID and Compuware are trademarks or registered trademarks of Compuware Corporation.

Dell Inc.:

Dell and the Dell logo are trademarks of Dell Inc.

Emtex Limited:

Emtex and VIP are trademarks of Emtex Limited.

Jean-loup Gailly and Mark Adler:

zlib is a registered trademark or trademark of Jean-loup Gailly and Mark Adler.

GNU General Public License:

Cygwin is free software released under the GNU General Public License.

Google Inc.:

Google and Google Chrome are registered trademarks of Google Inc.

Hewlett-Packard Development Company, L.P.:

HP and HP-UX are registered trademarks of Hewlett-Packard Development Company, L.P., and/or its subsidiaries.

Innovation Data Processing:

IAM is a registered trademark of Innovation Data Processing Corporation.

Kofax, Inc.:

Kofax, the Kofax logo and Kofax Capture are the trademarks or registered trademarks of Kofax, Inc., in the United States and other countries.

Linus Torvalds:

Linux is a registered trademark of Linus Torvalds.

Massachusetts Institute of Technology (MIT):

Kerberos is a trademark of the Massachusetts Institute of Technology (MIT).

Merrill Pty Ltd.:

MXG is a registered trademark of Merrill Pty Ltd.

Mozilla Foundation:

Firefox is a registered trademark of the Mozilla Foundation.

Mozilla Public License:

Expat is free software released under the Mozilla Public License.

Novell, Inc.:

openSUSE is a registered trademark of Novell, Inc.

The Open Group:

UNIX is a registered trademark of The Open Group.

Oracle Corporation:

EJB, Java, JDBC, JDK, JMX, JRE, JSP, JVM, Solaris and SunOS are trademarks or registered trademarks of Oracle Corporation and/or its affiliates. Oracle is a registered trademark, and other Oracle product names, service names, slogans or logos are trademarks or registered trademarks of Oracle Corporation.

Red Hat, Inc.:

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. in the United States and other countries.

SAP AG:

SAP, the SAP logo, the SAP Partner logo, SAP R/3, SAP ArchiveLink, SAP NetWeaver, SAPPHIRE and Duet are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

SAS Institute Inc.:

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries.

Simon Tatham:

PuTTY is copyright Simon Tatham.

Software AG:

Adabas and Natural are registered trademarks of Software AG. Software AG and all Software AG products are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc.

SPARC International, Inc.:

SPARC is a registered trademark of SPARC International, Inc. (Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.)

Standardware Inc.:

COPE is a trademark of Standardware Inc.

Sun Microsystems, Inc.:

Sun, Sun Microsystems, the Sun logo, MySQL and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries.

SUSE LLC:

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

Syncsort Inc.:

Syncsort is a registered trademark of Syncsort Inc.

Wireshark Foundation:

Wireshark and the “fin” logo are registered trademarks of the Wireshark Foundation.

XEROX CORPORATION:

XEROX, The Document Company and the stylized X are trademarks of XEROX CORPORATION.

X.Org Foundation:

X Window System is a trademark of the X.Org Foundation.

Additional trademarks and registered trademarks are the property of their respective owners.



Contents

Preface	21
Audience	22
How This Manual is Organized	22
Syntax Conventions	23
SSA release and dates in figures and examples	24
Customer Service.	24
 Chapter 1 Overview	 25
 Chapter 2 SSA Installation	 27
SSA Installation Requirements	28
Step 1: Download SSA FTP Distribution	30
Step 2: Allocate Additional SSA Libraries	31
Step 3: APF-Authorize the SSA Load Library	34
Step 4: Add AUTHTSF Entries	35
Step 5: Modify Logon Procedure	37
Step 6: Define the SCHEDULER Started Task (Optional)	38
Step 7: Define RACF Classes for SSA Security	40
Step 8: Define SSA Users and Administrators	43
Step 9: Define Default Configuration Profile	44
Step 10: Define Base Security Rules	46
Step 11: Install the CICS Direct Administration Module (Optional)	47
Step 12: Define Product Password	52
Step 13: Startup Panel Choice (Optional/Recommended)	54
Step 14: Start the SSA Started Tasks.	55
Step 15: Off-loading RACF Information	56
SSA Usage Recommendations	58

Chapter 3 SSA Reports	59
Report Global Conventions	60
JCL Sample (AAREP001 - Access Reports for Userids)	63
Reports Main Menu	65
Access Report for Userids	66
Report Data Selection	66
Report JCL	66
Control Cards	67
Access Report for Groups	68
Report Data Selection	68
Report JCL	68
Control Cards	69
Dataset Profile Permissions Report	70
Report Data Selection	70
Report JCL	70
Control Cards	70
Ownership Report	71
Report Data Selection	71
Report JCL	71
Control Cards	72
Group Connect Report	73
Report Data Selection	73
Report JCL	73
Control Cards	73
Default Group Report	74
Report Data Selection	74
Report JCL	74
Control Cards	74
Clauth/Group Special Report	75
Report Data Selection	75
Report JCL	75
Control Cards	75
Never Logged On Report	76
Report Data Selection	76
Report JCL	76
Control Cards	77
Global Attribute Report	78
Report Data Selection	78
Report JCL	79
Control Cards	79
Non-Expiring Password Report	80
Report Data Selection	80
Report JCL	80
Control Cards	81
True Dataset Authority Report	82
Report Data Selection	82

Report JCL	82
Control Cards (Entered under AASYSIN DD)	83
Notify Report	84
Report Data Selection	84
Report JCL	84
Control Cards	85
Break in Ownership Report	86
Report Data Selection	86
Report JCL	87
Control Cards	87
User/Group Repetitive Permits Report	88
Report Data Selection	88
Report JCL	88
Control Cards (Entered under DD AASYSIN)	88
Group Statistics Report	90
Report Data Selection	90
Report JCL	90
Control Cards	90
Obsolete Entries Report	92
Report Data Selection	92
Report JCL	92
Control Cards	92
Where a User/Group is Not in an Access List Report	93
Report Data Selection	93
Report JCL	93
Control Cards (Entered under DD AASYSIN)	93
General Resource Class Permission Report	95
Report Data Selection	95
Report JCL	95
Control Cards	95
Userid Statistics Report	97
Report Data Selection	97
Report JCL	97
Control Cards	97
Dataset Profile and Permission Report	99
Report Data Selection	99
Report JCL	99
Control Cards	99
RACF to Master Catalog Comparison Report	100
Report Data Selection	100
Report JCL	100
Control Cards	100
Chapter 4 Online Generic Searches	101
Generic Search Global Conventions	102
Adhoc Report Generation Options	107

General User Information	115
Search Examples	115
Various Mode Available Functions	116
Userid TSO Segment	118
Search Examples	118
Various Mode Available Functions	119
Userid CICS Segment	120
Search Examples	120
Various Mode Available Functions	121
Userid DFP Segment	122
Search Examples	122
Various Mode Available Functions	122
Userid LANGUAGE Segment	124
Search Examples	124
Various Mode Available Functions	124
Userid OPERPARM Segment	126
Search Examples	126
Various Mode Available Functions	127
Userid WORKATTR Segment	128
Search Examples	128
Various Mode Available Functions	128
Userid NETVIEW Segment	130
Search Examples	130
Various Mode Available Functions	130
Userid OMVS Segment	132
Search Examples	132
Various Mode Available Functions	132
Userid DCE Segment	134
Search Examples	134
Various Mode Available Functions	134
Userid RRSF Associations	136
Search Examples	136
Various Mode Available Functions	137
Connect Information	138
Search Examples	138
Various Mode Available Functions	139
CLAUTH Authorities	140
Search Examples	140
Various Mode Available Functions	140
Userid Security Categories	142
Search Examples	142
Various Mode Available Functions	142
General Group Information	144
Search Examples	144
Various Mode Available Functions	144
Group DFP Segment	146

Search Examples	146
Various Mode Available Functions	146
Group OMVS Segment	148
Search Examples	148
Various Mode Available Functions	148
General Dataset Profile Information	150
Search Examples	150
Various Mode Available Functions	151
Dataset Profile Permissions	152
Search Examples	152
Various Mode Available Functions	153
Dataset Profile Security Categories	154
Search Examples	154
Various Mode Available Functions	154
General Resource Profile Information	156
Search Examples	156
Various Mode Available Functions	157
General Resource Profile Permissions	158
Search Examples	158
Various Mode Available Functions	159
General Resource Members	160
Search Examples	160
Various Mode Available Functions	160
General Resource Session Segment	162
Search Examples	162
Various Mode Available Functions	162
General Resource DLF Segment	164
Search Examples	164
Various Mode Available Functions	164
General Resource Started Task Segment	165
Search Examples	165
Various Mode Available Functions	166
General Resource SystemView Segment	167
Search Examples	167
Various Mode Available Functions	167
General Resource Security Categories	168
Search Examples	168
Various Mode Available Functions	168
Online Generic Search Result Functions	169
Search Result Screen	169
Various Mode	170
Various Mode Pop-Up Panel Example	170
SSA ListDataset	170
SSA ListGroup	171
SSA ListUser	171
SSA Resource List	172

Display CICS Segment	173
Display CLAUTH Authorities.....	174
Display Connects	174
Display Connects with Group Special.....	175
Display DATASET Profiles (HLQ=Group)	175
Display DATASET Profiles (HLQ=UserID)	176
Display DCE Segment	177
Display DFP Segment	177
Display Jobnames.....	177
Display Language Segment	178
Display Members	178
Display NETVIEW Segment.....	179
Display OMVS Segment	179
Display OPERPARM Segment.....	180
Display Permits to Dataset Profiles	180
Display Permits to General Resource Profiles.....	181
Display RRSF Information	182
Display Security Categories	182
Display STDATA Segment	183
Display Subgroups	183
Display TSO Segment	184
Display Users in Group	184
Display Volume Information.....	185
Display WORKATTR Segment	186
Various Mode: RACF Command Generation	187
Various Mode: System Command Listings.....	189
Various Mode: Pass to Functionality.....	189
Adhoc Mode.....	190
Print Mode	192
Sort Mode Usage	192
Adhoc Report Generation	194
How to Specify Generic Search Criteria.....	194
How to Build an Adhoc Report Mask.....	195
Adhoc Report Control Cards.....	196
Chapter 5 Command Generation	201
Command Generation Global Conventions	202
Batch, Online, or SCHEDULE Operational Modes.....	202
Command Generation JCL	204
Command Syntax Rules	206
Initiating the Command Generation Process	206
Command Generation Main Menu.....	208
Replicate Userid Profiles	209
Replicate Userid Profile Overrides Options Screen.....	209
Command Generation Initiators	213
Replicate Userid Processing Notes	214
Replicate Group Profiles.....	215

Replicate Group Profile Overrides Options Screen	216
Command Generation Initiators	218
Replicate Group Profile Processing Notes	218
Replicate Dataset Profiles	219
Replicate Dataset Profile Overrides Options Screen	220
Command Generation Initiators	221
Replicate Dataset Profile Processing Notes	221
Replicate General Resource Profiles	222
Replicate General Resource Profile Overrides Options Screen	223
Command Generation Initiators	225
Replicate General Resource Profile Processing Notes	225
Replicate General Resource Classes	227
Replicate General Resource Class Overrides Options Screen	228
Command Generation Initiators	230
Replicate General Resource Class Processing Notes	230
Transfer Userid Profiles	232
Transfer Userid Profile Overrides Options Screen	233
Command Generation Initiators	236
Transfer Userid Profile Processing Notes	236
Transfer Group Profiles	238
Transfer Group Profiles Overrides Options Screen	239
Command Generation Initiators	241
Transfer Group Profiles Processing Notes	241
Transfer Dataset Profiles	242
Transfer Dataset Profile Overrides Options Screen	243
Command Generation Initiators	244
Transfer Dataset Profile Processing Notes	244
Transfer General Resource Profiles	245
Transfer General Resource Profile Overrides Options Screen	246
Command Generation Initiators	248
Transfer General Resource Profile Processing Notes	248
Transfer General Resource Classes	250
Transfer General Resource Class Overrides Options Screen	251
Command Generation Initiators	253
Transfer General Resource Class Processing Notes	253
Transfer Ownership	254
Transfer Ownership Overrides Options Screen	255
Command Generation Initiators	256
Transfer Ownership Processing Notes	256
Transfer Notifications	257
Transfer Notifications Overrides Options Screen	258
Command Generation Initiators	259
Transfer Notifications Processing Notes	259
Remove All References to a Userid	260
Remove All References to a Userid Overrides Options Screen	261
Command Generation Initiators	262

Remove All References to a Userid Processing Notes	262
Remove All References to a Group	263
Remove All References to a Group Overrides Options Screen.	264
Command Generation Initiators	265
Remove All References to a Group Processing Notes	265
Remove All Obsolete Entries	266
Command Generation Initiators	268
Processing Notes.	268
 Chapter 6 The SCHEDULER	269
The SCHEDULER Global Conventions.	270
Administrator and User Authority.	271
Schedule Entry Input Screen	272
Started Task Interface.	273
The SCHEDULER Main Menu.	275
Enter New Jobs or Commands to be Scheduled	276
Modify an Existing Scheduled Entry	277
Reschedule or Cancel an Existing Scheduled Entry	279
Report on Scheduled or Historical Entries	280
Approve/Deny/View Scheduled Entries.	281
 Chapter 7 TSO Direct Administration	285
TSO Direct Administration Global Conventions	286
Security	286
Example 'Authority' Profile Setup.	288
SSA-TDA Programs	293
TSO Direct Administration Main Menu	294
Userid Administration Screens.	295
Perform List User	295
List User Display	295
Add Userid	296
Change Password	296
Change Various Fields	297
Add/Replace User Installation Data	298
Update Existing User Installation Data	298
Group Administration Screens.	300
Perform List Group	300
List Group Display	300
Add Group	301
Change Various Fields	301
Add/Replace Group Installation Data.	302
Update Existing Group Installation Data	302
Connect Administration Screens	304
List All Connects	304
List All Connects Display.	304
List Specific Connect Display	305

Connect a User to a Group	305
Remove User from Group	306
Resume a Connect	307
Revoke a Connect.	308
Set a Resume Date on a Connect.	308
Set a Revoke Date on a Connect	309
Change Connect Authority	310
Set/Remove Connect Attributes	310
Password Administration Screens.	312
Perform List User	312
List User Display.	312
Set Password to Default Group and Resume User	313
Change Password	313
Resume a Userid.	314
Revoke a Userid	315
Set a Resume Date	315
Set a Revoke Date.	316
Set SuperRevoke.	316
Add/Replace User Installation Data	317
Update Existing User Installation Data	317
Dataset Administration Screens	319
Perform List Dataset Profile	319
List Dataset Profile Display	319
Add Dataset Profile.	320
Change Dataset Profile	320
Update Existing Dataset Profile Information.	321
Delete Dataset Profile	322
Resource Administration Screens.	323
Perform List Resource Profile.	323
List Resource Profile Display	323
Add Resource Profile	324
Change Resource Profile	325
Change Resource Profile - Installation/Application Data.	325
Update Existing Resource Profile Information	326
Delete Resource Profile	327
Dataset Permit Administration Screens	329
Perform List Dataset Profile Permits	329
List Dataset Profile Permits Display.	329
Add Dataset Profile Permit.	330
Change Dataset Profile Permit	331
Delete Dataset Profile Permit	331
Resource Permit Administration Screens.	333
Perform List Resource Profile Permits	333
List Resource Profile Permits Display	333
Add Resource Profile Permit	334
Change Resource Profile Permit	335
Delete Resource Profile Permit	335

Resource Member Administration Screens	337
Perform List Resource Profile Members	337
List Resource Profile Members Display	337
Add Resource Profile Member	338
Delete Resource Profile Member	338
User TSO Segment Administration Screens	340
Perform List User TSO Segment	340
List User TSO Segment Display	340
Add User TSO Segment	341
Change User TSO Segment	341
Delete User TSO Segment	342
User CICS Segment Administration Screens	344
Perform List User CICS Segment	344
List User CICS Segment Display	344
Add User CICS Segment	345
Change User CICS Segment	345
Delete User CICS Segment	346
Access Simulator	348
Access Simulator Results Screen	349
 Chapter 8 System Resource Monitor	 351
System Resource Monitor Global Conventions	352
Security	352
Batch or Online Operational Mode	352
Send Report Output	353
System Resource Monitor Report JCL	354
System Resource Monitor Menu	356
Reports and Options	356
System Resource Monitor Overrides	358
Authorized Program Facility (APF)	358
Link List Datasets (LLT)	358
Link Pack Area Datasets (LPA)	358
Class Descriptor Table (CDT)	359
Program Properties Table (PPT)	359
General RACF Information (GRI)	359
RACF Installation Exits (EXT)	359
RACF Database Datasets (RDS)	359
RACF Authorized Caller Table (RAU)	360
RACF Router Table (RFR)	360
System Management Facility (SMF)	360
Started Task Table (STC)	360
Supervisor Calls (SVC)	360
Authorized TSO Tables (ATT)	361
 Chapter 9 CICS Direct Administration	 363
CICS Direct Administration Global Conventions	365
Security	365

Function Explanations	371
Application Programming Interface.	371
CICS DIRECT Administration Main Menu	398
Transaction Table	398
USERID Administration Screens	400
Perform List User	400
List User Display.	400
Add Userid	401
Change Password	401
Change the User's Name or Owner.	402
Add/Replace User Installation Data	403
Update Existing User Installation Data	403
Userid Administration API Invocation.	405
Userid Administration API Example.	406
GROUP Administration Screens	407
Perform List Group.	407
List Group Display	407
Add Group	408
Change the Group's Owner or TERMUACC.	408
Add/Replace Group Installation Data.	409
Update Existing Group Installation Data.	410
Group Administration API Invocation.	411
Group Administration API Example	412
Connect Administration Screens	413
List All Connects.	413
List All Connects Display	413
List Specific Connect Display.	414
Connect a User to a Group.	414
Remove User from Group	415
Resume a Connect	416
Revoke a Connect.	417
Set a Resume Date on a Connect.	418
Set a Revoke Date on a Connect	418
Change Connect Authority	419
Set/Remove Connect Attributes	420
Connect Administration API Invocation	421
Connect Administration API Example	424
Password Administration Screens.	426
Perform List User	426
List User Display.	426
Set Password to Default Group and Resume User	427
Change Password	427
Resume a Userid.	428
Revoke a Userid	429
Set a Resume Date	429
Set a Revoke Date.	430
Set SuperRevoke.	431

Add/Replace User Installation Data	432
Update Existing User Installation Data	432
Password Administration API Invocation	434
Password Administration API Example	435
Dataset Administration Screens	436
Perform List Dataset Profile	436
List Dataset Profile Display	436
Add Dataset Profile	437
Change Dataset Profile	437
Update Existing Dataset Profile Information	438
Delete Dataset Profile	439
Dataset Administration API Invocation	440
Dataset Administration API Example	442
Resource Administration Screens	443
Perform List Resource Profile	443
List Resource Profile Display	443
Add Resource Profile	444
Change Resource Profile	445
Change Resource Profile - Installation/Application Data	446
Update Existing Resource Profile Information	447
Delete Resource Profile	448
Resource Administration API Invocation	450
Resource Administration API Example	452
Dataset Permit Administration Screens	454
Perform List Dataset Profile Permits	454
List Dataset Profile Permits Display	454
Add Dataset Profile Permit	455
Change Dataset Profile Permit	456
Delete Dataset Profile Permit	456
Dataset Permit Administration API Invocation	458
Dataset Permit Administration API Example	458
Resource Permit Administration Screens	460
Perform List Resource Profile Permits	460
List Resource Profile Permits Display	460
Add Resource Profile Permit	461
Change Resource Profile Permit	462
Delete Resource Profile Permit	463
Resource Permit Administration API Invocation	464
Resource Permit Administration API Example	464
Resource Member Administration Screens	466
Perform List Resource Profile Members	466
List Resource Profile Members Display	466
Add Resource Profile Member	467
Delete Resource Profile Member	468
Resource Member Administration API Invocation	470
Resource Member Administration API Example	470

User TSO Segment Administration Screens	471
Perform List User TSO Segment	471
List User TSO Segment Display	471
Add User TSO Segment	472
Change User TSO Segment	472
Delete User TSO Segment	473
User TSO Segment Administration API Invocation	475
User TSO Segment Administration API Example	476
User CICS Segment Administration Screens	478
Perform List User CICS Segment	478
List User CICS Segment Display	478
Add User CICS Segment	479
Change User CICS Segment	479
Delete User CICS Segment	480
User CICS Segment Administration API Invocation	482
User CICS Segment Administration API Example	486
Access Simulator Screens	488
Perform Access Simulation	488
Simulation Results	488
Access Simulator API Invocation	490
Access Simulator API Example	491
Cross Platform Administration	492
Setup Cross Platform Administration	493
Cross Platform Request Validation	497
Cross Platform Administration API Requirements	498
Chapter 10 Configuration	499
Configuration Main Menu	500
Edit Stored Configuration Values	501
Choose New Stored Configuration	505
Update Stored Configurations	507
Change The SCHEDULER Task Settings	511
Display SSA User or Group Authority	513
Run Extract Job	515
Unload Security	522
Setting Up SSA Users And Administrators	523
AAOPTION Configuration Module	524
Parameter Rules	525
AAOPTION Parameter Descriptions	528
Appendix A SSA Report Examples	537
Access Report for UserIDs - AAREP001	538
Access Report for Groups - AAREP002	539
Dataset Profile Permission Report - AAREP003	540
Ownership Report - AAREP004	540
Group Connect Report - AAREP005	541

Default Group Report - AAREP006	541
Clauth/Group Special Report - AAREP007	542
Never Logged On Report - AAREP008	542
Global Attribute Report - AAREP009	543
Non-Expiring Password Report - AAREP010	543
True Dataset Authority Report - AAREP011	544
Notify Report - AAREP012	544
Break in Ownership Report - AAREP013	545
User/Group Repetitive Permits Report - AAREP014	545
Group Statistics Report - AAREP015	546
Obsolete Entry Report - AAREP016	547
Where a User/Group Is Not in an Access List Report - AAREP017	547
General Resource Class Permission Report - AAREP018	548
Userid Statistics Report - AAREP019	548
Dataset Profile and Permission Report - AAREP020	549
RACF to Master Catalog Comparison Report - AAREP021	550
Online Generic Searches	551
Generic Search - General User Information	551
Generic Search - Userid TSO Segment	551
Generic Search - Userid CICS Segment	552
Generic Search - Userid DFP Segment	552
Generic Search - Userid Language Segment	553
Generic Search - Userid Operparm Segment	553
Generic Search - Userid Workattr Segment	554
Generic Search - Userid NetView Segment	554
Generic Search - Userid OMVS Segment	555
Generic Search - Userid DCE Segment	555
Generic Search - Userid RRSF Information	556
Generic Search - Userid Connect Information	556
Generic Search - Userid Clauth Authority	557
Generic Search - Userid Security Categories	557
Generic Search - General Group Information	558
Generic Search - Group DFP Segment	558
Generic Search - Group OMVS Segment	559
Generic Search - General Dataset Information	559
Generic Search - Dataset Permissions	560
Generic Search - Dataset Security Categories	560
Generic Search - General Resource Information	561
Generic Search - General Resource Permissions	562
Generic Search - General Resource Members	562
Generic Search - General Resource Session Segment	563
Generic Search - General Resource DLF Segment	563
Generic Search - General Resource Started Task Segment	563
Generic Search - General Resource SystemView Segment	564
Generic Search - General Resource Security Categories	564
System Resource Monitor	565

System Resource Monitor - Report Banner Page	565
System Resource Monitor - Authorized Program Facility.....	566
System Resource Monitor - Link List Datasets	566
System Resource Monitor - Link Pack Area Datasets.....	567
System Resource Monitor - Class Descriptor Table (Report 01)	567
System Resource Monitor - Class Descriptor Table (Report 02)	568
System Resource Monitor - Program Properties Table.....	569
System Resource Monitor - General RACF Information	569
System Resource Monitor - RACF Installation Exits	570
System Resource Monitor - RACF Database Datasets	571
System Resource Monitor - RACF Authorized Caller Table	571
System Resource Monitor - RACF Router Table	572
System Resource Monitor - System Management Facility (Report 01)	572
System Resource Monitor - System Management Facility (Report 02)	573
System Resource Monitor - Started Task Table	573
System Resource Monitor - Supervisor Calls	574
System Resource Monitor - Authorized TSO Tables	574
TSO Direct Administration and CICS Direct Administration	575
RACF Report Writer Example	575
 Appendix B SSA ISPF Tables	 583
Adhoc Field Substitution.....	584
Generic Search Table Usage	584
USERID Profile Related Tables	586
AATBLE01 Table.....	586
AATBLE05 Table.....	588
AATBLE07 Table.....	589
AATBLE08 Table.....	591
AATBLE09 Table.....	591
AATBLE10 Table.....	592
AATBLE06 Table.....	602
AATBLE29 Table.....	602
AATBLE11 Table.....	603
AATBLE30 Table.....	604
AATBLE31 Table.....	605
AATBLE32 Table.....	606
AATBLE33 Table.....	606
AATBLE03 TableA	607
AATBLE04 Table.....	608
AATBLE34 Table.....	608
AATBLE12 Table.....	610
Group Profile Related Tables	612
AATBLE13 Table.....	612
AATBLE15 Table.....	613
AATBLE02 Table.....	614
Dataset Profile Related Tables	615
AATBLE17 Table.....	615

- AATBLE20 Table 618
- AATBLE27 Table 619
- General Resource Profile Related Tables 620
 - AATBLE22 Table 620
 - AATBLE26 Table 624
 - AATBLE25 Table 626
 - AATBLE14 Table 627
 - AATBLE16 Table 628
 - AATBLE18 Table 628
 - AATBLE19 Table 630
 - AATBLE21 Table 630
 - AATBLE23 Table 631
 - AATBLE24 Table 632
 - AATBLE35 Table 632
 - AATBLE36 Table 633
- Appendix C **Miscellaneous SSA Features** 635
 - Revise or Delete Stored Jobs 636
 - Retrieve or Store Commands..... 638
 - MAIN SSA Screen 640
 - AAERASE CLIST 641



Preface

This manual describes Smart Security Administrator (hereafter “SSA”), which is part of the Smart Security family of RACF management tools offered by UNICOM Systems, Inc.

SSA gives administrators a complete package of tools to manage security at their site.

Audience

This manual is intended for security and system administrators. Readers are expected to understand RACF and z/OS concepts. Also, this manual describes SSA procedures that require site-specific changes to JCL batch jobs. Readers should be proficient editing JCL and familiar with their site's system standards

How This Manual is Organized

The manual contains these chapters:

- 'Overview' on page 25.
Gives an overview of SSA functions.
- 'SSA Installation' on page 27.
Describes procedures to install SSA.
- 'SSA Reports' on page 59.
Explains all SSA batch and online reports including JCL samples, panels, and so on.
- 'Online Generic Searches' on page 101.
Describes how to conduct SSA online generic searches. Included are search examples, search result examples, search result processing capabilities, and so on.
- 'Command Generation' on page 201.
Gives complete instructions on utilizing the SSA command generation functions including JCL samples, panels, control cards, and so on.
- 'The SCHEDULER' on page 269.
Explains the functionality of The SCHEDULER with which you can schedule commands or jobs to run on selected days and times helping to automate your workload.
- 'TSO Direct Administration' on page 285.
Describes TSO Direct Administration functions (that is, Password Administration, Userid Administration, and so on.) which do not require global or group special RACF authority and are completely live. Details include panels, messages and administration of the facilities.
- 'System Resource Monitor' on page 351.
Explains the System Resource Monitor facility and the Access Simulator function. Included are JCL samples, panels, control cards and the significance of each report and the information within.
- 'CICS Direct Administration' on page 363.
Explains the CICS based RACF direct administration module. Included are panels, security rules, syntax rules, API invocation examples, messages, and so on.

- ‘Configuration’ on page 499.

Describes panel configuration options in SSA, the setting up of SSA USERS and ADMINISTRATORS and configuring the AAOPTION Configuration module.

Several appendices then follow:

- ‘SSA Report Examples’ on page 537.

Presents examples of each SSA report.

- ‘SSA ISPF Tables’ on page 583.

Includes detailed layouts of the SSA ISPF tables and full details on the tie-in to the SSA adhoc report writing capability.

- ‘Miscellaneous SSA Features’ on page 635.

Describes miscellaneous features that are not specific to any specific SSA function.

Syntax Conventions

A syntax diagram is part of the description of each SSA command included in this manual. A diagram shows the possible parameters, values, and variables associated with a command.

Syntax diagrams adhere to common conventions. The physical appearance of a diagram’s elements indicates whether a command parameter, variable, or other values are required, optional, or included by default.

- An underlined parameter is the default assigned to the command.
- Command names are presented in MIXed case. The uppercase portion of a command name is the requisite abbreviated form. Lowercase letters represent the optional remainder of the command name that need not be specified to execute the command.
- An *italicized lowercase* parameter represents a value assigned by the user.
- A vertical bar (|) separates two or more mutually exclusive parameter values. Only one value can be specified for each parameter.
- Parameters enclosed within brackets [] are optional. Only one value can be specified to a parameter.
- Parameters values enclosed within braces { } are required. If unspecified, the parameter default is assigned to the command.
- Monospaced type represents text displayed from an online SSA report or examples of JCL. code. Also, SSA commands are shown as monospace examples.

SSA release and dates in figures and examples

Where relevant, in figures and code or report examples the SSA release number is indicated by V.V. Similarly, dates might be indicated by the formats MM/DD/YYYY, MM/DD/YYYY, YYYY-MM-DD, YY.DDD, and so on.

Customer Service

UNICOM Systems, Inc. customer service can be reached by the following methods:

Phone: 1 800 866 6224

Fax: 1 973 526 3899

E-mail: support@unicomsi.com

Normal business hours are from 7:00 a.m. to 4:00 p.m. Pacific Standard Time, Monday through Friday. Emergency customer service is available 24 hours a day, 7 days a week.

An answering service receives customer service calls beyond normal business hours. You may leave a message if it is not an urgent problem. A customer service representative will return your call at the start of the next business day.

Requests for urgent support outside of normal business hours are answered immediately. A customer service representative will be summoned to return your call. Leave a phone number where you can be reached. If you have not received a return call from a customer service representative within an hour of reporting the problem, please call back. Our representative may be experiencing difficulties returning your call.

International customers should contact their local distributor to report any problems with a UNICOM product.



CHAPTER 1

Overview

SSA is based on two simple principles:

Power:	Information is vital but well managed and organized information is power. With SSA's arsenal of features you have the power to tame your security environment. Super Generic Searches, extremely fast and flexible command generation, full function security, schedule jobs or commands automatically, decentralize password and connect administration - These are just some of the powerful features that will give administrators and auditors the tools and means to administrate and audit more effectively.
Ease of Use:	SSA is an extremely effective merging of Ease-of-Use and Power. A smarter and more sophisticated product means administrators and auditors alike can easily become acclimated and productive at new levels. SSA will assist the security administrator, security coordinator or auditor to effectively maintain and audit RACF information with concise reporting, command generation and ease of use. SSA is engineered to save the administrator at least 30% of their time by eliminating or expediting those tasks that can be arduous or lengthily in time. With SSA, you are freed up to pursue those items that you may have put aside because of time restraints. SSA will make you a better administrator, coordinator or auditor.



CHAPTER 2

SSA Installation

This chapter describes how to install SSA. The installation procedure is organized as an ordered sequence of steps. Each step includes a short procedure to complete a specific installation task. The steps must be completed in order. Also, each step must complete successfully before proceeding to the next installation step.

SSA Installation Requirements

The following list shows recommended releases of software that must be operational on the system that SSA will be installed.

TSO	Version 4.1 or greater
ISPF	Version 7.1 or greater
RACF	FMID HRF7730 or greater
z/OS	Version 2.1 or greater

If you have concerns because your site does not meet these software requirements, contact UNICOM Systems Inc. Customer Service. It is possible that your current software will allow SSA to perform all of its functions.

Throughout the documentation and JCL, datasets are prefixed with a high level qualifier SSA and the names used for members containing reports, listings or commands were created for administrative ease. Please keep in mind that you can change the aforementioned but that you must change all references to those datasets in the JCL.

Read the documentation to familiarize yourself with SSA. Because of the numerous enhancements introduced in different releases of the product, it would be advantageous for all users to take some time to review the SSA product documentation.

The SSA Installation procedure is designed to reduce time and possible errors. The installation procedure must be done in order and that you confirm each step has completed successfully before proceeding to the next step.

This installation procedure is designed for users with the authority to do the following:

- allocate datasets
- update system libraries
- update CICS JCL
- update CICS definitions
- issue RACF commands.

If you do not have the authority to complete all of the listed tasks, it may be necessary to coordinate the installation with other personnel at your site who have the appropriate authority.

The following steps must be completed to install SSA:

- ‘Step 1: Download SSA FTP Distribution’ on page 30
- ‘Step 2: Allocate Additional SSA Libraries’ on page 31
- ‘Step 3: APF-Authorize the SSA Load Library’ on page 34
- ‘Step 4: Add AUTHTSF Entries’ on page 35
- ‘Step 5: Modify Logon Procedure’ on page 37
- ‘Step 6: Define the SCHEDULER Started Task (Optional)’ on page 38
- ‘Step 7: Define RACF Classes for SSA Security’ on page 40
- ‘Step 8: Define SSA Users and Administrators’ on page 43
- ‘Step 9: Define Default Configuration Profile’ on page 44

‘Step 10: Define Base Security Rules’ on page 46

‘Step 11: Install the CICS Direct Administration Module (Optional)’ on page 47

‘Step 12: Define Product Password’ on page 52

‘Step 13: Startup Panel Choice (Optional/Recommended)’ on page 54

‘Step 14: Start the SSA Started Tasks’ on page 55

‘Step 15: Off-loading RACF Information’ on page 56

After completing these steps, you can begin using SSA.

Step 1: Download SSA FTP Distribution

Please contact Technical Support for download instructions for the SSA FTP distribution.

Step 2: Allocate Additional SSA Libraries

After the distribution has been downloaded (sample JCL to un-terse and restore the FTP distribution will be provided by Technical Support), most of the SSA libraries should be allocated with the exception of a few datasets.

To allocate the remaining datasets, which will complete the allocation of all SSA datasets, use the SSAALLOC sample job which is listed below.

```
//***** PLACE YOUR JOBCARD HERE *****
//*
//*****
//**          SMART SECURITY ADMINISTRATOR          **
//**          VERSION V.V          **
//**          **
//** (C) YYYY UNICOM SYSTEMS,INC.          **
//**          ALL RIGHTS RESERVED          **
//**          POST INSTALLATION JOB          **
//**          **
//*****
//*
//*****
//** THIS JOB WILL ALLOCATE AND REPRO          *
//** -----          *
//** &&AAPRF..RACFDATA.ISPTLIB          *
//** &&AAPRF..ISPTLIB          *
//** &&AAPRF..SCHED.DATABASE          *
//** &&AAPRF..SCHED.HISTORY          *
//**          *
//** TO CHANGE OUTPUT DATASETS TO UNIQUE HI-LEVEL QUALIFIER OF YOUR          *
//** CHOICE, CHANGE // SET AAPRFX='SSA.V140' JCL STATEMENT          *
//**          *
//** ALSO, CHANGE NAMES ON DEFINE CLUSTER          *
//** (STEP01.SYSIN AND STEP03.SYSIN)          *
//**          *
//** CHANGE VOLSER ON DEFINE CLUSTER TO VALID VOLSER          *
//** (STEP01.SYSIN AND STEP03.SYSIN)          *
//**          *
//*****
//INSTALL PROC
//*
// SET AAPRFX='SSA.V140'          <===CHANGE IF DESIRED
//**
//** ALLOCATE THE ISPF RACF TABLE AND JCL STORAGE LIBRARY
//**
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DSN=&AAPRF..&DSNDD1,DISP=(,CATLG),
// UNIT=SYSDA,
// SPACE=(CYL,(20,10,40)),
// DCB=(RECFM=FB,LRECL=80,BLKSIZE=23440)
//DD2 DD DSN=&AAPRF..&DSNDD2,DISP=(,CATLG),
// UNIT=SYSDA,
// SPACE=(CYL,(5,5,55)),
// DCB=(RECFM=FB,BLKSIZE=23440,LRECL=80)
//**
//**
//** ALLOCATE THE SCHEDULER DATABASE
//**
//STEP01 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//**
//** INITIALIZE THE SCHEDULER HISTORY FILE
```

```

/**
//STEP02 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//IN01 DD DSN=SSA.V140.VSAMINIT,DISP=OLD
//OUT01 DD DSN=&AAPRF..&DSNDD3,DISP=SHR
/**
/** ALLOCATE THE HISTORY DATABASE
/**
//STEP03 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
/**
/** INITIALIZE THE SCHEDULER HISTORY FILE
/**
//STEP04 EXEC PGM=IDCAMS,REGION=512K
//SYSPRINT DD SYSOUT=*
//IN02 DD DSN=SSA.V140.VSAMINIT,DISP=OLD
//OUT02 DD DSN=&AAPRF..&DSNDD4,DISP=SHR
/**
/** DELETE THE VSAM SEED RECORD
/**
//DELETE EXEC PGM=IDCAMS,COND=(0,NE)
//SYSPRINT DD SYSOUT=*
/**
//INSTALL PEND
//AAINST EXEC INSTALL,
// AAPRF=&AAPRF, DATASET PREFIX
// DSNDD1='RACFDATA.ISPTLIB', ISPF TABLE LIBRARY
// DSNDD2='ISPTLIB', JCL STORAGE TABLE LIBRARY
// DSNDD3='SCHED.DATABASE', THE SCHEDULER DATABASE
// DSNDD4='SCHED.HISTORY' THE SCHEDULER HISTORY FILE
/**
//STEP01.SYSIN DD *
DEFINE CLUSTER -
    (NAME(SSA.V140.SCHED.DATABASE) -
    VOLUME(VOL001) -
    SHAREOPTIONS(3 3) ) -
DATA -
    (NAME(SSA.V140.SCHED.DATABASE.DATA) -
    CYLINDERS(25 25) -
    KEYS(24 0) -
    RECORDSIZE(240 240) -
    FREESPACE(10 15) ) -
INDEX -
    (NAME(SSA.V140.SCHED.DATABASE.INDEX) -
    TRK(5 1) )
/*
//STEP02.SYSIN DD *
REPRO -
    INFILE(IN01) -
    OUTFILE(OUT01)
/*
//STEP03.SYSIN DD *
DEFINE CLUSTER -
    (NAME(SSA.V140.SCHED.HISTORY) -
    VOLUME(VOL001) -
    SHAREOPTIONS(2) ) -
DATA -
    (NAME(SSA.V140.SCHED.HISTORY.DATA) -
    CYLINDERS(25 25) -
    KEYS(24 0) -
    RECORDSIZE(240 240) -
    FREESPACE(10 15) ) -
INDEX -
    (NAME(SSA.V140.SCHED.HISTORY.INDEX) -
    TRK(5 1) )

```

```
/*
//STEP04.SYSIN      DD  *
    REPRO -
            INFILE(IN02) -
            OUTFILE(OUT02)
//*/
//DELETE.SYSIN      DD  *
    DELETE 'SSA.V140.VSAMINIT'
    IF MAXCC = 8 -
        THEN -
        SET MAXCC=0
    END
/*
```

Step 3: APF-Authorize the SSA Load Library

The SSA.LOADLIB library must be APF-authorized.

- 1 APF-authorize the SSA LOADLIB library by one of the methods listed below:
 - Add the library to the IEAAPF00 member of SYS1 .PARMLIB
 - Add the library to the PROG00 member of SYS1 .PARMLIB if the dynamic APF option is active
 - If you have the proper level of z/OS you can issue the SETPROG command:
SETPROG APF,ADD,DSN=SSA.LOADLIB,VOL=<volume>
 - Use a third party product to APF authorize the library
 - Add the library to the LNKLIST00 member of SYS1 .PARMLIB if the APF authorization is turned on for linklist datasets. The dataset has to be cataloged in your master catalog for this to work.

Note Some of the APF authorization methods require an IPL; others grant temporary authorization that is active only until the next IPL (that is, SETPROG command).

- 2 Run a RACF DSMON report to confirm the SSA LOADLIB library has been APF-authorized.

Below is a sample of the DSMON job located in member DSMON of the SSA install library).

```
//***** PLACE JOB CARD HERE *****/
//*
//* RACF DSMON REPORT ON APF AUTHORIZED LIBRARIES
//* - TO BE USED TO VERIFY THE APF AUTHORIZED STATUS OF THE
//* SSA LIBRARY
//*
//STEP010 EXEC PGM=ICHDSM00
//SYSPRINT DD SYSOUT=*
//SYSUT2 DD SYSOUT=*
//SYSIN DD *
FUNCTION SYSAPF
//*
```

Step 4: Add AUTHSF Entries

Add the following entries to the IKJTSO00 member in SYS1.PARMLIB in the AUTHTSF segment (an example is in member AUTHTSF of the SSA install library):

AUTHTSF Example

```

//*****
//**
//** SMART SECURITY ADMINISTRATOR **
//** **
//** VERSION V.V **
//** **
//** (C) YYYY UNICOM SYSTEMS, INC. **
//** ALL RIGHTS RESERVED **
//*****
//**
//** THIS IS A SAMPLE OF THE AUTHTSF ENTRIES THAT ARE REQUIRED FOR **
//** SSA TO OPERATE PROPERLY. THESE DEFINITIONS NEED TO BE ADDED TO **
//** THE IKJTS000 MEMBER OF SYS1.PARMLIB. **
//** **
AUTHTSF NAMES( /* PROGRAMS TO BE AUTHORIZED */ +
                /* WHEN CALLED THROUGH THE */ +
                /* TSO SERVICE FACILITY. */ +
                /* */ +
                /* SSA */ +
                /* VERSION V.V */ +
                /* */ +
AACMD001 /* SSA=PASSWORD ADMINISTRATION */ +
AACMD002 /* SSA=CONNECT ADMINISTRATION */ +
AACMD003 /* SSA=USERID ADMINISTRATION */ +
AACMD004 /* SSA=GROUP ADMINISTRATION */ +
AACMD005 /* SSA=DSN PROF ADMINISTRATION */ +
AACMD006 /* SSA=GENRSCE PROF ADMIN. */ +
AACMD007 /* SSA=DSN PERMIT ADMIN. */ +
AACMD008 /* SSA=USER TSO SEGMENT ADMIN. */ +
AACMD009 /* SSA=USER CICS SEGMENT ADMIN* / +
AACMD014 /* SSA=GENRSCE MEMBER ADMIN. */ +
AACMD015 /* SSA=GENRSCE PERMIT ADMIN. */ +
AACNG001 /* SSA=CONFIGURATION */ +
AACNG002 /* SSA=CONFIGURATION */ +
AACNG003 /* SSA=CONFIGURATION */ +
AAATHCHK /* SSA=AUTHORITY CHECKER */ +
AAPSWCHK /* SSA=PASSWORD CHECKER */ +
AAGRPUSR /* SSA=GROUP/USER CHECKER */ +
AAREP011 /* SSA=REPORT-DSN ACCESS */ +
MNAPFPRC /* SSA=MONITOR=APF */ +
MNGRPPRC /* SSA=MONITOR=APF */ +
MNCDTPRC /* SSA=MONITOR=CDT */ +
MNC02PRC /* SSA=MONITOR=CDT RACF 2.2 */ +
MNLTPRC /* SSA=MONITOR=LINKLIST */ +
MNLPAAPRC /* SSA=MONITOR=LINKPACKAREA */ +
MNPPTPRC /* SSA=MONITOR=PPT */ +
MNRACPRC /* SSA=MONITOR=GEN RACF INFO */ +
MNRA9PRC /* SSA=MONITOR=GEN RACF INFO */ +
MNRUPRC /* SSA=MONITOR=AUTH RACF CALLS */ +
MNRFRPRC /* SSA=MONITOR=RACF ROUTER */ +
MNSMFPRC /* SSA=MONITOR=SMF */ +
MNSM4PRC /* SSA=MONITOR=SMF MVS V4 */ +
MNSTCPRC /* SSA=MONITOR=STARTED TASK */ +
MNSVCPRC) /* SSA=MONITOR=SVC */ +
                /* */

```

Note This change can be activated by one of two means:

- Issue the PARMLIB UPDATE command that updates the IKJTSONn PARMLIB member which ends with the two characters you will be prompted for; usually 00. Please check with your site's support personnel who maintain SYS1.PARMLIB before issuing this command. Also, you must have UPDATE access to profile PARMLIB in the TSOAUTH class to issue the command to update the IKJTSONn entries.

When you entered and activated the AUTHTSF entries, issue the PARMLIST LIST command as shown below to confirm that the entries are in place:

Command Sample

```
PARMLIB LIST(AUTHTSF)
```


Step 5: Modify Logon Procedure

You must concatenate the SSA product libraries to the TSO session of each person expected to use SSA.

- 1 Modify TSO logon procedures by adding the following entries:

```
//SYSPROC DD DSN=SSA.ISPCLIB,DISP=SHR
//ISPPLIB DD DSN=SSA.ISPPLIB,DISP=SHR
//ISPMLIB DD DSN=SSA.ISPMLIB,DISP=SHR
//ISPSLIB DD DSN=SSA.ISPSLIB,DISP=SHR
//AADSTLIB DD DSN=SSA.ISPTLIB,DISP=SHR
//STEPLIB DD DSN=SSA.LOADLIB,DISP=SHR
//AASCHMST DD DSN=SSA.SCHED.DATABASE,DISP=SHR
//AASCHHST DD DSN=SSA.SCHED.HISTORY,DISP=SHR
```

The SSA.LOADLIB library must be concatenated to a TSO session by one of two means to retain its authorized status:

- Add the library to the LNKST00 member of SYS1 .PARMLIB to linklist the dataset
 - Add the library to the users logon proc under the STEPLIB DD.
 - All datasets that reside under the STEPLIB DD must be APF-authorized or the authorization will ‘fall off’.
- 2 Verify the dataset names match those created in ‘Step 2: Allocate Additional SSA Libraries’ on page 31.

A sample copy of these entries is in member LOGONPRC in the SSA install library:

Step 6: Define the SCHEDULER Started Task (Optional)

This step is optional. If you are not licensed for the SCHEDULER function, proceed to ‘Step 7: Define RACF Classes for SSA Security’ on page 40.

The SSA scheduler feature uses a started task to monitor and submit scheduled entries. This step explains how to prepare the started task.

- 1 Edit the SCHEDULER started task JCL shown below.

A sample of the JCL is in member AASTC01 of the SSA install library.

```
//AASTC01 PROC
//*
//*****
//**
//**      SMART SECURITY ADMINISTRATOR      **
//**
//**      VERSION V.V                      **
//**
//** (C) YYYY UNICOM SYSTEMS, INC.          **
//**      ALL RIGHTS RESERVED              **
//*****
//STEP001 EXEC PGM=AASTC01,REGION=4M
//STEPLIB DD DSN=SSA.LOADLIB,DISP=SHR
//AASCHLOG DD SYSOUT=*,DCB=BLKSIZE=133
//AAHSTLOG DD SYSOUT=*,DCB=BLKSIZE=133
//AAPRGLOG DD SYSOUT=*,DCB=BLKSIZE=133
//AASCHMST DD DSN=SSA.SCHED.DATABASE,DISP=SHR
//AASCHHST DD DSN=SSA.SCHED.HISTORY,DISP=SHR
//INTRDR DD SYSOUT=(A,INTRDR)
//*
```

- 2 Make the following changes to the JCL:

- a Change the load library specified on the STEPLIB DD to the SSA APF authorized load library.
- b Change the dataset specified on the AASCHMST DD to the SSA scheduler database.
- c Change the dataset specified on the AASCHHST DD to the SSA scheduler history database.

- 3 Copy the JCL into a PROCLIB dataset that is available to your Job Entry Subsystem (JES).

Contact your systems programmer if you are not sure where an appropriate available PROCLIB dataset is.

- 4 Define the started task to RACF by one of the following methods:

- Add an entry to the Started Task Table (ICHRIN03) and then add the userid to RACF.
- Add a userid to RACF and then add a RACF profile to the STARTED class with the appropriate STDATA segment.

Because this is a shop-specific choice no samples are provided. Contact your SSA technical support representative if you need more information about defining the started task.

Important Security Note

The SCHEDULER started task can receive and process requests when it submits jobs or commands. The SCHEDULER uses its own authority, or the submitters utilizing SURROGAT permissions. Therefore, you must give the RACF userid the started task is running with, sufficient RACF authority to successfully submit the commands or jobs and for the commands or jobs to complete successfully. It is recommended the started task be given RACF Global Special. However, this is a security issue that must be decided on a shop by shop basis. See ‘The SCHEDULER’ on page 269.

Defining Surrogate Profiles

The SCHEDULER started task can be called to submit jobs with the authority of the requestor of the scheduled event. You must permit, through SURROGAT class profiles, the started task the ability to submit jobs on the ‘behalf’ of the requestor. See the *RACF (or z/OS) Security Administrator’s Guide* - Allowing Surrogate Job Submission section for details on permitting a userid to submit jobs on the behalf of another userid.

Step 7: Define RACF Classes for SSA Security

SSA uses a Group/Member RACF class combination to store security rules, configuration values, and product passwords. The number of steps necessary to define the SSA RACF classes is dependent on your Operating System release.

Choose either a **Static Class Descriptor Table** or a **Dynamic Class Descriptor Table**. Please note the following:

- The samples below show the required attributes of the SSA classes that will ensure that the product works properly.
- It is highly recommended that you choose a POSIT number and ID number that are unique to the two classes. There are 1024 POSIT numbers, of which 19-56 and 128-527 are available for your installation's use.
- It is important to note that there are two classes; a group class and a member class. You must use two classes with a group/member relationship.

Static Class Descriptor Table

1 ICHERCDE Sample:

ICHERCDE	CLASS=GAA\$RULE,	CLASS NAME	X
	ID=128,	RECOMMENDED ID NUMBER	X
	POSIT=128,	RECOMMENDED POSIT NUMBER	X
	MEMBER=MAA\$RULE,	MEMBER CLASS	X
	MAXLNTH=60,	MAXIMUM LENGTH OF NAME	X
	FIRST=ALPHA,	FIRST CHARACTER OF NAME	X
	OTHER=ANY,	REST OF CHARACTERS	X
	RACLIST=ALLOWED,	RACLIST?	X
	DFTUACC=NONE,	DEFAULT UACC IF NONE SPECIFIED	X
	OPER=NO	IGNORE OPERATIONS ATTRIBUTE	
ICHERCDE	CLASS=MAA\$RULE,	CLASS NAME	X
	ID=128,	RECOMMENDED ID NUMBER	X
	POSIT=128,	RECOMMENDED POSIT NUMBER	X
	MEMBER=GAA\$RULE,	GROUPING CLASS	X
	MAXLNTH=60,	MAXIMUM LENGTH OF NAME	X
	FIRST=ALPHA,	FIRST CHARACTER OF NAME	X
	OTHER=ANY,	REST OF CHARACTERS	X
	RACLIST=ALLOWED,	RACLIST?	X
	DFTUACC=NONE,	DEFAULT UACC IF NONE SPECIFIED	X
	OPER=NO	IGNORE OPERATIONS ATTRIBUTE	
ICHERCDE		THIS GENERATES AN END STATEMENT	

Please refer to the RACF Macros and Interfaces manual (section RACF Customization Macros) for assistance in implementing the ICHERCDE definitions.

2 Define the classes to the z/OS Router Table using the ICHRFRTB macro.

Below is a sample of the definitions (A sample is in member ICHRFRTB in the SSA install library). Please refer to the RACF Macros and Interfaces manual (section RACF Customization Macros) for assistance in implementing the ICHRFRTB definitions.

ICHRFRTB Sample:

```
ICHRFR01 CSECT
ICHRFRTB CLASS=GAA$RULE,ACTION=RACF
ICHRFRTB CLASS=MAA$RULE,ACTION=RACF
ENDTAB ICHRFRTB TYPE=END
END ICHRFRTB
```

- 3 IPL your system to activate the definitions.
- 4 Activate the classes in RACF.

It is highly recommended that the classes be RACLIST'd and made Generic profile/command capable. The following samples of commands show the activation, RACLISTing and Generic activation of the classes. It is important to note that all the commands shown below must be executed against the member class you have defined not the group class. You must have Global Special authority to issue these commands.

RACF Commands Sample:

```
SETRPTS GENERIC(MAA$RULE)
SETRPTS CLASSACT(MAA$RULE)
SETRPTS RACLIST(MAA$RULE)
```

Note If you choose to follow the recommendations to RACLIST the SSA security classes, please note that you will have to issue a refresh after issuing commands that make changes or additions to those classes. The refresh command is to be issued only against the member class defined for SSA. Below is a sample of that command.

```
SETRPTS RACLIST(MAA$RULE) REFRESH
```

Dynamic Class Descriptor Table**DYNCLAS Sample:**

```
//SSADEF JOB 1,SSA,CLASS=A,MSGCLASS=X
//STEP1 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=X
//SYSPRINT DD SYSOUT=X
//SYSTSIN DD *
RDEFINE CDT GAA$RULE CDTINFO(CASE(UPPER) DEFAULTTRC(4) +
DEFAULTUACC(NONE) FIRST(ALPHA NATIONAL) +
GENLIST(DISALLOWED) KEYQUALIFIERS(0) MACPROCESSING(NORMAL) +
MAXLENX(60) MAXLENGTH(60) MEMBER(MAA$RULE) +
OPERATIONS(NO) OTHER(ALPHA NATIONAL NUMERIC SPECIAL) +
POSIT(128) PROFILESALLOWED(YES) +
RACLIST(ALLOWED) SIGNAL(NO) SECLABELSREQUIRED(NO))
```

```
RDEFINE CDT MAA$RULE CDTINFO(CASE(UPPER) DEFAULTRC(4)      +
DEFAULTUACC(NONE) FIRST(ALPHA NATIONAL) GENLIST(DISALLOWED) +
GROUP(GAA$RULE) KEYQUALIFIERS(0) MACPROCESSING(NORMAL)     +
MAXLENX(60) MAXLENGTH(60) OPERATIONS(NO)                   +
OTHER(ALPHA NATIONAL NUMERIC SPECIAL) POSIT(128)           +
PROFILESALLOWED(YES) RACLIST(ALLOWED) SIGNAL(NO)           +
SECLABELSREQUIRED(NO))
SETROPTS CLASSACT(CDT) RACLIST(CDT)
/*
```

A corresponding entry to the RACF Router Table is no longer required.

The class names utilized by SSA for security and configuration can be changed to names more suited to your shop standards by modifying the AAOPTION module. See ‘Configuration’ on page 499 for directions on changing the AAOPTION module.

Step 8: Define SSA Users and Administrators

The authority to use SSA is based upon the role assigned to a user. A SSA user can be classified as either an ADMINISTRATOR or USER. Below is a list of the differences between the two roles.

- An ADMINISTRATOR can approve or deny entries put in The SCHEDULER that require approval.
- An ADMINISTRATOR can enter entries into The SCHEDULER to run with the started tasks authority without approval.
- An ADMINISTRATOR can run reports on all entries in The SCHEDULER.
- An ADMINISTRATOR can manipulate the stored configurations for SSA users given they have the proper RACF authority to change the RACF profiles holding the stored configurations.
- An ADMINISTRATOR can change the operational settings of The SCHEDULER started task.
- An ADMINISTRATOR can display a users or groups authority to the many SSA features.
- An ADMINISTRATOR can create the extract jobs and given they have the correct access to the profiles protecting the off-load process, they can submit them.

User roles are set by assigning their userid as a member to the appropriate grouping profile. The default profile (defaults set in module AAOPTION - see 'Configuration' on page 499 to change if desired) for USERS is MEGASOLVE-SSA.USERS and the default profile for ADMINISTRATORS is MEGASOLVE-SSA.ADMINISTRATORS. Below is a sample of the command to define the users profile and the addition of IBMUSER as a USER of SSA.

Important Security Note

Be sure to define yourself (the installer) as an ADMINISTRATOR. The ADMINISTRATOR level of authority will be necessary to complete the installation. You must have either Global Special authority or CLAUTH authority to the SSA classes to issue these commands.

RACF Command Sample

```
RDEFINE GAA$RULE MEGASOLVE-SSA.USERS UACC(NONE) OWNER(SYS1) -
  DATA('GROUP PROFILE DEFINING THE USERS OF SSA') -
  ADDMEM(IBMUSER)
RDEFINE GAA$RULE MEGASOLVE-SSA.ADMINISTRATORS UACC(NONE) OWNER(SYS1) -
  DATA('GROUP PROFILE DEFINING THE ADMINISTRATORS OF SSA') -
  ADDMEM(IBMUSER)
```

Important Security Note

Remember that an ADMINISTRATOR can submit commands and jobs to The SCHEDULER to run with the started tasks authority without approval. Thus, if the started task has a higher authority than the user with ADMINISTRATOR status, that user can use the higher authority of the started task to run commands and jobs.

Step 9: Define Default Configuration Profile

SSA configuration settings necessary to use the SSA ISPF interface are now stored in RACF profiles. This allows the existence of multiple configurations and the ability to dynamically switch between them.

All configuration ‘groupings’ must start with the prefix set in the AAOPTION module (See ‘Configuration’ on page 499 for details on changing prefix). The default prefix is AACONFIG-. Also contained in AAOPTION is the value set for the default configuration that must exist and is referred to by the SSA startup if no other configuration is available.

Below is a sample of the RACF command needed to setup the default configuration (A sample is in member AACONFIG of the SSA JCL library). You must have either Global Special authority or CLAUTH authority to the SSA classes to issue these commands.

RACF Command Sample:

```
RDEFINE GAA$RULE AACONFIG-DEFAULT OWNER(SYS1) UACC(READ) ADDMEM(-
  AA_DATABASE=SSA.RACFDATA.ISPTLIB -
  AA_ISPCLIB=SSA.ISPCLIB -
  AA_ISPMLIB=SSA.ISPMLIB -
  AA_ISPPLIB=SSA.ISPPLIB -
  AA_ISPSLIB=SSA.ISPSLIB -
  AA_LOADLIB=SSA.LOADLIB -
  SCHED_DB=SSA.SCHED.DATABASE -
  SCHED_HIST=SSA.SCHED.HISTORY -
  PERM_ALLOC_UNIT=SYSDA -
  TEMP_ALLOC_UNIT=SYSDA -
  SORT_ALLOC_UNIT=SYSDA -
  ISPF_SYS_MLIB=SYS1.SISPMENU -
  ISPF_SYS_TLIB=SYS1.SISPTENU -
  ALLOCATION_PREFIX=$USERID$ -
  MENU_FORMAT=SHORT -
  PRINT_PROMPT=Y -
  CLEAR_SELECTIONS=Y -
  EXECUTE_COMMANDS=N -
  LINES_PER_PAGE=55)
```

Make the following changes to define the default configuration:

- 1** Change all SSA dataset names to match your SSA naming conventions.
- 2** Change the esoteric generic unit names to names appropriate in your shop.
- 3** Change the library referenced on label ISPF_SYS_MLIB to your system ISPF system message library.

This library can almost always be found on your logon proc and can be identified as the correct library if it contains the member ISPV01. You **MUST** put the correct library or a majority of SSA’s jobs will fail. It is important to note that this library will not be updated; it is only used to establish an ISPF environment in batch.

- 4** Change the library referenced on label ISPF_SYS_TLIB to your system ISPF system table library.

This library can be identified as the correct library if it contains the member ISPSPROF or ISPPROF. You **MUST** put the correct library or a majority of SSA's jobs will fail. It is important to note that this library will not be updated; it is only used to establish an ISPF environment in batch.

- 5** All other settings are set to recommended standards.

Refer to 'Configuration' on page 499 for a complete explanation of constructing an SSA configuration.

Step 10: Define Base Security Rules

It is recommended that two default security rules be established for installation expediency and product trials. The first is a single default security rule covering all restrictions to SSA functions. The second rule adds a SuperRevoke group for the Password Administration function. Adding both security rules ensures the SSA installer and tester are able to use all SSA functions.

Below is a sample of both security rules. The default security rule definition includes a subsequent permission that gives access to all SSA functions with the exception of those functions protected by the users status (USER vs. ADMINISTRATOR). Also shown is a SETROPTS REFRESH command which is only necessary if you RACLISTed the SSA classes. You must have either Global Special authority or CLAUTH authority to the SSA classes to issue these commands.

RACF Command Sample:

```
RDEFINE GAA$RULE MEGASOLVE-SSA.DEFAULT-SECURITY OWNER(SYS1) UACC(NONE) -
  DATA('BASE SECURITY RULE COVERING ALL SSA FUNCTIONS') -
  ADDMEM(MEGASOLVE-SSA.***)
PERMIT MEGASOLVE-SSA.DEFAULT-SECURITY CLASS(GAA$RULE) ID(IBMUSER) -
  ACCESS(ALTER)
SETROPTS RACLIST(MAA$RULE) REFRESH
ADDGROUP $SREVOKE SUPGROUP(SYS1) OWNER(SYS1) -
  DATA('SUPERREVOKE GROUP FOR DIRECT ADMINISTRATION')
```

Important Note

Each of the chapter references listed below have a security section describing security features for the listed SSA function. Be sure to consult these chapters after installation to determine what security you want to use.

- 'SSA Reports' on page 59
- 'Command Generation' on page 201
- 'The SCHEDULER' on page 269
- 'TSO Direct Administration' on page 285
- 'System Resource Monitor' on page 351
- 'CICS Direct Administration' on page 363
- 'Configuration' on page 499

Step 11: Install the CICS Direct Administration Module (Optional)

This step is optional. If you are not licensed for the CICS Direct Administration function, proceed to ‘Step 12: Define Product Password’ on page 52.

The CICS Direct Administration function uses two pieces: 1) CICS transactions and programs utilizing TCP/IP and 2) a started task that receives the requests and processes them. To install the CICS Direct Administration module you must do the following:

- 1 Define the CICS Direct Administration started task to your system.

If you have already done this when installing an earlier version, proceed to the part four of this step. Below are the steps to accomplish that:

- 2 Edit the started task JCL as shown below.

A sample of the JCL is in member AASTC02 of the SSA install library.

```
//AASTC02 PROC
//*
//*****
//**                                     **
//**      SMART SECURITY ADMINISTRATOR      **
//**                                     **
//**              VERSION V.V              **
//**                                     **
//** (C) YYYY UNICOM SYSTEMS, INC.          **
//**      ALL RIGHTS RESERVED              **
//*****
//*
//* CICS DIRECT ADMINISTRATION STARTED TASK
//*
//STEP001 EXEC PGM=AASTC02,REGION=4M,TIME=1440
//STEPLIB DD DSN=SSA.LOADLIB,DISP=SHR
//AASTCLOG DD SYSOUT=*,DCB=BLKSIZE=133
//*
```

Make the following changes to the JCL:

- Change the load library specified on the STEPLIB DD to the SSA APF authorized load library.

When you have modified the JCL, it must be copied into a PROCLIB dataset that is available to your Job Entry Subsystem (JES). Contact your systems programmer if you are not sure where an appropriate available PROCLIB dataset is.

After successfully modifying and copying the JCL into an appropriate library, the started task must be defined to RACF. This can be accomplished in 2 ways:

- Add an entry to the Started Task Table (ICHRIN03) and then add a userid to RACF.
- Add a userid to RACF and then add a RACF profile to the STARTED class with the appropriate STDATA segment.

Because this is a shop-specific choice no samples are provided. Contact your SSA technical support representative if you need more information about defining the started task.

- 3 Assign a TCP/IP PORT address to the CICS Direct Administration started task.

Below is an example of the PORT entry.

```
PORT
      3500 TCP AASTC02 NOAUTOLOG ; SSA - CICS Direct Administration
```

A sample of the PORT assignment is in member PORT in the SSA install library. To activate the PORT you must make the following changes:

- Change 3500 to a port number that is unique in your system.
- Change AASTC02 to the name you used to install the CICS Direct Administration started task.

Update TCP/IP to reserve the PORT used by CICS Direct Administration:

- Edit the profile dataset currently used by your TCP/IP started task and refresh that profile by recycling the TCP/IP started task.

Note This definition is maintained in the dataset pointed to by DD PROFILE on the JCL for the TCP/IP started task.

- 4 Edit AAOPTION member in the SSA install library and change the TCP/IP settings for your system.

Below is the excerpt of the AAOPTION member that requires updating:

```
AAOPTION TCP/IP Example:
*****
**                                                    **
** TCPIP CONSTANTS                                **
**                                                    **
*****
TCPIP_NAME      DC  CL8'TCIPMVS'
DEFAULT_STC_IP  DC  CL15'205.185.254.3'  DEFAULT IP ADDRESS
DEFAULT_STC_PT  DC  H'3500'              DEFAULT PORT ADDRESS
```

Make the following changes:

- Change the task name from TCIPMVS to the started task name of TCP/IP on the system utilizing the CICS Direct Administration function.
 - Change the IP address from 205.185.254.3 to the IP address of the TCP/IP started task on the system utilizing the CICS Direct Administration function.
 - Change port address from 3500 to the port address assigned in the prior step of the CICS Direct Administration started task.
 - After making your changes you must assemble AAOPTION. Refer to 'Configuration' on page 499 for other parts of AAOPTION you may wish to change and assembly instructions.
- 5 Edit AATCPIP member in the SSA install library and change the TCP/IP settings for your default system.

Below is the excerpt of the AATCPIP member that requires updating:

A sample of the JCL is in member AASTC02 of the SSA install library.

DFLT_TRANS	DC	CL4'DFLT'	REQUIRED - DEFAULT TRANSACTION
DFLT_TCPIP	DC	CL8'TCIPMV'S'	TCPIP JOB NAME
DFLT_CICS	DC	CL8'SENTCICS'	CICS JOB NAME
DFLT_DISPLAY	DC	C'N'	N=DO NOT DISPLAY,Y=DISPLAY
DFLT_IP_ADDR	DC	CL15'205.185.254.3'	
DFLT_PORT	DC	H'3500'	TCPIP PORT NUMBER
DFLT_DESC	DC	CL40'DEFAULT SYSTEM'	

Make the following changes (Do not change DFLT. This is the default setting):

- Change TCIPMV'S on the DFLT_TCPIP label to the name of the TCP/IP started task on the default system you are installing SSA on.
- Change SENTCICS on the DFLT_CICS label to the name of the CICS region you are installing the SSA-CDA function into.
- Change 205.185.254.3 on the DFLT_IP_ADDR label to the IP address of the TCP/IP started task on the default system you are installing SSA on.
- Change 3500 on the DFLT_PORT label to the PORT number assigned to the SSA-CDA started task.

After making the appropriate changes, you must assemble AATCPIP. You can use member ASSEMBLE in the install library. See 'CICS Direct Administration' on page 363 (cross platform administration part) for more details on AATCPIP.

- 6** CICS Direct Administration uses TCP/IP CICS sockets. You must make sure that the CICS TCP/IP API is installed and active.

All details concerning the installation and activation of the CICS TCP/IP API is in the CICS TCP/IP Socket Interface Guide. Make sure the API is active before proceeding with the installation of the CICS Direct Administration function. Call your SSA representative if you need assistance or information concerning the installation of TCP/IP CICS Sockets.

- 7** Define CICS Direct Administration components to the CICS region you want to perform administration from.

To define the transactions, programs and mapsets you must edit and submit the supplied CSD updating job \$RDO located in the SSA install library. Below is a sample of that job which utilizes the IBM utility DFHCSDUP to update the CICS CSD file:

```

***** PUT YOUR JOB CARD HERE *****
*****
/**
/**      SMART SECURITY ADMINISTRATOR      **
/**                                          **
/**      VERSION V.V                      **
/**                                          **
/** (C) YYYY UNICOM SYSTEMS, INC.         **
/**      ALL RIGHTS RESERVED              **
*****
/* JCL TO INSTALL THE CICS RESOURCE DEFINITIONS INTO CICS GROUP SSA
/*
//CSDINIT EXEC PGM=DFHCSDUP
//STEPLIB DD DSN=CICS.SDFHLOAD,DISP=SHR    <=== CHANGE AS REQUIRED
//DFHCSD DD DSN=CICS.DFHCSD,DISP=SHR      <=== CHANGE AS REQUIRED
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
*=====
* CICS/RACF SSA DFHCSDUP RESOURCE DEFINITION STATEMENTS
*=====
*
*=====

```

```

*   DEFINE THE MAPS
*=====
*
DEFINE MAPSET(AAZAUT ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZCON ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZDSA ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZDSP ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZGRP ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZMBA ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZMN  ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZMNU ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZPWA ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZPWC ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZPWS ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZRSA ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZRSP ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZUID ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZUSR ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZUTC ) GROUP(SSA) RESIDENT(YES)
DEFINE MAPSET(AAZUTP ) GROUP(SSA) RESIDENT(YES)
*
*=====
*   DEFINE THE PROGRAMS
*=====
*
DEFINE PROG(AAZAUT01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZCLNT ) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZCON01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZDSA01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZDSP01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZGRP01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZMN01 ) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZMBA01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZMNU01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZPWA01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZPWC01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZPWS01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZRSA01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZRSP01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AATCPIP ) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZUID01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZUSR01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZUTP01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZUTC01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY01) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY02) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY03) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY04) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY05) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY06) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY07) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY08) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY09) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY14) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFY15) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
DEFINE PROG(AAZVFYAU) L(ASSEMBLER) EXECKEY(CICS) GROUP(SSA)
*
*=====
*   DEFINE THE TRANSACTIONS
*=====
*
DEFINE TRANSACTION(SAAU) PROG(AAZAUT01)
      GROUP(SSA) DESCRIPTION(SSA - AUTHORIZATION CHECK)
DEFINE TRANSACTION(SACN) PROG(AAZCON01)
      GROUP(SSA) DESCRIPTION(SSA - CONNECT ADMINISTRATION)
DEFINE TRANSACTION(SADS) PROG(AAZDSA01)
      GROUP(SSA) DESCRIPTION(SSA - DATASET ADMINISTRATION)
DEFINE TRANSACTION(SAGP) PROG(AAZGRP01)
      GROUP(SSA) DESCRIPTION(SSA - GROUP ADMINISTRATION)
DEFINE TRANSACTION(SAMA) PROG(AAZMBA01)
      GROUP(SSA) DESCRIPTION(SSA - MEMBER ADMINISTRATION)
DEFINE TRANSACTION(SAMD) PROG(AAZMN01)

```

```

        GROUP(SSA) DESCRIPTION(SSA - REMOTE ADMINISTRATION MAIN MENU)
DEFINE TRANSACTION(SAMN) PROG(AAZMNU01 )
        GROUP(SSA) DESCRIPTION(SSA - MAIN MENU)
DEFINE TRANSACTION(SAPW) PROG(AAZPWA01)
        GROUP(SSA) DESCRIPTION(SSA - PASSWORD ADMINISTRATION)
DEFINE TRANSACTION(SAPR) PROG(AAZPWS01)
        GROUP(SSA) DESCRIPTION(SSA - PASSWORD ADMINISTRATION-SHORT)
DEFINE TRANSACTION(SARP) PROG(AAZRSP01)
        GROUP(SSA) DESCRIPTION(SSA - RESOURCE PERMIT)
DEFINE TRANSACTION(SARS) PROG(AAZRSA01)
        GROUP(SSA) DESCRIPTION(SSA - RESOURCE ADMINISTRATION)
DEFINE TRANSACTION(SASP) PROG(AAZDSP01)
        GROUP(SSA) DESCRIPTION(SSA - DATASET PERMIT)
DEFINE TRANSACTION(SAUR) PROG(AAZUSR01)
        GROUP(SSA) DESCRIPTION(SSA - USERID ADMINISTRATION)
DEFINE TRANSACTION(SAUC) PROG(AAZUTC01)
        GROUP(SSA) DESCRIPTION(SSA - USER CICS SEGMENT ADMIN)
DEFINE TRANSACTION(SAUT) PROG(AAZUTP01)
        GROUP(SSA) DESCRIPTION(SSA - USER TSO SEGMENT ADMIN)
//*
```

To submit this job you must do the following:

- Replace the first line of this job with your job card.
- Change the loadlib referenced on the STEPLIB DD with your CICS system load library that contains the DFHCSDUP module.
- Change the CSD file referenced on the DFHCSD DD to the CSD file of the region you are installing the software.

After the job has completed successfully, you must logon to the CICS region where you are installing the product and install the definition group SSA. The installation is done by executing transaction CEDA. Below is an example of that transaction/command:

```
CEDA INSTALL GROUP(SSA)
```

8 You must add the SSA load library to the CICS region's RPL.

Below is a sample of adding the dataset:

```
//DFHRPL DD DSN=CICS.SDFHLOAD,
//          DISP=SHR
//          DD DSN=SSA.LOADLIB,
//          DISP=SHR
```

When the addition has been made, the region must be recycled to activate the change.

9 It is highly recommended that all SSA-CDA transactions be secured at the transaction level as well.

Since the implementation of RACF security on CICS transactions is specific to the shop no examples are included. Contact your SSA representative if you require assistance or information concerning CICS transaction security.

Step 12: Define Product Password

For SSA release 1.3 and lower, a resource profile under the SSA resource class was used to store security rules, configuration values and product passwords. This resource class (usually GAA\$RULE) was in either a static or dynamic RACF Class Descriptor Table entry.

For SSA version 1.4 and higher, the product password is no longer stored in a resource profile with a password member (typically MEGASOLVE-SSA.PASSWORDS); all other resource profiles are still needed except for the password profile. Also, for SSA release 1.4 and higher, a new procedure is required to activate the product and to enable optional product features.

Listed below are the steps needed to install and activate the product.

- 1 Obtain a password from UNICOM Systems Customer Service. You must provide the real CPU ID and model number. To get this information, use this command:

```
D M=CPU
```

Here is a typical response from the command:

```
RESPONSE=USZOS113
IEE174I 11.21.29 DISPLAY M 935
PROCESSOR STATUS
ID  CPU                      SERIAL
00  +                        A432102098
01  +                        A432102098
02  +I                       A432102098

CPC ND = 002098.E10.IBM.51.000000123ABC
CPC SI = 2098.J04.IBM.51.0000000000123ABC
      Model: E10
CPC ID = 00

+ ONLINE      - OFFLINE      . DOES NOT EXIST      W WLM-MANAGED
N NOT AVAILABLE

I          INTEGRATED INFORMATION PROCESSOR (zIIP)
CPC ND  CENTRAL PROCESSING COMPLEX NODE DESCRIPTOR
CPC SI  SYSTEM INFORMATION FROM STSI INSTRUCTION
CPC ID  CENTRAL PROCESSING COMPLEX IDENTIFIER
```

In this example, string CPC SI identifies the real CPU ID as 0123ABC and the model/submodel is 2098/J04.

- 2 When Customer Service receives the output from the D M=CPU' command, they will supply you with a password that is used by new program SSA\$V140 (supplied in the SSA LOAD library) through a SYSIN DD. You may run instream SYSIN data instead of creating a dataset and member as in the example (SSA.SSAINIT(SSAPASS)).

Here is an example of the JCL required:


```
//SSAV140 PROC APF='SSA.V140.LOADLIB'
//*-----
//* THIS JOB IS RUN ONCE AFTER IPL
//*-----
//STEP1 EXEC PGM=SSA$V140
//STEPLIB DD DISP=SHR,DSN=&APF
//SYSIN DD DISP=SHR,DSN=SSA.SSAINIT(SSAPASS)
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
```

Make sure the SSA library is APF-authorized before this job is run. If the SSA load modules are in LINKLST, remove the STEPLIB DD. This program *must* be run once after each IPL, either as a started task or batch job.

The SYSIN DD PDS member (SSA.SSAINIT(SSAPASS)) looks similar to this (Starting in column one):

```
CUSTOMER_NAME='UNICOM INTERNAL FOR TESTING      '
*  RULER-LINE 12345678901234567890123456789012
*  RULER-LINE          1          2          3
*
CUSTOMER_NO=00000000
*
PRODUCT_CODE=YYYYYYYY
*
CPUID=123ABC
*
MODEL=2098/J04
*
EXPIRATION_DATE=TEMP
*
PASSWORD=XXXXX,XXXXX,XXXXX,XXXXX,XXXXX,XXXXX,XXXXX,XXXXX,XXXXX,XXXXX
      (password has been changed to all X)
*
* PRODUCT PASSWORD FOR: UNICOM/SSA V VvRrMm GENERATED
      MM/DD/YYYY HH:MM
*
** GENERATED BY: UNICOM
```

- 3 Look through your z/OS SYSLOG for the message AALM081I: Unicom SSA -> RACF V140 Started Successfully. This indicates that the your SSA license was successfully installed.

Important note

SSA consists of common and optional components. Reports and Generic Searches are part of the default product. All other features are optional components that can be purchased separately.

Trial passwords permit the temporary usage of all SSA component functions. However, permanent passwords activate only those features that have been licensed to your company. Be sure to tell the Customer Service representative what SSA features have been licensed by your company.

Step 13: Startup Panel Choice (Optional/Recommended)

SSA should be available as an option on your ISPF product menu. To do so, you must first add a selection note to the BODY section of your product menu panel as shown below:

```
M      SMART SECURITY ADMINISTRATOR
```

Second, you must insert the selection into the PROC section within the selection logic as shown below:

```
M, ' PGM(AASTART) '
```

Now, users can access SSA by just entering an 'M' on the ISPF product panel you modified.

Step 14: Start the SSA Started Tasks

The SCHEDULER Started Task:

Note If you are not licensed for The SCHEDULER function, proceed to the CICS Direct Administration part of step 14.

To fully activate The SCHEDULER feature, you must start The SCHEDULER started task. This can be accomplished by either issuing the start command on the systems master console, or by issuing the command through SDSF (if you are authorized). Below is a sample of the start command on a master console.

Console Command Sample:

```
S AASTC01
```

When the task has started and issues its WTOR (a message to the operator requiring a response), ensure the tasks operating status by issuing a response to the outstanding WTOR with a D to display the current options the started task is using. You should receive a response like the sample below. If you do not, report the problem to your SSA technical support representative.

Started Task Current Options Sample:

```
*16 AASTC01 ENTER VALID SSA SCHEDULE FACILITY COMMAND
R 16,D
IEE600I REPLY TO 16 IS;D
AASTC02 SCAN INTERVAL:    00 HRS 01 MINS 00 SECS
AASTC02 WAKEUP INTERVAL:  00 HRS 00 MINS 30 SECS
AASTC02 HISTORY RETAIN:   007 DAYS
```

CICS Direct Administration Started Task:

Note If you are not licensed for the CICS Direct Administration, proceed to ‘Step 15: Off-loading RACF Information’ on page 56.

To fully activate the CICS Direct Administration feature, you must start the CICS Direct Administration started task. This can be accomplished by either issuing the start command on the systems master console or by issuing the command through SDSF (if you are authorized). Below is a sample of the start command on a master console.

Console Command Sample:

```
S AASTC02
```

When the task has started, it will issue a status through WTOs. If you do not see these messages, report the problem to your SSA technical support representative. Below is a sample of those messages. Keep in mind that the TCP/IP jobname and the started task name may differ depending on your shops values.

Started Task Startup Messages:

```
AAMG207 OPTIONS HAVE BEEN SUCCESSFULLY UPDATED
AAMG203 TCP/IP JOBNAME: TCPIPMVS
AAMG203 STARTED TASK:    AASTC02
```

Step 15: Off-loading RACF Information

SSA uses off-loaded RACF information for a majority of its functions (reporting, online generic searches, command generation, and so on.). To generate the off-load job do the following:

- 1** Logon to the proc you modified in step 5.
- 2** Start SSA by either executing program AASTART from option 6 of ISPF, or if available, use the menu startup option done in step 13.
- 3** Proceed to option 9 - Configuration and then option 1 - Edit Stored Configuration Values.

Make sure all values are correct and the specified jobcard works in your shop.

- 4** Proceed to Configuration option 6 - Run Extract Jobs.

When you enter option 6, you will be asked if you want to use the SSA off-load process or the IBM off-load process. Each process has its unique pros and cons. Below is that list for your consideration:

Function/Process	SSA off-load (AADBU00)	IBM Off-load (IRRDBU00)
Access Necessary to Database	Access is only governed by SSA security rules	Must have UPDATE authority to database being off-loaded
Screen Records Off-loaded According to Security Rules	All profiles can be subjected to a security check allowing individualized and specialized off loads	Dumps all records
Off-load Secondary or Backup Databases	No, only off loads live database	Can off-load secondary or backup databases

The following sequence will demonstrate the recommended SSA Off-load choice. For a detailed explanation and walk-through of the IBM Off-load option refer to 'Configuration' on page 499.

When you have chosen the SSA off-load process, you will be presented with the Review Generated JCL screen from which you can Edit, View, Submit, Store and Schedule the JCL.

```
----- SSA -----  
Review Generated JCL  
  
Command ==>  
  
Dataset In Use ==> 'IBMUSER.SSA.TEMP.JCL(BATCH)'  
  
OPTION ==> E  
  
Enter E to Edit the Generated JCL  
V to View the Generated JCL  
S to Submit the Generated JCL  
ST to Store the Generated JCL  
SC to Schedule the Generated JCL  
  
Hit Enter to Continue PF03=EXIT/PF01=HELP
```

It is recommended that you edit the JCL and manually submit the job by typing SUB at the command line and hitting ENTER.

After submitting the job, you must check the condition codes for both steps. Step020, of either job, using IKJEFT01 (to create an ISPF environment) can get a condition code of 0 but unsuccessfully load the SSA ISPF tables. It is important to check that unload status messages are produced under DD AASTATMN. If you notice error messages under DD ISPLOG or anything else other than a successful unload, note the problem immediately to your SSA technical support representative for resolution.

You have successfully completed the SSA installation. It is highly recommended that the administrator or systems programmer in charge of maintaining SSA and its security rules review the chapters listed on page 46.

SSA Usage Recommendations

Listed below are recommendations for using SSA.

- The samples below show the required attributes of the SSA classes that will ensure that the product works properly.
- The SSA off-load job should be placed in The SCHEDULER to run during non-production hours.
- If you are licensed for the CICS Direct Administration module, proceed to ‘CICS Direct Administration’ on page 363 for usage details.
- Try to maintain the naming conventions specified during installation. This allows you to more quickly reference the material, perform trouble shooting, and expedite any communications with your SSA representative.
- Start with high-level generic protection profiles for all secured functions before ‘releasing’ these functions to the appropriate personnel and departments.
- Enlarge the size of your ISPF profile dataset. SSA can store a large amount of information in your ISPF profile. You should increase the allocation by at least 50%.
- Some ISPF tables may contain a large number of rows depending on the size of your RACF database. Allow adequate storage during LOGON (in the SIZE field) so that ISPF can read the entire table into virtual storage. SSA users should allow approximately 200 bytes of storage for each ISPF table row to accommodate the largest table. For example, if the largest table is ‘TOTAL CONNECTS’ and there are 40,020 connect records, SSA will require at least 7.6 MB (200 bytes X 40,020 = 8,004,000). More information can be found by viewing the LEGEND pop-up on the first SSA (AAMAIN) panel or by checking the AASTAMN DD in STEP020 of the ‘Extract Job’ (ISPF Record Count Tally).
- All prior users of SSA should execute CLIST AAERASE, to purge all variables stored in their ISPF profiles for Admin-Aide version 3.1 through SSA version 1.3 and higher.
- Enabling logon statistic suppression is not recommended since SSA uses RACF LJDATE and LJTIME fields.



CHAPTER 3

SSA Reports

SSA provides a series of batch and online reports ranging from access to ownership. All reports offer selectivity, a well organized and extremely informational format.

Report Global Conventions

SSA reports adhere to several "global" conventions. The following conventions apply:

Security: All reports have security built into their panel dialog programs and report generators. MAA\$RULE is the default security class. SSA.REPORTnnn is the default security profile, where nnn is the numeric sequence of the report (see 'Configuration' on page 499 if you wish to change defaults). For example, Access Report for Userids is the first report. Therefore, the security profile is SSA.REPORT001.

Users must have read access to the profile to use the report panel dialog and run the report generating program. Below is a table showing the report and the protecting RACF profile.

Report	RACF Profile
Access Report for Userids	MEGASOLVE-SSA.REPORT001
Access Report for Groups	MEGASOLVE-SSA.REPORT002
Dataset Profile Permission Report	MEGASOLVE-SSA.REPORT003
Ownership Report	MEGASOLVE-SSA.REPORT004
Group Connect Report	MEGASOLVE-SSA.REPORT005
Default Group Report	MEGASOLVE-SSA.REPORT006
Clauth/Group Special Report	MEGASOLVE-SSA.REPORT007
Never Logged On Report	MEGASOLVE-SSA.REPORT008
Global Attribute Report	MEGASOLVE-SSA.REPORT009
Non-Expiring Password Report	MEGASOLVE-SSA.REPORT010
True Dataset Authority Report	MEGASOLVE-SSA.REPORT011
Notify Report	MEGASOLVE-SSA.REPORT012
Break in Ownership Report	MEGASOLVE-SSA.REPORT013
User/Group Repetitive Permits Report	MEGASOLVE-SSA.REPORT014
Group Statistics Report	MEGASOLVE-SSA.REPORT015
Obsolete Entries Report	MEGASOLVE-SSA.REPORT016
Where a User/Group is Not in an Access List Report	MEGASOLVE-SSA.REPORT017
General Resource Class Permission Report	MEGASOLVE-SSA.REPORT018
Userid Statistics Report	MEGASOLVE-SSA.REPORT019
Dataset Profile and Permission Report	MEGASOLVE-SSA.REPORT020
RACF to Master Catalog Comparison Report	MEGASOLVE-SSA.REPORT021

Operational Batch or online.

Mode:

Batch mode generates the JCL necessary to create the SSA report you requested based upon your selections. SSA displays the Review Generated JCL panel as shown below.

```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'TSGBAT.TSCSSA.TEMP.JCL(BATCH)'

OPTION ==> S

Enter E to Edit the Generated JCL
V to View the Generated JCL
S to Submit the Generated JCL
ST to Store the Generated JCL
SC to Schedule the Generated JCL

Hit Enter to Continue PF03=EXIT/PF01=HELP
  
```

Report Data Selection

- E Select E if you want to be placed in an EDIT session.
- V Select V if you want to be placed in a VIEW session.
- S Select S if you want to submit the generated JCL.
- ST Select ST if you want to store the generated JCL in the SSA storage facility.
- SC Select SC if you want to schedule the generated JCL through The SCHEDULER. Refer to 'The SCHEDULER' on page 269 for instructions.

Online mode creates the report based upon your selections. The report appears in a browse session, as shown below, from which you can print the report..

```

Print Parm ----- SSA ----- Print Par
Command ==>                                         Scroll ==> CSR

Do you want to print this display (Y/N): N

Sysout    ==> A  Copies    ==> 01  Title      ==> N
Hold (Y/N) ==> N  Page Length ==> 55  Destination ==>

BROWSE - USER01.TEST.TSCSSA.REPORT.OUTPUT ----- LINE 00000000 COL 001 08
***** Top of Data*****
1
Date: 07/14/1998
Time: 09:38

SSA Version
User Access Report for

UserID:      IBMUSER      Name:                               Defau
Create-Date: 06/06/95     Last-Used-Date: 10/21/96      Passd

Global Attributes
-----

Special:      Yes  Operations:      Yes  Auditor:      Yes
Grpacc:       No   Uaudit:         No   Oldcard:       No

```

Send Report Output

S or D (SYSOUT or DATASET).

S (SYSOUT)

Batch reports are sent to SYSOUT (if the JOB is expanded through SDSF a DDNAME of AAREPORT is used). Does not apply to online reports.

D (DATASET)

Batch or online modes. In either mode the output is directed to the output dataset.

Report JCL

All Report options use the same JCL with the exception of report 11 (True Dataset Authority Report) and report 21 (RACF to Master Catalog Comparison Report).

Report 11 is a non-ISPF based report that must run in an authorized environment. Report 21 has a number of DD and allocation changes to accommodate the IDCAMS output. Its differences will be discussed in that reports part.

Below is a sample of the general report job. In each explanation of a report, references are made to the two distinguishing factors concerning the JCL. Those two factors are:

DD AACTLCDS

Control cards that tell the report what it should contain.

DD AASYSIN

Input entries that are to be reported on (that is, IBMUSER, if you want to run an access report on IBMUSER).

JCL Sample (AAREP001 - Access Reports for Userids)

```

/*
/*
/******
/***                                     **
/***          SMART SECURITY ADMINISTRATOR          **
/***                                     **
/***          VERSION V.V                          **
/***                                     **
/*** (C) YYYY UNICOM SYSTEMS, INC.                  **
/***          ALL RIGHTS RESERVED                   **
/******
/*
/* JCL CREATED BY USER01
/* JCL CREATED ON MM/DD/YYYY
/* JCL CREATED AT 14:37
/*
/* JOB FUNCTION: ACCESS_REPORT_FOR_USERIDS
/*
/*STEP010      EXEC PGM=IKJEFT01,DYNAMNBR=30,TIME=1440,REGION=4096K
/*SYSPROC      DD  DISP=SHR,
/*              DSN=SSA.ISPCLIB
/*ISPPROF      DD  DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
/*              DCB=(LRECL=80,BLKSIZE=6160,RECFM=FB),UNIT=SYSDA
/*ISPPLIB      DD  DISP=SHR,
/*              DSN=SSA.ISPPLIB
/*ISPSLIB      DD  DISP=SHR,
/*              DSN=SSA.ISPSLIB
/*ISPMLIB      DD  DISP=SHR,
/*              DSN=SYS1.SISPMENU
/*              DD  DISP=SHR,
/*              DSN=SSA.ISPMLIB
/*ISPTLIB      DD  DISP=SHR,
/*              DSN=SYS1.SISPTENU
/*AADBTLIB DD  DISP=SHR,
/*              DSN=SSA.RACFDATA.ISPTLIB
/*STEPLIB      DD  DISP=SHR,
/*              DSN=SSA.LOADLIB
/*ISPCTL1      DD  DSN=&CNTL1,DISP=(,PASS),UNIT=SYSDA,
/*              DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),SPACE=(TRK,(5,5))
/*ISPCTL2      DD  DSN=&CNTL2,DISP=(,PASS),UNIT=SYSDA,
/*              DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),SPACE=(TRK,(5,5))
/*SYSTSPRT     DD  SYSOUT=*,DCB=(BLKSIZE=19019,LRECL=133,RECFM=FBA)
/*SYSPRINT     DD  SYSOUT=*,DCB=(BLKSIZE=20000,LRECL=200,RECFM=FBA)
/*ISPLOG       DD  SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
/*SYSOUT       DD  SYSOUT=*
/*TEMPWK01     DD  UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE
/*TEMPWK02     DD  UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE
/*SORTWK01     DD  UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE
/*AAREPORT     DD  SYSOUT=*,
/*              DCB=(RECFM=FBA,LRECL=133)
/*AASYSIN      DD  *
IBMUSER
/*
/*AACTLCDS     DD  *
USER-DETAILS
UACC
CONNECT-PERMISSIONS
OWNERSHIP
EXPAND-MEMBERS
SUMMARY
LINES-PER-PAGE=55
/*
/*SYSTSIN      DD  *
ISPSTART PGM(AAREP001)
/*

```

JCL DDs

Below is a brief explanation of the DDs and what they must reference:

SYSPROC Must reference the SSA CLIST library.

ISPPLIB	Must reference the SSA ISPF panel library.
ISPSLIB	Must reference the SSA skeleton JCL library.
ISPMLIB	Must reference the SSA ISPF message library and ISPF system message library.
ISPTLIB	Must reference the ISPF system table library.
STEPLIB	Must reference the SSA APF Authorized load library.
AADBTLIB	Must reference the SSA RACF information table library.
AAREPORT	This DD can either reference an output dataset with the following DCBs: RECFM=FBA,LRECL=133 or can be directed to SYSOUT.
AACTLCDS	Must reference the control cards for the report program.
AASYSIN	Must reference the input entries for the report program.

Control Cards

The DD AACTLCDS references control cards that tell the report what to contain or reference. The following control cards apply to a majority of the reports; they will not be discussed again.

LINE-PER-PAGE=nn	This card controls the number of lines per page on the report. The value can be from 10 to 99.
SUMMARY	This card will produces a summary report. NOSUMMARY is the default.

Note These conventions are not mentioned in the remainder of this chapter.

Reports Main Menu

Shown below is the SSA Report Main menu. This example shows the short version of the SSA Report Main Menu. The long version of the menu provides greater detail concerning report content and data filtering.

The long version can be viewed by changing the Menu Format configuration setting to LONG. This can be done through Configuration option 1. You can also enter CLISTs to display short or long versions of SSA menus. Execute the CLIST AASHORT to display the short menu, or AALONG to display the long menu.

Reports	SSA	Reports
Main Menu		
Option ==>		More: +
1	Access Report for Userids	
2	Access Report for Groups	
3	Dataset Profile Permission Report	
4	Ownership Report	
5	Group Connect Report	
6	Default Group Report	
7	Clauth/Group Special Report	
8	Never Logged On Report	
9	Global Attribute Report	
10	Non-Expiring Password Report	
11	True Dataset Authority Report	
12	Notify Report	
13	Break in Ownership Report	
14	User/Group Repetitive Permits Report	
15	Group Statistics Report	
16	Obsolete Entry Report	
17	Where a User/Group Is Not in an Access List Report	
18	General Resource Class Permission Report	
19	Userid Statistics Report	
20	Dataset Profile and Permission Report	
21	RACF to Master Catalog Comparison Report	
Hit Enter to Continue		PF03=EXIT/PF01=HELP

The remainder of this chapter describes how to create each SSA report. Each report is described in a separate chapter section that includes an example of the report data selection panel, batch JCL examples, and control card explanations. Refer to 'SSA Report Examples' on page 537 for examples of each SSA report.

Access Report for Userids

Provides a detailed cross reference access report by Userid.

```
Reports ----- SSA ----- Reports
                        Access Report for Userids
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include...):
                        -----
                        User Details           (Y/N): Y   UACCs           (Y/N): Y
                        User Connect Permissions (Y/N): Y   Ownership      (Y/N): Y
                        Expand Group Resource Profiles (Y/N): Y   Summary       (Y/N): Y

Userids:
==> IBMUSER  ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

User Details	Indicate if you want profile details concerning the userid to be included in the report.
UACCs	Indicate if you want permission through UACCs to be included in the report.
User Connect Permissions	Indicate if you want permissions through the userids group connects to be included in the report.
Ownership	Indicate if you want all occurrences of ownership by the userid to be included in the report.
Expand Group Resource Profiles	Indicate if you want group resource profiles expanded to show the members of those groups.
Summary	Indicate if you want a summary produced.
Groups	You must enter at least one userid.

Report JCL

```
//AACTLCDS DD *
USER-DETAILS
UACC
CONNECT-PERMISSIONS
OWNERSHIP
EXPAND-MEMBERS
SUMMARY
//*
//AASYSIN DD *
IBMUSER
/*
```

Control Cards

USERID(variable)	Specify at least one userid to report on. Each user must be on a separate line starting in column 1.
USER-DETAIL	Specify this parm to include Userid details such as segment information, group connects, global attributes, and so on.
CONNECT-PERMISSIONS	Specify this parm to include access to resources that are obtained through group connections. This type of access will include the group name in the group name column on the report.
EXPAND-MEMBERS	Specify this parm to expand member resources of grouping class profiles. For example, to include a list of CICS transactions in your report, use the EXPAND-MEMBERS parm if you are using the group resource class.
UACC	Specify this parm to include all access obtained through universal access, warning attribute, or ‘ * ‘ access list permissions.
OWNERSHIP	Specify this parm to report on all occurrences of ownership.

Access Report for Groups

Provides a detailed cross reference access report by Group.

```
Reports ----- SSA ----- Reports
                        Access Report for Groups
Command ==>>

                        Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): S
-----
Report Specifications (Do you want to include....):
-----
Group Details           (Y/N): Y      UACCs           (Y/N): Y
Expand Group Resource Profiles (Y/N): Y      Ownership (Y/N): Y
Summary                 (Y/N): Y

Groups:
==> SYS1      ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

Group Details	Indicate if you want profile details concerning the group to be included in the report.
UACCs	Indicate if you want permission through UACCs to be included in the report.
Expand Group Resource Profiles	Indicate if you want group resource profiles expanded to show the members of those groups.
Ownership	Indicate if you want all occurrences of ownership by the userid to be included in the report.
Summary	Indicate if you want a summary produced.
Groups	You must enter at least one group.

Report JCL

```
//AACTLCDS DD *
GROUP-DETAILS
UACC
OWNERSHIP
EXPAND-MEMBERS
SUMMARY
//*
//AASYSIN DD *
SYS1
/*
```


Control Cards

GROUP (variable)	Specify at least one group to report on. Each group must be on a separate line starting in column 1.
GROUP-DETAIL	Specify this parm to include Groups details such as segment information, userid connects, and so on.
EXPAND-MEMBERS	Specify this parm to expand member resources of grouping class profiles. For example to include a list of CICS transactions in your report use the EXPAND-MEMBERS parm if you are using the group resource class.
OWNERSHIP	Specify this parm to include all occurrences of ownership by the groups specified.
UACC	Specify this parm to include all access obtained through universal access or ' * ' standard access list permissions.

Dataset Profile Permissions Report

Provides a detailed report of permissions by dataset high-level qualifier.

```
Reports ----- SSA ----- Print Issued
                        Dataset Profile Permissions Report
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): D
-----
Report Specifications (Do you want to include....):
-----
                        Summary (Y/N): Y

HLQs:
==> SYS1_____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

- Summary Indicate if you want a summary produced.
- HLQs You must enter at least one high level qualifier.

Report JCL

```
//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
SYS1
/*
```

Control Cards

- HLQ (variable) Specify at least one HLQ to report on. Each HLQ must be on a separate line starting in column 1.

Ownership Report

Provides a detailed profile ownership report.

```
Reports ----- SSA ----- Entry is Necessary
                                Ownership Report
Command ==>

                                Operational Mode (Batch/Online) ==> BATCH
-----
                                Direct Report Output to Sysout or Dataset (S/D): S
-----
                                Report Specifications (Do you want to include...):
-----
                                User Profiles      (Y/N): Y      Group Profiles  (Y/N): Y
                                Connect Profiles   (Y/N): Y      Dataset Profiles (Y/N): Y
                                General Resource Profiles (Y/N): Y --> Expand      (Y/N): Y
                                Summary              (Y/N): Y
-----

Userids or Groups:
==> IBMUSER ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

- User Profiles Indicate if you want user profile ownership reported on.
- Group Profiles Indicate if you want group profile ownership reported on.
- Connect Profiles Indicate if you want connect profile ownership reported on.
- Dataset Profiles Indicate if you want dataset profile ownership reported on.
- General Resource Profiles Indicate if you want general resource profile ownership reported on.
- Expand Indicate if you want group resource profiles expanded to show the members of those groups.
- Summary Indicate if you want a summary produced.
- Userids or Groups You must enter at least one userid or group to report on.

Report JCL

```
//AACTLCDS DD *
INCLUDE=USER
INCLUDE=GROUP
INCLUDE=CONNECT
INCLUDE=DATASET
INCLUDE=RESOURCE,EXPAND
SUMMARY
//*
//AASYSIN DD *
IBUSER
/*
```

Control Cards

USERID or GROUP (variable)	Specify at least one user or group to report on. Each user or group must be on a separate line starting in column 1.
EXPAND-MEMBERS	Specify this parm to expand member resources of grouping class profiles; for example to include a list of CICS transactions in your report.
INCLUDE	Specify this parm to indicate what resources to include in the report.
INCLUDE=USER	Includes User profile information.
INCLUDE=CONNECT	Includes Connect profile information.
INCLUDE=RESOURCE	Includes Resource profile information.
INCLUDE=GROUP	Includes Group profile information.
INCLUDE=DATASET	Includes Dataset profile information.

Group Connect Report

Provides a detailed report on all users connected to particular groups.

Reports ----- SSA ----- Reports

Group Connect Report

Command ==>

Operational Mode (Batch/Online) ==> BATCH

Direct Report Output to Sysout or Dataset (S/D): S

Report Specifications (Do you want to include...):

Summary (Y/N): Y

Groups:

==> SYS1

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

Hit Enter to Continue

PF03=EXIT/PF01=HELP

Report Data Selection

- Summary
- Indicate if you want a summary produced.
- Groups
- You must specify at least one group to report on.

Report JCL

```
//AACTLCDS DD *  
SUMMARY  
//*  
//AASYSIN DD *  
SYS1  
//*
```

Control Cards

- GROUP (variable)
- Specify at least one group to report on. Each group must be on a separate line starting in column 1.

Default Group Report

Provides a detailed report on all users having a particular default group.

```
Reports ----- SSA ----- Reports
                        Default Group Report
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include....):
                        -----
                        Summary (Y/N): Y

Groups:
==> SYS1      ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

- Summary Indicate if you want a summary produced.
- Groups You must enter at least one group to report on.

Report JCL

```
//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
SYS1
/*
```

Control Cards

GROUP (variable) Specify at least one group to report on. Each group must be on a separate line starting in column 1.

Clauth/Group Special Report

Provides a detailed report showing users who have CLAUTH authority to a particular class and group special.

Reports ----- SSA ----- Reports

Clauth/Group Special Report

Command ==>

Operational Mode (Batch/Online) ==> BATCH

Direct Report Output to Sysout or Dataset (S/D): S

Classes:

==> MAA\$RULE

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

==>

Hit Enter to Continue

PF03=EXIT/PF01=HELP

Report Data Selection

Classes You must enter at least one general resource class to report on.

Report JCL

```
//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
CLASS=MAA$RULE
/*
```

Control Cards

CLASSES Specify at least one general resource class to report on.

Never Logged On Report

Provides a detailed report showing Userids that have never logged on.

```

Reports ----- SSA ----- Reports
                        Never Logged On Report

Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include...):
                        -----
                        Summary (Y/N): Y

Include (Use Generic mask to screen by Default Group - i.e., GRPA*)
==> TSO*      ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>

Exclude (Use Generic mask to screen by Default Group - i.e., GRPB*)
==> CICS*     ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Report Data Selection

- Summary** Indicate if you want a summary produced.
- Include** Specify a mask to indicate by default group which userids you want included in the report. See control cards section for a more detailed explanation.
- Exclude** Specify a mask to indicate by default group which userids you want excluded in the report. See control cards section for a more detailed explanation.
- Note** You do not have to put any include or exclude masks if you want all userids to appear in the report.

Report JCL

```

//AACTLCDS DD *
INCLUDE=TSO*
EXCLUDE=CICS*
SUMMARY
//*
//AASYSIN DD *
//*
  
```


Control Cards

INCLUDE:	Specify a mask to screen the input records and determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
INCLUDE=TSO*	Includes all Userids whose default group begins with TSOAD.
EXCLUDE:	Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=CICS*	Excludes all Userids whose default group begins with CICS.

Global Attribute Report

Provides a detailed report showing Userids that have global (user) attributes.

```

Reports ----- SSA ----- Reports
                                Global Attribute Report

Command ==>

                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Report Specifications (Do you want to include...):
                                -----
                                Special (Y/N): Y   Operations (Y/N): Y   Auditor (Y/N): Y
                                Uaudit  (Y/N): Y   ADSP      (Y/N): Y   Grpacc  (Y/N): Y
                                Revoked (Y/N): Y   Oidcard   (Y/N): Y   Summary (Y/N): Y

Include (Use Generic mask to screen by Default Group - i.e., GRPA*)
==> SYS1*      ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

Exclude (Use Generic mask to screen by Default Group - i.e., GRPB*)
==> USER*      ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Report Data Selection

Special	Indicate if you want users with global-special to be reported on.
Operations	Indicate if you want users with global-operations to be reported on.
Auditor	Indicate if you want users with global-auditor to be reported on.
Uaudit	Indicate if you want users with global-uaudit to be reported on.
ADSP	Indicate if you want users with global-adsp to be reported on.
GRPACC	Indicate if you want users with global-grpacc to be reported on.
Revoked	Indicate if you want users with global-revoke to be reported on.
Oidcard	Indicate if you want users with global-oidcard to be reported on.
Summary	Indicate if you want a summary produced.
Include	Specify a mask to indicate by default group which userids you want included in the report. See control cards section for a more detailed explanation.
Exclude	Specify a mask to indicate by default group which userids you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all userids to appear in the report.

Report JCL

```
//AACTLCDS DD *
SPECIAL
OPERATIONS
AUDITOR
REVOKED
OIDCARD
UAUDIT
ADSP
GRPACC
INCLUDE=TSO*
EXCLUDE=CICS*
SUMMARY
//*
//AASYSIN DD *
//*
```

Control Cards

ATTRIBUTES	Specify one or more of the following attributes to include in the report. If no attributes are selected, then all attributes appear in the report.
SPECIAL	Include all Userids with user SPECIAL attribute
OPERATIONS	Include all Userids with user OPERATIONS attribute
UAUDIT	Include all Userids with user UAUDIT attribute
AUDITOR	Include all Userids with user AUDITOR attribute
ADSP	Include all Userids with user ADSP attribute
OIDCARD	Include all Userids with user OIDCARD attribute
GRPACC	Include all Userids with user GRPACC attribute
REVOKED	Include all Userids with user REVOKED attribute
OIDCARD	Include all Userids with user OIDCARD attribute
INCLUDE	Specify a mask to determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
INCLUDE=TSO*	Includes all Userids whose default group begins with TSOAD.
EXCLUDE	Specify a mask to determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=CICS*	Excludes all Userids whose default group begins with CICS.

Non-Expiring Password Report

Provides a detailed report showing Userids that have non-expiring passwords.

```

Reports ----- SSA ----- Reports
                                Non-Expiring Password Report

Command ==>

                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Report Specifications (Do you want to include...):
                                -----

                                Summary (Y/N): Y

Include (Use Generic mask to screen by Default Group - i.e., GRPA*)
==> TSO*      ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>

Exclude (Use Generic mask to screen by Default Group - i.e., GRPB*)
==> CICS*     ==>      ==>      ==>      ==>
==>          ==>      ==>      ==>      ==>

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Report Data Selection

Summary Indicate if you want a summary produced.

Include Specify a mask to indicate by default group which userids you want included in the report. See control cards section for a more detailed explanation.

Exclude Specify a mask to indicate by default group which userids you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all userids to be reported on.

Report JCL

```

//AACTLCDS DD *
INCLUDE=TSO*
EXCLUDE=CICS*
SUMMARY
//*
//AASYSIN DD *
//*

```

Control Cards

INCLUDE	Specify a mask to screen the input records and determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
INCLUDE=TSO*	Includes all Userids whose default group begins with TSOAD.
EXCLUDE	Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to default group. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=CICS*	Excludes all Userids whose default group begins with CICS.

True Dataset Authority Report

Provides a detailed report showing users or groups tested authority to datasets by either HLQ or volume.

```

Reports ----- SSA ----- Reports
                True Dataset Authority Report

Command ==>

                Operational Mode (Batch/Online) ==> BATCH
                -----
                Direct Report Output to Sysout or Dataset (S/D): S
                -----
                Report Specifications (Do you want to include....):
                -----

                User/Group to Report On ==> IBMUSER

                Report by HLQ or Volume (H/V): H

                HLQ    ==> SYS1
                Volume ==> _____ Unit ==> _____

                Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Report Data Selection

User/Group to Report On	Enter a userid or group whose authority you want analyzed.
Report by HLQ or Volume	Enter “H” if you want to look for datasets by their HLQ or “V” if you want all datasets on a volume analyzed.
HLQ	If you chose the HLQ option, you must enter a HLQ.
Volume	If you chose the volume option , you must enter a volume.
Unit	The valid unit reference for the volume must be entered if you chose the volume option.

Report JCL

Report 11 (True Dataset Authority Report) uses JCL that is distinct from the other reporting programs. Below is a sample of that JCL:

```

/* JOB FUNCTION: TRUE_DATASET_AUTHORITY_REPORT
/*
//STEP010 EXEC PGM=AAREP011
//STEPLIB DD DISP=SHR,
//         DSN=SSA.LOADLIB
//SYSIN   DD DSN=&TEMP01,DISP=(,PASS),
//         UNIT=SYSDA,
//         SPACE=(CYL,(5,5),RLSE),
//         DCB=(RECFM=FB,LRECL=80,BLKSIZE=7440)
//SYSPRINT DD DSN=&TEMP02,DISP=(,PASS),
//         UNIT=SYSDA,
//         SPACE=(CYL,(5,5),RLSE)
//AAREPORT DD SYSOUT=*,
//         DCB=(RECFM=FBA,LRECL=133)
//AACTLCDS DD *
SUMMARY
LINES-PER-PAGE=55
/*
//AASYSIN DD *
USER=IBMUER
TYPE=H
HLQ=SYS1
/*

```

Note The control cards for Report 11 are entered under DD AASYSIN instead of AACTLCDS.

Control Cards (Entered under AASYSIN DD)

USER	Enter a user or group whose authority you want analyzed. You can only enter one user/group to be analyzed and the entry must be valid; its validity is checked against the live database not the SSA ISPF tables.
TYPE	Enter “H” for dataset searching by HLQ (High Level Qualifier) or “V” for dataset searching based on a volume. You can only enter on HLQ or volume. If the HLQ or volume does not exist, your report will be empty.
HLQ	Enter a valid HLQ if you chose the HLQ option.
VOLUME	Enter a valid volume if you chose the volume option.
UNIT	If you chose the volume option, you must enter the unit for the volume. The unit can be the esoteric generic unit name (that is, SYSDA) or it can be the physical unit name (that is, 3390). If you specify the volume and not the unit, the job will fail.

Notify Report

Provides a detailed report of notifies specified on resource profiles.

```

Reports ----- SSA ----- Reports
                                Notify Report

Command ==>

                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Report Specifications (Do you want to include...):
                                -----
                                Expand Group Resource Profiles (Y/N): Y      Summary (Y/N): Y

Include (Use Generic mask to screen by Notify Userid - i.e., USERA*)
==> IBMUSER* ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

Exclude (Use Generic mask to screen by Notify Userid - i.e., USERB*)
==> USERIBM* ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Report Data Selection

Expand Group Resource Profiles	Indicate if you want group resource profiles expanded to show the members of those groups.
Summary	Indicate if you want a summary produced.
Include	Specify a mask to indicate by notify userid which profiles you want included in the report. See control cards section for a more detailed explanation.
Exclude	Specify a mask to indicate by notify userid which profiles you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all profiles with notifies to be reported on.

Report JCL

```

//AACTLCDS DD *
EXPAND-MEMBERS
INCLUDE=IBMUSER*
EXCLUDE=USERIBM*
SUMMARY
//*
//AASYSIN DD *
//*
  
```


Control Cards

INCLUDE	Specify a mask to screen the input records and determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to the notify userid entry. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
INCLUDE=IBMUSER*	Includes all profiles whose notify userid begins with USERA.
EXCLUDE	Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to notify userid entry. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=USERIBM*	Excludes all profiles whose notify userid begins with USERB.
EXPAND-MEMBERS	Specify this parm if you want group general resource profiles with members expanded to show all members under those profiles; for example to include CICS transactions that are grouped together.

Break in Ownership Report

Provides a detailed report showing RACF profiles that have breaks in ownership.

```
Reports ----- SSA ----- Reports
                                Break in Ownership Report

Command ==>

                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Report Specifications (Do you want to include...):
                                -----
                                User Profiles   (Y/N): Y   Group Profiles   (Y/N): Y
                                Connect Profiles (Y/N): Y   Dataset Profiles (Y/N): Y
                                Summary         (Y/N): Y

Include (Use Generic mask to screen by Owner - i.e., GRPA*)
==> TSO*      ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

Exclude (Use Generic mask to screen by Owner - i.e., GRPA*)
==> CICS*     ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Report Data Selection

- User Profiles Indicate if you want user profiles to be analyzed. A break in ownership is indicated by the default group not matching the profile owner.
- Group Profiles Indicate if you want group profiles to be analyzed. A break in ownership is indicated by the superior group not matching the profile owner.
- Connect Profiles Indicate if you want connect profiles to be analyzed. A break in ownership is indicated by the connect group not matching the connect owner.
- Dataset Profiles Indicate if you want dataset profiles to be analyzed. A break in ownership is indicted by the HLQ not matching the profile owner.
- Summary Indicate if you want a summary produced.
- Include Specify a mask to indicate by owner which profiles you want included in the report. See control cards section for a more detailed explanation.
- Exclude Specify a mask to indicate by owner which profiles you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all profiles to be reported on.

Report JCL

```
//AACTLCDS DD  *
USER
GROUP
CONNECT
DATASET
INCLUDE=TSO*
EXCLUDE=CICS*
SUMMARY
//*
//AASYSIN  DD  *
/*
```

Control Cards

PROFILE TYPE	Specify one or more of the following parms to include that type of profile in the report. If a specific profile type is not selected then all types will be reported on.
USER	To include all USER profiles
DATASET	To include all DATASET profiles
CONNECT	To include all CONNECT profiles
GROUP	To include all GROUP profiles
INCLUDE	Specify a mask to screen the input records and determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to owner. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
INCLUDE=TSO*	Includes all profiles whose owner begins with TSO.
EXCLUDE	Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to owner. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=CICS*	Excludes all profiles whose owner begins with CICS.

User/Group Repetitive Permits Report

Report showing repetitive permits for users and their connect group permits.

```

Reports ----- SSA ----- Reports
                        User/Group Repetitive Permits Report
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include...):
                        -----
                        All Permits/User=Low/Equal Level/User=High (A/L/E/H): A

                        User Mask ==> IBMUSER*
                        Class Mask ==> FACILITY

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP
  
```

Report Data Selection

All Permits/ Enter “A” if you want all permits analyzed, “L” if you want permits
 User=Low/ where the users access level is lower than the connect group in
 Equal Level/ question, “E” if you want permits of equal access levels, or “H” if
 User=High you want permits where the users access level is higher than the
 connect group in question. User Mask Enter a mask indicating which
 userids you want analyzed. The entry can be a specific userid or use
 * to report on all userids. Class Mask Enter a mask indicating which
 classes you want analyzed. The entry can be a specific general
 resource class or use * to report on all classes.

Report JCL

```

//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
COND=ALL
USER=IBMUSER*
CLASS=FACILITY
//*
  
```

Note The control cards for Report 14 are entered under DD AASYSIN instead of AACTLCDS.

Control Cards (Entered under DD AASYSIN)

COND Enter “ALL” if you want all permits analyzed, LOW if you want
 permits where the users access level is lower than the connect group in
 question, EQUAL if you want permits of equal access levels, or HIGH
 if you want permits where the users access level is higher than the
 connect group in question. The default is ALL.

USER	Enter a mask for the userids you want analyzed. The default is “*” for all users.
CLASS	Enter a mask for the classes you want analyzed. The default is DATASET, however, if you enter anything else except dataset explicitly, only general resource classes will be loaded and searched. For example, if you entered DATA*, only general resource classes starting with DATA would be included in the report, DATASET however, would not.

Group Statistics Report

Provides a detailed statistical report of the occurrences of RACF groups.

```

Reports ----- SSA ----- Reports
                        Group Statistics Report

Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include...):
                        -----
                        Summary (Y/N): Y

Include (Use Generic mask to screen by Group - i.e., GRPA*)
==> TSO*      ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

Exclude (Use Generic mask to screen by Group - i.e., GRPA*)
==> CICS*     ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Report Data Selection

- Summary** Indicate if you want a summary produced.
- Include** Specify a mask to indicate by group which profiles you want included in the report. See control cards section for a more detailed explanation.
- Exclude** Specify a mask to indicate by group which profiles you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all groups to be reported on.

Report JCL

```

//AACTLCDS DD *
INCLUDE=TSO*
EXCLUDE=CICS*
SUMMARY
//*
//AASYSIN DD *
//*

```

Control Cards

- INCLUDE** Specify a mask to screen the input records and determine what records are included in the report. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to group. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.
- INCLUDE=TSO*** Includes all groups beginning with TSO.

EXCLUDE	Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to group. A maximum of 10 EXCLUDE statements may be entered.
EXCLUDE=CICS*	Excludes all groups beginning with CICS.

Obsolete Entries Report

Provides a detailed statistical report of the occurrences of RACF groups.

```

Reports ----- SSA ----- Reports
                        Obsolete Entries Report

Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----

                        Hit Enter to Continue      PF03=EXIT/FF01=HELP
  
```

Report Data Selection

All obsolete entries are included in the report. Those entries are:

- Permits for Dataset and General Resource profiles
- Ownership of users, groups, connects, dataset profiles and general resource profiles
- Notifies on dataset and general resource profiles
- Entries in the SURROGAT class
- Entries in the GLOBAL class - SURROGAT profile
- Entries in the GLOBAL class - DATASET profile (based on HLQ)
- PROGRAM class datasets (based on HLQ)
- STDATA segment - users
- STDATA segment - group

Report JCL

```

//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
//*
  
```

Control Cards

N/A

Where a User/Group is Not in an Access List Report

Report shows where a user or group is not specifically in an access list.

```

Reports ----- SSA ----- Reports
Where a User/Group is Not in an Access List Report
Command ==>

Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): S
-----
Report Specifications (Do you want to include...):
-----

User Mask    ==> IBMUSER*
Group Mask   ==> *
Class Mask   ==> DATASET
Profile Mask ==> *

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Report Data Selection

User Mask	Enter a mask indicating which userids you want analyzed.
Group Mask	Enter a mask indicating which groups you want analyzed.
Class Mask	Enter a mask indicating which classes you want analyzed.
Profile Mask	Enter a mask indicating which profiles within the classes you chose you want analyzed.

Report JCL

```

//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
USER=IBMUSER*
GROUP=*
CLASS=DATASET
PROFILE=*
//*

```

Note The control cards for Report 17 are entered under DD AASYSIN instead of AACTLCDS.

Control Cards (Entered under DD AASYSIN)

USER	Enter a mask for the userids you want analyzed. The default is "*" for all users.
GROUP	Enter a mask for the groups you want analyzed. The default is "*" for all groups.

- CLASS** Enter a mask for the classes you want analyzed. The default is DATASET, however, if you enter anything else except dataset explicitly, only general resource classes will be loaded and searched. For example, if you entered DATA*, only general resource classes starting with DATA would be included in the report, DATASET however, would not.
- PROFILE** Enter a mask for the profiles within the classes you have chosen that you want analyzed. The default is "*" for all profiles.

General Resource Class Permission Report

Provides a detailed listing by general resource class of all permissions.

```

Reports ----- SSA ----- Reports
                        General Resource Class Permission Report
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S
                        -----
                        Report Specifications (Do you want to include...):
                        -----
                        Expand: Group Resource Profiles (Y/N): Y   Group Permits (Y/N): Y
                               Summary (Y/N): Y

Classes:
==> GAA$RULE ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP
  
```

Report Data Selection

Expand Group Resource Profiles	Indicate if you want members displayed for all group general resource profiles reported on.
Expand Group Permits	Indicate if you want group permits expanded to show all users connected to that particular group.
Summary	Indicate if you want a summary produced.
Classes	You must enter at least one general resource class to report on. USER, GROUP, CONNECT and DATASET are not valid general resource classes.

Report JCL

```

//AACTLCDS DD *
SUMMARY
EXPAND-GROUPS
EXPAND-MEMBERS
//*
//AASYSIN DD *
GAA$RULE
//*
  
```

Control Cards

EXPAND-MEMBERS	Specify this parm to expand member resources of grouping class profiles.
EXPAND-GROUPS	Specify this parm to expand group permissions showing all users connected to that particular group.

CLASSES (variable) Specify at least one general resource class to report on.
Each class must be on a separate line starting in column 1.

Userid Statistics Report

Provides a detailed statistical report of the occurrences of RACF userids.

```

Reports ----- SSA ----- Reports
                        Userid Statistics Report

Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
-----
                        Direct Report Output to Sysout or Dataset (S/D): S
-----
                        Report Specifications (Do you want to include....):
-----
                        Summary (Y/N): Y

Include (Use Generic mask to screen by Userid - i.e., USR*)
==> IBMUSER* ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

Exclude (Use Generic mask to screen by Userid - i.e., USR*)
==> USERIBM* ==> _____ ==> _____ ==> _____ ==> _____
==> _____ ==> _____ ==> _____ ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Report Data Selection

Summary Indicate if you want a summary produced.

Include Specify a mask to indicate by userid whom you want included in the report. See control cards section for a more detailed explanation.

Exclude Specify a mask to indicate by userid whom you want excluded in the report. See control cards section for a more detailed explanation.

Note You do not have to put any include or exclude masks if you want all userids to be reported on.

Report JCL

```

//AACTLCDS DD *
INCLUDE=IBMUSER*
EXCLUDE=USERIBM*
SUMMARY
//*
//AASYSIN DD *
//*

```

Control Cards

INCLUDE

Specify a mask to screen the input records and determine what records are to be included. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to userid. A maximum of 10 INCLUDE statements may be entered, however, you are not required to enter any include mask statements.

INCLUDE=IBMUSER* Includes all userids beginning with IBMUSER.

EXCLUDE Specify a mask to screen the input records and determine what records are to be excluded. The value must be a generic mask with an "*" as the last character. The mask screens the input records according to userid. A maximum of 10 EXCLUDE statements may be entered.

EXCLUDE=USERIBM* Excludes all userids beginning with USERIBM.

Dataset Profile and Permission Report

Provides a detailed report of dataset profiles and any permissions they have by High Level Qualifier.

```

Reports ----- SSA ----- Reports
                        Dataset Profile and Permission Report
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): S
-----
Report Specifications (Do you want to include....):
-----
                        Summary (Y/N): Y

HLQs (A generic mask can be specified - i.e., SYS*):
==> SYS1*      ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>
==>           ==>      ==>      ==>      ==>

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Report Data Selection

Summary	Indicate if you want a summary produced.
HLQs	You must enter at least one HLQ. The entry can be a generic mask (that is, all dataset profiles starting with SYS would be SYS*). It is also important to note that you can put a single asterisk as an entry; reporting will be done on all dataset profiles and any permissions they may have. However, specifying any kind of mask may cause the report process to run for a considerable amount of time.

Report JCL

```

//AACTLCDS DD *
SUMMARY
//*
//AASYSIN DD *
SYS1*
//*
  
```

Control Cards

HLQ (variable)	Specify at least one HLQ to report on. Each HLQ must be on a separate line starting in column 1. The entry can be a mask to encompass more than 1 HLQ.

RACF to Master Catalog Comparison Report

Report shows where catalog entries are not protected by RACF profiles and RACF dataset profiles that are not protecting any cataloged datasets.

```

Reports ----- SSA ----- Reports
              RACF to Master Catalog Comparison Report
Command ==>

              Operational Mode (Batch/Online) ==> BATCH
-----
              Direct Report Output to Sysout or Dataset (S/D): S
-----
              Report Specifications (Do you want to include....):
-----
              Summary (Y/N): Y

              Master Catalog ==> SYS1.CATALOG

              Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Report Data Selection

Summary	Indicate if you want a summary produced.
Master Catalog	Enter the master catalog you want analyzed. This must be entered and must be the master catalog on your system to insure the validity of the report. Also, it is equally important that the SSA stored RACF information is up to date with the master catalog being used.

Report JCL

Report 21 uses most of the standard report JCL shown on page 63. Below are the changes necessary for this report program to run successfully.

```

//SYSIN      DD   DSN=&TEMP01,DISP=(,PASS),
//            UNIT=SYSDA,
//            SPACE=(CYL,(5,5),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=7440)
//SYSPRINT DD   DSN=&TEMP02,DISP=(,PASS),
//            UNIT=SYSDA,
//            SPACE=(CYL,(5,5),RLSE)
//AASYSIN     DD   DSN=&TEMP03,DISP=(,PASS),
//            UNIT=SYSDA,
//            SPACE=(CYL,(5,5),RLSE),
//            DCB=(RECFM=FB,LRECL=80,BLKSIZE=7440)
//AAREPORT DD   SYSOUT=*,
//            DCB=(RECFM=FBA,LRECL=133)
//AACTLCDS DD   *
CATALOG=SYS1.CATALOG
SUMMARY
//*

```

Control Cards

CATALOG	Enter the master catalog you want analyzed. Do not enter a user catalog, the results are unpredictable.



CHAPTER 4

Online Generic Searches

Generic searches provides a query facility to find information within your RACF database. You can search for specific RACF resources by fully qualifying your search arguments, or you can use wildcards to select a range of data that meets your filter criteria.

A generic search can be conducted in batch or online mode. In online mode, after a search is completed and the results are displayed, you can then use up to 30 additional SSA or RACF functions against the search results. In batch mode, you can use the standard report layout, or build a report filter that specifies the format of search results.

Generic Search Global Conventions

Security: Each Generic Search option invocation is protected in both online and batch mode. Security administrators can define a high-level profile to cover all Generic Search options, or more specific profiles to restrict certain options to selected users.

The following table lists each Generic Search, and the fully qualified RACF profile checked for authorized access. The default general resource class is MAA\$RULE and the access required is READ.

Online Generic Search Option	RACF Profile
General Userid	MEGASOLVE-SSA.ONLGEN.USER
Userid TSO Segment	MEGASOLVE-SSA.ONLGEN.USERTSO
Userid CICS Segment	MEGASOLVE-SSA.ONLGEN.USERCICS
Userid DFP Segment	MEGASOLVE-SSA.ONLGEN.USERDFP
Userid Language Segment	MEGASOLVE-SSA.ONLGEN.USERLANGUAGE
Userid OPERPARM Segment	MEGASOLVE-SSA.ONLGEN.USEROPERPARM
Userid WORKATTR Segment	MEGASOLVE-SSA.ONLGEN.USERWORKATTR
Userid NETVIEW Segment	MEGASOLVE-SSA.ONLGEN.USERNETVIEW
Userid OMVS Segment	MEGASOLVE-SSA.ONLGEN.USEROMVS
Userid DCE Segment	MEGASOLVE-SSA.ONLGEN.USERDCE
RRSF Associations	MEGASOLVE-SSA.ONLGEN.USERRRSF
Connects	MEGASOLVE-SSA.ONLGEN.USERCONNECTS
CLAUTH Authorities	MEGASOLVE-SSA.ONLGEN.USERCLAUTH
Userid Security Categories	MEGASOLVE-SSA.ONLGEN.USERSECCATS
General Group	MEGASOLVE-SSA.ONLGEN.GROUP
Group DFP Segment	MEGASOLVE-SSA.ONLGEN.GROUPDFP
Group OMVS Segment	MEGASOLVE-SSA.ONLGEN.GROUPOMVS
General Dataset	MEGASOLVE-SSA.ONLGEN.DATASET
Dataset Permissions	MEGASOLVE-SSA.ONLGEN.DATASETPERMS
Dataset Security Categories	MEGASOLVE-SSA.ONLGEN.DATASETSECCATS
General Resource	MEGASOLVE-SSA.ONLGEN.RSCE
General Resource Permissions	MEGASOLVE-SSA.ONLGEN.RSCEPERMS
General Resource Members	MEGASOLVE-SSA.ONLGEN.RSCEMEMBERS

Online Generic Search Option	RACF Profile
General Resource Session Segment	MEGASOLVE-SSA.ONLGEN.RSCESESSION
General Resource DLFDATA Segment	MEGASOLVE-SSA.ONLGEN.RSCEDLF
General Resource STDATA Segment	MEGASOLVE-SSA.ONLGEN.RSCESTC
General Resource SystemView Segment	MEGASOLVE-SSA.ONLGEN.RSCESYSVIEW
General Resource Security Categories	MEGASOLVE-SSA.ONLGEN.RSCESECCATS

Security Details SSA Security for Online Generic Searches uses a proprietary protection scheme that allows the protection of ISPF panel options. Call for more information.

Using Online Generic Searches SSA has 28 search categories: everything from general userid information to general resource started task information. Below is the Online Generic Search main menu from which you must pick the information category you wish to explore and what type of search capability you wish to use.

Online Generic Search Main Menu

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Main Menu
Option ==>

                               Standard or Extended Search (S/E) ==> E

 1 General User Information
 2 TSO Segment              3 CICS Segment          4 DFP Segment
 5 LANGUAGE Segment        6 OPERPARM Segment    7 WORKATTR Segment
 8 NETVIEW Segment         9 OMVS Segment        10 DCE Segment
11 RRSF                    12 Connects           13 Clauth Authorities
14 Security Categories

15 General Group Information
16 DFP Segment             17 OMVS Segment

18 General Dataset Profile Information
19 Permissions             20 Security Categories

21 General Resource Profile Information
22 Permissions             23 Members              24 Session Segment
25 DLFDATA Segment        26 Started Task Segment 27 SystemView Segment
28 Security Categories

                               Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Choose a Search Type

Standard Search

Standard Searching uses ISPF search capabilities to retrieve the information required. Character fields, like a userid, can contain either an explicit value or a masked value. The masking only uses the '*' and is a left to right search. For example:

Character Field Examples

- An example of an explicit value is to request a search that only displays the user USERBOB.

```
userid      ==> USERBOB                      EQ
```

- An example of a masked value is to request a search that displays all userids that begin with CICS.

```
userid      ==> CICS*                          EQ
```

Specific value character fields contain fixed values like 'Y', a date format, or an access level like READ.

Specific Value Character Field Examples

- Display all users that have the global SPECIAL attribute.

```
Special (Y/N/*):  Y
```

- Display all users that DO NOT have a TSO segment.

```
TSO (Y/N/*):      N
```

Character fields or data fields can be subjected to not only a mask but also logical operator fields. For example:

Logical Operator Fields

EQ	is equal to
NE	is not equal to
LT	is less than
GT	is greater than
LE	is less than or equal to
GE	is greater than or equal to

Extended Search

Extended Searching uses a combination of ISPF search capabilities and SSA proprietary capabilities that enhance the standard search capabilities greatly. Character fields, like a userid, can contain either an explicit value or a masked value but DO NOT use a logical operator. The condition is always equal. Extended masking allows you to do a number of distinct searches utilizing the following rules:

- An asterisk by itself indicates an all inclusive mask (that is, '*').
- An asterisk at the end of a string does a left to right mask (that is, 'user*').

- An asterisk at the beginning and end of a string searches for that text through out the string (that is, '*ken*').
- A percent sign '%' masks an individual character and can be used multiple times (that is, 'user%%%%').
- An asterisk used in any other fashion is interpreted as a non masking character (that is, 'user*bob*').

Below are some examples:

Character Field Examples

- An example of an explicit value is to request a search that only displays the user USERBOB.

```
Userid      ==> USERBOB
```

- An example of a masked value is to request a search that displays all userids that begin with CICS.

```
Userid      ==> CICS*
```

- An example of searching for the characters BOB in the users name field.

```
Userid Name ==> *BOB*
```

- An example of single character masking is to request a search that displays all userids that are seven characters long and the third character is X.

```
Userid      ==> %%X%%%%%
```

Note Extended Searching only applies to fields that are 3 characters or longer and do not have a set value list (that is, UACC on dataset profiles).

Operational Mode: Batch or Online

Batch Mode

BATCH mode processing generates the SSA JCL necessary to create the report you requested based upon your selections. The batch process involves the following steps:

- 1 After indicating what search category you want to use and what type of search (standard or extended), you must enter the search criteria that determines what records are to be included in the report. Below is an example of the standard generic search criteria specification screen.:

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                General User Information
Command -->
                                Operational Mode (Batch/Online) --> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Enter your search criteria below:
                                More:      +

Userid      --> *                      EQ
Userid Name --> *                      EQ
Default Group --> *                   EQ
Owner       --> *                      EQ
Create-Date --> *                      EQ
Last-Used-Date --> *                   EQ
Last-Used-Time --> *                   EQ
Model Dataset --> *                   EQ
Revoke Date --> *                      EQ
Resume Date --> *                      EQ

Attributes:
Special (Y/N/*): * Operations (Y/N/*): * Audit (Y/N/*): *
GRPACC (Y/N/*): * Uaudit (Y/N/*): * ADSP (Y/N/*): *
Oidcard (Y/N/*): * Revoke (Y/N/*): *

Password Related:
PSW-INTVL      --> *
Passdate       --> *
Unsuccessful Logon Attempts --> *
Password Generation Number --> *
Need Password To Logon (Y/N/*): *

Segments:
TSO (Y/N/*): * CICS (Y/N/*): * DFP (Y/N/*): *
Operparm (Y/N/*): * DCE (Y/N/*): * NetView (Y/N/*): *
OMVS (Y/N/*): * Language (Y/N/*): * WorkAttr (Y/N/*): *

Other: RRSF (Y/N/*): * CLAUTH (Y/N/*): *

Security Information Related:
Default Security Label --> *
Security Level (Numeric) --> *
Security Level Name --> *
Security Categories (Y/N/*): *

Logon Days:
Monday (Y/N/*): * Tuesday (Y/N/*): * Wednesday (Y/N/*): *
Thursday (Y/N/*): * Friday (Y/N/*): * Saturday (Y/N/*): *
Sunday (Y/N/*): *

Logon Times:
Start Time --> *
End Time --> *

Installation Data --> *

                                <-- EQ
                                Hit Enter to Continue PF03=EXIT/PF01=HELP

```

- 2** After entering your search criteria, you are presented with the Adhoc Report Generation options. For a full explanation of the choices available here, please see the Adhoc Report Generation part of this section.

Use Default Report Layout Indicate if you want to use the default report layout or create and adhoc report mask for the Online Generic Search report to use.

Include Titles On Report Indicate if you want titles to be printed on the report. This option is available mainly to assist a user who just wants to generate a listing of information with no titles or page breaks.

Include Summary	Indicate if you want a summary printed that includes totals and the masking used to produce the report.
Company on Title	Enter a value to override the company field on the report title. The default is SSA and the version.
New Report Title	Enter a value to override the initial title field on the report. This is not related to the adhoc report mask titles you might put in if you are using a mask. The default is the function being used (that is, General Userid Information Generic Search).

Note For a complete explanation of the control cards used to indicate these choices, see the Adhoc Report Generation part of this chapter.

Adhoc Report Generation Options

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                General User Information
Command ==>
                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Adhoc Report Generation -----
                                Command ==>
Use |                               Use Default Report Layout (Y/N): Y
Use |                               Include Titles On Report  (Y/N): Y
Def |                               Include Summary          (Y/N): Y
Own |
Cre |
Las |                               Company on Title ==> _____
Las |                               New Report Title ==>  _____
Mod |
Ins |                               Hit Enter to Continue    PF03=EXIT/PF01=HELP
                                -----
                                <==
                                Hit Enter to Continue    PF03=EXIT/PF01=HELP

```

- 3 If you chose to create an adhoc report mask and not use the default report layout, you will be presented with the Adhoc Report Input panel. For a full explanation of this panel and its fields, please see the Adhoc Report Generation part of this section.

```

Adhoc Report Generation ----- SSA ----- Adhoc Report Generation
                                Adhoc Report Input
Command ==>

        Enter the Adhoc Layout you Want to Produce. Leave all
        lines blank if you want the report to use the default.

Title Lines:
Line 1 ==> _____
           ==> _____
Line 2 ==> _____
           ==> _____
Line 3 ==> _____
           ==> _____
Line 4 ==> _____
           ==> _____

Substitution Lines:
Line 1 ==> _____
           ==> _____
Line 2 ==> _____
           ==> _____
Line 3 ==> _____
           ==> _____
Line 4 ==> _____
           ==> _____
Line 5 ==> _____
           ==> _____

                                Hit Enter to Continue    PF03=EXIT/PF01=HELP

```

- 4** Next, you will be prompted to indicate how you want the entries in the report sorted. For a full explanation see the Sort Mode part of this section.

```

Onl .----- SSA -----
Co  Command ==>

        Enter the number of the field and the sort direction below.

                                Available Fields:
                                1. SEL      3. NAME      5. PROFILE OWNER  7. LAST USED DATE
                                2. USERID  4. DEFAULT GROUP  6. CREATE DATE   8. REVOKE

U  -----
U  Sort  Field      Sort
D  Order Number  Direction (A,D)  Description
O
C   1      2        A          USERID,ASCENDING
L   2      -        -
L   3      -        -
M   4      -        -
   5      -        -
I   6      -        -
   7      -        -
   8      -        -

                                Hit Enter to Continue    PF03=EXIT/PF01=HELP

```

- 5** After indicating how you want the report sorted, you will proceed to the Review Generated JCL panel as shown below. If you chose to not use the default layout, you will be presented with the adhoc report input screen which is described in complete detail in the Adhoc Report Generation part of this section.


```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'DEMO001.SSA.TEMP.JCL(BATCH) '

OPTION ==> E

Enter E to Edit the Generated JCL
V to View the Generated JCL
S to Submit the Generated JCL
ST to Store the Generated JCL
SC to Schedule the Generated JCL

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

- E Select E if you want to be placed in an EDIT session.
- V Select V if you want to be placed in a VIEW session.
- S Select S if you want to submit the generated JCL.
- ST Select ST if you want to store the generated JCL in the SSA storage facility.
- SC Select SC if you want to schedule the generated JCL through The SCHEDULER. For details on scheduling, please see ‘The SCHEDULER’ on page 269.

JCL Mechanics

All online generic search adhoc report generation options use the same JCL. Below is a sample of that JCL.

```

/*
/*
/******
/**
/**          SMART SECURITY ADMINISTRATOR          **
/**
/**          VERSION V.V                          **
/**
/** (C) YYYY UNICOM SYSTEMS, INC.                  **
/**          ALL RIGHTS RESERVED                   **
/******
/*
/* JCL CREATED BY USER01
/* JCL CREATED ON MM/DD/YYYY
/* JCL CREATED AT 14:37
/*
/* JOB FUNCTION: GENERAL_USER_INFORMATION_GENERIC_SEARCH
/*
//STEP010 EXEC PGM=IKJEFT01,
//          DYNAMNBR=30,TIME=1440,REGION=4096K
//SYSPROC DD DISP=SHR,
//          DSN=SSA.ISPCLIB
//ISPPROF DD DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
//          DCB=(LRECL=80,BLKSIZE=6160,
//          RECFM=FB),UNIT=SYSALLDA
//ISPPLIB DD DISP=SHR,
//          DSN=SSA.ISPPLIB
//ISPSLIB DD DISP=SHR,
//          DSN=SSA.ISPSLIB
//ISPMLIB DD DISP=SHR,

```

```
//          DSN=SYS1.SISPMENU
//          DD  DISP=SHR,
//          DSN=SSA.ISPMLIB
//ISPTLIB DD  DISP=SHR,
//          DSN=SYS1.SISPTENU
//AADBTLIB DD  DISP=SHR,
//          DSN=SSA.RACFDATA.ISPTLIB
//STEPLIB DD  DISP=SHR,
//          DSN=SSA.LOADLIB
//ISPCTL1 DD  DSN=&CNTL1,DISP=(,PASS),UNIT=SYSALLDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//ISPCTL2 DD  DSN=&CNTL2,DISP=(,PASS),UNIT=SYSALLDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//SYSTSPRT DD  SYSOUT=*,DCB=(BLKSIZE=19019,
//          LRECL=133,RECFM=FBA)
//SYSPRINT DD  SYSOUT=*,DCB=(BLKSIZE=20000,
//          LRECL=200,RECFM=FBA)
//ISPLOG DD  SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
//SYSOUT DD  SYSOUT=*
//TEMPWK01 DD  UNIT=SYSALLDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK02 DD  UNIT=SYSALLDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK01 DD  UNIT=SYSALLDA,SPACE=(CYL,(5,5),RLSE)
//AARPTOUT DD  SYSOUT=*,
//          DCB=(RECFM=FBA,LRECL=133)
//AASYSIN DD  *
AAUSER=X*
//*
//AACTLCDS DD  *
LINE=PER-PAGE=55
SORT1=AAUSER,CH,A
SUMMARY
//*
//SYSTSIN DD  *
ISPSTART PGM(AAGSRU01)
//*
```

JCL DDs

Below is a brief explanation of the DDs and what they must reference:

SYSPROC	Must reference the SSA CLIST library
ISPPLIB	Must reference the SSA Panel library
ISPSLIB	Must reference the SSA Skeleton JCL library
ISPMLIB	Must reference the ISPF system message library and the SSA ISPF message library
ISPTLIB	Must reference the ISPF table library
AADBTLIB	Must reference the SSA RACF information table library
STEPLIB	Must reference the SSA APF authorized load library
AARPTOUT	This DD must reference an output dataset with the following DCBs: RECFM=FB,LRECL=133,DSORG=PS
AASYSIN	This DD is where the search criteria is specified. See the Adhoc Report part of this section for details.
AACTLCDS	Must reference the control cards for the adhoc report program. See the Adhoc Report part of this section for details.

SYSTSIN This DD is where the SSA program for activating adhoc command generation is entered.

Note Instructions on specifying the generic search parameters and adhoc mask entries when running online generic searches in batch is in the Adhoc Report Generation part of this section.

Online Mode

Online mode processes the search immediately and places you in a search results screen. Below is an example of the general userid information search results screen. General Userid Information Search Results Screen:

Online Generic Searches			SSA		Online Generic Searches		
General User Information							
Command ==>				Scroll ==> CSR			
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V							
SEL	Userid	Name	Default Group	Profile Owner	Create Date	Last-Used Date	Rvk?
___	AASTC01	STARTED TASK	STARTASK	STARTASK	1997-03-05	1998-06-03	N
___	APPC	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCH	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCHINT	STARTED TASK	STARTASK	STARTASK	1996-10-21	1998-05-29	N
___	BLSJPRMI	#####	STARTASK	STARTASK	1995-06-13	1998-05-29	N
___	BMLTDRB	RAY FONFIELD	BMLTD	BMLTD	1997-05-27		N
___	BMLTDSO	STEVE TREND	BMLTD	BMLTD	1997-05-27		N
___	CICSTART	#####	STARTASK	STARTASK	1996-06-19	1996-06-19	N
___	CICSUSER	#####	CICS	CICS	1996-10-21	1998-06-01	N
___	DCEKERN	#####	STARTASK	STARTASK	1995-10-30		N
___	DSN3UR00	STARTED TASK	STARTASK	STARTASK	1996-10-21		N
___	DUMPSRV	STARTED TASK	STARTASK	STARTASK	1995-10-19	1998-05-29	N
___	EZAFTPAP	#####	STARTASK	STARTASK	1996-06-26	1998-02-14	N
___	FTPSERVE	STARTED TASK	STARTASK	STARTASK	1997-02-13	1998-06-11	N
___	GTF	STARTED TASK	STARTASK	STARTASK	1996-06-10	1996-06-10	N

You can select any of the entries from the search results screen for further processing. Scroll DOWN to view all entries that met the search criteria. If you selected entries, those selections have specific effects on further processing. The table below summarizes this effect.

	Various Mode	Ad-Hoc Mode	Print Mode	Sort Mode
Selections Made	Required	Allowed; only those selected will be processed.	Allowed; only those selected will be processed.	Not Applicable; however any selections made will be retained.
No Selections Made	Not Allowed	All entries will be used	All entries will be used.	Not Applicable

Determine what to do with the search results or selections:

After you have successfully completed a generic search, SSA will present a table display as show above, showing the results that meet your criteria. At this point you have several modes for processing the information.

Various (V)	This mode will allow you to select up to 30 additional SSA or RACF commands or functions to use against the selections from the search results. For example, you may do a RACF LU command, an SSA List User, or a 'Pass To' the SSA Replicate User.
Ad-Hoc (A)	This mode will allow you to generate 'ad-hoc' commands using either all or your specific selections from the search results screen.
Print (P)	This mode will format a report using either all or your specific selections from the search results screen which then can be printed.
Sort (S)	This mode will sort the search results based on the order of your own choosing. For example, you may Sort a Userid results screen by Default Group.

Note For Print and Ad-hoc modes you may choose to use all search results that met your search criteria, or you may select specific entries to Print or generate Ad-hoc commands.

Short/Long Displays

SSA provides the ability to display the search results screen in either a Short or Long format. This option may be changed by specifying a Y or N for the Report Menu Format (Long/Short) option field in Enter Configuration Values off of option 10 - Configuration from the SSA Main menu, or by executing the AASHORT or AALONG CLIST.

```

Configuration ----- SSA ----- Configuration
Command ==>

                        Enter Configuration Values

Sort or Work Areas           ==> SYSALLDA
Temporary Datasets           ==> SYSALLDA
Allocation Prefix             ==> IBMUSER

Operational Information:
Lines Per Page (Print Parm)   ==> 55
Report Menu Format (Long/Short) ==> SHORT
More: -

```

To change to the long displays execute AALONG from anywhere in ISPF.

```

Online Generic Searches ----- SSA ----- Online Generic
Searches

                        Main Menu

Option ==> TSO AALONG
                        Standard or Extended Search (S/E) ==> S

1 General User Information
2 TSO Segment           3 CICS Segment           4 DFP Segment
5 LANGUAGE Segment      6 OPERPARM Segment      7 WORKATTR Segment
8 NETVIEW Segment       9 OMVS Segment          10 DCE Segment

```

To change to the short displays execute AASHORT from anywhere in ISPF.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Main Menu
Option ==> TSO AASHORT
                                Standard or Extended Search (S/E) ==> S

1 General User Information
2 TSO Segment                3 CICS Segment                4 DFP Segment
5 LANGUAGE Segment          6 OPERPARM Segment          7 WORKATTR Segment
8 NETVIEW Segment           9 OMVS Segment              10 DCE Segment

```

Note The example search results screens in the manual show only the SHORT displays.

Process generated commands or print reports

Anytime that you use Online Generic Search reporting or command generation options, the following screens will be displayed for further processing.

```

Process Generated Commands ----- SSA ----- Process Generated Commands
Command ==>                                Scroll ==> CSR

                                Action Command                Action Taken
                                -----
                                AAEXEC                        Execute Commands Immediately
                                AABATCH                       Place Commands in Batch JCL
                                AASCHED                       Schedule Commands
                                AASTORE                       Store or Retrieve Commands

EDIT ----- USER02.TSCSSA.ADHOC.OUTPUT----- COLUMNS 00001 00072
***** ***** Top of Data *****
=NOTE= COMMANDS ARE READY FOR EXECUTION
000001 ALTUSER USER02 PASSWORD RESUME
000002 CONNECT USER02 GROUP(SYS1) OW(SYS1)
000003 ALTUSER USER02 NOCICS
000004 ALTUSER USER01 PASSWORD RESUME
000005 CONNECT USER01 GROUP(SYS1) OW(SYS1)
000006 ALTUSER USER01 NOCICS
***** ***** Bottom of Data *****

```

To process the generated commands execute the listed Action Commands by typing the command on the command line.

- AAEXEC:** The commands generated will be executed immediately. Each command being displayed on the screen as they are executed.
- AABATCH** Encapsulates your commands in an IKJEFT01 step. Use the TSO SUBMIT command to run the job.
- AASCHED** Interfaces with SSA's The SCHEDULER to schedule the generated commands to be run on a specific date and time.
- AASTORE** Allows storage of, and retrieval of (previously stored), generated commands.

```

Print Parms ----- SSA ----- Print Parms
Command ==>                                Scroll ==> CSR

                                Do you want to print this display (Y/N): Y

                                Sysout ==> A Copies ==> 01 Title ==> N
                                Hold (Y/N) ==> N Page Length ==> 55 Destination ==>

BROWSE - USER02TSCSSA.REPORT.OUTPUT ----- LINE 00000000 COL 001 080
***** ***** Top of Data *****
1
Date: 07/03/1998
Time: 14:16

                                SSA Version
                                Generic UserID Table Repor

```

To print the report to the appropriate SYSOUT class you must specify Y in the 'print this display' field, and then press the PF03 (END) key.

Note The Hold, Copies, Page Length, and Title fields on this panel are for the DSPRINT command. Please refer to your IBM documentation for a full description of these fields.

The remainder of this section of the manual is divided as follows:

- A) Initial Generic Search screens, search examples, search result screens, and available Various Mode Functions.
- B) Online Generic Search Result Functions
- C) Adhoc Report Generation

General User Information

Initial Generic Search screen for general Userid information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                General User Information
Command -->
                                Operational Mode (Batch/Online) --> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S
                                -----
                                Enter your search criteria below:
                                More:      +

Userid      --> *                      EQ
Userid Name --> *                      EQ
Default Group --> *                   EQ
Owner       --> *                      EQ
Create-Date --> *                      EQ
Last-Used-Date --> *                   EQ
Model Dataset --> *                   EQ
Revoke Date --> *                      EQ
Resume Date --> *                      EQ

Attributes:
  Special (Y/N/*): * Operations (Y/N/*): * Audit (Y/N/*): *
  GRPACC (Y/N/*): * Uaudit (Y/N/*): * ADSP (Y/N/*): *
  Oidcard (Y/N/*): * Revoke (Y/N/*): *

Password Related:
  PSW-INTVL      --> *                      EQ
  Passdate       --> *                      EQ
  Unsuccessful Logon Attempts --> *          EQ
  Password Generation Number --> *          EQ
  Need Password To Logon (Y/N/*): *
  Never Logged On (Y/N/*): *

Segments:
  TSO (Y/N/*): * CICS (Y/N/*): * DFP (Y/N/*): *
  Operparm (Y/N/*): * DCE (Y/N/*): * NetView (Y/N/*): *
  OMVS (Y/N/*): * Language (Y/N/*): * WorkAttr (Y/N/*): *

Other: RRSF (Y/N/*): * CLAUTH (Y/N/*): *

Security Information Related:
  Default Security Label --> *                      EQ
  Security Level (Numeric) --> *                      EQ
  Security Level Name --> *                      EQ
  Security Categories (Y/N/*): *

Logon Days:
  Monday (Y/N/*): * Tuesday (Y/N/*): * Wednesday (Y/N/*): *
  Thursday (Y/N/*): * Friday (Y/N/*): * Saturday (Y/N/*): *
  Sunday (Y/N/*): *

Logon Times:
  Start Time --> *                      EQ
  End Time --> *                      EQ

Installation Data --> *

                                <--      EQ
                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids in SYSTEMS default Group that begin with MVS.

```

Userid          ==> MVS*
Default Group   ==> SYSTEMS
EQ
EQ

```

Online Generic Searches ----- SSA ----- Online Generic Searches							
General User Information							
Command ==>		Scroll ==> CSR					
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V							
SEL	Userid	Name	Default Group	Profile Owner	Create Date	Last-Used Date	Rvk?
---	---	---	---	---	---	---	---
___	AASTC01	STARTED TASK	STARTASK	STARTASK	1997-03-05	1998-06-03	N
___	APPC	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCH	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCHINT	STARTED TASK	STARTASK	STARTASK	1996-10-21	1998-05-29	N
___	BLSJPRMI	#####	STARTASK	STARTASK	1995-06-13	1998-05-29	N
___	BMLTDRB	RAY FONFIELD	BMLTD	BMLTD	1997-05-27		N
___	BMLTDS	STEVE TREND	BMLTD	BMLTD	1997-05-27		N
___	CICSTART	#####	STARTASK	STARTASK	1996-06-19	1996-06-19	N
___	CICSUSER	#####	CICS	CICS	1996-10-21	1998-06-01	N
___	DCEKERN	#####	STARTASK	STARTASK	1995-10-30		N
___	DSN3UR00	STARTED TASK	STARTASK	STARTASK	1996-10-21		N
___	DUMPSRV	STARTED TASK	STARTASK	STARTASK	1995-10-19	1998-05-29	N
___	EZAFTPAP	#####	STARTASK	STARTASK	1996-06-26	1998-02-14	N
___	FTPSEVE	STARTED TASK	STARTASK	STARTASK	1997-02-13	1998-06-11	N
___	GTF	STARTED TASK	STARTASK	STARTASK	1996-06-10	1996-06-10	N

Various Mode Available Functions

- A) SSA List User
- B) Display Connects
- C) Display DATASET Profiles (HLQ=USERID)
- D) Display Permits to DATASET Profiles
- E) Display Permits to General Resources
- F) Edit Installation Data
- G) Display TSO Segment
- H) Display CICS Segment
- I) Display LANGUAGE Segment
- J) Display WORKATTR Segment
- K) Display DFP Segment
- L) Display OPERPARM Segment
- M) Display OMVS Segment
- N) Display NETVIEW Segment
- O) Display DCE Segment
- P) Display RRSF Information
- Q) Pass to Replicate User
- R) Pass to Remove All References
- S) Pass to Password Administration
- T) Pass to Connect Administration
- U) Pass to Transfer UserID
- V) Pass to Transfer Ownership
- W) Pass to Transfer Notifications

- X) Pass to Access Report
- Y) Pass to Ownership Report
- Z) List Catalog Entry (LISTC Command)
 - 1) Display Security Categories
 - 2) Display CLAUTH Authorities
 - 3) RACF LISTUSER

Userid TSO Segment

Initial generic search screen for Userid TSO Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid TSO Segment
Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid           ==> *           EQ
Userid Name      ==> *           EQ
Logon Procedure  ==> *           EQ
Region Size      ==> *           EQ
Max Region Size  ==> *           EQ
Unit             ==> *           EQ
Destination      ==> *           EQ
Hold Class       ==> *           EQ
Job Class        ==> *           EQ
Message Class    ==> *           EQ
Sysout Class     ==> *           EQ
Userdata         ==> *           EQ
Performance Grp  ==> *           EQ
Default Logon SecLabel ==> *     EQ
Account Number   ==> *           EQ
Command Issued at Logon ==> *     EQ

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with TSO and have a region size of 4096 or greater.

```

Userid           ==> TSO*           EQ
Region Size      ==> 4096           GE

```

- Search for all Userids that do NOT have a Logon Procedure of TSOUSER.

```

Logon Procedure ==> TSOUSER           NE

```

- Search for all Userids that begin with PAY and have a User Data value of 01010101.

```

Userid           ==> PAY*           EQ
Userdata         ==> 01010101       EQ

```

Online Generic Searches ----- SSA ----- Online Generic Searches				Userid TSO Segment				Scroll ==> CSR			
Command ==>											
				Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V							
				--- Classes ---							
SEL	Userid	Logon Procedure	Size	MaxSize	JOB	MSG	HOLD	SYSOUT	Unit		
---	---	---	---	---	---	---	---	---	---		
---	BMLTDRB	ADMIN510	0006144	0000000	J	M	H	M	SYSALLDA		
---	BMLTDSD	ADMIN510	0006144	0000000	J	M	H	M	SYSALLDA		
---	MEGAM0	ADMIN510	0006144	0000000							
---	MEGAPO	ADMIN510	0006144	0000000							
---	MEGAPX0	ADMIN510	0006144	0000000					SYSALLDA		
---	MEGAPY0	ADMIN510	0006144	0000000					SYSALLDA		
---	USER02	ADMIN510	0006144	0000000	J	M	H	M	SYSALLDA		
---	TSGBXT	ADMIN510	0006144	0000000	J	M	H	M	SYSALLDA		
---	TSGMCT	ADMIN510	0006144	0000000					SYSALLDA		
---	TSGMXT	ADMIN510	0006144	0000000					SYSALLDA		

Various Mode Available Functions

- A) SSA List User
- B) Rebuild TSO Segment
- C) Remove TSO Segment
- D) Issue TSO Segment Command
- E) Display DATASET Profiles (HLQ=USERID)
- F) Display Permits to DATASET Profiles
- G) Display Permits to General Resources
- H) Pass to Replicate User
- I) Pass to Remove All References
- J) Pass to Password Administration
- K) Pass to Transfer UserID
- L) Pass to Transfer Ownership
- M) Pass to Transfer Notifications
- N) Pass to Access Report
- O) Pass to Ownership Report
- P) List Catalog Entry (LISTC Command)
- Q) RACF LISTUSER

Userid CICS Segment

Initial generic search screen for Userid CICS Segment information.

Online Generic Searches ----- SSA ----- Online Generic Searches

Userid CICS Segment

Command ==>

Operational Mode (Batch/Online) ==> ONLINE

Direct Report Output to Sysout or Dataset (S/D): S

Enter your search criteria below:

Userid ==> * EQ

Userid Name ==> * EQ

Operator Priority ==> * EQ

Operator Id ==> * EQ

Timeout ==> * EQ

Force (Y/N/*) ==> *

Opclasses: 01 (Y/N/*): * 02 (Y/N/*): * 03 (Y/N/*): * 04 (Y/N/*): *

05 (Y/N/*): * 06 (Y/N/*): * 07 (Y/N/*): * 08 (Y/N/*): *

09 (Y/N/*): * 10 (Y/N/*): * 11 (Y/N/*): * 12 (Y/N/*): *

13 (Y/N/*): * 14 (Y/N/*): * 15 (Y/N/*): * 16 (Y/N/*): *

17 (Y/N/*): * 18 (Y/N/*): * 19 (Y/N/*): * 20 (Y/N/*): *

21 (Y/N/*): * 22 (Y/N/*): * 23 (Y/N/*): * 24 (Y/N/*): *

Hit Enter to Continue PF03=EXIT/PF01=HELP

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with CICS and who have an OPID = XYZ.

Userid ==> CICS* EQ

Operator Id ==> XYZ EQ

- Search for all Userids that have a Operator Priority greater than 155.

Operator Priority==> 155 GT

SEARCH RESULT PANEL:

Online Generic Searches ----- SSA ----- SSA ----- Online Generic Searches

Userid CICS Segment

Command ==>

Scroll ==> CSR

Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL	Userid	Name	Opid	Operator Priority	Timeout	Force
---	BMLTDRB	RAY FONFIELD		000	00:00	N
---	BMLTDSO	STEVE TREND		000	00:00	N
---	IBMUSER			000	00:13	N
---	MEGAPXO	ENDUSER, JOSEPH		000	00:00	Y
---	MEGAPYO			000	00:00	Y
---	USER02	BILL GENUSERID		000	00:00	N
---	TSGBXT	BILL GENUSERID		000	00:00	Y
---	TSGMCT	MARY LAZARS		000	00:00	N
---	TSGMXT	LAZARS, MARY		000	00:00	Y
---	USER01	ENDUSER, JOSEPH	ABC	000	03:20	N

Various Mode Available Functions

- A) SSA List User
- B) Rebuild CICS Segment
- C) Remove CICS Segment
- D) Issue CICS Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid DFP Segment

Initial generic search screen for Userid DFP Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Userid DFP Segment

Command ==>

                Operational Mode (Batch/Online) ==> ONLINE
                -----
                Direct Report Output to Sysout or Dataset (S/D): S

                Enter your search criteria below:

Userid           ==> *           EQ
Userid Name      ==> *           EQ
Data Class       ==> *           EQ
Management Class ==> *           EQ
Storage Class    ==> *           EQ
Data Application ==> *           EQ

HitEnter to Continue PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with TUSR and have a Data Class value of ALLUSER.

```

Userid           ==> TUSR*           EQ
Data Class       ==> ALLUSER         EQ
  
```

- Search for all Userids that have a Storage Class of SYSALLDA.

```

Storage Class    ==> SYSALLDA         EQ
SEARCH RESULT PANEL:
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Userid DFP Segment
Command ==>                               Scroll ==> CSR

                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL  Userid  Data Class  Management Class  Storage Class  Data Application
---  ---
___  USER01  _____  TESTMGMT
___  TSTU004  _____  TESTMGMT
___  TSTU015  _____  TESTMGMT
___  TSTU016  _____  TESTMGMT
___  TSTU017  _____  TESTMGMT
___  TSTU048  _____  TESTMGMT
___  TSTU065  _____  TESTMGMT
___  TSTU069  _____  TESTMGMT
*****Bottomofdata*****
  
```

Various Mode Available Functions

- A) SSA List User
- B) Rebuild DFP Segment
- C) Remove DFP Segment

- D) Issue DFP Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid LANGUAGE Segment

Initial generic search screen for Userid LANGUAGE Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          Userid Language Segment

Command ==>

                          Operational Mode (Batch/Online) ==> ONLINE
-----
Direct Report Output to Sysout or Dataset (S/D): S

Enter your search criteria below:

Userid           ==> *           EQ
Userid Name      ==> *           EQ
Primary Language ==> *           EQ
Secondary Language ==> *         EQ

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with HR and have a PRIMARY LANGUAGE of Spanish.

```

Userid           ==> HR*           EQ
Primary Language ==> ESP           EQ

```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          Userid Language Segment

Command ==>                               Scroll ==> PAGE

                          Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL  Userid      Name                Primary Language  Secondary Language
-----
___  MEGAMO      MIKE ONADA                      ENU
___  MEGAPX0     ENDUSER, JOSEPH                 ENU                ESP
___  MEGAPY0     ENDUSER, JOSEPH                 ENU                ESP
___  TESTP0      JOSEPH ENDUSER                  ENU                ESP
___  TESTP03     JOSEPH ENDUSER                  ENU                ESP
___  USER02     BILL GENUSERID                 ENU                ESP
___  TSGBXT      BILL GENUSERID                 ENU                ESP
___  TSGMCT      MARY LAZARS                     ENU                ESP
___  USER01     ENDUSER, JOSEPH                 ENU                ESP
___  TSTBAT1     NEW NAME FOR BILL ID            ENU                ESP
___  TSTPA0      ENDUSER, JOSEPH TEST            ENU                ESP
___  TSTPA02     ENDUSER, JOSEPH                 ENU                ESP
___  TSTPA04     ENDUSER, JOSEPH                 ENU                ESP
___  TSTPA05     NEW NAME FIELD                  ENU                ESP
___  TSTPA06     ENDUSER, JOSEPH                 ENU                ESP
___  TSTPA07     ENDUSER, JOSEPH                 ENU                ESP

```

Various Mode Available Functions

- SSA List User
- Rebuild LANGUAGE Segment
- Remove LANGUAGE Segment

- D) Issue LANGUAGE Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid OPERPARM Segment

Initial generic search screen for Userid OPERPARM Segment information.

Online Generic Searches ----- SSA ----- Online Generic Searches

Userid Operparm Segment

Command ==>

Operational Mode (Batch/Online) ==> BATCH

Direct Report Output to Sysout or Dataset (S/D): S

Enter your search criteria below:

More: +

Userid ==> * EQ

Userid Name ==> * EQ

Cmdsys ==> * EQ

Altgrp ==> * EQ

Storage ==> * EQ

Key ==> * EQ

Del Oper Msg ==> * EQ (Normal/All/None)

Logcmdresp ==> * EQ (System/No)

Specify Y, N, or * for fields below:

Auth: Master: * All: * Info: * Cons: * Io: * Sys: *

Level: NB: * All: * R: * I: * CE: * E: * IN: *

Mform: J: * M: * S: * T: * X: *

Migid: *

UD: *

Monitor: Jobnames: * Jobnamest: *

Sess: * Sesst: * Status: *

Mscope: *: * *All: *

Routcode: All: * None: *

001: * 002: * 003: * 004: *

005: * 006: * 007: * 008: *

009: * 010: * 011: * 012: *

013: * 014: * 015: * 016: *

017: * 018: * 019: * 020: *

021: * 022: * 023: * 024: *

025: * 026: * 027: * 028: *

029: * 030: * 031: * 032: *

033: * 034: * 035: * 036: *

037: * 038: * 039: * 040: *

041: * 042: * 043: * 044: *

045: * 046: * 047: * 048: *

049: * 050: * 051: * 052: *

053: * 054: * 055: * 056: *

057: * 058: * 059: * 060: *

061: * 062: * 063: * 064: *

065: * 066: * 067: * 068: *

069: * 070: * 071: * 072: *

073: * 074: * 075: * 076: *

077: * 078: * 079: * 080: *

081: * 082: * 083: * 084: *

085: * 086: * 087: *

*88 TO 128 Routcodes Not Supported due to ISPF limitations

Hit Enter to Continue PF03=EXIT/PF01=HELP

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with OPER and have a OPERPARM Segment.

Userid ==> OPER* EQ

Online Generic Searches ----- SSA ----- Online Generic Searches									
Userid Operparm Segment									
Command ==>									
Scroll ==> PAGE									
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V									

Various Mode Available Functions

- A) SSA List User
- B) Rebuild OPERPARM Segment
- C) Remove OPERPARM Segment
- D) Issue OPERPARM Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid WORKATTR Segment

Initial generic search screen for Userid WORKATTR Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid Workattr Segment
Command ==>
                                Operational Mode (Batch/Online) ==> BATCH
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:
Userid      ==> *                      EQ
Userid Name ==> *                      EQ
Name        ==> *                      EQ
Bldg        ==> *                      EQ
Dept        ==> *                      EQ
Room        ==> *                      EQ
Addr1       ==> *                      EQ
Addr2       ==> *                      EQ
Addr3       ==> *                      EQ
Addr4       ==> *                      EQ
Accnt       ==> *                      EQ

                                <==    EQ

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with ACCT and have a Addr3 value of 1234 Any Street -7th Floor.

```

Userid      ==> ACCT*                      EQ
Addr3       ==> 1234 ANY STREET - 7TH FLOOR EQ

```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid Workattr Segment
Command ==>
                                Scroll ==> CSR

                                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL  Userid      Workattr Name
-----
___  USER02  1234567890123456789012345678901234567890NAME FLD FILLED OUT5
___  USER01
___  TSTU004  1234567890123456789012345678901234567890NAME FLD FILLED OUT5
___  TSTU015
___  TSTU016
___  TSTU017
___  TSTU045
___  TSTU047
___  TSTU048
___  TSTU065
___  TSTU069
***** Bottom of data *****

```

Various Mode Available Functions

- A) SSA List User
- B) Rebuild WORKATTR Segment

- C) Remove WORKATTR Segment
- D) Issue WORKATTR Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid NETVIEW Segment

Initial generic search screen for Userid NETVIEW Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid Netview Segment

Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid              ==> *              EQ
Userid Name         ==> *              EQ
CTL                ==> *              EQ
Default Console Name ==> *              EQ

Receive Messages   (Y/N/*) ==> *
Authorized to NGMF (Y/N/*) ==> *

Command List ==> *

                                <==      EQ

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with T and are Authorized to the NGMF Facility in NetView.

```

Userid              ==> T*              EQ
Authorized to NGMF (Y/N/*) ==> Y
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid Netview Segment

Command ==>                                Scroll ==> CSR

                                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V
  
```

SEL	Userid	Name	CTL	Default Console	Receive Messages	Authorized to Graphic Monitor
___	USER02	BILL GENUSEID	SPECIFIC	CNSOLE01	Y	N
___	USER01	ENDUSER, JOSEPH	SPECIFIC	CNSOLE01	Y	N
___	TSTU004	STRICTLY TEST USERS	SPECIFIC		N	N
___	TSTU006	STRICTLY TEST USERS	GLOBAL		N	Y
___	TSTU007	STRICTLY TEST USERS	SPECIFIC		N	N
___	TSTU008	STRICTLY TEST USERS	SPECIFIC		N	N
___	TSTU015	STRICTLY TEST USERS	SPECIFIC	CNSOLE01	Y	N
___	TSTU016	STRICTLY TEST USERS	SPECIFIC	CNSOLE01	Y	N
___	TSTU046	STRICTLY TEST USERS	SPECIFIC		Y	N
___	TSTU065	TESTTTS NEW NAME FLD	SPECIFIC	CNSOLE01	Y	N
___	TSTU069	TESTTTS NEW NAME FLD	SPECIFIC	CNSOLE01	Y	N

***** Bottom of data *****

Various Mode Available Functions

- SSA List User
- Rebuild NETVIEW Segment
- Remove NETVIEW Segment

- D) Issue NETVIEW Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid OMVS Segment

Initial generic search screen for Userid OMVS Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid OMVS Segment

Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid           ==> *                EQ
Userid Name      ==> *                EQ
UUID            ==> *                EQ
Home Path        ==> *                EQ
Default Program  ==> *                EQ

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that have a UUID that begins with 0 (zero) and has a Home Path of Root.

```

UUID           ==> 0*                EQ
Home Path      ==> /root              EQ
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid OMVS Segment

Command ==>                                Scroll ==> CSR

                                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL   Userid      Name                UID
---   -
___   DCEKERN     #####                0000000000
___   EZAFTPAP    #####                0000000000
___   IBMUSER     #####                0000000000
___   IMWEBSRV    STARTED TASK          0000000000
___   MEGAPX0     ENDUSER, JOSEPH
___   MEGAPY0
___   OMVS        STARTED TASK          0000000000
___   OMVSKERN    #####                0000000000
___   OPEN1       STRICTLY TEST USERID 0000000000
___   OPEN2       STRICTLY TEST USERID 0000000000
___   OPEN3       STRICTLY TEST USERID 0000000000
___   ROUTEDMV    #####                0000000447
___   ROUTEDOE    #####                0000000448
___   TCPIPMVS    #####                0000000445
___   TCPIPOE     #####                0000000000
  
```

Various Mode Available Functions

- SSA List User
- Rebuild OMVS Segment

- C) Remove OMVS Segment
- D) Issue OMVS Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid DCE Segment

Initial generic search screen for Userid DCE Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid DCE Segment

Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid           ==> *           EQ
Userid Name      ==> *           EQ
UUID            ==> *           EQ
Principal Name   ==> *           EQ
DCE Cell Name    ==> *           EQ
DCE Cell UUID    ==> *           EQ
Automatic Logon (Y/N/*) ==> *

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that begin with ACCT, a UUID greater than 0, and has automatic logon activated.

```

Userid           ==> ACCT*           EQ
UUID            ==> 0               GT
Automatic Logon (Y/N/*) ==> Y

```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid DCE Segment

Command ==>                                Scroll ==> CSR

                                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL  Userid      Name                      Principal UUID                      Auto-
-----
___  USER02     BILL GENUSEID             87654321-1234-1234-1234-123456789012  Y
___  USER01     ENDUSER, JOSEPH          87654321-1234-1234-1234-123456789012  Y
___  TSTU008     STRICTLY TEST USERS                     87654321-1234-1234-1234-123456789012  N
___  TSTU015     STRICTLY TEST USERS                     87654321-1234-1234-1234-123456789012  Y
___  TSTU065     TESTTTS NEW NAME FLD 87654321-1234-1234-1234-123456789012  Y
___  TSTU069     TESTTTS NEW NAME FLD 87654321-1234-1234-1234-123456789012  Y
***** Bottom of data *****

```

Various Mode Available Functions

- SSA List User
- Rebuild DCE Segment
- Remove DCE Segment

- D) Issue DCE Segment Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID
- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

Userid RRSF Associations

Initial generic search screen for Userid RRSF information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Userid RRSF Information
Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid           ==> *                EQ
Userid Name      ==> *                EQ
Target Node Name ==> *                EQ
Target Userid    ==> *                EQ
Record Version   ==> *                EQ
User Who Created Entry ==> *        EQ
Define Date      ==> *                EQ
Define Time      ==> *                EQ
Approve/Refuse Date ==> *            EQ
Approve/Refuse Time ==> *            EQ
Peer Userid      (Y/N/*) ==> *
Userid is Manager (Y/N/*) ==> *
Remote is Manager (Y/N/*) ==> *
Local Association Pending (Y/N/*) ==> *
Remote Association Pending (Y/N/*) ==> *
Password Synchronization (Y/N/*) ==> *
Error on Remote System (Y/N/*) ==> *

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that have a target UserID that begins with SYS and is a peer association.

```

Target Userid           ==> SYS*                EQ
Peer Userid (Y/N/*)     ==> Y

```

- Search for all Userids that have password synchronization active.

```

Password Synchronization (Y/N/*) ==> Y

```

Online Generic Searches ----- SSA -----					Online Generic Searches				
Userid RRSF Information									
Command ==>					Scroll ==> CSR				
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V									
SEL	Userid	Name	Target Node/Userid	Peer	Manager User/Remote		Pending Lcl/Remote		
---	---	---	---	---	---	---	---	---	
___	USER02	BILL GENUSERID	TSGNJE	TSGBXT	Y	N	N	N	
___	USER02	BILL GENUSERID	TSGNJE	WALK02	N	Y	N	N	
___	TSGBXT	BILL GENUSERID	TSGNJE	USER02	Y	N	N	N	
___	TSTU004	STRICTLY TEST USERS	TSGNJE	WALK02	Y	N	N	Y	
___	TSTU009	STRICTLY TEST USERS	TSGNJE	WALK02	Y	N	N	Y	
___	WALK01	PRODUCT WALK-THRU UI	TSGNJE	WALK02	N	N	Y	N	
___	WALK01	PRODUCT WALK-THRU UI	TSGNJE	P390C	N	N	Y	N	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	WALK01	N	Y	N	N	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	P390C	Y	N	N	N	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	P390G	Y	N	N	N	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	P390H1	N	Y	N	Y	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	WALK03	N	N	Y	N	
___	WALK02	PRODUCT WALK-THRU UI	TSGNJE	USER02	N	N	Y	N	
___	WALK03	TESTID	TSGNJE	WALK02	N	Y	N	N	
***** Bottom of data *****									

Various Mode Available Functions

- A) SSA List User
- B) Define New Association
- C) Undefine the Association For Peer Associations:
- D) Model the Association
- E) Change the Association For Managed Associations:
- F) Model the Association
- G) Change the Association
- H) Pass to Replicate User
- I) Pass to Remove All References
- J) Pass to Password Administration
- K) Pass to Transfer UserID
- L) Pass to Transfer Ownership
- M) Pass to Transfer Notifications
- N) Pass to Access Report
- O) Pass to Ownership Report
- P) RACF LISTUSER (Current Node Only)

Connect Information

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Connect Information

Command ==>

                                Operational Mode (Batch/Online) ==> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Userid      ==> *           EQ
Userid Name ==> *           EQ
Group       ==> *           EQ
Profile Owner ==> *        EQ
UACC        ==> *          EQ (None,Read,Update,Control,Alter)
UACC (Nmb)  ==> *          EQ (0=None,2=Read,3=Update,4=Control,5=Alter)
Authority   ==> *          EQ (None,Use,Create,Connect,Join)
Authority(Nmb) ==> *       EQ (0=None,1=Use,2=Create,3=Connect,4=Join)

Special (Y/N/*): *
Operations (Y/N/*): *
Auditor (Y/N/*): *
Grpacc (Y/N/*): *
ADSP (Y/N/*): *
Revoke (Y/N/*): *
NOTERMUACC (Y/N/*): *

Revoke Date ==> *           EQ
Resume Date ==> *           EQ
Date of Connection ==> *      EQ
Last Connect Date ==> *       EQ
Last Connect Time ==> *       EQ
Nmb of Racinits ==> *         EQ
Default Group (Y/N/*) ==> *

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that have group-Operations to any group.

```
Operations (Y/N/*):Y
```

- Search for all Userids that begin with CICS and have group-REVOKE.

```
Userid      ==>CICS*           EQ
Revoke (Y/N/*):  Y
```

- Search for all Userids that begin with TSO and are in groups that begin with PAY.

```
Userid      ==> TSO*           EQ
Group       ==> PAY*           EQ
```

Online Generic Searches ----- SSA ----- Online Generic Searches						
Connect Information						
Command ==>				Scroll ==> CSR		
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V						
SEL	Userid	Name	Group	Profile Owner	Authority	UACC
---	AASTC01	STARTED TASK	STARTASK	STARTASK	USE	NONE
---	AASTC01	STARTED TASK	SYS1	SYS1	USE	NONE
---	APPC	STARTED TASK	STARTASK	STARTASK	USE	NONE
---	APPC	STARTED TASK	SYS1	SYS1	USE	NONE
---	ASCH	STARTED TASK	STARTASK	STARTASK	USE	NONE
---	ASCH	STARTED TASK	SYS1	SYS1	USE	NONE
---	ASCHINT	STARTED TASK	STARTASK	STARTASK	USE	NONE
---	ASCHINT	STARTED TASK	SYS1	SYS1	USE	NONE
---	BLSJPRMI	#####	STARTASK	STARTASK	USE	NONE
---	BLSJPRMI	#####	SYS1	SYS1	USE	NONE
---	BMLTDRB	RAY FONFIELD	BMLTD	BMLTD	USE	NONE
---	BMLTDSO	STEVE TREND	BMLTD	BMLTD	USE	NONE
---	CICSTART	#####	STARTASK	STARTASK	USE	NONE
---	CICSTART	#####	SYS1	SYS1	USE	NONE
---	CICSUSER	#####	CICS	CICS	USE	NONE

Various Mode Available Functions

- A) SSA List User
- B) Re-Issue (Modify) the Connect
- C) Remove the Connect Profile
- D) Issue Connect For Another Userid
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Connect Administration
- I) Pass to Transfer UserID
- J) Pass to Transfer Ownership
- K) Pass to Transfer Notifications
- L) Pass to Access Report
- M) Pass to Ownership Report
- N) RACF LISTUSER

CLAUTH Authorities

Initial generic search screen for Userid Clauth Authorities.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          Clauth Authorities

Command ==>

                Operational Mode (Batch/Online) ==> BATCH
                -----
                Direct Report Output to Sysout or Dataset (S/D): S

                Enter your search criteria below:

Userid           ==> *                               EQ
Userid Name      ==> *                               EQ
Class            ==> *                               EQ

                Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that have CLAUTH authority to the User class.

```

Class           ==> USER                               EQ

```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          Clauth Authorities
Command ==>                               Scroll ==> CSR

                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL   Userid      Name              Class
---   -
____ SENCICS      STARTED TASK          TCICSTRN
____ USER01      ENDUSER, JOSEPH        USER
____ TSTU002      STRICTLY TEST USERS    GCICSTRN
____ TSTU004      STRICTLY TEST USERS    USER
____ TSTU004      STRICTLY TEST USERS    GCICSTRN
____ TSTU007      STRICTLY TEST USERS    TCICSTRN
____ TSTU015      STRICTLY TEST USERS    USER
____ TSTU016      STRICTLY TEST USERS    USER
____ TSTU017      STRICTLY TEST USERS    USER
____ TSTU027      STRICTLY TEST USERS    USER
____ TSTU065      TESTTTS NEW NAME FLD  USER
____ TSTU069      TESTTTS NEW NAME FLD  USER
***** Bottom of data *****

```

Various Mode Available Functions

- A) SSA List User
- B) Re-Issue the CLAUTH Authority
- C) Remove the CLAUTH Authority
- D) Issue CLAUTH Command
- E) Display Connects with Group Special
- F) Pass to Replicate User

- G) Pass to Remove All References
- H) Pass to Password Administration
- I) Pass to Transfer UserID
- J) Pass to Transfer Ownership
- K) Pass to Transfer Notifications
- L) Pass to Replicate Resource Class
- M) Pass to Transfer Resource Class
- N) Pass to Access Report
- O) Pass to Ownership Report
- P) RACF LISTUSER

Userid Security Categories

Initial generic search screen for Userid Security Categories.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                          Userid Security Categories

Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Userid      ==> *          EQ
Userid Name ==> *          EQ
Category    ==> *          EQ
Category (Nmb) ==> *      EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Userids that have the TOPSECRETINFO category.
Category ==> TOPSECRETINFO EQ
- Search for all Userids that have a security category number greater than 5.
Category (Nmb) ==> 00005 GT

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                          Userid Security Categories
                          Command ==>
                          Scroll ==> CSR

                          Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL  Userid      Name      Security Category
-----
___ TSGBXT      BILL GENUSEID  MORETOPSECRETDATA
                          Numeric Value ==> 00002
___ USER01      ENDUSER, JOSEPH  TOPSECRETDATA
                          Numeric Value ==> 00001
***** Bottom of data *****
```

Various Mode Available Functions

- A) SSA List User
- B) Re-Issue the Security Category Entry
- C) Remove the Security Category Entry
- D) Issue Security Category Command
- E) Pass to Replicate User
- F) Pass to Remove All References
- G) Pass to Password Administration
- H) Pass to Transfer UserID

- I) Pass to Transfer Ownership
- J) Pass to Transfer Notifications
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTUSER

General Group Information

Initial generic search screen for General Group information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          General Group Information

Command ==>

                          Operational Mode (Batch/Online) ==> ONLINE
                          -----
                          Direct Report Output to Sysout or Dataset (S/D): S

                          Enter your search criteria below:

Group           ==> *           EQ
Profile Owner   ==> *           EQ
Superior Group  ==> *           EQ
Model Dataset   ==> *                               EQ
Creation Date   ==> *           EQ
Default UACC    ==> *           EQ (None,Read,Update,Control,Alter)
Dflt UACC (Nmb)==> *           EQ (0=None,2=Read,3=Update,4=Control,5=Alter)
Termuacc        (Y/N/*) ==> *
Has Users       (Y/N/*) ==> *
Has Sub-Groups (Y/N/*) ==> *
Installation Data ==> *

                          <== EQ

                          Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Groups that begin with PAY and do not have any users.

```

Group           ==>          PAY*           EQ
Has Users (Y/N/*):      N
  
```

- Search for all Groups that have a superior group of HR and have sub-groups.

```

Superior Group ==>          HR           EQ
Has Sub-groups (Y/N/*):  Y
  
```

Online Generic Searches ----- SSA -----				Online Generic Searches				
General Group Information								
Command ==>				Scroll ==> PAGE				
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V								
SEL	Group	Superior Group	Profile Owner	NOTERMUACC	Has Users	Has Sub-Groups	Creation Date	Default UACC
___	\$SREVOKE	DEVL	DEVL	Y	Y	Y	1996-10-21	NONE
___	ADMIN	DEVL	DEVL	N	Y	Y	1996-10-21	NONE
___	ADMINAID	ADMIN	ADMIN	N	Y	N	1996-10-21	NONE
___	ADMINX	\$SREVOKE	\$SREVOKE	N	N	N	1997-04-14	NONE
___	BACKUP	PROD	PROD	N	N	N	1996-10-21	NONE
___	DBS	SYSTEM	SYSTEM	N	N	N	1997-03-17	NONE
___	DBSDZN	SYSTEM	SYSTEM	N	N	N	1997-03-17	NONE

Various Mode Available Functions

A) SSA List Group

- B) Display Users in Group
- C) Display DATASET Profiles (HLQ=GROUP)
- D) Display Permits to DATASET Profiles
- E) Display Permits to General Resources
- F) Edit Installation Data
- G) Display DFP Segment
- H) Display OMVS Segment
- I) Pass to Replicate Group
- J) Pass to Remove All References
- K) Pass to Transfer Group
- L) Pass to Transfer Ownership
- M) Pass to Access Report
- N) Pass to Ownership Report
- O) List Catalog Entry (LISTC Command)
- P) RACF LISTGROUP

Group DFP Segment

Initial generic search screen for Group DFP Segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Group DFP Segment

Command ==>

                Operational Mode (Batch/Online) ==> ONLINE
                -----
                Direct Report Output to Sysout or Dataset (S/D): S

                Enter your search criteria below:

Group           ==> *           EQ
Management Class ==> *           EQ
Storage Class   ==> *           EQ
Data Class      ==> *           EQ
Data Application ==> *           EQ

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Groups that begin with PAY and have a Management Class of ENDUSER.

```

Group           ==> PAY*           EQ
Management Class ==> ENDUSER       EQ
  
```

- Search for all Groups that have Storage Class of SYSDA and do not have a Data Application of DATAGRP.

```

Storage Class    ==> SYSDA           EQ
Data Application ==> DATAGRP         NE
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Group DFP Segment

Command ==>

                                Scroll ==> CSR

                Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL      Group      Management Class      Storage Class      Data Class      Data Application
-----
___ BMLTD      USERMGMT      USERSTOR      USERCLAS      USERAPPL
___ MEGA       USERMGMT      USERSTOR      USERCLAS      USERAPPL
___ SYS1       PRODMGMT      PRODSTOR      PRODCLAS      PRODAPPL
___ TSTG003    TESTMGMT      TESTSTOR      TESTCLAS      TESTAPPL
***** Bottom of data *****
  
```

Various Mode Available Functions

- A) SSA List Group
- B) Rebuild DFP Segment
- C) Remove DFP Segment

- D) Issue DFP Segment Command
- E) Display Users in Group
- F) Display Subgroups
- G) Pass to Replicate Group
- H) Pass to Remove All References
- I) Pass to Transfer Group
- J) Pass to Transfer Ownership
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTGROUP

Group OMVS Segment

Initial generic search screen for Group OMVS Segment information

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Group OMVS Segment

Command ==>

                               Operational Mode (Batch/Online) ==> ONLINE
                               -----
                               Direct Report Output to Sysout or Dataset (S/D): S

                               Enter your search criteria below:

Group      ==> *                EQ
GID        ==> *                EQ

                               Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Groups that begin with PAY.

```
Group      ==> PAY*                EQ
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                               Group OMVS Segment

Command ==>                               Scroll ==> CSR

                               Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL      Group      GID
-----
___ DCEGRP      0000000002
___ IMWEB       0000000205
___ OMVSGRP     0000000001
___ SPECIAL     0000000255
___ SYS1        0000000000
___ TSTGEMPL    0000000500
___ TSTGEXTL    0000000999
___ TTY         0000000000
***** Bottom of data *****

```

Various Mode Available Functions

- A) SSA List Group
- B) Rebuild OMVS Segment
- C) Remove OMVS Segment
- D) Issue OMVS Segment Command
- E) Display Users in Group
- F) Display Subgroups
- G) Pass to Replicate Group
- H) Pass to Remove All References
- I) Pass to Transfer Group

- J) Pass to Transfer Ownership
- K) Pass to Access Report
- L) Pass to Ownership Report
- M) RACF LISTGROUP

General Dataset Profile Information

Initial generic search screen for General Dataset profile information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Dataset Profile Information

Command ==>

                        Operational Mode (Batch/Online) ==> ONLINE
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Profile                ==> *                               More:      +
Type (G/D/M/T/*)      ==> *                               EQ
                        (G=Generic,D=Discrete,M=Model,T=Tape)
Volume                ==> *                               EQ
Owner                 ==> *                               EQ
UACC                  ==> *                               EQ (None,Execute,Read,Update,Control,Alter)
UACC (Nmb)             ==> *                               EQ (0=None,1=Exc,2=Read,3=Updt,4=Ctl,5=Alt)
Warn (Y/N/*)           ==> *
Notify                 ==> *                               EQ
Resowner              ==> *                               EQ
Level                 ==> *                               EQ
Erase (Y/N/*)          ==> *
Device Type            ==> *                               EQ
Create Date            ==> *                               EQ
Create Group           ==> *                               EQ
SecLevel               ==> *                               EQ
SecLevel (Nmb)         ==> *                               EQ
SecLabel               ==> *                               EQ
Grp Dsn (Y/N/*)        ==> *

Audit Levels:
Local Audit Level      ==> *                               EQ (All,Success,Fail,None)
Lcl Successful Audit Level ==> *                               EQ (None,Read,Update,Cntl,Alter)
Lcl Failure Audit Level ==> *                               EQ (None,Read,Update,Cntl,Alter)
Global Audit Level     ==> *                               EQ (All,Success,Fail,None)
Glb Successful Audit Level ==> *                               EQ (None,Read,Update,Cntl,Alter)
Glb Failure Audit Level ==> *                               EQ (None,Read,Update,Cntl,Alter)

Installation Data ==> *

                        <==      EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Dataset profiles that begin with SYS1 that are NOT owned by SYS1.

```

Profile                ==> SYS1*                               EQ
Owner                  ==> SYS1                               NE

```

- Search for all Dataset profiles that have the warning attribute on.

```

Warn (Y/N/*)          ==> Y
SEARCH RESULT PANEL:

```

Online Generic Searches ----- SSA -----			Online Generic Searches		
General Dataset Profile Information					
Command ==>			Scroll ==> CSR		
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V					
SEL	Dataset Profile	Type	Profile Owner	UACC	Volume
----	-----	----	-----	-----	-----
___	ADMIN.V*.ASM	G	ADMIN	NONE	
___	ADMIN.V*.COBOL	G	ADMIN	NONE	
___	ADMIN.V*.ISPTLIB	G	ADMIN	NONE	
___	ADMIN.*	G	ADMIN	NONE	
___	BACKUP.*	G	BACKUP	NONE	
___	BACKUP.SENT01.G0001V00	D	USER01	NONE	B00001
___	BMLTDRB.*	G	BMLTDRB	NONE	
___	BMLTDSD.*	G	BMLTDSD	NONE	
___	CICDZN.*	G	CICDZN	NONE	
___	CICS.*	G	CICS	NONE	
___	CICSMPE.*	G	CICSMPE	NONE	
___	CICTZN.*	G	CICTZN	NONE	
___	DBS.*	G	DBS	NONE	
___	DBSDZN.*	G	DBSDZN	NONE	
___	DBSTZN.*	G	DBSTZN	NONE	

Various Mode Available Functions

- A) SSA List Dataset
- B) Delete DATASET Profile
- C) Issue Permit Command
- D) Print List of Datasets Protected By Profile
- E) Display Permits to DATASET Profiles
- F) Edit Installation Data
- G) Pass to Replicate DATASET
- H) Pass to Transfer DATASET
- I) RACF LISTDSD

Dataset Profile Permissions

Initial generic search screen for Dataset profile permission information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Dataset Profile Permissions
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Profile      ==> *                               EQ
Type         ==> *                               EQ (G=Generic,D=Discrete,T=Tape,M=Model )
Volume       ==> *                               EQ
Access Id    ==> *                               EQ
Access Id Type ==> *                             EQ (User,Group,General,Obsolete)
Name         ==> *                               EQ (When Access Id Type is USER)
Access Level ==> *                               EQ (None,Execute,Read,Update,Control,Alter)
Acc Lvl (Nmb) ==> *                             EQ (0=None,1=Exec,2=Read,3=Updt,4=Cntl,5=Altr)
Access Type  ==> *                               EQ (STD=Standard,CND=Conditional)

If Conditional:
Conditional Class ==> *                           EQ
Conditional Entity ==> *                           EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Discrete Dataset profiles that begin with SYS1 that have obsolete access entries.

```

Profile      ==> SYS1*                           EQ
Type         ==> D                               EQ
Access Id Type ==> Obsolete                       EQ (User,Group,General,Obsolete)
  
```

- Search for all Dataset profiles where groups that begin with PAY have access.

```

Access Id    ==> PAY*                             EQ
Access Id Type ==> GROUP                           EQ
  
```

Online Generic Searches ----- SSA ----- Online Generic Searches				
Dataset Profile Permissions				
Command ==>	Scroll ==> CSR			
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V				
SEL	Dataset Profile	Access Entry	Access Level	Entry Type
----	-----	-----	-----	-----
___	ADMIN.V*.ASM	USER02	ALTER	USER
___	ADMIN.V*.ASM	MEGA	ALTER	GROUP
___	ADMIN.V*.ASM	*	NONE	GENERAL
___	ADMIN.V*.COBOL	MEGA	ALTER	GROUP
___	ADMIN.V*.COBOL	*	NONE	GENERAL
___	ADMIN.V*.ISPTLIB	USER02	ALTER	USER
___	ADMIN.V*.ISPTLIB	MEGA	ALTER	GROUP
___	ADMIN.V*.ISPTLIB	BMLTD	CONTROL	GROUP
___	ADMIN.V*.ISPTLIB	AASTC01	CONTROL	USER
___	ADMIN.V*.ISPTLIB	WALK	CONTROL	GROUP
___	ADMIN.*	MEGA	ALTER	GROUP
___	ADMIN.*	BMLTD	READ	GROUP
___	ADMIN.*	AASTC01	CONTROL	USER

Various Mode Available Functions

- A) SSA List Dataset
- B) Re-Issue the Permit
- C) Remove the Permit
- D) Issue Permit Command
- E) Print List of Datasets Protected By Profile
- F) Display Users in Group
- G) RACF LISTDSD

Dataset Profile Security Categories

Initial generic search screen for Dataset Profile Security Categories.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Dataset Profile Security Categories
Command ==>

                        Operational Mode (Batch/Online) ==> ONLINE
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Profile          ==> *                               EQ
Type             ==> *                               EQ (G=Generic,D=Discrete,T=Tape,M=Model)
Volume           ==> *                               EQ
Security Category ==> *                               EQ
SecCat (Nmb)     ==> *                               EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Discrete Dataset profiles that begin with SYS1 that have security category of TOPSECRETINFO.

```

Profile          ==> SYS1*                               EQ
Type             ==> D                                   EQ
Category         ==> TOPSECRETINFO                       EQ
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Dataset Profile Security Categories
Command ==>                                Scroll ==> CSR

                        Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL          Dataset Profile          Type  Volume  Security
-----
-----
Category ==> TOPSECRETDATA
-----
USER01.*          G                      00001
Category ==> TOPSECRETDATA
***** Bottom of data *****
  
```

Various Mode Available Functions

- A) SSA List Dataset
- B) Re-Issue the Security Category Entry
- C) Remove the Security Category Entry
- D) Issue Security Category Command
- E) Delete DATASET Profile
- F) Print List of Datasets Protected By Profile
- G) Pass to Replicate DATASET
- H) Pass to Transfer DATASET

I) RACF LISTDSD

General Resource Profile Information

Initial generic search screen for General Resource Profile information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                General Resource Information

Command -->

                                Operational Mode (Batch/Online) --> ONLINE
                                -----
                                Direct Report Output to Sysout or Dataset (S/D): S

                                Enter your search criteria below:

Profile      --> *                               More:      +
Class        --> *                               EQ
Type         --> *                               (G=Generic,D=Discrete)
Owner        --> *                               EQ
UACC         --> *                               EQ (None,Execute,Read,Update,Control,Alter)
UACC (Nmb)   --> *                               EQ (0=None,1=Exec,2=Read,3=Updt,4=Cntl,5=Altr)
Warn (Y/N/*) --> *
Notify       --> *                               EQ
Level        --> *                               EQ
Create Date  --> *                               EQ
Last Referenced Date --> *                       EQ
Last Changed Date --> *                       EQ
Security Level --> *                               EQ
SecLevel (Nmb) --> *                       EQ
Security Label --> *                       EQ

If Class - TAPEVOL:
One Dataset   (Y/N/*) --> *
Automatic Protection (Y/N/*) --> *
Table of Contents (Y/N/*) --> *

If Class - TERMINAL:
Use on Sunday   (Y/N/*) --> *
Use on Monday   (Y/N/*) --> *
Use on Tuesday   (Y/N/*) --> *
Use on Wednesday (Y/N/*) --> *
Use on Thursday  (Y/N/*) --> *
Use on Friday    (Y/N/*) --> *
Use on Saturday  (Y/N/*) --> *
Time to Logon    --> *                               EQ
Time unable to Logon --> *                       EQ
Terminals Timezone --> *                       EQ
Timezone Shift   --> *                       (E=East,W=West)

Audit Levels:
Local Audit Level --> *                       EQ (All,Success,Fail,None)
Lcl Successful Audit Level --> *               EQ (None,Read,Update,Cntl,Alter)
Lcl Failure Audit Level --> *                 EQ (None,Read,Update,Cntl,Alter)
Global Audit Level --> *                     EQ (All,Success,Fail,None)
Glb Successful Audit Level --> *             EQ (None,Read,Update,Cntl,Alter)
Glb Failure Audit Level --> *               EQ (None,Read,Update,Cntl,Alter)
Installation Data --> *

Application Data --> *                       <-- EQ

                                <-- EQ
                                Hit Enter to Continue PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all general resource profiles in the Facility Class.

```
Class      ==> Facility      EQ
```


- Search for all general resource profiles that have the warning attribute on.

Warn (Y/N/*) ==> Y

Online Generic Searches ----- SSA ----- Online Generic Searches

General Resource Information

Command ==>

Scroll ==> CSR

Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL	Resource Profile	Resource Class	Type	Profile Owner	UACC
___	&ABC	RACFVARS	D	USER01	NONE
___	&DELETE	RACFVARS	D	USER02	NONE
___	&TESTIT	RACFVARS	D	USER01	NONE
___	&XYZ	RACFVARS	D	USER01	NONE
___	SYSHIGH	SECLABEL	D	IBMUSER	NONE
___	SYSLOW	SECLABEL	D	IBMUSER	NONE
___	SYSNONE	SECLABEL	D	IBMUSER	NONE
___	ABCDEF	TAPEVOL	D	USER01	NONE
___	A00001	TAPEVOL	D	USER01	NONE
___	B00019	TAPEVOL	D	USER01	NONE
___	TESTTERM	TERMINAL	D	USER01	NONE
___	IMSP	APPL	D	WALK02	NONE
___	RTM*	TCICSTRN	G	USER01	NONE
___	CICSALL	GCICSTRN	D	CICS	NONE
___	CICSCAT1	GCICSTRN	D	CICS	NONE

Various Mode Available Functions

- A) SSA Resource List
- B) Delete Resource Profile
- C) Display Permits to General Resources
- D) Display Members
- E) Edit Installation Data
- F) Edit Application Data
- G) Pass to Replicate Resource Profile
- H) Pass to Replicate Resource Class
- I) Pass to Transfer Resource Profile
- J) Pass to Transfer Resource Class
- K) Display STDATA Segment
- L) Display Security Categories
- M) Display Volume Information
- N) RACF RLIST

General Resource Profile Permissions

Initial generic search screen for General Resource Profile permission information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Profile Permissions
Command ==>

                        Operational Mode (Batch/Online) ==> BATCH
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Profile           ==> *                               EQ
Class             ==> *                               EQ
Access Id         ==> *                               EQ
Access Id Type    ==> *                               EQ (User,Group,General,Obsolete)
Name              ==> *                               EQ (When Access Id Type is USER)
Access Level      ==> *                               EQ (None,Execute,Read,Update,Control,Alter)
Acc Lvl (Nmb)    ==> *                               EQ (0=None,1=Exec,2=Read,3=Updt,4=Cntl,5=Altr)
Access Type       ==> STD                             EQ (STD=Standard,CND=Conditional)

If Conditional:
Conditional Class ==> *                               EQ
Conditional Entity ==> *                             EQ

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Resource profiles in the Facility Class that have the RACF ‘*’ entry in the standard access list.

```

Class           ==> Facility           EQ
Access Id       ==> **                 EQ
Access Type     ==> STD                 EQ (STD=Standard,CND=Conditional)

```

OR

```

Class           ==> Facility           EQ
Access Id Type  ==> GENERAL             EQ
Access Type     ==> STD                 EQ

```

- Search for all Resource profiles that begin with APPL that have a conditional access entry.

```

Profile         ==> APPL*              EQ
Access Type     ==> CNDEQ

```

Online Generic Searches ----- SSA ----- Online Generic Searches		General Resource Profile Permissions			
Command ==>		Scroll ==> PAGE			
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V					
SEL	Resource Profile	Resource Class	Access Entry	Access Level	Entry Type
___	&ABC	RACFVARS	USER01	ALTER	USER
___	&ABC	RACFVARS	SNOOPER	ALTER	OBSOLETE
___	&ABC	RACFVARS	SYS1	READ	GROUP
___	&ABC	RACFVARS	ADMIN	READ	GROUP
___	&ABC	RACFVARS	TSTU005	ALTER	USER
___	&ABC	RACFVARS	TSTU015	ALTER	USER
___	&ABC	RACFVARS	TSTU016	ALTER	USER
___	&ABC	RACFVARS	TSTU017	ALTER	USER
___	&ABC	RACFVARS	TSTU046	ALTER	USER
___	&ABC	RACFVARS	TSTU048	ALTER	USER
___	&ABC	RACFVARS	TSTU051	ALTER	USER
___	&ABC	RACFVARS	TSTU065	ALTER	USER
___	&ABC	RACFVARS	TSTU068	ALTER	USER
___	&ABC	RACFVARS	TSTU069	ALTER	USER
___	&ABC	RACFVARS	TSTREPUR	ALTER	USER

Various Mode Available Functions

- A) SSA Resource List
- B) Re-Issue the Permit
- C) Remove the Permit
- D) Issue Permit Command
- E) Delete Resource Profile
- F) Display Members
- G) Pass to Replicate Resource Profile
- H) Pass to Transfer Resource Profile
- I) Display Users in Group
- J) RACF RLIST

General Resource Members

Initial generic search screen for Resource member information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Profile Members

Command ==>

                        Operational Mode (Batch/Online) ==> ONLINE
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

                        Enter your search criteria below:

Profile           ==> *                               EQ
Class             ==> *                               EQ
Type              ==> *                               (G=Generic,D=Discrete)
Member            ==> *                               EQ
GLOBAL Access Level ==> *                               EQ (None,Read,Update,Control,Alter)
PADS              ==> *                               EQ (Padchk,Nopadchk)
PADS Volume       ==> *                               EQ
Seclevel (Nmb)    ==> *                               EQ
SecCategory (Nmb) ==> *                               EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all general resource profiles in the GCICSTRN Class that have the transaction CEMT.

```

Class           ==> GCICSTRN                               EQ
Member          ==> CEMT                                   EQ
  
```

- Search for all general resource profiles that have CEMT as a member.

```

Member          ==> CEMT                                   EQ
  
```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Profile Members

Command ==>

                        Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V
                        Scroll ==> PAGE

SEL              Resource Profile          Resource
-----          -----          Class   Member (24 Characters)
___ &ABC          RACFVARS TESTP03
___ &ABC          RACFVARS TESTP0
___ &ABC          RACFVARS MEGAPO
___ &DELETE       RACFVARS DELTEST
___ CICSALL       GCICSTRN CMAC
___ CICSALL       GCICSTRN CRTX
___ CICSALL       GCICSTRN CSGM
___ CICS CAT1     GCICSTRN CDBD
___ CICS CAT1     GCICSTRN CXCU
___ CICS CAT1     GCICSTRN CSTP
___ CICS CAT1     GCICSTRN CGRP
  
```

Various Mode Available Functions

A) SSA Resource List

- B) Issue ADDMEM Command
- C) Issue DELMEM Command
- D) Display Permits to General Resources
- E) Pass to Replicate Resource Profile
- F) Pass to Transfer Resource Profile
- G) RACF RLIST

General Resource Session Segment

Initial generic search screen for General Resource Session segment information.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
General Resource Session Segment

Command ==>

      Operational Mode (Batch/Online) ==> ONLINE
-----
Direct Report Output to Sysout or Dataset (S/D): S

      Enter your search criteria below:

Profile           ==> *                               EQ
Class             ==> *                               EQ
APPC Session Key  ==> *                               EQ
Security Checking ==> *      EQ (None,Convsec,Persistv,Alreadyv,Avpv)
Days Key is Valid ==> *                               EQ
Current Failed Attempts ==> *                       EQ
Failed Attempts Before Lockout ==> *                 EQ
Profile is Locked (Y/N/*) ==> *
Last Date Key Changed ==> *                       EQ

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all general resource profiles that have a no security checking and where the current failed attempts is greater than 7.

```
Security Checking      ==> NONE          EQ
Current Failed Attempts ==> 00007        GT
```

```
Online Generic Searches ----- SSA ----- Online Generic Searches
General Resource Session Segment

Command ==>                               Scroll ==> PAGE

      Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL           Resource Profile           APPC Session Key  Nmb of Days
-----
--- TEST-SESS                                00001
Class ==> APPCLU  Profile Locked ==> N
--- XYYYSESS                                00005
Class ==> APPCLU  Profile Locked ==> Y
--- YYYYSESS                                00001
Class ==> APPCLU  Profile Locked ==> N
--- TEST                                XYZ      00000
Class ==> SURROGAT Profile Locked ==> N
--- TEST.*                                00010
Class ==> STARTED Profile Locked ==> N
***** Bottom of data *****
```

Various Mode Available Functions

- A) SSA Resource List
- B) Remove Session Segment

- C) Display Permits to General Resources
- D) Pass to Replicate Resource Profile
- E) Pass to Transfer Resource Profile
- F) RACF RLIST

General Resource DLF Segment

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          General Resource DLF Segment
Command ==>

                          Operational Mode (Batch/Online) ==> ONLINE
-----
Direct Report Output to Sysout or Dataset (S/D): S

Enter your search criteria below:

Profile          ==> *                               EQ
Class            ==> *                               EQ
Resource is Retained (Y/N/*) ==> *

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all general resource profiles that begin with SYS and retain resources.

```

Profile          ==> SYS*                               EQ
Resource is Retained (Y/N/*) ==> Y

```

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          General Resource DLF Segment
Command ==>                               Scroll ==> CSR

                          Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL          Resource Profile          Class      Resource is
-----
___  TEST          SURROGAT              Y
___  TESTDLF       DLFCLASS              N
___  XXXXDLF       DLFCLASS              N
***** Bottom of data *****

```

Various Mode Available Functions

- A) SSA Resource List
- B) Rebuild DLF Segment
- C) Remove DLF Segment
- D) Display Jobnames
- E) Display Permits to General Resources
- F) Pass to Replicate Resource Profile
- G) Pass to Transfer Resource Profile
- H) RACF RLIST

General Resource Started Task Segment

Initial generic search screen for General Resource Started Task segment information.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Started Task Segment

Command ==>

                        Enter your search criteria below:

                        Operational Mode (Batch/Online) ==> ONLINE
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

Profile                ==> *                                EQ
Class                  ==> *                                EQ
User                   ==> *                                EQ
Group                  ==> *                                EQ
Privileged (Y/N/*)    ==> *
Trusted (Y/N/*)       ==> *
Trace Entry (Y/N/*)   ==> *

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all started tasks that are both trusted and privileged.
Privileged (Y/N/*) ==> Y
Trusted (Y/N/*) ==> Y
- Search for all Started Tasks that have the group STARTASK associated with them.

Group ==> STARTASK EQ

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Started Task Segment

Command ==>                                Scroll ==> CSR

                        Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL          Resource Profile                User    Group    PRIV/TRUSTED
-----
--- AASTC01.*                                AASTC01   STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- APPC.*                                    APPC      STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- ASCH.*                                    ASCH      STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- ASCHINT.*                                ASCHINT   STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- DSN3UR00.*                                DSN3UR00  STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- DUMPSRV.*                                DUMPSRV   STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- FTPSERVE.*                                FTPSERVE   STARTASK  N / N
      Class ==> STARTED                      Trace = N
--- GTF.*                                    GTF       STARTASK  N / N
      Class ==> STARTED                      Trace = N
  
```

Various Mode Available Functions

- A) SSA Resource List
- B) Rebuild STDATA Segment
- C) Remove STDATA Segment
- D) Set/Remove Privileged Attribute
- E) Set/Remove Trusted Attribute
- F) Set/Remove Trace Attribute
- G) SSA List User
- H) SSA List Group
- I) Display Permits to General Resources
- J) Pass to Replicate Resource Profile
- K) Pass to Transfer Resource Profile
- L) RACF LISTUSER
- M) RACF LISTGROUP
- N) RACF RLIST

General Resource SystemView Segment

Initial generic search screen for General Resource SystemView segment information.

Online Generic Searches ----- SSA ----- Online Generic Searches

General Resource SystemView Segment

Command ==>

Enter your search criteria below:

Operational Mode (Batch/Online) ==> ONLINE

Direct Report Output to Sysout or Dataset (S/D): S

Profile ==> * EQ

Class ==> * EQ

Script Name ==> * EQ

Parm Name ==> * EQ

Hit Enter to Continue PF03=EXIT/PF01=HELP

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all Resource profiles that have a parm name of HOST1.

Parm Name ==> HOST1 EQ

Online Generic Searches ----- SSA ----- Online Generic Searches

General Resource SystemView Segment

Command ==>

Scroll ==> CSR

Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL	Resource Profile	Resource Class	Script Name	Parm Name
---	-----	-----	-----	-----
___	TESTSCRIPT	SYSMVIEW	SCRNAME	PARNAME
___	TESTVIEW	SYSMVIEW	SCRPTER	PARMER
***** Bottom of data *****				

Various Mode Available Functions

- A) SSA Resource List
- B)# Rebuild SystemView Segment
- C) Remove SystemView Segment
- D) Display Permits to General Resources
- E) Pass to Replicate Resource Profile
- F) Pass to Transfer Resource Profile
- G) RACF RLIST

General Resource Security Categories

Initial generic search screen for General Resource Security Category information.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Security Categories

Command ==>

                        Enter your search criteria below:

                        Operational Mode (Batch/Online) ==> ONLINE
                        -----
                        Direct Report Output to Sysout or Dataset (S/D): S

Profile           ==> *                               EQ
Class             ==> *                               EQ
Security Category ==> *                               EQ
SecCategory (Nmb) ==> *                               EQ

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Search Examples

These examples only indicate the changes to the SSA installed default values.

- Search for all General Resource profiles that begin with S that have security category of TOPSECRETINFO.

```
Profile           ==> S*                               EQ
Category          ==> TOPSECRETINFO                   EQ
```

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                        General Resource Security Categories

Command ==>                               Scroll ==> CSR

                        Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V

SEL           Resource Profile           Resource   Security
-----
TEST.PROFILE  TEST PROFILE               $TSTCLAS   00003
Security Category ==> TESTCAT
***** Bottom of data *****
```

Various Mode Available Functions

- A) SSA Resource List
- B) Re-Issue the Security Category Entry
- C) Remove the Security Category Entry
- D) Delete Resource Profile
- E) Display Permits to General Resources
- F) Pass to Replicate Resource Profile
- G) Pass to Transfer Resource Profile
- H) RACF RLIST

Online Generic Search Result Functions

Search Result Screen

Search result screens allow you to further process any entries that meet the specified search criteria.

Online Generic Searches ----- SSA ----- Online Generic Searches							
General User Information							
Command ==>				Scroll ==> CSR			
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> V							
SEL	Userid	Name	Default Group	Profile Owner	Create Date	Last-Used Date	Rvk?
___	AASTC01	STARTED TASK	STARTASK	STARTASK	1997-03-05	1998-06-03	N
___	APPC	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCH	STARTED TASK	STARTASK	STARTASK	1995-06-07	1998-05-29	N
___	ASCHINT	STARTED TASK	STARTASK	STARTASK	1996-10-21	1998-05-29	N
___	BLSJPRMI	#####	STARTASK	STARTASK	1995-06-13	1998-05-29	N
___	BMLTDRB	RAY FONFIELD	BMLTD	BMLTD	1997-05-27		N
___	BMLTDSO	STEVE TREND	BMLTD	BMLTD	1997-05-27		N
___	CICSTART	#####	STARTASK	STARTASK	1996-06-19	1996-06-19	N
___	CICSUSER	#####	CICS	CICS	1996-10-21	1998-06-01	N
___	DCEKERN	#####	STARTASK	STARTASK	1995-10-30		N
___	DSN3UR00	STARTED TASK	STARTASK	STARTASK	1996-10-21		N
___	DUMPSRV	STARTED TASK	STARTASK	STARTASK	1995-10-19	1998-05-29	N
___	EZAFTPAP	#####	STARTASK	STARTASK	1996-06-26	1998-02-14	N
___	FTPSEVE	STARTED TASK	STARTASK	STARTASK	1997-02-13	1998-06-11	N
___	GTF	STARTED TASK	STARTASK	STARTASK	1996-06-10	1996-06-10	N

Search result screens display RACF entries that met the specified search criteria. Below is an example search result screen. You can select any of the entries for further processing. Scroll DOWN to view all entries that met the search criteria.

The remainder of this chapter is as follows:

- A) Various Mode
- B) Ad-hoc Mode
- C) Print Mode
- D) Sort Mode
- E) Adhoc Report Generation

Various Mode

Various Mode Pop-Up Panel Example

Each search result screen has its own Various Mode pop-up panel. Various Mode provides up to 30 different functions after the search result panel has been displayed.

Online Generic Searches			SSA		Online Generic Searches	
Searches			General User Information		Scroll ==> CSR	
Command ==>			Modes - Va		SSA	
			Command ==>			
SEL	Userid	Name	Type An Option and Press Enter: C			
S	AASTC01	STARTED TASK	More: +			
___	APPC	STARTED TASK	A	SSA List User		
___	ASCH	STARTED TASK	B	Display Connects		
S	ASCHINT	STARTED TASK	C	Display DATASET Profiles (HLQ=USERID)		
___	BLSJPRMI	#####	D	Display Permits to DATASET Profiles		
___	BMLTDRB	RAY FONFIELD	E	Display Permits to General Resources		
___	BMLTDS	STEVE TREND	F	Edit Installation Data		
S	CICSTART	#####	G	Display TSO Segment		
___	CICSUSER	#####	H	Display CICS Segment		
___	DCEKERN	#####	I	Display LANGUAGE Segment		
___	DSN3UR00	STARTED TASK	J	Display WORKATTR Segment		
S	DUMPSRV	STARTED TASK	K	Display DFP Segment		
___	EZAFTAP	#####	L	Display OPERPARM Segment		
___	FTPSE	STARTED TASK				
S	GTF	STARTED TASK	STARTASK STARTASK 1996-06-10 1996-06-10 N			

At this point simply type in the option you would like to use and press the ENTER key. SSA will then process the chosen option on each selection made from the search result screen, and prompt you for any additional information, or will move you to the appropriate screen.

Some screens will allow you to select information for additional processing. These types of screens will have a SUB-FUNCTION: description under the EXPLANATION to describe what additional options you have available.

SSA ListDataset

Provides a listing of dataset information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          SSA ListDataset
Command ==>

Dataset Profile    ==> CICS.*
Profile Type       ==> GENERIC
Volume            ==>
Profile Owner      ==> CICS
UACC              ==> NONE
Warning Active     ==> NO
Notify ID         ==>
DFP Resowner      ==>
Profile Level      ==> 00
Scratch on Delete  ==> NO
Creation Date      ==> 1996-06-10
Last Referenced    ==> 1996-06-10
Last Changed Date  ==> 1996-06-10
Alter Count        ==> 00000
Control Count      ==> 00000
Update Count       ==> 00000
Read Count         ==> 00000
Device Type Name   ==>
Creator Connect Group ==> SYS1
Local Audit Level  ==> FAIL
Local OK Level     ==>
Local Failure Level ==> READ
Global Audit Level ==> NONE
Global OK Level    ==>
Global Failure Level ==>
Security Level     ==> 000
Seclevel Name      ==>
Retention Period   ==> 00000
Security Label     ==>

-----
Installation Data ==>

<==
Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

SSA will display pertinent profile information in a highly organized and readable fashion. To continue viewing any other selections you may have made just press the ENTER key. If the SSA configuration option Print After Browse is set to Y then a browse dataset panel with a report of all the selected entries that were just displayed will be presented.

SSA ListGroup

Provides a listing of group information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                          SSA ListGroup
Command ==>

Group              ==> BACKUP
Superior Group     ==> PROD
Profile Owner      ==> PROD
Model Dataset      ==>
TERMUACC          ==> NO
Users Connected?   ==> NO
Subgroups?         ==> NO
Creation Date      ==> 1996-10-21
Default UACC       ==> NONE
Installation Data   ==> THIS IS THE HLQ FOR BACKUPS

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

SSA ListUser

Provides a listing of userid information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                SSA List User

Command ==>

                                More:      +

Userid           ==> AASTC01
Userid Name      ==> STARTED TASK
Default Group    ==> STARTASK
Owner            ==> STARTASK
Create-Date      ==> 1997-03-05
Last-Used-Date   ==> 1998-09-25
Model Dataset    ==>
Revoke Date      ==>
Resume Date      ==>

Attributes:
Special: YES   Operations: YES   Audit: NO
GRPACC: NO    Uaudit:   NO    ADSP: NO
Oidcard: NO   Revoke:   NO

Password Related:
PSW-INTVL           ==> 180
Passdate            ==>
Unsuccessful Logon Attempts ==> 000
Password Generation Number ==> 000
Need Password To Logon   ==> NO
Never Logged On         ==> YES

Segments:
TSD:      NO   CICS:      NO   DFP:      NO
Operparm: NO   DCE:      NO   NetView: NO
OMVS:     NO   Language: NO   WorkAttr: NO

Other:      RRSF: NO   CLAUTH: NO

Security Information Related:
Default Security Label ==>
Security Level (Numeric) ==> 000
Security Level Name     ==>
Security Categories      ==> NO

Logon Days:
Monday:  YES   Tuesday: YES   Wednesday: YES
Thursday: YES   Friday:  YES   Saturday:  YES
Sunday:   YES

Logon Times:
Start Time ==> ANYTIME
End Time   ==> ANYTIME

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

SSA Resource List

Provides a listing of general resource information in a highly organized manner.

Online Generic Searches ----- SSA ----- Online Generic Searches	
SSA Resource List	
Command --->	
Profile	--> ABCDEF
Class	--> TAPEVOL
	More: +
Type	--> DISCRETE
Owner	--> GOODPAO
UACC	--> NONE
Warn	--> NO
Notify	-->
Level	--> 00
Create Date	--> 1997-01-02
Last Referenced Date	--> 1998-01-02
Last Changed Date	--> 1998-01-02
Security Level	--> 000
Security Label	-->
Class - TAPEVOL Fields: (These fields are relevant for TAPEVOL profiles)	
One Dataset	--> NO
Automatic Protection	--> NO
TVTOC	--> NO
Class - TERMINAL Fields: (These fields are relevant for TERMINAL profiles)	
Use on Sunday	--> YES
Use on Monday	--> YES
Use on Tuesday	--> YES
Use on Wednesday	--> YES
Use on Thursday	--> YES
Use on Friday	--> YES
Use on Saturday	--> YES
Start time to Logon	--> ANYTIME
End time to Logon	--> ANYTIME
Terminals TimeZone	-->
TimeZone Shift	-->
Audit Levels:	
Local Audit Level	--> FAIL
Lcl Successful Audit Level	-->
Lcl Failure Audit Level	--> READ
Global Audit Level	--> NONE
Glb Successful Audit Level	-->
Glb Failure Audit Level	-->

Installation Data	-->
Application Data ---> <---	
<---	
Hit Enter to Continue PF03=EXIT/PF01=HELP	

Display CICS Segment

Provides a listing of CICS Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                CICS Segment
Command ==>

Userid   ==> USER02
User Name ==> BILL GENUSERID

Operator Priority ==> 000
Terminal Time Out ==> 00:00
Operator Identifier ==>
XRF Force/Noforce ==> N
Operator Classes:
                                01: NO   02: YES  03: NO   04: NO
                                05: NO   06: NO   07: NO   08: NO
                                09: NO   10: NO   11: NO   12: NO
                                13: NO   14: NO   15: NO   16: NO
                                17: NO   18: NO   19: NO   20: NO
                                21: NO   22: NO   23: NO   24: NO

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Display CLAUTH Authorities

Provides a table display listing all CLAUTH Authority information for a user.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                CLAUTH Authorities
Command ==>                                Scroll ==> CSR

                                CLAUTH Authorities for ==> USER01
                                Name ==> ENDUSER, JOSEPH

                                Select entries to manipulate:

SEL  Class
---  -----
__  USER
***** Bottom of data *****

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Remove the CLAUTH Authority
- B) Re-Issue the CLAUTH Authority
- C) Issue CLAUTH Command
- D) Print CLAUTH Authority Information

Display Connects

Provides a table display listing all connect groups for a user. This option is chosen from a various mode main pop-up panel.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                                Connect Information
Command ==>                               Scroll ==> CSR
                                Connects for User ==> USER02
                                Name ==> BILL GENUSERID

                                Select entries to manipulate:

SEL      RACF  Profile
Group    Owner Authority  UACC  Spec Oper Audt Revk Adsp Grpa
-----
___ ADMIN  USER02  USE      NONE   N   N   N   N   N   N
___ ADMINAID USER02  USE      NONE   N   N   N   N   N   N
___ MEGA    MEGA    USE      NONE   N   N   N   N   N   N
___ SYS1    SYS1    USE      NONE   N   N   N   N   N   N
***** Bottom of data *****
```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Issue (Modify) the Connect Profile
- B) Remove the Connect Profile
- C) Issue Connect Command For Another Userid
- C) Print Connect Information

Display Connects with Group Special

Provides a table display listing all users that have a group special attribute on any connect profile.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                                Connects with Group Special
Command ==>                               Scroll ==> CSR
                                Connects for User ==> USER01
                                Name ==> ENDUSER, JOSEPH

                                Select entries to manipulate:

SEL      Profile
Group    Owner Authority  UACC
-----
___ TEST  USER02  USE      NONE
***** Bottom of data *****
```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Issue (Modify) the Connect Profile
- B) Remove the Connect Profile
- C) Issue Connect Command For Another Userid
- D) Print Connect Information

Display DATASET Profiles (HLQ=Group)

Display all dataset profiles where the High Level Qualifier equals the Group selected.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Dataset Profiles
Command ==>
                        Scroll ==> CSR

                        Dataset Profiles for HLQ ==> ADMIN

                        Select entries to manipulate:

SEL          Dataset Profile          Type   UACC   Volume  Warn
-----
___ ADMIN.V*.ASM                      G      NONE           N
___ ADMIN.V*.COBOL                   G      NONE           N
___ ADMIN.V*.ISPTLIB                 G      NONE           N
___ ADMIN.*                           G      NONE           N
***** Bottom of data *****

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Delete Dataset Profile
- B) Clear out Access List Entries
- C) Issue Permit Command
- D) Print List of Datasets Protected By Profile
- E) Print Profile Information

Display DATASET Profiles (HLQ=UserID)

Display all dataset profiles where the High Level Qualifier equals the UserID selected.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Dataset Profiles
Command ==>
                        Scroll ==> CSR

                        Dataset Profiles for HLQ ==> USER01
                        Name ==> ENDUSER, JOSEPH

                        Select entries to manipulate:

SEL          Dataset Profile          Type   UACC   Volume  Warn
-----
___ USER01.*                      G      NONE           N
___ USER01.RACF.PROFILE.MODEL     M      NONE    *MODEL      N
***** Bottom of data *****

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Delete Dataset Profile
- B) Clear out Access List Entries
- C) Issue Permit Command
- D) Print List of Datasets Protected By Profile
- E) Print Profile Information

Display DCE Segment

Provides a listing of DCE Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                DCE Segment
Command ==>

Userid    ==> USER01
User Name ==> ENDUSER, JOSEPH

Principal UUID      ==> 87654321-1234-1234-1234-123456789012
Principal Name      ==> start of the hmenme
Cell Name           ==> /.../test
Cell UUID           ==> 12345678-1234-1234-1234-123456789012
Automatic Login     ==> Y

Note: The Principal Name and Cell Name show only the
      first 40 characters of a possible 1023 characters.

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Display DFP Segment

Provides a listing of DFP Segment information in a highly organized manner

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                DFP Segment
Command ==>

Userid    ==> USER01
User Name ==> ENDUSER, JOSEPH

Data Class      ==> TESTCLAS
Management Class ==> TESTMGMT
Storage Class   ==> TESTSTOR
Data Application ==> TESTAPPL

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Display Jobnames

Display general resource DLF Segment Jobname information in a highly organized format.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Resource DLFDATA Jobname Information
Command ==>
                        Scroll ==> CSR

Resource ==> TESTDLF
Class    ==> DLFCLASS

                        Select entries to manipulate:

SEL      Jobname
---      -----
_____  XYZ
***** Bottom of data *****

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Add Jobname
- B) Delete Jobname
- C) Print Jobname Information

Display Language Segment

Provides a listing of Language Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        LANGUAGE Segment
Command ==>

Userid    ==> USER02
User Name ==> BILL GENUSERID

      Primary Language ==> ENU
      Secondary Language ==> ESP

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Display Members

Display general resource member information in a highly organized format.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Resource Member Information
Command ==>
Resource ==> CICSCAT1
Class ==> GCICSTRN

                        Select entries to manipulate:

SEL          Member
---          -
---          CDBO
---          CDBN
---          CDBD
---          CXRE
---          CXCU
---          CSTP
---          COVR
---          CGRP
---          CSSY
---          CPLT
---          CSNE
---          CSTF

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Add the Member
- B) Remove the Member
- C) Print Member Information

Display NETVIEW Segment

Provides a listing of NETVIEW Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                        Netview Segment
Command ==>

Userid ==> USER01
User Name ==> ENDUSER, JOSEPH

CTL Value ==> SPECIFIC
Receive Messages ==> Y
Default Console Name ==> CNSOLE01
Authorized to NGMF ==> N
Command List ==> NETVIEW IC COMMAND FIELD

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Display OMVS Segment

Provides a listing of OMVS Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                OMVS Segment

Command ==>

Userid    ==> USER02
User Name ==> BILL GENUSERID

OMVS UID          ==> 0000000000
OMVS Home Path    ==> testout and this is the final test of wh
OMVS Default Program ==> testout and this is the final test of wh

Note: The Home Path and Default Program show only the
      first 40 characters of a possible 1023 characters.

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Display OPERPARM Segment

Provides a listing of OPERPARM Segment information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                OPERPARM Segment

Command ==>

Userid    ==> USER02
User Name ==> BILL GENUSERID

Storage    ==> 02000
Key        ==> ZZZZ
Cmdsys     ==> XXYX
Dom        ==> NORMAL
Logcmdresp ==> SYSTEM
Migid     ==> Y
UD         ==> N
AltGroup   ==> XXXXX1
Auto-Message ==> Y
Auth:      Master: Y All: N Info: N Cons: N Io: N Sys: N
Level:     NB: Y All: N R: Y I: Y CE: Y E: Y IN: Y
Mform:     J: Y M: Y S: Y T: Y X: Y
Monitor:   Jobnames: N Jobname: Y
Sess:      Y Sess: N Status: Y

Routcodes:
All: N
None: N
001: Y 002: N 003: N 004: N 005: Y 006: N 007: N 008: N
009: N 010: N 011: N 012: N 013: N 014: N 015: N 016: N
017: N 018: Y 019: N 020: N 021: N 022: N 023: N 024: N
025: N 026: N 027: N 028: N 029: N 030: N 031: N 032: N
033: N 034: N 035: N 036: N 037: N 038: N 039: N 040: N
041: N 042: N 043: N 044: N 045: N 046: N 047: N 048: N
049: N 050: N 051: N 052: N 053: N 054: N 055: N 056: N
057: N 058: N 059: N 060: N 061: N 062: N 063: N 064: N
065: N 066: N 067: N 068: N 069: N 070: N 071: N 072: N
073: N 074: N 075: N 076: N 077: N 078: N 079: N 080: N
081: N 082: N 083: N 084: N 085: N 086: N 087: N 088: N
089: N 090: Y 091: N 092: N 093: N 094: N 095: N 096: N
097: N 098: N 099: N 100: N 101: N 102: N 103: N 104: N
105: N 106: N 107: N 108: N 109: N 110: N 111: N 112: N
113: N 114: N 115: N 116: N 117: N 118: N 119: N 120: N
121: N 122: N 123: N 124: N 125: N 126: N 127: N 128: Y
Mscope:   * Mscopes are not displayed *

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Display Permits to Dataset Profiles

Display permissions to Dataset profiles.

Online Generic Searches ----- SSA ----- Online Generic Searches		
Dataset Permissions		
Command ==>		Scroll ==> CSR
Permissions for UserID ==> USER02		
Name ==> BILL GENUSERID		
Select those you want to manipulate:		
SEL	Dataset Profile	Access Level - Conditional - Class Entity
----	-----	-----
___ ADMIN.V*.ASM		ALTER
___ ADMIN.V*.ISPTLIB		ALTER
___ BACKUP.*		UPDATE
___ USER01.*		UPDATE
___ TSTGS31.*		ALTER
___ TSTU015.RACF.PROFILE.MODEL		ALTER

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Remove the Permit
- B) Re-Issue the Permit
- C) Issue Permit Command
- D) Print List of Datasets Protected By Profile
- E) Print Permit Information

Display Permits to General Resource Profiles

Display permissions to General Resource profiles.

Online Generic Searches ----- SSA ----- Online Generic Searches		
General Resource Permissions		
Command ==>		Scroll ==> CSR
Permissions for Userid ==> USER02		
Name ==> BILL GENUSERID		
Select those you want to manipulate:		
SEL	General Resource Profile	Class Access Level
----	-----	-----
___ &DELETE		RACFVARS ALTER
___ CICSCAT1	Conditional (CLASS/ENTITY)==>	GCICSTRN ALTER
___ CICSCAT3	Conditional (CLASS/ENTITY)==>	GCICSTRN ALTER
___ **	Conditional (CLASS/ENTITY)==>	PCICSPSB ALTER
___ DATASET	Conditional (CLASS/ENTITY)==>	GLOBAL ALTER
___ \$RESET.*	Conditional (CLASS/ENTITY)==>	FACILITY ALTER

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Remove the Permit

- B) Re-Issue the Permit
- C) Issue Permit Command
- D) Print Permit Information

Display RRSF Information

Provides a listing of RRSF information in a highly organized manner.

Online Generic Searches ----- SSA ----- Online Generic Searches

Userid RRSF Information

Command ==>

Scroll ==> CSR

Associations for User ==> WALK02

Name ==> PRODUCT WALK-THRU UI

Select entries to manipulate:

SEL	Target Node/Userid	Peer	Manager User/Remote	Pending Lcl/Remote	Password Synchronized	Create Userid
___	TSGNJE WALK01	N	Y N	N N	N	WALK02
___	TSGNJE P390C	Y	N N	N N	Y	WALK02
___	TSGNJE P390G	Y	N N	N N	N	WALK02
___	TSGNJE P390H1	N	Y N	N Y	N	WALK02
___	TSGNJE WALK03	N	N Y	N N	N	WALK03
___	TSGNJE USER02	N	N Y	N N	N	USER02

*****Bottomofdata*****

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Define New Association
- B) Undefine the Association
- Peer Associations
- C) Model the Association
- D) Change the Association
- Managed Associations
- E) Model the Association
- F) Change the Association
- G) Approve the Association
- H) Print RRSF Association Information

Display Security Categories

Provides a listing of Security Category information in a highly organized manner.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                                Security Categories
Command ==>                                Scroll ==> CSR

                                Security Categories for ==> USER01
                                Name ==> ENDUSER, JOSEPH

                                Select entries to manipulate:

SEL      Security Category Name      Numeric Value
-----
__ TOPSECRETDATA                      00001
***** Bottom of data *****
```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Remove the Security Category Entry
- B) Re-Issue the Security Category Entry
- C) Issue Security Category Command
- D) Print Security Category Information

Display STDATA Segment

Provides a listing of STDATA Segment information in a highly organized manner.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                                General Resource STDATA Segment
Command ==>                                Scroll ==> CSR

Resource ==> RACF.*
Class ==> STARTED

                                Select those you want to manipulate:

SEL      User      Group      Privileged      Trusted      Traced
-----
__ RACF      STARTASK      Y      N      N
*****Bottomofdata*****
```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Add the STDATA Segment
- B) Remove the STDATA Segment
- C) Print STDATA Segment Information

Display Subgroups

Provides a listing of subgroup information in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                Subgroups Information

Command ==>                                                                Scroll ==> PAGE

                                Group ==> SYS1

                                Select entries to manipulate:

SEL      Group      Superior  Profile  Has      Has
-----  -
DEVL     SYS1       SYS1      SYS1      N         N         Y
NONIBM   SYS1       SYS1      SYS1      N         N         Y
OTHERS   SYS1       SYS1      SYS1      N         N         Y
PROD     SYS1       SYS1      SYS1      N         N         Y
SYSTEM   SYS1       SYS1      SYS1      N         N         Y
TEST     SYS1       SYS1      SYS1      N         Y         Y
TESTREM2 SYS1       IBMUSER   SYS1      N         N         N
USERS    SYS1       SYS1      SYS1      N         N         Y

***** Bottom of data *****

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Change Superior Group
- B) Pass to Replicate Group
- C) Pass to Remove All References
- D) Print Group Information

Display TSO Segment

Provides a listing of TSO Segment information in a highly organized manner.

Online Generic Searches		SSA		Online Generic Searches	
Command ==>		TSO Segment			
Userid ==> USER01					
User Name ==> ENDUSER, JOSEPH					
Logon Procedure ==> ADMIN510					
Unit ==> SYSALLDA					
UserData ==> 0000					
Size ==> 0008192					
Max Size ==> 0000000					
Hold Class ==> H					
Job Class ==> J					
Message Class ==> M					
Sysout Class ==> M					
Destination ==>					
Account ==> ACCT#					
Performance Group ==> 0000016448					
Default Logon Security Label ==>					
Command issued at Logon ==> TSPF					

Display Users in Group

Provides a listing of users connected to a group in a highly organized manner.

```

Online Generic Searches ----- SSA ----- Online Generic Searches
                                UserIDs In Group
Command ==>                                Scroll ==> CSR

                                Users in Group ==> SYS1

                                Select entries to manipulate:

SEL      RACF  Profile
  UserID  Owner  Authority  UACC  Spec  Oper  Audt  Revk  Adsp  Grpa
-----
___ AASTC01  SYS1  USE      NONE  N    N    N    N    N    N
___ APPC     SYS1  USE      NONE  N    N    N    N    N    N
___ ASCH     SYS1  USE      NONE  N    N    N    N    N    N
___ ASCHINT  SYS1  USE      NONE  N    N    N    N    N    N
___ BLSJPRMI SYS1  USE      NONE  N    N    N    N    N    N
___ CICSTART SYS1  USE      NONE  N    N    N    N    N    N
___ CICSUSER SYS1  USE      NONE  N    N    N    N    N    N
___ DSN3UR00 SYS1  USE      NONE  N    N    N    N    N    N
___ DUMPSRV  SYS1  USE      NONE  N    N    N    N    N    N
___ EZAFTPAP SYS1  USE      NONE  N    N    N    N    N    N
___ FTPSERVE SYS1  USE      NONE  N    N    N    N    N    N

```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- A) Re-Issue (Modify) the Connect Profile
- B) Remove the Connect Profile
- C) Issue Connect Command For Another Userid
- D) Print Connect Information

Display Volume Information

Provides a listing of general resource TAPEVOL profile volume information in a highly organized manner.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
General Resource Volume Information
Command ==>
Scroll ==> CSR
Resource ==> A00001
Class ==> TAPEVOL
Select those you want to manipulate:
SEL Volume
--- -----
___ A00001
***** Bottom of data *****
```

Available Sub-functions

If a selection is made from the table display the following sub-functions are available:

- Issue ADDVOL Command
- Issue DELVOL Command
- Print Volume Information

Display WORKATTR Segment

Provides a listing of WORKATTR Segment information in a highly organized manner.

```
Online Generic Searches ----- SSA ----- Online Generic Searches
                                WORKATTR Segment

Command ==>

Userid    ==> USER01
User Name ==> ENDUSER, JOSEPH

Delivery:
Room      ==> ROOM 003
Department ==> DEPT FOR ME
Building  ==> BLDG FOR ME
Name      ==>

Address Lines:
Line 1    ==> ADDR1 FOR ME
Line 2    ==> ADDR2 FOR ME
Line 3    ==> ADDR3 FOR ME
Line 4    ==> ADDR4 FOR ME

Account Number ==> ACCOUNT NUMBER:009001 SPECIAL NOTE:01013456881

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Various Mode: RACF Command Generation

The following table lists in alphabetical order the many Various Mode RACF Commands that may be generated.

Various Mode Option	Possible RACF Command Generated
Change the Managed Association	RACLINK
Change the Peer Association	RACLINK
Define New Association	RACLINK
Delete DATASET Profile	DELDSO
Delete Resource Profile	RDELETE
Edit Application Data	RALTER
Edit Installation Data	ALTUSER, ALTGROUP, ALTDSD, RALTER
Issue ADDMEM Command	RALTER
Issue CICS Segment Command	ALTUSER
Issue CLAUTH Command	ALTUSER
Issue Connect For Another Userid	CONNECT
Issue DCE Segment Command	RALTER
Issue DELMEM Command	RALTER
Issue DFP Segment Command	ALTUSER, RALTER
Issue LANGUAGE Segment Command	ALTUSER
Issue NETVIEW Segment Command	ALTUSER
Issue OMVS Segment Command	ALTUSER, ALTGROUP
Issue OPERPARM Segment Command	ALTUSER
Issue Permit Command	PERMIT
Issue Security Category Command	ALTUSER, ALTDSD, RALTER
Issue TSO Segment Command	ALTUSER
Issue WORKATTR Segment Command	ALTUSER
Model the Managed Association	RACLINK
Model the Peer Association	RACLINK
RACF LISTDSO	RACF Command
RACF LISTGROUP	RACF Command
RACF LISTUSER (Current Node Only)	RACF Command
RACF RLIST	RACF Command
Re-Issue (Modify) the Connect	CONNECT

Various Mode Option	Possible RACF Command Generated
Re-Issue the CLAUTH Authority	ALTUSER
Re-Issue the Permit	PERMIT
Re-Issue the Security Category Entry	RALTER
Rebuild CICS Segment	ALTUSER
Rebuild DCE Segment	RALTER
Rebuild DFP Segment	ALTUSER, RALTER
Rebuild DLF Segment	RALTER
Rebuild LANGUAGE Segment	ALTUSER
Rebuild NETVIEW Segment	ALTUSER
Rebuild OMVS Segment	ALTUSER
Rebuild OPERPARM Segment	ALTUSER
Rebuild STDATA Segment	RALTER
Rebuild SystemView Segment	RALTER
Rebuild TSO Segment	ALTUSER
Rebuild WORKATTR Segment	ALTUSER
Remove CICS Segment	ALTUSER
Remove DCE Segment	RALTER
Remove DFP Segment	ALTUSER, RALTER
Remove DLF Segment	RALTER
Remove LANGUAGE Segment	ALTUSER
Remove NETVIEW Segment	ALTUSER
Remove OMVS Segment	ALTUSER
Remove OPERPARM Segment	ALTUSER
Remove Session Segment	RALTER
Remove STDATA Segment	RALTER
Remove SystemView Segment	RALTER
Remove the CLAUTH Authority	ALTUSER
Remove the Connect Profile	REMOVE
Remove the Permit	PERMIT
Remove the Security Category Entry	ALTUSER, RALTER
Remove TSO Segment	ALTUSER
Remove WORKATTR Segment	ALTUSER
Set/Remove Privileged Attribute	RALTER

Various Mode Option	Possible RACF Command Generated
Set/Remove Trace Attribute	RALTER
Set/Remove Trusted Attribute	RALTER
Undefine the Association	RACLINK

Various Mode: System Command Listings

The following table describes those various mode options that issue system or RACF commands to list data. A browse dataset panel is displayed. You have the option of printing out the listing after browsing.

Various Mode Option	Possible System Command Generated
List Catalog Entry (LISTC Command)	LISTC ENT('userid or group')
Print List of Datasets Protected By Profile	LISTDSD 'profile name' DSNS NORACF

Various Mode: Pass to Functionality

The following table lists the various mode 'pass to' options available. Descriptions of the 'pass to' functions can be found in the manual sections noted. Please refer to the appropriate section in this manual for a full explanation of each option.

Various Mode Pass To Option	SSA Manual Section
Pass to Access Report	Reporting
Pass to Connect Administration	Connect Administration
Pass to Ownership Report	Reporting
Pass to Password Administration	Password Administration
Pass to Remove All References	Command Generation
Pass to Replicate DATASET	Command Generation
Pass to Replicate Group	Command Generation
Pass to Replicate Resource Class	Command Generation
Pass to Replicate Resource Profile	Command Generation
Pass to Replicate User	Command Generation
Pass to Transfer DATASET	Command Generation
Pass to Transfer Group	Command Generation
Pass to Transfer Notifications	Command Generation
Pass to Transfer Ownership	Command Generation
Pass to Transfer Resource Class	Command Generation
Pass to Transfer Resource Profile	Command Generation

Various Mode Pass To Option	SSA Manual Section
Pass to Transfer UserID	Command Generation

Adhoc Mode

Each generic search function has the capability of generating commands utilizing the information that is a result of your original search criteria. Each function has unique fields that can be used. Those fields or variable are listed on each ad-hoc command panel. Below is an example ad-hoc mode screen for the General User Information generic search. You may use all of the entries that met your search criteria, or you may select specific entries to include in the ad-hoc mode command generation.

To demonstrate the use of this powerful feature, consider the following scenario: You have to connect all users starting with TEST that have a default group that starts with TST to a new group called PRODCICS that you have just created.

- 1 Set the search criteria on the General User Information generic search initial screen:

```
Userid          ==> TEST*          EQ
Default Group   ==> TST*           EQ
```

Online Generic Searches ----- SSA ----- Online Generic Searches								
General User Information								
Command ==>				Scroll ==> CSR				
Modes - Various/Adhoc/Print/Sort (V/A/P/S) ==> A								
SEL	Userid	Name		Default Group	Profile Owner	Create Date	Last-Used Date	Rvk?
S__	TSTU001	STRICTLY	TEST USERS	TSTG001	SN00PER	1997-05-22		N
___	TSTU002	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
___	TSTU003	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
S__	TSTU004	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		Y
___	TSTU005	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
___	TSTU006	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
S__	TSTU007	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
S__	TSTU008	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
___	TSTU009	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N
___	TSTU010	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26	1998-06-03	N
___	TSTU011	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26	1998-06-03	N
S__	TSTU012	STRICTLY	TEST USERS	TSTG001	TSTG001	1997-05-26		N

- 2 As shown on the screen example, the search results screen is displayed. Change the Operational Mode to A for ad-hoc, and press ENTER.

Note You may have done a more general search and then used 'select and scroll' functionality to select only the specific entries to issue the ad-hoc commands for. In the sample screen on the previous page, there were only 5 entries selected for further processing. Please see the Global Conventions located at the beginning of this section for a description of 'select and scroll'.

- 3 You will be presented with the screen below where you would enter the displayed command mask:

```

Ad-Hoc Command Generation ----- SSA ----- Ad-Hoc Command Generation
                                General User Information

Command ==>

                                Symbolic      What is Substituted?
                                -----
                                @USER         Userid
                                @DFGP         Default Group
                                @OWNR         Profile Owner

                                Here are some examples: alu @USER df1(@DFGP) ow(@OWNR)
                                                co @USER group(xyz)

                                Enter the command(S) you want generated below:
==>  CONNECT @USER GROUP(CICSPROD) OWNER(CICSPROD)
==>  _____
==>  _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

- 4** SSA then generates the commands, substituting the userids found in the search (or selected from the search results screen) into the command where the variable @USER is.

```

Process Generated Commands ----- SSA ----- Process Generated Commands
Command ==>                                Scroll ==> CSR

                                Action Command      Action Taken
                                -----
                                AAEXEC              Execute Commands Immediately
                                AABATCH             Place Commands in Batch JCL
                                AASCHED             Schedule Commands
                                AASTORE             Store or Retrieve Commands

EDIT ----- USER02.TSCSSA.ADHOC.OUTPUT----- COLUMNS 00001 00072
***** ***** Top of Data *****
=NOTE= COMMANDS ARE READY FOR EXECUTION
==CHG> CONNECT TESTU001 GROUP(CICSPROD) OWNER(CICSPROD)
==CHG> CONNECT TESTU004 GROUP(CICSPROD) OWNER(CICSPROD)
==CHG> CONNECT TESTU007 GROUP(CICSPROD) OWNER(CICSPROD)
==CHG> CONNECT TESTU008 GROUP(CICSPROD) OWNER(CICSPROD)
==CHG> CONNECT TESTU012 GROUP(CICSPROD) OWNER(CICSPROD)
***** ***** Bottom of Data *****

```

Print Mode

Each generic search function has the capability of printing a report that includes information that is a result of your original search criteria. You may use all of the entries that met your search criteria, or you may select specific entries to include in the report. If you select some entries to include in the report, then a note will be put into the report that indicates that not all entries that met the search criteria were included in the report.

To use the print mode:

- 1 Select specific entries if you do not want all entries (default) to be included in the report.
- 2 Set the Operational Mode to P for Print and press ENTER.
- 3 Your report will be generated and displayed on the screen. You may then choose to send the output to a specified SYSOUT class, and by setting the 'send report output' to Y.

```

Print Params ----- SSA ----- Print Params
Command ==>                               Scroll ==> CSR

                Do you want to print this display (Y/N): Y

    Sysout    ==> A   Copies    ==> 01   Title      ==> N
    Hold (Y/N) ==> N   Page Length ==> 55   Destination ==>

BROWSE - USER02.TSCSSA.REPORT.OUTPUT ----- LINE 00000000 COL 001 080
***** Top of Data *****
1
Date: 07/03/1998
Time: 15:29

                                           SSA Version
                                           Generic Userid Table Report

   RACF      Name      Default  Profile  Create   Last-Used   Pas
   UserID                                Group   Owner    Date       Date
-----
TESTU004  STRICTLY TEST USERS  TSTG001  TSTG001  1997-05-26
TESTU015  STRICTLY TEST USERS  TSTG001  TSTG001  1997-05-26
TESTU016  STRICTLY TEST USERS  TSTG001  TSTG001  1997-05-26
TESTU017  STRICTLY TEST USERS  TSTG001  TSTG001  1997-05-26

```

Sort Mode Usage

Each generic search function has the capability of sorting the display in a order of your own choosing. You may sort on multiple fields in different sort sequences. For example, you may sort on the Name field, in ascending order, and the Default Group, in descending order at the same time. You may even sort on any selections that you made, to move them all up towards the top of the display.

To use the sort mode:

- 1 Set the Operational Mode to S for Sort and press ENTER.
- 2 The sort pop-up panel appropriate for the information you have searched on is displayed. Choose the field(s) and order(s) to sort on. If you space out an existing Sort Field Number then that field will not be included, and will be removed upon pressing the ENTER key.

```

Onl .----- SSA -----
Co  Command ==>

      Enter the number of the field and the sort direction below.

SEL                                     Available Fields:
---      1. SEL      3. NAME      5. PROFILE OWNER  7. LAST USED DATE
---      2. USERID   4. DEFAULT GROUP  6. CREATE DATE   8. REVOKE
-----
Sort      Field      Sort
Order    Number    Direction (A,D)  Description
-----
1         2         A              USERID,ASCENDING
2         -         -
3         -         -
4         -         -
5         -         -
6         -         -
7         -         -
8         -         -

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

The above will sort any selected entries to the top of the display (an 'S' is located after a '<blank>' character in the IBM EBCDIC code page), and then sort by the name field in ascending order.

Adhoc Report Generation

SSA has the ability to not only run Online Generic Searches in batch but also the ability to create an adhoc report which uses a format you design. This part of the manual will describe in detail:

- How to specify the generic search criteria and masks.
- How to specify the control cards for general formatting of the report.
- How to build an adhoc report mask to create a unique report layout of your choosing.

How to Specify Generic Search Criteria

Although the Online Generic Search panels will build the search criteria and control cards for you, it is important to understand how to construct the control cards from scratch, or at the least be able to interpret what the control cards mean in a particular job run.

The generic search control cards use the ISPF table name assigned to the particular field in the information you are reporting on. The ISPF tables are fully documented in Appendix B including special details concerning the Adhoc Report Generation process in relation to the variable names and their substitution mask values. For example, the General Userid Information Generic Search uses ISPF table AATBLE01. The userid field is labeled AAUSER. Therefore, to indicate a search criteria for the user field you would build a control card with the field label, an equal sign ('=') and the mask you want that field subjected to. If you are using standard searching, you can also set the condition for the mask. For example, you may want to set the condition to 'Not Equal'. Thus, you would build a control card with the field label, an underscore ('_'), the keyword 'COND', and equal sign ('=') and the two letter condition. Below is an example for the userid field in the general userid information search:

Standard Search Control Card Sample

```
AASYSIN      DD *
AAUSER=X*    Indicates every userid that starts with X
AAUSER_COND=NE Indicates a Not Equal condition
```

Extended Search Control Card Sample

```
AASYSIN      DD *
AAUSER=%X%%%% Indicates every userid that is seven characters long
                  and has a X in position three
```

The following rules apply to the search control cards:

- All control cards must start in column one or they will be marked as invalid cards and ignored.
- The mask specified can only be as long as the variable in question. For example, the userid field AAUSER in the ISPF table AATBLE01 is a maximum of eight characters, therefore, the maximum the mask can be is eight characters.
- The mask can be an explicit value.
- Standard masking is a left to right match that only uses the asterisk ('*') at the end of the input.

- Extended masking can use a percent sign ('%') for individual character masking and an asterisk as an end of string mask. See the search details in the global conventions part of this section for more details.
- Extended masking always uses an equal condition.
- If you specify more than one mask for the same field, the last in order will be used.
- Extended masking only applies to fields that are 3 characters or longer. Fields that have set value lists like the UACC on dataset profiles (that is, NONE, READ, and so on.), can only use explicit standard searches.
- Search criteria cards are entered under DD AASYSIN.

How to Build an Adhoc Report Mask

When you run the Online Generic Searches in batch, you have the choice of using the default report layout or building an adhoc report mask. Building an adhoc report mask only requires three pieces of information: 1) What do you want the report to look like, 2) Which generic search will generate the information required and 3) How to input the mask/design. The first piece is up to you. You must spend a little bit of time designing the layout and titles of your report. The second piece requires you to choose which of the 28 search categories best fits your information needs. When you have chosen the category, you must construct the adhoc report mask to create the report you originally designed.

Adhoc report masks use literal substitution. That means that if you have an eight character field like a userid, you must enter the mask value that not only tells SSA what to put in that position but also reserves that space. For example, let us say you wanted to generate a simple report of userid, name and default group. Below is an example of what the mask might look like and the substituted results:

Adhoc Report Mask Sample

RACF Userid	Name	Default Group
-----	-----	-----
aauser	aausname	aausdflg

Substitution Results Sample

RACF Userid	Name	Default Group
-----	-----	-----
USERBOB1	SMITH, ROBERT	SYS1

Important Rules

- See Appendix B for details on what mask value to specify for substituting the field you want.
- If a mask is shorter than the actual value that is going to be substituted (that is, AAUSER is only six characters and the RACF userid field is eight characters) you must leave a sufficient amount of spaces to 'pad' the mask. In the case of the mask variable AAUSER, you must specify two spaces after the mask to allow for eight character substitution.

- The masks must be either all uppercase or all lowercase. If you mix cases, the mask will be ignored.
- You can specify as many masks per input line as you want as long as you allow for the proper amount of 'padding'.

Adhoc Report Control Cards

When running an Online Generic Search in batch you can control the format and processing. Below is a complete list of the control cards categorized under the DDNAME which they must reside. Keep in mind that all control cards are optional; if none are specified the program will produce a standard report with no masking and sequenced in the order the table was originally sorted when originally stored.

DDNAME=AACTLCDS

SEARCH=EXTENDED	This indicates that any search criteria you enter is to use the extended search feature. The default is standard search.
NOTITLE	This indicates you do not want titles printed on this report. The default is set to use titles.
SUMMARY	This indicates you want a summary produced which includes totals and the masking used to produce the report. The default is no summary.
OVRTITLE=	Enter up to 40 characters you want SSA to use to override the high level title on the report. The default value is a description of the Online Generic Search report being run.
COMPANY=	Enter up to 40 characters you want SSA to use to override the company information used on the report. The default is SSA and the version of SSA.
TTL1A= & TTL1B=	TTL1A and TTL1B are put together to form the first title line of the report. Each entry can take up to 66 characters and is used for the entire 66 character section. Therefore, if you put a small value in TTL1A, the remainder up to 66 characters will be padded with spaces and then the text in TTL1B will be tacked on for the remaining 66 characters.
TTL2A= & TTL2B=	See explanation for TTL1A & TTL1B. Keep in mind that 2A and 2B makeup the second title line.
TTL3A= & TTL3B=	See explanation for TTL1A & TTL1B. Keep in mind that 3A and 3B makeup the third title line.
TTL4A= & TTL4B=	See explanation for TTL1A & TTL1B. Keep in mind that 4A and 4B makeup the fourth title line.
INP1A= & INP1B=	INP1A and INP1B are put together to form the first adhoc report mask line of the report. Each entry can take up to 66 characters and is used for the entire 66 character section. Therefore, if you put a small value in INP1A, the remainder up to 66 characters will be padded with spaces and then the mask in INP1B will be tacked on for the remaining 66 characters.

INP2A= & INP2B=	See explanation for INP1A & INP1B. Keep in mind that 2A and 2B makeup the second adhoc report mask line.
INP3A= & INP3B=	See explanation for INP1A & INP1B. Keep in mind that 3A and 3B makeup the third adhoc report mask line.
INPUT4A= & INPUT4B=	See explanation for INP1A & INP1B. Keep in mind that 4A and 4B makeup the fourth adhoc report mask line.
INP5A= & INP5B=	See explanation for INP1A & INP1B. Keep in mind that 5A and 5B makeup the fifth adhoc report mask line.
SORT1=	Indicate the sorting you want performed on the information you are reporting on. If no sorting is specified, the table used is sorted in the order the table was originally sorted when originally stored. SSA uses ISPF sorting and the sort card specification on the control card uses the same syntax. Below are the syntax instructions for ISPF sorting.

ISPF Sort Syntax Instructions

When building an ISPF sort instruction you must supply the field name, the format of the field and the direction that particular field should be sorted.

Field Name: The field name must be retrieved from the ISPF table that is supplying the generic search you are using (See Appendix B for details).

Field Format: The format of the field can be:

C = Character

N = Numeric

B = Binary

Note SSA always uses Character.

Direction: The sort direction can be:

A = Ascending

B = Descending

An example of a correct sort control card is:

```
SORT1=AAUSER,C,A
```

This control card indicates that you want the table sorted on field AAUSER which is character based and in ascending order. If you wanted to sort on a secondary field you would simply add the information for that field on to the end of the card as shown below:

```
SORT1=AAUSER,C,A,AAUSNAME,C,D
```

This card indicates you want the table sorted on field AAUSER which is character based first in ascending order then you want the table sorted by field AAUSNAME which is character based in descending order.

Note You have two sort input cards available. SORT1 is the first part of the sort sequence and allows for a string up to 66 characters. If your sort sequence is longer than that, you can use the SORT2 control card for another 66 characters. SORT1 and SORT2 are strung together to makeup the total sort control card.

LINES - PER - PAGE=*nn*

Indicate the number of lines per page you want the report paginated into. The value must be from 11 to 99. The default is 55.

EXPAND - GROUPS

Indicates that you want to expand the users in groups. This control card is only applicable to Dataset and Resource permit searches. Also, this control card cannot be used with the Adhoc Report process. It only applies to the standard report for permits.

DDNAME=SYSTSIN

DD SYSTSIN must include the ISPF start statement for the appropriate reporting program. Below is an example of the proper ISPF invocation of the report program for General User Information Generic Search:

Generic Search Report Program Invocation Sample

```
//SYSTSIN DD *
ISPSTART PGM(AAGSRU01)
//*
```

Below is a table showing the reporting program name used by each generic search category and the ISPF table used:

Online Generic Search Option	Report Program Name	SSA ISPF Table Used
General Userid	AAGSRU01	AATBLE01
Userid TSO Segment	AAGSRU02	AATBLE05
Userid CICS Segment	AAGSRU03	AATBLE07
Userid DFP Segment	AAGSRU04	AATBLE08
Userid Language Segment	AAGSRU05	AATBLE09
Userid OPERPARM Segment	AAGSRU06	AATBLE10
Userid WORKATTR Segment	AAGSRU07	AATBLE29
Userid NETVIEW Segment	AAGSRU08	AATBLE30
Userid OMVS Segment	AAGSRU09	AATBLE11
Userid DCE Segment	AAGSRU10	AATBLE33
RRSF Associations	AAGSRU11	AATBLE34
Connects	AAGSRU12	AATBLE12
CLAUTH Authorities	AAGSRU13	AATBLE04
Userid Security Categories	AAGSRU14	AATBLE03
General Group	AAGSRG01	AATBLE13
Group DFP Segment	AAGSRG02	AATBLE15
Group OMVS Segment	AAGSRG03	AATBLE02

Online Generic Search Option	Report Program Name	SSA ISPF Table Used
General Dataset	AAGSRD01	AATBLE17
Dataset Permissions	AAGSRD02	AATBLE20
Dataset Security Categories	AAGSRD03	AATBLE27
General Resource	AAGSRR01	AATBLE22
General Resource Permissions	AAGSRR02	AATBLE26
General Resource Members	AAGSRR03	AATBLE25
General Resource Session Segment	AAGSRR04	AATBLE18
General Resource DLFDATA Segment	AAGSRR05	AATBLE21
General Resource STDATA Segment	AAGSRR06	AATBLE24
General Resource SystemView Segment	AAGSRR07	AATBLE35
General Resource Security Categories	AAGSRR08	AATBLE16



CHAPTER 5

Command Generation

A common concern of RACF administrators is the time spent on repetitive tasks to maintain an established database. Security administrators need tools that allow them to define large numbers of similar groups, userids, and other profiles. SSA provides the ability to replicate profiles or remove all references to profiles to reduce repetitive, 'data entry-like' tasks.

It is important to understand how SSA creates the commands and what functions are available.

- SSA creates all the commands for your review and eventual submission. SSA does not submit any generated commands unless requested.
- SSA uses information stored in the SSA ISPF tables. This information is only as valid and complete as the last time the ISPF tables were updated. The exception is the CHECK option, which does a live check of the RACF database to see if the new profile exists before building the commands.
- You must validate all generated commands. It is your responsibility to ensure the accuracy of your commands and those you choose to submit.
- SSA can use any old copies of the version 1.x ISPF tables to build commands from. You can also use the RACF utility IRRDBU00 to process 'old' copies of your RACF database and use all the SSA features based on that information.
- SSA does not use RACF modeling commands. SSA creates all the commands necessary to recreate a profile without having to rely on the original profile actually existing in your database. Therefore, you will not see an RDEFINE FROM command, but rather an RDEFINE and any other subsequent commands necessary to recreate the original profile from scratch.

Command Generation Global Conventions

Through-out the SSA product and manual there are several “global” conventions that occur. For the Command Generation section the following conventions apply.

Security: All SSA command generation features are protected at both the screen dialog level and at the command generation level. The default RACF general resource class is MAASRULE and READ is the required access level. Below is a list of the command generation options and the default security profiles that a user must have access to in order to execute the option. Refer to ‘Configuration’ on page 499 about changing the default protecting class or profiles if you want to change them.

Command Generation Option	RACF Profile
Replicate Userid Profiles	MEGASOLVE-SSA.REPLICATE.USERID
Replicate Group Profiles	MEGASOLVE-SSA.REPLICATE.GROUP
Replicate Dataset Profiles	MEGASOLVE-SSA.REPLICATE.DSNPROF
Replicate General Resource Profiles	MEGASOLVE-SSA.REPLICATE.RSCPROF
Replicate General Resource Classes	MEGASOLVE-SSA.REPLICATE.RSCCLAS
Transfer Userid Profiles	MEGASOLVE-SSA.TRANSFER.USERID
Transfer Group Profiles	MEGASOLVE-SSA.TRANSFER.GROUP
Transfer Dataset Profiles	MEGASOLVE-SSA.TRANSFER.DSNPROF
Transfer General Resource Profiles	MEGASOLVE-SSA.TRANSFER.RSCPROF
Transfer General Resource Classes	MEGASOLVE-SSA.TRANSFER.RSCCLAS
Transfer Ownership	MEGASOLVE-SSA.TRANSFER.OWNER
Transfer Notifies	MEGASOLVE-SSA.TRANSFER.NOTIFY
Remove All References to a Userid	MEGASOLVE-SSA.REMOVE.USERID
Remove All References to a Group	MEGASOLVE-SSA.REMOVE.GROUP
Remove Obsolete Entries	MEGASOLVE-SSA.REMOVE.OBSOLETE

Batch, Online, or SCHEDULE Operational Modes

BATCH mode processing generates the necessary JCL to create the SSA commands you requested. SSA then displays the Review Generated JCL screen as shown below.

```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'IBMUSER.TSCSSA.TEMP.JCL(BATCH)'

OPTION ==> S

Enter E to Edit the Generated JCL

V to View the Generated JCL

S to Submit the Generated JCL

ST to Store the Generated JCL

SC to Schedule the Generated JCL

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

- E Select E if you want to be placed in an EDIT session.
- V Select V if you want to be placed in a VIEW session.
- S Select S if you want to submit the generated JCL.
- ST Select ST if you want to store the generated JCL in the SSA storage facility.
- SC Select SC if you want to schedule the generated JCL through The SCHEDULER. For details on scheduling, see 'The SCHEDULER' on page 269.

ONLINE mode processing creates the commands automatically based upon your entries and selections and places you in an EDIT session labeled Process Generated Commands, as shown below.

```

Process Generated Commands ----- SSA ----- Process Generated Comm
Command ==>                               Scroll ==> C

Action Command          Action Taken
-----
AAEXEC                  Execute Commands Immediately
AABATCH                 Place Commands in Batch JCL
AASCHED                 Schedule Commands
AASTORE                 Store or Retrieve Commands

EDIT ----- IBMUSERTSCSSA.ADHOC.OUTPUT----- COLUMNS 00001 00
***** ***** Top of Data *****
=NOTE= COMMANDS ARE READY FOR EXECUTION
000001 ALTUSER USER02 PASSWORD RESUME
000002 CONNECT USER02 GROUP(SYS1) OW(SYS1)
000003 ALTUSER USER02 NOCICS
000004 ALTUSER USER01 PASSWORD RESUME
000005 CONNECT USER01 GROUP(SYS1) OW(SYS1)
000006 ALTUSER USER01 NOCICS
***** ***** Bottom of Data *****

```

To process the generated commands execute the listed Action Commands by typing the command on the command line.

- AAEXEC The generated commands are executed immediately. The commands appear on the screen as they are executed.
- AABATCH Encapsulates your commands in an IKJEFT01 step. Use the TSO SUBMIT command to run the job.

- AASCHED** Interfaces with SSA's The SCHEDULER to schedule the generated commands to be run on a specific date and time.
- AASTORE** Allows storage and retrieval of (previously stored), generated commands.

SCHEDULE mode processing creates the commands automatically based upon your entries and selections and places you in an BROWSE session labeled Process Generated Commands, as shown below. From this screen, you can choose whether or not you want to schedule the commands. Your access to enter an item into the SCHEDULER will be verified before command generation is performed. For information about scheduling items, see 'The SCHEDULER' on page 269.

```

Command Generation ----- SSA ----- Command Generation
                        Process Generated Commands
Command ==>                                Scroll ==> C

Do you wish to schedule generated commands? (Y/N): Y

BROWSE - IBMUSERTSCSSA.COMMAND.OUTPUT --- LINE 00000000 COL 001
***** Top of Data *****
ADDUSER NEWUSER NAME(' ') -
DFLTGRP(SYS1 ) OWNER(IBMUSER )
ALTUSER NEWUSER SPECIAL OPERATIONS AUDITOR
PASSWORD USER(NEWUSER ) INTERVAL(030)
CONNECT NEWUSER GROUP(SYSCTLG ) OWNER(IBMUSER ) -
AUTH(USE ) -
UACC(READ )
CONNECT NEWUSER GROUP(SYS1 ) OWNER(SYS1 ) -
AUTH(CONNECT) -
UACC(READ )
PERMIT **
CLASS(PCICSPSB) ID(NEWUSER ) -
ACCESS(ALTER )

```

Command Generation JCL

All command generation options use the same JCL. Below is a sample of that JCL.

```

/*
/*
/******
/**
/**          SMART SECURITY ADMINISTRATOR          **
/**
/**          VERSION V.V          **
/**
/**          (C) YYYY UNICOM SYSTEMS, INC.          **
/**          ALL RIGHTS RESERVED          **
/******
/*
/* JCL CREATED BY USER01
/* JCL CREATED ON MM/DD/YYYY
/* JCL CREATED AT 14:37
/*
/* JOB FUNCTION: REPLICATE_USERID_PROFILES
/*
//STEP010 EXEC PGM=IKJEFT01,DYNAMNBR=30,TIME=1440,REGION=4096K
//SYSPROC DD DISP=SHR,
//          DSN=SSA.ISPCLIB

```



```

//ISPPROF DD DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
//          DCB=(LRECL=80,BLKSIZE=6160,RECFM=FB),UNIT=SYSDA
//ISPPLIB DD DISP=SHR,
//          DSN=SSA.ISPPLIB
//ISPSLIB DD DISP=SHR,
//          DSN=SSA.ISPSLIB
//ISPMLIB DD DISP=SHR,
//          DSN=SYS1.SISPMENU
//          DD DISP=SHR,
//          DSN=SSA.ISPMLIB
//ISPTLIB DD DISP=SHR,
//          DSN=SYS1.SISPTENU
//AADBTLIB DD DISP=SHR,
//          DSN=SSA.RACFDATA.ISPTLIB
//STEPLIB DD DISP=SHR,
//          DSN=SSA.LOADLIB
//ISPCTL1 DD DSN=&CNTL1,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//ISPCTL2 DD DSN=&CNTL2,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//SYSTSPRT DD SYSOUT=*,DCB=(BLKSIZE=19019,LRECL=133,RECFM=FBA)
//SYSPRINT DD SYSOUT=*,DCB=(BLKSIZE=20000,LRECL=200,RECFM=FBA)
//ISPLLOG DD SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
//SYSOUT DD SYSOUT=*
//TEMPWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//AACMDOUT DD DISP=SHR,
//          DSN=USER01.TSCSSA.COMMAND.OUTPUT
//SYSTSIN DD *
REPUSR IBMUSER NEWUSER NAME('KEN SMITH')
ISPSTART PGM(AAREPUSR)
//*
```

Below is a brief explanation of the JCL DDs and what they must reference:

SYSPROC	Must reference the SSA CLIST library
ISPPLIB	Must reference the SSA Panel library
ISPSLIB	Must reference the SSA Skeleton JCL library
ISPMLIB	Must reference the ISPF system message library and the SSA ISPF message library
ISPTLIB	Must reference the ISPF table library
AADBTLIB	Must reference the SSA RACF information table library
STEPLIB	Must reference the SSA APF authorized load library
AACMDOUT	This DD must reference an output dataset with the following DCBs: RECFM=FB,LRECL=133,DSORG=PS
SYSTSIN	This DD is where the SSA commands for activating command generation are entered

Command Syntax Rules

All replication, transfer or removal command generation processes have the following syntax rules for the operands that control that particular process:

- UPPERCASE LETTERS or WORDS must be coded as they appear in the syntax diagrams, but do not have to be uppercase.
- Lowercase letters or words represent variables for which you can supply a value.
- Parentheses () must be entered exactly as they appear in the syntax diagram.
- An ellipsis ... (three consecutive periods) indicates that you can enter the preceding item more than once.
- A single item in brackets [] indicates that the enclosed item is optional. Do not specify the brackets in your command.
- Stacked items in brackets [] indicate that the enclosed items are optional. You can choose one or none. Do not specify the brackets in your command.
- Stacked items in braces { } indicate that the enclosed items are alternatives. You must specify one of the items. Do not specify the braces in your command.
- When you select a bracket that contains braces, you must specify one of the alternatives enclosed within the braces.
- Items separated by a vertical bar | indicate that you may specify only one of the items. Do not specify the vertical bar in your command.
- An underlined operand indicates the default value when no alternate value is specified.
- **BOLDFACE** or indicates information that must be given for a command.
- Single quotes ‘ ’ indicate that information must be enclosed in single quotes.
- Stacked items in brackets [] and separated by a comma indicate that the enclosed items are optional and that you can choose more than one.

Initiating the Command Generation Process

All command generators have two components to initiate command generation. The first component processes the choices you have selected/coded and the second initiates the command building process. The example below is for replicating a userid. The first component REPUSR reviews and stores your choices. The second component AAREPUSR initiates the building process.

Example for replicating a userid:

```
//SYSTSIN DD *
  REPUSR USERBOB USERKEN NAME('KEN SMITH')
  ISPSTART PGM(AAREPUSR)
//*
```

The rules for the initiating components are:

- The command verifying component (control card program) must be before the command generation initiator component.

- The command verifying component can have parameters that span several lines but each line must not exceed column 70 and must be continued with a plus sign or dash.

Command Generation Main Menu

The Command generation Main Menu contains three groups of options for command replication, transfer, and removal.

```
Command Generation ----- SSA ----- Command Generation
                               Main Menu
Option ==>

      Replicate:  1  Replicate Userid Profiles
                  2  Replicate Group Profiles
                  3  Replicate Dataset Profiles
                  4  Replicate General Resource Profiles
                  5  Replicate General Resource Classes

      Transfer:   6  Transfer Userid Profiles
                  7  Transfer Group Profiles
                  8  Transfer Dataset Profiles
                  9  Transfer General Resource Profiles
                 10  Transfer General Resource Classes
                 11  Transfer Ownership
                 12  Transfer Notifications

      Remove:     13  Remove All References to a Userid
                  14  Remove All References to a Group
                  15  Remove All Obsolete Entries

                               Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Replicate:

Replication uses the ‘old’ entry as a model to build a new entry. It does not modify the ‘old’ entry; it only models it.
- Transfer:

The Transfer process removes the ‘old’ entry and builds a new entry to replace the ‘old’.
- Remove:

The Removal process removes all references to either a userid or group. The Removal of Obsolete Entries removes all entries in the database that qualify as obsolete. Usually an obsolete entry is noted as such when the entry doesn’t have a corresponding userid or group.

Note Care should be taken when using the Transfer or Removal processes because they generate commands to delete RACF profiles and, if requested, physical datasets.

Replicate Userid Profiles

Replicate Userid Profiles creates, based upon your selection criteria, all the commands to replicate a userid.

```

Command Generation ----- SSA ----- Command Generation
                          Replicate Userid Profiles
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----

      Model Userid   New Userid   Name (If Different)   Default Options (Y/N)?
==> IBMUSER        ==> NEWUSER   ==> KEN SMITH                ==> N
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -
==>                ==>          ==>                          ==> -

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

- Model UserID** Specify the userid to be replicated. The model userid must be specified. The userid does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables.
- New UserID** Specify the userid that will be the recipient of the generated commands. The New UserID must be specified. The userids status in RACF is only dependant on the options you choose to replicate. If you choose to replicate the entire Model UserID then the New UserID should not exist. If you choose to replicate only a portion of the Model UserID, then the New UserID must exist for the commands to execute successfully.
- Name** You can optionally override the name field of the model userid.
- Default Options** Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, refer to ‘Replicate Userid Profile Overrides Options Screen’ below.

Replicate Userid Profile Overrides Options Screen

Replicate Userid Profiles creates all commands to replicate userid profiles based upon your selection criteria.

----- SSA -----

Replicate Userid Profile Overrides

Command ==>

Model
Userid
IBMUUSER

New
Userid
NEWUSER

Name
KEN SMITH

Main Options

Userid Segments

	More:	+		More:	+
Adduser	(Y/N)	Y	All Segments	(Y/N)	Y
Attributes	(Y/N)	Y	TSO	(Y/N)	Y
Connects	(Y/N)	Y	CICS	(Y/N)	Y
All Permits	(Y/N)	Y	DFP	(Y/N)	Y

AluADD ==> _____

Alias ==> _____

Installation Data ==> _____

_____ <==

Hit Enter to Process Entry PF03=Bypass Entry/PF01=HELP

If you chose to override the default settings for the replicate userid process, you will be presented with the override screen. Below is a brief explanation of those options. Options are in alphabetical order; not the order they appear on the screen.

Note Be sure to use the scrolling boxes to display all override options available.

- ADDUSER

Indicate if you want an ADDUSER command to be generated for the New Userid. “Y” is the default.
- Alias

Specify the user catalog to be used in a define alias command. The catalog name can be up to 44 characters long and SSA will not check the existence of the catalog. The syntax of the command generated is:

DEFINE ALIAS(NAME(‘USERBOB’) -
RELATE(‘USER.CATALOG’))
- All Permits

Indicate if you want all permits (dataset and general resource) of the Model Userid to be replicated. “Y” is the default. If you specify “N”, the choice will fall to the individual questions concerning dataset or general resource permits.
- All Segments

Indicate if you want all userid segments of the Model Userid to be replicated. “Y” is the default. If you specify “N”, the choice will fall to the questions concerning the individual segments.
- ALUADD

Enter up to 60 characters that will be added to an ALTUSER command that follows the initial ADDUSER command if you replicated the entire Model Userid. The data entered is the responsibility of the user and will not be validated by SSA.
- At

Enter a RRSF destination that will be specified on each command generated using the AT parameter.
- Attributes

Indicate if you want all global attributes on the Model Userid to be replicated. “Y” is the default.
- Check

Indicate if you want the existence of the New Userid to be validated before generating commands. If it exists, no ADDUSER command will be generated, however, the remainder of the commands will be generated accordingly. “N” is the default.

CICS Segment	Indicate if you want the CICS segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Connects	Indicate if you want all connect profiles on the Model Userid to be replicated. “Y” is the default.
Dataset Profiles	Indicate if you want all dataset profiles where the Model Userid is the HLQ to be replicated. The replication process will include all aspects of those dataset profiles including but not limited to permits, installation data, audit levels, etc. “Y” is the default. If you indicate “Y”, the Default Dataset Profiles flag will be turned off to deactivate default dataset profile creation.
DCE Segment	Indicate if you want the DCE segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Default Dataset Profiles	Indicate if you want a default generic dataset profile created for the New Userid. “N” turns off default dataset profile creation, “G” activates the creation of a non-EGN default dataset profile (that is, IBMUSER.*), and “E” activates the creation of a EGN default dataset profile (that is, IBMUSER.**). “N” is the default.
Default Group	Enter a group to override the default group found on the Model Userid.
DFP Segment	Indicate if you want the DFP segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
DSN Permits	Indicate if you want all dataset permits of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.
Installation Data	Enter up to 255 characters to override the installation data found on the Model Userid.
Language Segment	Indicate if you want the LANGUAGE segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
NetView Segment	Indicate if you want the NETVIEW segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
OMVS Segment	Indicate if you want the OMVS segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
OnlyAt	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
OPERPARM Segment	Indicate if you want the OPERPARM segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Password	Enter a password that be used to override the default password assigned by RACF when a new userid is added.
Profile Owner	Enter a valid userid or group that will be used to override the replicated profile owner at the userid profile level on the Model Userid.

RSC Permits	Indicate if you want all general resource permits of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.
Security Entries	Indicate if you want all security labels, levels and categories of the Model Userid to be replicated. “Y” is the default.
TSO Segment	Indicate if you want the TSO segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
WORKATTR Segment	Indicate if you want the WORKATTR segment of the Model Userid to be replicated. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.

Command Generation Initiators

Request Parser: REPUSR

The complete syntax of the Command is:

REPUSR	Model Userid
	New Userid
	[<u>ADU</u> NOADU]
	[ALIAS(catalog to add alias to)]
	[ALUADD('additions to ALU commands')]
	[AT(additions to commands for RRSF)]
	[<u>ATTR</u> NOATTR]
	[<u>CON</u> NOCON]
	[DATA('new installation data')]
	[DFL(new default group)]
	[<u>DSN</u> NODSN]
	[NAME('override model name')]
	[<u>NOCHECK</u> CHECK]
	[<u>NOGEN</u> NOEGN EGN]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> (
	[<u>ALL</u> NONE]
	[DSN, RSC])
	[PSW(new password)]
	[<u>SEC</u> NOSEC]
	[<u>SEG</u> (
	[<u>ALL</u> NONE]
	[TSO NOTSO]
	[CICS NOCICS]
	[DCE NODCE]
	[DFP NODFP]
	[LANGUAGE NOLANGUAGE]
	[OPERPARM NOOPERPARM]
	[WORKATTR NOWORKATTR]
	[OMVS NOOMVS AOMVS]
	[NETVIEW NONETVIEW])

Request Initiator: AAREPUSR

Execution sample:

```
//SYSTSIN DD *
  REPUSR USERBOB USERKEN NAME('KEN SMITH')
  ISPSTART PGM(AAREPUSR)
//*
```

Replicate Userid Processing Notes

Keep the following in mind when using the Replicate Userid function:

- If you enter both an AT and ONLYAT override only the AT will be processed.
- If a value of NONE on the KEY field of the OPERPARM segment is encountered it will be treated as no key.
- If a value of 00000 on the STORAGE field of the OPERPARM segment is encountered it will be treated as no storage although the RACF ALTUSER OPERPARM(.....) command creates this value as a default when storage is not specified.

Replicate Group Profiles

Replicate Group Profiles creates all commands to replicate a group based upon your selection criteria.

```

Command Generation ----- SSA ----- Command Generation
                          Replicate Group Profiles
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----
Model Group  New Group  Supgroup (If Different) Default Options (Y/N)
==> SYS1      ==> NEWSYS1 ==> _____ ==> N
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -
==> _____ ==> _____ ==> _____ ==> -

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Model Group	Specify the group to be replicated. The Model Group must be specified. The group does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables.
New Group	Specify the group that will be the recipient of the generated commands. The New Group must be specified. The groups status in RACF is only dependant on the options you choose to replicate. If you choose to replicate the entire Model Group then the New Group should not exist. If you choose to replicate only a portion of the Model Group, then the New Group must exist for the commands to execute successfully.
Supgroup	You can optionally override the superior group of the Model Group.
Default Options	Specify "Y" if you want all default options to remain or "N" if you wish to specify options on the override screen. For details, see 'Replicate Group Profile Overrides Options Screen' below.

Replicate Group Profile Overrides Options Screen

----- SSA -----

Replicate Group Profile Overrides

Command ==>

Model
Group
SYS1

New
Group
NEWSYS1

Superior
Group

Main Options

Group Segments

More: +

Addgroup(Y/N) Y

Attributes(Y/N) Y

Connects(Y/N) Y

All Segments(Y/N) Y

DFP(Y/N) Y

OMVS(Y/N) Y

AlgADD ==> _____

Alias ==> _____

Installation Data ==> _____

_____ <==

Hit Enter to Process Entry PF03=Bypass Entry/PF01=HELP

If you chose to override the default settings for the replicate group process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Note Be sure to use the scrolling boxes to display all override options available.

- Addgroup

Indicate if you want an ADDGROUP command to be generated for the New Group. “Y” is the default.
- Alias

Specify the user catalog to be used in a define alias command. The catalog name can be up to 44 characters long and SSA will not check the existence of the catalog. The syntax of the command generated is:

DEFINE ALIAS(NAME(‘NEWSYS1’) -
RELATE(‘USER.CATALOG’))
- All Permits

Indicate if you want all permits (dataset and general resource) of the Model Group to be replicated. “Y” is the default. If you specify “N”, the choice will fall to the individual questions concerning dataset or general resource permits.
- All Segments

Indicate if you want all group segments of the Model Group to be replicated. “Y” is the default. If you specify “N”, the choice will fall to the questions concerning the individual segments.
- AlgADD

Enter up to 60 characters that will be added to an ALTGROUP command that follows the initial ADDGROUP command if you replicated the entire Model Group. The data entered is the responsibility of the user and will not be validated by SSA.
- AT

Enter a RRSF destination that will be specified on each command generated using the AT parameter.
- Attributes

Indicate if you want all group attributes on the connects to the Model Group to be replicated. “Y” is the default.

Check	Indicate if you want the existence of the New Group to be validated before generating commands. If it exists, no ADDGROUP command will be generated, however, the remainder of the commands will be generated accordingly. "N" is the default.
Connect	Indicate if you want all connect profiles on the Model Group to be replicated. "Y" is the default.
Dataset Profiles	Indicate if you want all dataset profiles where the Model Group is the HLQ to be replicated. The replication process will include all aspects of those dataset profiles including but not limited to permits, installation data, audit levels, etc. "Y" is the default. If you indicate "Y", the Default Dataset Profiles flag will be turned off to deactivate default dataset profile creation.
Default Dataset Profiles	Indicate if you want a default generic dataset profile created for the New Group. "N" turns off default dataset profile creation, "G" activates the creation of a non-EGN default dataset profile (that is, NEWSYS1.*), and "E" activates the creation of a EGN default dataset profile (that is, NEWSYS1.**). "N" is the default.
DFP Segment	Indicate if you want the DFP segment of the Model Group to be replicated. "Y" is the default which is duplicated by the "Y", if specified, on All Segments.
DSN Permits	Indicate if you want all dataset permits of the Model Group to be replicated. "Y" is the default which is duplicated by the "Y", if specified, on All Permits.
Installation Data	Enter up to 255 characters to override the installation data found on the Model Group.
OMVS Segment	Indicate if you want the OMVS segment of the Model Group to be replicated. "Y" is the default which is duplicated by the "Y", if specified, on All Segments.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Profile Owner	Enter a valid userid or group that will be used to override the replicated profile owner at the group profile level on the Model Group.
RSC Permits	Indicate if you want all general resource permits of the Model Group to be replicated. "Y" is the default which is duplicated by the "Y", if specified, on All Permits.
Security Entries	Indicate if you want all security labels, levels and categories of the Model Group to be replicated. "Y" is the default.
Superior Group	Enter a valid group that will be used to override the superior group found for the Model Group.

Command Generation Initiators

Request Parser: REPGRP

The complete syntax of the Command is:

REPGRP	Model Group
	New Group
	[<u>ADG</u> NOADG]
	[ALGADD('additions to ALG commands')]
	[ALIAS(catalog to add alias to)]
	[AT(additions to commands for RRSF)]
	[<u>ATTR</u> NOATTR]
	[<u>CON</u> NOCON]
	[DATA('new installation data')]
	[<u>DSN</u> NODSN]
	[<u>NOCHECK</u> CHECK]
	[<u>NOGEN</u> GEN EGN]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> ([<u>ALL</u> NONE] [DSN, RSC])
	[<u>SEC</u> NOSEC]
	[<u>SEG</u> ([ALL NONE] [<u>DFP</u> NODFP] [OMVS NOOMVS AOMVS])
	[SUP(new superior group)]

Request Initiator: AAREPGRP

Execution sample:

```
//SYSTSIN DD *  
  REPGRP SYS1 NEWSYS1 SUP(NEWSUPGP)  
  ISPSTART PGM(AAREPGRP)  
//*
```

Replicate Group Profile Processing Notes

N/A

Replicate Dataset Profiles

The Replicate Dataset Profiles screen provides options to create all commands to replicate a specific dataset profile.

```

Command Generation ----- SSA ----- Command Generation
                        Replicate Dataset Profiles
Command ==>
                        Operational Mode (Batch/Online/Schedule) ==> BATCH
                        -----
Model Profile                                Model Volume
1 => SYS1.*                                => _____
2 => _____                            => _____
3 => _____                            => _____
4 => _____                            => _____
5 => _____                            => _____
6 => _____                            => _____

New Profile                                New Volume    Default
1 => NEWSYS1.*                            => _____    Options
2 => _____                            => _____    ==> N
3 => _____                            => _____    ==> -
4 => _____                            => _____    ==> -
5 => _____                            => _____    ==> -
6 => _____                            => _____    ==> -

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Model Profile	Specify the dataset profile to be replicated. The Model Dataset Profile must be specified. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables.
Model Volume	If the Model Profile is discrete, you must specify the volume. If you do not specify the volume, SSA will consider the Model Profile a fully qualified generic profile and will search and replicate accordingly.
New Profile	Specify the dataset profile that will be the recipient of the generated commands. The New Profile must be specified. The profiles status in RACF is only dependant on the options you choose to replicate. If you choose to replicate the entire Model Profile then the New Profile should not exist. If you choose to replicate only a portion of the Model Profile, then the New Profile must exist for the commands to execute successfully.
New Volume	If the Model Profile is discrete and you wish to define the New Profile as discrete, you must specify a New Volume.
Default Options	Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Replicate Dataset Profile Overrides Options Screen’ below.

Replicate Dataset Profile Overrides Options Screen

----- SSA -----

Replicate Dataset Profile Overrides

Command ==>

Model ==> SYS1.*

New ==> NEWSYS1.*

Volume ==>

Volume ==>

Add Dataset Profile (Y/N) Y

Permits (Y/N) Y

DFP Segment (Y/N) Y

Security Entries (Y/N) Y

Check New DSN Profile (Y/N) N

Profile Owner ==> _____

RRSF At ==> _____

RRSF Onlyat ==> _____

AldADD ==> _____

Installation Data ==> _____

_____ <==

Hit Enter to Process Entry PF03=Bypass Entry/PF01=HELP

If you chose to override the default settings for the replicate dataset profile process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Add Dataset Profile	Indicate if you want an ADDSD command to be generated for the New Profile. “Y” is the default.
AldADD	Enter up to 60 characters that will be added to an ALTDSD command that follows the initial ADDSD command if you replicated the entire Model Profile. The data entered is the responsibility of the user and will not be validated by SSA.
AT	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Profile to be validated before generating commands. If it exists, no ADDSD command will be generated, however, the remainder of the commands will be generated accordingly. “N” is the default.
DFP Segment	Indicate if you want the DFP segment of the Model Profile to be replicated. “Y” is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the Model Profile.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits of the Model Profile to be replicated. “Y” is the default.
Profile Owner	Enter a valid userid or group that will be used to override the replicated profile owner at the dataset profile level on the Model Profile.
Security Entries	Indicate if you want all security labels, levels and categories of the Model Profile to be replicated. “Y” is the default.

Command Generation Initiators

Request Parser: REPDSN

The complete syntax of the Command is:

REPDSN	Model Dataset Profile
	New Dataset Profile
	[<u>ADDSD</u> NOADDSD]
	[ALDADD('additions to ALD commands')]
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DFP</u> NODFP]
	[NEWVOL(volume of new dataset profile)]
	[<u>NOCHECK</u> CHECK]
	[OLDVOL(volume of discrete model dataset profile)]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[<u>SEC</u> NOSEC]

Request Initiator: AAREPDSN

Execution sample:

```
//SYSTSIN DD *
  REPDSN SYS1.* NEWSYS1.*
  ISPSTART PGM(AAREPDSN)
//*
```

Replicate Dataset Profile Processing Notes

N/A

Replicate General Resource Profiles

The Replicate General Resource Profiles screen provides options to create all commands to replicate a specific General Resource profile.

```
Command Generation ----- SSA ----- Command Generation
                          Replicate General Resource Profiles
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----

Model Profile ==> SUBMIT.IBMUSER

                          <==
Model Class   ==> SURROGAT

New Profile   ==> SUBMIT.NEWUSER

                          <==
New Class     ==> SURROGAT   Default Options (Y/N) ==> N

                          Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Model Profile

Specify the general resource profile to be replicated. The Model General Resource Profile must be specified. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables.
- Model Class

Specify the general resource class to which the Model Profile is defined. You must specify the Model Class. USER, GROUP, CONNECT and DATASET are not valid general resource classes.
- New Profile

Specify the general resource profile that will be the recipient of the generated commands. The New Profile must be specified. The profiles status in RACF is only dependant on the options you choose to replicate. If you choose to replicate the entire Model Profile then the New Profile should not exist. If you choose to replicate only a portion of the Model Profile, then the New Profile must exist for the commands to execute successfully.
- New Class

Specify a New Class to override the model class. If you do not specify a New Class, the Old Class will be used.
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Replicate General Resource Profile Overrides Options Screen’ below.

Replicate General Resource Profile Overrides Options Screen

```

----- SSA -----
Replicate General Resource Profile Overrides
Command ==>
Model Profile ==> SUBMIT.IBMUSER

               <==      Model Class      ==> SURROGAT
New Profile   ==> SUBMIT.NEWUSER

               <==      New Class       ==> SURROGAT
Installation Data ==> _____
_____
_____
Application Data ==> _____ <==
_____
_____
_____ <==
_____ More:      +
RaltADD ==> _____
Owner   ==> _____

Hit Enter to Process Entry      PF03=EXIT/PF01=HELP

```

If you chose to override the default settings for the replicate general resource profile process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Application Data	Enter up to 255 characters to override the application data found on the Model Profile.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Profile to be validated before generating commands. If it exists, no RDEFINE command will be generated, however, the remainder of the commands will be generated accordingly. "N" is the default.
DLFdata Segment	Indicate if you want the DLFDATA segment of the Model Profile to be replicated. "Y" is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the Model Profile.
Members	Indicate if you want all members of the Model Profile to be replicated. "Y" is the default.
Onlyat	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits of the Model Profile to be replicated. "Y" is the default.
Profile Owner	Enter a valid userid or group that will be used to override the replicated profile owner at the general resource profile level on the Model Profile.
RALTADD	Enter up to 60 characters that will be added to an RALTER command that follows the initial RDEFINE command if you replicated the entire Model Profile. The data entered is the responsibility of the user and will not be validated by SSA.

RDEFINE	Indicate if you want an RDEFINE command to be generated for the New Profile. “Y” is the default.
Security Entries	Indicate if you want all security labels, levels and categories of the Model Profile to be replicated. “Y” is the default.
Session Segment	Indicate if you want the SESSION segment of the Model Profile to be replicated. “Y” is the default.
STDATA Segment	Indicate if you want the STDATA (Started Task) segment of the Model Profile to be replicated. “Y” is the default.
SYSTEMVIEW Segment	Indicate if you want the SYSTEMVIEW segment of the Model Profile to be replicated. “Y” is the default.

Command Generation Initiators

Request Parser: REPRSC

The complete syntax of the Command is:

REPRSC	Model Resource Profile
	New Resource Profile
	Model Resource Class
	[APPLDATA('new application data')]
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DLFDATA</u> NODLFDATA]
	[<u>MEM</u> NOMEM]
	[NEWCLS(new resource class)]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[RALTADD('additions to RALT commands')]
	[<u>RDEF</u> NORDEF]
	[<u>SEC</u> NOSEC]
	[<u>SESSION</u> NOSESSION]
	[<u>SYSTEMVIEW</u> NOSYSTEMVIEW]
	[<u>STDATA</u> NOSTDATA]

Request Initiator: AAREPRSC

Execution sample:

```
//SYSTSIN DD *
  REPRSC SUBMIT.IBMUSER -
        SUBMIT.NEWUSER -
        SURROGAT
  ISPSTART PGM(AAREPRSC)
//*
```

Replicate General Resource Profile Processing Notes

Keep the following in mind when using the Replicate General Resource Profile function:

- AAREPRSC will validate that the request for particular segments are appropriate. The appropriateness of the request is determined by the Model Class and the segment requested. For example, if you requested that the STDATA segment be part of the replication process, yet the New Class you requested was FACILITY, the request for the STDATA segment replication would not be processed. This is important to help maintain a 'clean' database by eliminating definitions that have no use and ensuring that all commands generated are valid.

- If you enter a grouping class profile that has members as the Model Profile and a non-grouping class profile as the New Profile, SSA will still generate the ADDMEM commands for all members found on the Model Profile even though the commands will fail. It is the responsibility of the user to enter appropriate classes.
- If you enter a Model Class and a New Class that have incompatibilities in their CDT definitions, SSA will still generate all commands as requested. It is the responsibility of the user to enter classes that are compatible.

Replicate General Resource Classes

Replicate a General Resource Class creates all commands to replicate a specific General Resource class.

```

Command Generation ----- SSA ----- Command Generation
                          Replicate General Resource Classes
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----

Model Class      New Class      Default Options (Y/N)?
==> _____  ==> _____  ==> Y
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> -

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Model Class	Specify the general resource class to be replicated. The Model Class must be specified. The Model Class does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables.
New Class	Specify the general resource class that will be the recipient of the generated commands. The New Class must be specified and must exist in RACF for the generated commands to execute successfully.
Default Options	Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Replicate General Resource Class Overrides Options Screen’ below.

Replicate General Resource Class Overrides Options Screen

----- SSA -----

Replicate General Resource Class Overrides

Command ==>

Model Class GCICSTRN

New Class G\$PRDTRN

Installation Data ==> _____

_____ <==

Application Data ==> _____

_____ <==

More: +

RaltADD ==> _____

Owner ==> _____

RDEFINE (Y/N) ==> Y

Permits (Y/N) ==> Y

Members (Y/N) ==> Y

DLFDATA Segment (Y/N) ==> Y

Hit Enter to Process Entry PF03=Bypass Entry/PF01=HELP

If you chose to override the default settings for the replicate general resource class process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Application Data	Enter up to 255 characters to override the application data found on the profiles defined to the Model Class.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Class to be validated before generating commands. If it does not exist, no commands will be generated. "N" is the default.
DLFDATA Segment	Indicate if you want the DLFDATA segment found on the profiles defined to the Model Class to be replicated. "Y" is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the profiles defined to the Model Class.
Members	Indicate if you want all members found on the profiles defined to the Model Class to be replicated. "Y" is the default.
ONLYAT:	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits found on the profiles defined to the Model Class to be replicated. "Y" is the default.
Profile Owner	Enter a valid userid or group that will be used to override the replicated profile owner at the general resource profile level on the Model Class.
RALTADD:	Enter up to 60 characters that will be added to an RALTER command that follows the initial RDEFINE command if you replicated the entire Model Class. The data entered is the responsibility of the user and will not be validated by SSA.

RDEFINE:	Indicate if you want an RDEFINE command to be generated for all the profiles found on the profiles defined to the Old Class. “Y” is the default.
Security Entries	Indicate if you want all security labels, levels and categories found on the profiles defined to the Model Class to be replicated. “Y” is the default.
Session Segment	Indicate if you want the SESSION segment found on the profiles defined to the Model Class to be replicated. “Y” is the default.
STDATA Segment	Indicate if you want the STDATA segment found on the profiles defined to the Model Class to be replicated. “Y” is the default.
SYSTEMVIEW Segment	Indicate if you want the SYSTEMVIEW segment found on the profiles defined to the Model Class to be replicated. “Y” is the default.

Command Generation Initiators

Request Parser: REPCLS

The complete syntax of the Command is:

REPCLS	Model Resource Class
	New Resource Class
	[APPLDATA('new application data')]
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DLFDATA</u> NODLFDATA]
	[<u>MEM</u> NOMEM]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[RALTADD(additions to RALT commands)]
	[<u>RDEF</u> NORDEF]
	[<u>SEC</u> NOSEC]
	[<u>SESSION</u> NOSESSION]
	[<u>SYSTEMVIEW</u> NOSYSTEMVIEW]
	[<u>STDATA</u> NOSTDATA]

Request Initiator: AAREPCLS

Execution sample:

```
//SYSTSIN DD *
  REPCLS GCICSTRN G$PRDTRN
  ISPSTART PGM(AAREPCLS)
//*
```

Replicate General Resource Class Processing Notes

Keep the following in mind when using the Replicate General Resource Class function:

- AAREPCLS will validate that the request for particular segments are appropriate. The appropriateness of the request is determined by the Model Class and the segment requested. For example, if you requested that the STDATA segment be part of the replication process, yet the New Class you requested was FACILITY, the request for the STDATA segment replication would not be processed. This is important to help maintain a 'clean' database by eliminating definitions that have no use insuring that all generated commands are valid.
- If you enter a grouping class that has members as the Model Class and a non-grouping class as the New Class, SSA will still generate the ADDMEM commands for all members found on the Model Class even though the commands will fail. It is the responsibility of the user to enter appropriate classes.

- If you enter a Model Class and a New Class that have incompatibilities in their CDT definitions, SSA will still generate all commands as requested. It is the responsibility of the user to enter classes that are compatible.

Transfer Userid Profiles

The Transfer Userid Profiles process creates all commands to transfer all or some of one userid to another based upon your selection criteria.

```
Command Generation ----- SSA ----- Command Generation
                          Transfer Userid Profiles
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----

      Old Userid      New Userid      Default Options (Y/N)?
==> IBMUSER          ==> NEWUSER1      ==> N
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Old Userid

Specify the userid to be replaced. The Old Userid must be specified. The userid does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some of the commands will fail (that is, DELUSER).
- New Userid

Specify the userid that will be the recipient of the generated commands. The New Userid must be specified and the New Userid should not exist in RACF for all the commands to complete successfully (that is, ADDUSER).
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer Userid Profile Overrides Options Screen’ below.

Transfer Userid Profile Overrides Options Screen

```

----- SSA -----
Transfer Userid Profile Overrides

Command ==>

                Old      New
                Userid   Userid
                IBMUSER  NEWUSER1

Main Options                                Userid Segments
-----
| More: + | | More: + |
| Attributes (Y/N) Y | | All Segments (Y/N) Y |
| Connects (Y/N) Y | | TSO (Y/N) Y |
| All Permits (Y/N) Y | | CICS (Y/N) Y |
| DSN Permits (Y/N) Y | | DFP (Y/N) Y |
-----

Alias ==> _____
AluADD ==> _____
Installation Data ==> _____

_____ <==
Hit Enter to Process Entry      PF03=Bypass Entry/PF01=HELP

```

If you chose to override the default settings for the transfer userid process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Note Be sure to use the scrolling boxes to display all override options available.

Alias	Specify the user catalog to be used in a define alias command. The catalog name can be up to 44 characters long and SSA will not check the existence of the catalog. The syntax of the command generated is: DEFINE ALIAS(NAME('USERBOB') - RELATE('USER.CATALOG'))
All Permits	Indicate if you want all permits (dataset and general resource) of the Old Userid to be transferred. "Y" is the default. If you specify "N", the choice will fall to the individual questions concerning dataset or general resource permits.
All Segments	Indicate if you want all userid segments of the Old Userid to be transferred. "Y" is the default. If you specify "N", the choice will fall to the questions concerning the individual segments.
ALUAdd	Enter up to 60 characters that will be added to an ALTUSER command that follows the initial ADDUSER command. The data entered is the responsibility of the user and will not be validated by SSA.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Attributes	Indicate if you want all global attributes on the Old Userid to be transferred. "Y" is the default.
Cataloged Datasets	Indicate if you want rename commands generated for physical datasets where the Old Userid was the HLQ. VSAM and tape datasets will not be processed. 'N' is the default.

Check	Indicate if you want the existence of the New Userid to be validated before generating commands. If it exists, no ADDUSER command will be generated, however, the remainder of the commands will be generated accordingly. “N” is the default.
CICS Segment	Indicate if you want the CICS segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Connects	Indicate if you want all connect profiles on the Old Userid to be transferred. “Y” is the default.
Dataset Profiles	Indicate if you want all dataset profiles where the Old Userid is the HLQ to be transferred. The replication process will include all aspects of those dataset profiles including but not limited to permits, installation data, audit levels, etc. “Y” is the default.
DCE Segment	Indicate if you want the DCE segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Default Group	Enter a group to override the default group found on the Old Userid.
DFP Segment	Indicate if you want the DFP segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
DSN Permits	Indicate if you want all dataset permits of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.
Installation Data	Enter up to 255 characters to override the installation data found on the Old Userid.
Language Segment	Indicate if you want the LANGUAGE segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Netview Segment	Indicate if you want the NETVIEW segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
OMVS Segment	Indicate if you want the OMVS segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
OPERPARM Segment	Indicate if you want the OPERPARM segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
Password	Enter a password that be used to override the default password assigned by RACF when a new userid is added.
Profile Owner	Enter a valid userid or group that will be used to override the transferred profile owner at the userid profile level on the Old Userid.
RSC Permits	Indicate if you want all general resource permits of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.

Security Entries	Indicate if you want all security labels, levels and categories of the Old Userid to be transferred. “Y” is the default.
TSO Segment	Indicate if you want the TSO segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
WORKATTR Segment	Indicate if you want the WORKATTR segment of the Old Userid to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.

Command Generation Initiators

Request Parser: TRNUSR

The complete syntax of the Command is:

TRNUSR	Old Userid
	New Userid
	[ALUADD('additions to ALU commands')]
	[AT(additions to commands for RRSF)]
	[ALIAS(catalog to add alias to)
	[<u>ATTR</u> NOATTR]
	[CATDSN <u>NOCATDSN</u>]
	[<u>CON</u> NOCON]
	[DATA('new installation data')]
	[DFL(new default group)]
	[<u>DSN</u> NODSN]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[PER (
	[<u>ALL</u> NONE DSN RSC])
	[PSW(new password)]
	[<u>SEC</u> NOSEC]
	[SEG (
	[ALL NONE]
	[TSO NOTSO]
	[CICS NOCICS] [DCE NODCE]
	[DFP NODFP]
	[LANGUAGE NOLANGUAGE]
	[OPERPARM NOOPERPARM]
	[WORKATTR NOWORKATTR]
	[OMVS NOOMVS]
	[NETVIEW NONETVIEW])

Request Initiator: AATRNUSTR

Execution Sample:

```
//SYSTSIN DD *
  TRNUSR USERBOB USERKEN
  ISPSTART PGM(AATRNUSTR)
//*
```

Transfer Userid Profile Processing Notes

Keep the following in mind when using the Transfer Userid function:

- If you enter both an AT and ONLYAT override only the AT will be processed.

- If a value of NONE on the KEY field of the OPERPARM segment is encountered it will be treated as no key.
- If a value of 00000 on the STORAGE field of the OPERPARM segment is encountered it will be treated as no storage although the command creates this value as a default.
- All RACLINK commands will have no passwords and are only viable when executed from the appropriate node.
- The renaming of dataset profiles and physical datasets may produce truncated names if you transfer a userid which is shorter in length than the new userid and the old userid has long RACF dataset profiles or physical datasets.

Transfer Group Profiles

The Transfer Group Profiles process creates all commands to transfer all or some of one group to another naming convention based upon your selection criteria.

```
Command Generation ----- SSA ----- Command Generation
                          Transfer Group Profiles
Command ==>

      Operational Mode (Batch/Online/Schedule) ==> BATCH
      -----

      Old Group      New Group      Default Options (Y/N)?
==> SYS1            ==> NEWSYS1      ==> N
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Old Group

Specify the group to be transferred. The Old Group must be specified. The group does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some of the commands will fail (that is, DELGROUP).
- New Group

Specify the group that will be the recipient of the generated commands. The New Group must be specified and the New Group should not exist in RACF for all the commands to complete successfully (that is, ADDGROUP).
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer Group Profiles Overrides Options Screen’ below.

Transfer Group Profiles Overrides Options Screen

```

----- SSA -----
Transfer Group Profiles Overrides

Command ==>

Model Group      New Group
SYS1             NEWSYS1

Main Options      Group Segments
-----
| More:  + | | All Segments (Y/N) Y |
| Attributes (Y/N) Y | | DFP (Y/N) Y |
| Connects (Y/N) Y | | OMVS (Y/N) Y |
| All Permits (Y/N) Y |
-----

AlgADD ==> _____
Alias ==> _____
Installation Data ==> _____

_____ <==
Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

If you chose to override the default settings for the transfer group process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Note Be sure to use the scrolling boxes to display all override options available.

Alias	Specify the user catalog to be used in a define alias command. The catalog name can be up to 44 characters long and SSA will not check the existence of the catalog. The syntax of the command generated is: DEFINE ALIAS(NAME('NEWSYS1') - RELATE('USER.CATALOG'))
All Permits	Indicate if you want all permits (dataset and general resource) of the Model Group to be transferred. "Y" is the default. If you specify "N", the choice will fall to the individual questions concerning dataset or general resource permits.
All Segments	Indicate if you want all segments of the Old Group to be transferred. "Y" is the default. If you specify "N", the choice will fall to the questions concerning the individual segments.
AlgADD	Enter up to 60 characters that will be added to an ALTGROUP command that follows the initial ADDGROUP command. The data entered is the responsibility of the user and will not be validated by SSA.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Attributes	Indicate if you want all group attributes on connects to the Old Group to be transferred. "Y" is the default.
Cataloged Datasets	Indicate if you want rename commands generated for physical datasets where the Old Group was the HLQ. VSAM and tape datasets will not be processed. 'N' is the default.

Check	Indicate if you want the existence of the New Group to be validated before generating commands. If it exists, no ADDGROUP command will be generated, however, the remainder of the commands will be generated accordingly. “N” is the default.
Connects	Indicate if you want all connect profiles on the Old Group to be transferred. “Y” is the default.
Dataset Profiles	Indicate if you want all dataset profiles where the Old Group is the HLQ to be transferred. The replication process will include all aspects of those dataset profiles including but not limited to permits, installation data, audit levels, etc. “Y” is the default.
DFP Segment	Indicate if you want the DFP segment of the Old Group to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
DSN Permits	Indicate if you want all dataset permits of the Old Group to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.
Installation Data	Enter up to 255 characters to override the installation data found on the Old Group.
OMVS Segment	Indicate if you want the OMVS segment of the Old Group to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Segments.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Profile Owner	Enter a valid userid or group that will be used to override the transferred profile owner at the group profile level on the Old Group.
RSC Permits	Indicate if you want all general resource permits of the Old Group to be transferred. “Y” is the default which is duplicated by the “Y”, if specified, on All Permits.
Security Entries	Indicate if you want all security labels, levels and categories of the Old Group to be transferred. “Y” is the default.

Command Generation Initiators

Request Parser: TRNGRP

The complete syntax of the Command is:

TRNGRP	Old Group
	New Group
	[ALGADD('additions to ALG commands')]
	[ALIAS(catalog to add alias to)]
	[AT(additions to commands for RRSF)]
	[<u>ATTR</u> NOATTR]
	[CATDSN <u>NOCATDSN</u>]
	[CON <u>NOCON</u>]
	[DATA('new installation data')]
	[<u>DSN</u> NODSN]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> ([<u>ALL</u> NONE DSN RSC])
	[<u>SEC</u> NOSEC]
	[<u>SEG</u> (
	[<u>ALL</u> NONE]
	[DFP NODFP]
	[OMVS NOOMVS])
	[SUP(new superior group)]

Request Initiator: AATRNGRP

Execution sample:

```
//SYSTSIN DD *
  TRNGRP SYS1 NEWSYS1
  ISPSTART PGM(AATRNGRP)
//*
```

Transfer Group Profiles Processing Notes

The renaming of dataset profiles and physical datasets can produced truncated names if you transfer a group whose length than the New Group and the Old Group has long RACF dataset profiles or physical datasets.

Transfer Dataset Profiles

The Transfer Dataset Profiles process creates all the commands to transfer all or some of one dataset profile to another naming convention based upon your selection criteria.

Command Generation ----- SSA ----- Command Generation

Transfer Dataset Profiles

Command ==>

Operational Mode (Batch/Online/Schedule) ==> BATCH

Old Profile

Old Volume

1 => SYS1.*

2 =>

3 =>

4 =>

5 =>

6 =>

New Profile

New Volume

Default Options

1 => NEWSYS1.*

2 =>

3 =>

4 =>

5 =>

6 =>

==> N

==> -

==> -

==> -

==> -

==> -

Hit Enter to Continue PF03=EXIT/PF01=HELP

- Old Profile

Specify the dataset profile to be transferred. The Old Dataset Profile must be specified. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some of the commands will fail (that is, DELDSD).
- Old Volume

If the Old Profile is discrete, you must specify the volume. If you do not specify the volume, SSA will consider the Old Profile a fully qualified generic profile and will search and transfer accordingly.
- New Profile

Specify the dataset profile that will be the recipient of the generated commands. The New Profile must be specified and the New Profile should not exist in RACF for all the commands to complete successfully (that is, ADDSD).
- New Volume

If the Old Profile is discrete and you wish to define the New Profile as discrete, you must specify a New Volume.
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer Dataset Profile Overrides Options Screen’ below.

Transfer Dataset Profile Overrides Options Screen

```

----- SSA -----
                Transfer Dataset Profile Overrides

Command ==>

Olddsn ==> SYS1.*                      Oldvol ==>
Newdsn ==> NEWSYS1.*                  Newvol ==>

Permits                (Y/N) Y
DFP Segment            (Y/N) Y
Security Entries       (Y/N) Y
Check New DSN Profile  (Y/N) N

Profile Owner ==> _____
RRSF At              ==> _____
RRSF Onlyat          ==> _____

AldADD ==> _____
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

If you chose to override the default settings for the transfer dataset profile process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

AldADD	Enter up to 60 characters that will be added to an ALTDSD command that follows the initial ADDSD command. The data entered is the responsibility of the user and will not be validated by SSA.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Profile to be validated before generating commands. If it exists, no ADDSD command will be generated, however, the remainder of the commands will be generated accordingly. "N" is the default.
DFP Segment	Indicate if you want the DFP segment of the Old Profile to be transferred. "Y" is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the Old Profile.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits of the Old Profile to be transferred. "Y" is the default.
Profile Owner	Enter a valid userid or group that will be used to override the transferred profile owner at the dataset profile level on the Old Profile.
Security Entries	Indicate if you want all security labels, levels and categories of the Old Profile to be transferred. "Y" is the default.

Command Generation Initiators

Request Parser: TRNDSN

The complete syntax of the Command is:

TRNDSN	Old Dataset Profile
	New Dataset Profile
	[ALDADD('additions to ALD commands')]
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DFP</u> NODFP]
	[NEWVOL(volume of new dataset profile)]
	[<u>NOCHECK</u> CHECK]
	[OLDVOL(volume of discrete old dataset profile)]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[<u>SEC</u> NOSEC]

Request Initiator: AATRNSN

Execution sample:

```
//SYSTSIN DD *
    TRNDSN SYS1.* NEWSYS1.*
    ISPSTART PGM(AATRNSN)
//*
```

Transfer Dataset Profile Processing Notes

N/A

Transfer General Resource Profiles

The Transfer General Resource Profiles process creates all commands to transfer all or some of one general resource profile to another naming convention based upon your selection criteria.

```

Command Generation ----- SSA ----- Command Generation
                        Transfer General Resource Profiles
Command ==>

                        Operational Mode (Batch/Online/Schedule) ==> ONLINE
                        -----

Old Profile ==> SUBMIT.IBMUSER

Old Class  ==> SURROGAT                                     <==

New Profile ==> SUBMIT.NEWUSER1

New Class  ==> SURROGAT   Default Overrides (Y/N) ==> N                                     <==

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Old Profile	Specify the general resource profile to be transferred. The Old General Resource Profile must be specified. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some commands will fail (that is, RDELETE).
Old Class	Specify the general resource class to which the Old Profile is defined. You must specify the Old Class.
New Profile	Specify the general resource profile that will be the recipient of the generated commands. The New Profile must be specified and the New Profile should not exist in RACF for all the commands to complete successfully (that is, RDEFINE).
New Class	Specify a New Class to override the Old Class. If you do not specify a New Class, the Old Class will be used.
Default Options	Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer General Resource Profile Overrides Options Screen’ below.

Transfer General Resource Profile Overrides Options Screen

```
----- SSA -----
                Transfer General Resource Profile Overrides
Command ==>
Old Profile ==> SUBMIT.IBMUSER

                <== Old Class ==> SURROGAT
New Profile ==> SUBMIT.NEWUSER1

                <== New Class ==> SURROGAT
Installation Data ==> TEST LEAD

                <==
Application Data ==> LEAD

                <==
                                                More: +
RaltADD ==> _____
Owner ==> _____

                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

If you chose to override the default settings for the transfer general resource profile process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Application Data	Enter up to 255 characters to override the application data found on the Old Profile.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Profile to be validated before generating commands. If it exists, no RDEFINE command will be generated, however, the remainder of the commands will be generated accordingly. “N” is the default.
DLFDATA Segment	Indicate if you want the DLFDATA segment of the Old Profile to be transferred. “Y” is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the Old Profile.
Members	Indicate if you want all members of the Old Profile to be transferred. “Y” is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits of the Old Profile to be transferred. “Y” is the default.
Profile Owner	Enter a valid userid or group that will be used to override the transferred profile owner at the general resource profile level on the Old Profile.
RALTADD	Enter up to 60 characters that will be added to an RALTER command that follows the initial RDEFINE command if you transferred the entire Old Profile. The data entered is the responsibility of the user and will not be validated by SSA.

RDEFINE	Indicate if you want an RDEFINE command to be generated for the New Profile. “Y” is the default.
Security Entries	Indicate if you want all security labels, levels and categories of the Old Profile to be transferred. “Y” is the default.
Session Segment	Indicate if you want the SESSION segment of the Old Profile to be transferred. “Y” is the default.
STDATA Segment	Indicate if you want the STDATA (Started Task) segment of the Old Profile to be transferred. “Y” is the default.
SystemView Segment	Indicate if you want the SYSTEMVIEW segment of the Old Profile to be transferred. “Y” is the default.

Command Generation Initiators

Request Parser: TRNRSC

The complete syntax of the Command is:

TRNRSC	Old Resource Profile
	New Resource Profile
	Old Resource Class
	[APPLDATA('new application data')
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DLFDATA</u> NODLFDATA]
	[<u>MEM</u> NOMEM]
	[NEWCLS(new resource class)]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[RALTADD('additions to RALT commands')]
	[<u>SEC</u> NOSEC]
	[<u>SESSION</u> NOSESSION]
	[<u>SYSTEMVIEW</u> NOSYSTEMVIEW]
	[<u>STDATA</u> NOSTDATA]

Request Initiator: AATRNRSC

Execution sample:

```
//SYSTSIN DD *
  TRNRSC SUBMIT.IBMUSER -
        SUBMIT.NEWUSER1 -
        SURROGAT
  ISPSTART PGM(AATRNRSC)
//*
```

Transfer General Resource Profile Processing Notes

Keep the following in mind when using the Transfer General Resource Profile function:

- AATRNRSC will validate that the request for particular segments are appropriate. The appropriateness of the request is determined by the Old Class and the segment requested. For example, if you requested that the STDATA segment be part of the replication process, yet the New Class you requested was FACILITY, the request for the STDATA segment replication would not be processed. This is important to help maintain a ‘clean’ database by eliminating definitions that have no use insuring that all generated commands are valid.

- If you enter a grouping class profile that has members as the Old Profile and a non-grouping class profile as the New Profile, SSA will still generate the ADDMEM commands for all members found on the Old Profile even though the commands will fail. It is the responsibility of the user to enter appropriate classes.
- If you enter an Old Class and a New Class that have incompatibilities in their CDT definitions, SSA will still generate all commands as requested. It is the responsibility of the user to enter classes that are compatible.

Transfer General Resource Classes

The Transfer General Resource Class process creates all commands to transfer a general resource class to another based upon your selection criteria..

```
Command Generation ----- SSA ----- Command Generation
                          Transfer General Resource Classes
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----

      Old Class      New Class      Default Options (Y/N)?
==> GCICSTRN      ==> G$PRDTRN      ==> N
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Old Class

Specify the general resource class to be transferred. The Old Class must be specified. The Old Class does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, all the removal commands will fail.
- New Class

Specify the general resource class that will be the recipient of the generated commands. The New Class must be specified and must exist in RACF for the generated commands to execute successfully.
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer General Resource Class Overrides Options Screen’ below.

Transfer General Resource Class Overrides Options Screen

```

----- SSA -----
Transfer General Resource Class Overrides

Command ==>

                Old      New
                Class    Class
                GCICSTRN  G$PRDTRN

Installation Data ==> _____
_____
_____ <==
Application Data ==> _____
_____
_____ <==
_____ More: +

RaltADD ==> _____
Owner ==> _____
Permits (Y/N) ==> Y
Members (Y/N) ==> Y
DLFDATA Segment (Y/N) ==> Y
Session Segment (Y/N) ==> Y

Hit Enter to Process Entry PF03=Bypass Entry/PF01=HELP

```

If you chose to override the default settings for the transfer general resource class process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

Application Data	Enter up to 255 characters to override the application data found on the profiles defined to the Old Class.
At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Class to be validated before generating commands. If it does not exist, no commands will be generated. "N" is the default.
DLFDATA Segment	Indicate if you want the DLFDATA segment found on the profiles defined to the Old Class to be transferred. "Y" is the default.
Installation Data	Enter up to 255 characters to override the installation data found on the profiles defined to the Old Class.
Members	Indicate if you want all members found on the profiles defined to Old Class to be transferred. "Y" is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits	Indicate if you want all permits found on the profiles defined to the Old Class to be transferred. "Y" is the default.
Profile Owner	Enter a valid userid or group that will be used to override the transferred profile owner at the general resource profile level on the Old Class.
RALTADD:	Enter up to 60 characters that will be added to an RALTER command that follows the initial RDEFINE command. The data entered is the responsibility of the user and will not be validated by SSA.

RDEFINE:	Indicate if you want an RDEFINE command to be generated for all the profiles in the New Class. “Y” is the default.
Security Entries	Indicate if you want all security labels, levels and categories found on the profiles defined to the Old Class to be transferred. “Y” is the default.
Sesssion Segment	Indicate if you want the SESSION segment found on the profiles defined to the Old Class to be transferred. “Y” is the default.
STDATA Segment	Indicate if you want the STDATA (Started Task) segment found on the profiles defined to the Old Class to be transferred. “Y” is the default.
SystemView Segment	Indicate if you want the SYSTEMVIEW segment found on the profiles defined to the Old Class to be transferred. “Y” is the default.

Command Generation Initiators

Request Parser: TRNCLS

The complete syntax of the Command is:

TRNCLS	Old Resource Class
	New Resource Class
	[APPLDATA('new application data')]
	[AT(additions to commands for RRSF)]
	[DATA('new installation data')]
	[<u>DLFDATA</u> NODLFDATA]
	[<u>MEM</u> NOMEM]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]
	[OWN(new profile owner)]
	[<u>PER</u> NOPER]
	[RALTADD('additions to RALT commands')]
	[<u>SEC</u> NOSEC]
	[<u>SESSION</u> NOSESSION]
	[<u>SYSTEMVIEW</u> NOSYSTEMVIEW]
	[<u>STDATA</u> NOSTDATA]

Request Initiator: AATRNCLS

Execution sample:

```
//SYSTSIN DD *
  TRNCLS GCICSTRN G$PRDTRN
  ISPSTART PGM(AATRNCLS)
//*
```

Transfer General Resource Class Processing Notes

Keep the following in mind when using the Transfer General Resource Class function:

- AATRNCLS verifies if the request for particular segments are appropriate. The appropriateness of the request is determined by the Old Class and the segment requested. For example, if you requested that the STDATA segment be part of the replication process, yet the New Class you requested was FACILITY, the request for the STDATA segment replication would not be processed. This is important to help maintain a 'clean' database by eliminating definitions that have no use insuring that all generated commands are valid.
- If you enter a grouping class that has members as the Old Class and a non-grouping class as the New Class, SSA will still generate the ADDMEM commands for all members found on the Old Class even though the commands will fail. It is the responsibility of the user to enter appropriate classes.
- If you enter a Old Class and a New Class that have incompatibilities in their CDT definitions, SSA will still generate all commands as requested. It is the responsibility of the user to enter classes that are compatible.

Transfer Ownership

Transfer Ownership creates all commands to transfer ownership of resources to a new owner.

```
Command Generation ----- SSA ----- Command Generation
                          Transfer Ownership
Command ==>

      Operational Mode (Batch/Online/Schedule) ==> BATCH
-----

      Old Owner      New Owner      Default Options (Y/N)?
==> SYS1            ==> NEWSYS2      ==> N
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _
==> _____      ==> _____      ==> _

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Old Owner

Specify the owner to be transferred. The Old Owner must be specified. The Owner does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables and all ownership is being transferred with alter commands, not delete commands.
- New Owner

Specify the userid or group that will be the recipient of the generated commands. The New Owner must be specified and must exist in RACF for the generated commands to execute successfully.
- Default Options

Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, ‘Transfer Ownership Overrides Options Screen’ below.

Transfer Ownership Overrides Options Screen

```

----- SSA -----
                        Transfer Ownership Overrides
Command ==>

                        Old      New
                        Owner    Owner
                        SYS1     NEWSYS2

Main Options:
Check New Owner Entry (Y/N): Y
Profiles:
All (Y/N): N
User (Y/N): Y
Connect (Y/N): Y
Group (Y/N): Y
Dataset (Y/N): Y
General Resource (Y/N): Y

RRSF
At ==> _____
Onlyat ==> _____

Hit Enter to Process Entry      PF03=Bypass Entry/PF01=HELP

```

If you chose to override the default settings for the transfer ownership process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Owner to be validated before generating commands. If it does not exist, no profile altering commands will be generated. "N" is the default.
All Profiles	Indicate if you want ownership of all types of ownership to be transferred. If you indicate "N", the process will default to the individual profile choices. "Y" is the default.
User Profiles	Indicate if you want user profile ownership included in the process. "Y" is the default.
Group Profiles	Indicate if you want group profile ownership included in the process. "Y" is the default.
CONNECT Profiles	Indicate if you want connect profile ownership included in the process. "Y" is the default.
DATASET Profiles	Indicate if you want dataset profile ownership included in the process. "Y" is the default.
General Resource	Indicate if you want general resource profile ownership included in the process. "Y" is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.

Command Generation Initiators

Request Parser: TRNOWN

The complete syntax of the Command is:

TRNOWN	Old Owner
	New Owner
	[AT(additions to commands for RRSF)]
	[<u>NOCHECK</u> CHECK]
	[<u>ONLYAT</u> ONLYAT]
	[<u>PROFILES</u> ([<u>ALL</u> USR] [CON GRP] [DSN RSC])]

Request Initiator: AATRNOWN

Execution sample:

```
//SYSTSIN DD *  
    TRNOWN SYS1 NEWSYS2  
    ISPSTART PGM(AATRNOWN)  
//*
```

Transfer Ownership Processing Notes

N/A

Transfer Notifications

The Transfer Notifications process will create all the commands to transfer notifications on dataset and general resource profiles from one userid to another.

```

Command Generation ----- SSA ----- Command Generation
                          Transfer Notifications
Command ==>

                          Operational Mode (Batch/Online/Schedule) ==> BATCH
                          -----
Old Notify      New Notify      Default Options (Y/N)?
==> IBMUSER_    ==> NEWUSER3      ==> N
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _
==> _____ ==> _____      ==> _

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Old Notify	Specify the notify entity to be transferred. The Old Notify must be specified. The Old Notify does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables and all notifications are being transferred with only alter commands, not delete commands that would effect the Old Notify.
New Notify	Specify the userid that will be the recipient of the generated commands. You can also specify NONOTIFY which will cause NONOTIFY commands to be generated instead of transfer notifications to the New Notify. If you enter a New Notify to transfer the notifications to, the New Notify must exist in RACF for the generated commands to execute successfully. If you leave the entry blank, NONOTIFY will be used.
Default Options	Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Transfer Notifications Overrides Options Screen’ below.

Transfer Notifications Overrides Options Screen

----- SSA -----

Transfer Notifications Overrides

Command ==>

Old
Notify
IBMUSER

New
Notify
NEWUSER3

Main Options:

Check New Notify Entry (Y/N): Y

Profiles:

All

(Y/N): N

Dataset

(Y/N): Y

General Resource

(Y/N): Y

RRSF

At ==> _____

Onlyat ==> _____

Hit Enter to Process Entry

PF03=Bypass Entry/PF01=HELP

If you chose to override the default settings for the transfer notifications process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

AT	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Notify to be validated as being a valid existing userid before generating commands. If it does not exist, no profile altering commands will be generated. "N" is the default.
All Profiles	Indicate if you want all notifications on all types of profiles transferred. If you indicate "N", the process will default to the individual profile choices. "Y" is the default.
Dataset Profiles	Indicate if you want dataset profile notifications included in the process. "Y" is the default.
General Resource	Indicate if you want general resource profile notifications included in the process. "Y" is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.

Command Generation Initiators

Request Parser: TRNNTF

The complete syntax of the Command is:

TRNNTF	Old Notify
	[AT(additions to commands for RRSF)]
	[NEWNTF(new notify)]
	[<u>NOCHECK</u> CHECK]
	[<u>NONOTIFY</u>]
	[ONLYAT(additions to commands for RRSF)]
	[<u>PROFILES</u> (
	[<u>ALL</u> DSN RSC])

Request Initiator: AATRNTF

Execution sample:

```
//SYSTSIN DD *
    TRNNTF IBMUSER NEWNTF(NEWUSER3)
    ISPSTART PGM(AATRNTF)
//*
```

Transfer Notifications Processing Notes

N/A

Remove All References to a Userid

Remove All References to a Userid creates all commands to remove all references of a userid.

```
Command Generation ----- SSA ----- Command Generation
                        Remove All References to a Userid
Command ==>

                        Operational Mode (Batch/Online/Schedule) ==> BATCH
                        -----

Old Userid      New Owner      New Notify      Default Options (Y/N)?
==> IBMUSER      ==> NEWUSER1      ==> NEWUSER1      ==> N
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -
==> _____  ==> _____  ==> _____  ==> -

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- Old Userid** Specify the Old Userid to be removed. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some of the commands will fail (that is, DELUSER).
- New Owner** Specify the userid or group that will be the recipient of the generated commands to transfer ownership. The New Owner must exist in RACF for the generated commands to execute successfully.
- New Notify** Specify the userid that will be the recipient of the generated commands to transfer notifications. You can also specify NONOTIFY which will cause NONOTIFY commands to be generated instead of transfer notifications to the New Notify. If you enter a New Notify to transfer the notifications to, the New Notify must exist in RACF for the generated commands to execute successfully.
- Default Options** Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Remove All References to a Userid Overrides Options Screen’ below.

Remove All References to a Userid Overrides Options Screen

```

----- SSA -----
Remove All References to a Userid Overrides
Command ==>

          Old      New      New
          Userid   Owner   Notify
          IBMUSER  NEWUSER1 NEWUSER1

Main Options:

Delete Cataloged Datasets          (Y/N): Y
Check New Owner and New Notify Entries (Y/N): Y

          RRSF
At      ==> _____
Onlyat ==> _____

Hit Enter to Process Entry      PF03=Bypass Entry/PF01=HELP

```

If you chose to override the default settings for the remove all references to a userid process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Owner and New Notify to be validated. The New Notify will be validated as a valid userid. If they do not exist, no profile altering commands will be generated. "N" is the default.
Delete Cataloged Datasets	Indicate if you want all physical datasets where the user is the HLQ to be deleted. "N" is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.

Command Generation Initiators

Request Parser: REMUSR

The complete syntax of the Command is:

REMUSR	New Owner
	[AT(additions to commands for RRSF)]
	[CATDSN <u>NOCATDSN</u>]
	[NEWNTF(new notify)]
	[<u>NOCHECK</u> CHECK]
	[<u>NONOTIFY</u>]
	[ONLYAT(additions to commands for RRSF)]

Request Initiator: AAREMUSR

Execution sample:

```
//SYSTSIN DD *
  REMUSR IBMUSER NEWUSER1
  ISPSTART PGM(AAREMUSR)
//*
```

Remove All References to a Userid Processing Notes

Keep the following in mind when using the Remove all References to a Userid function: The process can produce delete commands for catalog datasets where the userid is the HLQ. VSAM and tape datasets are not included in the process. Review the generated commands carefully before submitting them.

Remove All References to a Group

Remove All References to a Group will create all the commands to remove all references of a group.

```

Command Generation ----- SSA ----- Command Generation
                        Remove All References to a Group
Command ==>

                        Operational Mode (Batch/Online/Schedule) ==> BATCH
                        -----
Old Group      New Owner      New SupGroup  Default Options (Y/N)?
==> TEST      ==> NEWTEST    ==> NEWTEST    ==> N
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
==> _____ ==> _____    ==> _____    ==> _
Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Old Group	Specify the Old Group to be removed. The profile does not need to exist in RACF because the information used for command generation is retrieved from the SSA ISPF tables, however, some of the commands will fail (that is, DELGROUP).
New Owner	Specify the userid or group that will be the recipient of the generated commands to transfer ownership. The New Owner must exist in RACF for the generated commands to execute successfully.
New Supgroup	Specify a group that will be used to replace all occurrences where the Old Group was the superior group of another group. The New Superior Group must exist in RACF for the generated commands to execute successfully.
Default Options	Specify “Y” if you want all default options to remain or “N” if you wish to specify options on the override screen. For details, see ‘Remove All References to a Group Overrides Options Screen’ below.

Remove All References to a Group Overrides Options Screen

```
----- SSA -----
Remove All References to a Group Overrides

Command ==>

          Old      New      New
          Group    Owner    SupGroup
          TEST     NEWTEST  NEWTEST

Main Options:

Delete Cataloged Datasets (Y/N): Y
Check New Owner and New SupGroup Entries (Y/N): Y
Process Userids with Old Group as Default Group (Y/N): Y
Process Groups with Old Group as Superior Group (Y/N): Y

RRSF
At ==> _____
Onlyat ==> _____

Hit Enter to Process Entry      PF03=Bypass Entry/PF01=HELP
```

If you chose to override the default settings for the remove all references to a group process, you will be presented with the override screen. Below is a brief explanation of those options; options are in alphabetical order not the order they are displayed on the screen.

At	Enter a RRSF destination that will be specified on each command generated using the AT parameter.
Check	Indicate if you want the existence of the New Owner and New Superior Group to be validated before generating commands. If they do not exist, no profile altering commands will be generated. "N" is the default.
Delete Cataloged Datasets	Indicate if you want all physical datasets where the group is the HLQ to be deleted. "N" is the default.
ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Process Userids with Old Group as Default Group	Indicate if you want userids, whose default group is the group being removed, to be changed from that default group to the group specified as the superior group. "Y" is the default.
Process Groups with Old Group as Superior Group	Indicate if you want groups, whose superior group is the group being removed, to be changed from that superior group to the group specified as the superior group. "Y" is the default.

Command Generation Initiators

Request Parser: REMGRP

The complete syntax of the Command is:

REMGRP	Group to Remove
	Replacement Group
	Replacement Owner
	[AT(additions to commands for RRSF)]
	[CATDSN <u>NOCATDSN</u>]
	[<u>DFLCHK</u> NODFLCHK]
	[<u>GRPCHK</u> NOGRPCHK]
	[<u>NOCHECK</u> CHECK]
	[ONLYAT(additions to commands for RRSF)]

Request Initiator: AAREMGRP

Execution sample:

```
//SYSTSIN DD *
  REMGRP TEST NEWTEST NEWTEST
  ISPSTART PGM(AAREMGRP)
//*
```

Remove All References to a Group Processing Notes

Keep the following in mind when using the Remove all References to a Group function:
The process can produce delete commands for catalog datasets where the group is the HLQ. VSAM and tape datasets are not included in the process. Review the generated commands carefully before submitting them.

Remove All Obsolete Entries

The Remove All Obsolete Entries process creates all commands to remove obsolete access list entries, notify entries, ownership entries, and SURROGAT class entries.

```
Command Generation ----- SSA ----- Command Generation
                        Remove All Obsolete Entries
Command ==>

                        Operational Mode (Batch/Online/Schedule) ==> BATCH
                        -----

New Owner                ==> _____
New Notify               ==> _____
Ownership:
  Userid Profiles        (Y/N) ==> Y
  Connect Profiles      (Y/N) ==> Y
  Group Profiles        (Y/N) ==> Y
  Dataset Profiles      (Y/N) ==> Y
  General Resource Profiles (Y/N) ==> Y
Permits:
  Dataset Profiles      (Y/N) ==> Y
  General Resource Profiles (Y/N) ==> Y
  Surrogat Profiles    (Y/N) ==> Y
  Check New Owner      (Y/N) ==> N
  RRSF AT              ==> _____
  RRSF Onlyat         ==> _____

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

- New Owner Specify a userid or group that will be the recipient of any commands generated to correct obsolete ownership entries. You must enter the New Owner and it is recommended that you specify a group. The New Owner must exist or the generated commands will fail.
- New Notify Specify a userid that will be the recipient of any commands generated to correct obsolete notification entries. The New Notify is optional; if not specified the process will default to NONOTIFY which will remove all the obsolete notifications.
- At Enter a RRSF destination that will be specified on each command generated using the AT parameter.
- Check Indicate if you want the existence of the New Owner to be validated before generating commands. If it does not exist, no profile altering commands will be generated. "N" is the default.
- Ownership - User Profiles Indicate if you want user profile ownership included in the process. "Y" is the default.
- Ownership - Group Profiles Indicate if you want group profile ownership included in the process. "Y" is the default.
- Ownership - Connect Profiles Indicate if you want connect profile ownership included in the process. "Y" is the default.
- Ownership - Dataset Profiles Indicate if you want dataset profile ownership included in the process. "Y" is the default.
- Ownership - General Resource Profiles Indicate if you want general resource profile ownership included in the process. "Y" is the default.

ONLYAT	Enter a RRSF destination that will be specified on each command generated using the ONLYAT parameter.
Permits - Dataset Profiles	Indicate if you want dataset profile permissions included in the process. “Y” is the default.
Permits - General Resource Profiles	Indicate if you want general resource profile permissions included in the process. “Y” is the default.
SURROGAT Profiles	Indicate if you want SURROGAT profiles included in the process. “Y” is the default.

Command Generation Initiators

Request Parser: CLEAN

The complete syntax of the Command is:

CLEAN	Replacement Owner
	[AT(additions to commands for RRSF)]
	[NEWNTF(new notify)]
	[<u>NOCHECK</u> CHECK]
	[<u>NONOTIFY</u>]
	[<u>OWN</u> ([<u>ALL</u> NONE] [USR, CON, GRP, DSN, RSC])]
	[ONLYAT(additions to commands for RRSF)]
	[<u>PER</u> ([<u>ALL</u> NONE] [DSN, RSC])]
	[<u>SURROGAT</u> NOSURROGAT]

Request Initiator: AACLEAN

Execution sample:

```
//SYSTSIN DD *  
  CLEAN NEWOWN NEWNTF(NEWNTF)  
  ISPSTART PGM(AACLEAN)  
//*
```

Processing Notes

N/A



CHAPTER 6

The SCHEDULER

Security administrators need an automated facility to submit requests and update profiles at designated intervals. Because of security implications associated with typical schedulers, administrators are obligated to monitor requests and updates. Security administrators also need a facility to manually enter and submit requests and updates. A scheduling facility would prove useful as a request system interface that handles decentralized security for administrators, coordinators, and auditors.

- The SCHEDULER meets these requirements and more. Below is a list of its capabilities and their applications:
- The SCHEDULER is an automated system with a started task at the core of the facility. The task verifies and submits requests entered by all users and administrators. The task automatically scans and submits verified scheduled requests.
- The SCHEDULER started task can submit requests with its own authority, or the authority of the requester. Requests to run with the authority of the task must receive the proper approval.
- Submitting requests is controlled by RACF. The ability to approve, view, and deny those requests is also controlled by RACF.
- Users can enter requests that are beyond their 'regular' RACF authority to run under the task's authority which can be approved or denied by an administrator. This allows the administrator to decentralize functions without giving the user the actual authority that might have been necessary to perform the request.
- The SCHEDULER submits any form of JCL or TSO command, therefore, you can schedule non-RACF related events as well.

The SCHEDULER Global Conventions

Through-out the SSA product and manual there are several "global" conventions that occur. For The SCHEDULER, the following conventions apply:

Security: All of The SCHEDULER features are protected based upon the ability to enter a request and your user or administrator status. To enter a request, regardless of which option you use, you must have READ access to the default security profile SSA.SCHEDULE.GENERAL in the default RACF general resource class is MAA\$RULE. See 'Update Stored Configurations' on page 507 on changing the default protecting class or profile if you want to change them

When you enter a request into The SCHEDULER, you are asked if you want to run the job or commands with your authority or the authority of The SCHEDULER task. If you request the job or commands to run with your authority, the request is inputted with no checking since it is your authority that will be used to run the scheduled entry, however, if you request that the job or commands are to be run with the authority of the started task, SSA will check if you are an user or administrator. If you are an user, the request is inputted and marked as needing approval. If you are an administrator, the request is inputted and marked as approved to run; no further approval is necessary for that request.

All requests marked for approval can only be approved by an user with SSA administrator status. All other functions, Modify, Reschedule, and so on, are geared toward the user initiating the function not the status of the user. For example, Bob can only modify scheduled events scheduled by Bob. Joe, an administrator, can not modify the scheduled event, only approve, view or deny if the request is in need of approval.

Started Task: The SCHEDULER started task must run with a RACF userid, preferably the same name as the proc supplies - AASTC01. If the started task is going to be called upon to submit jobs under its own authority, you must insure that the started task has sufficient authority to successfully run the requests scheduled. It is recommended that the started task be given Global-Special and whatever dataset authority the administrator deems appropriate. This is a issue that is shop specific and should be given sufficient consideration.

Note The started task does not need to run privileged or trusted to perform all of its functions.

SURROGAT: When an approved request is to be run with the started tasks authority, the started task places a USER= entry into the jobcard of the scheduled event. In order for the started task to successfully submit the entry, it must be permitted to do so. Therefore, the started task must be permitted to profile(s) in the SURROGAT class for every user entering requests that are to be run with the started tasks authority. This applies for both users and administrators. Below is an example of a SURROGAT definition and permission.

SURROGAT Sample

```
RDEFINE SURROGAT IBMUSER.SUBMIT OW(SYS1) UACC(NONE)-
  DATA('SURROGAT PROFILE FOR USER=IBMUSER')
PERMIT IBMUSER.SUBMIT CLASS(SURROGAT) ID(AASTC01) -
  ACCESS(READ)
```

Note Be sure to consult the RACF (or z/OS) Security Administrator's Guide - Allowing Surrogate Job Submission section for details on permitting a userid to submit jobs on the behalf of another userid. Once again, this is a shop specific issue and needs to be given sufficient consideration.

Administrator and User Authority

It is important to understand the differences between administrator and user authority in regard to scheduled events. The following table lists scheduler functions and the corresponding administrator and user authority for that function.

Function	User	Administrator
Enter Scheduled Item	Authorized if permitted to scheduler profile	Authorized if permitted to scheduler profile
Run Scheduled Item Under Started Tasks Authority	Authorized if permitted to scheduler profile Item must have administrator approval	Authorized if permitted to scheduler profile Item does not require approval; will run as scheduled
Modify an Existing Item	Authorized if permitted to scheduler profile Can only be an item entered by modifier	Authorized if permitted to scheduler profile Can only be an item entered by modifier
Reschedule or Cancel an Item	Authorized if permitted to scheduler profile Can only be an item entered by modifier	Authorized if permitted to scheduler profile Can only be an item entered by modifier
Report on Schedule or Historical Items	Authorized if permitted to scheduler profile	Authorized if permitted to scheduler profile

Function	User	Administrator
	Can only be an item entered by user initiating report	Can be either only those items entered by user initiating report or all entries
Approve Item	Not authorized	Authorized if permitted to scheduler profile Authorized to approve all items requiring approval

Schedule Entry Input Screen

When a request is made to schedule JCL or commands, the user is presented with the Entry Input screen shown in the following figure. There are variations to the Entry Input screen. The variation is the inclusion of a type determiner. When the Entry Input screen appears, you can enter the following:

Scheduled Date	Enter the month, day, and year you want the scheduled item to run on. You can enter a date in the past, which would cause the item to be run as soon as it was approved or entered by an administrator and the started task reviewed it.
Scheduled Time	Enter the hour and minute you want the item scheduled to run at. You can enter any valid time. If the time is past in conjunction with the scheduled date, the item will run as soon as it was approved or entered by an administrator and the started task reviewed it. The time used is military time which ranges from 0001 to 2400.
Run With Schedulers Authority or Your Authority	Indicate if you want the item to run with the authority of the started task, or your authority. If you indicate your authority, the started task will SURROGATE authority to submit the job/commands on your behalf. If you indicate the started tasks authority, the task will submit the job/commands normally using its userids authority.
Receive Notification	Indicate if you want the started task to send a message indicating that a job was submitted at your request.
Description	Enter up to a 40-character description of the scheduled job or commands. It is important to note from a users perspective that the description serves as the initial description/indication that the administrator sees when approving or denying the request (if approval is required).

```

The SCHEDULER ----- SSA ----- The SCHEDULER
Command ==>

Enter the Scheduled Date, Time and Authority with
which you want the job and/or commands to be run.

Scheduled Date:
Month (MM)      ==> 07
Day (DD)       ==> 02
Year (YYYY)    ==> 1998
Scheduled Time:
Hour (HH)      ==> 16
Minute (MM)    ==> 50

Scheduled Run Settings:
Run with Scheduler Authority* or
Your Authority (S/Y) ==> Y
Receive Notification (Y/N) ==> Y

Description ==> _____

* = Requires Administrator Status or Approval

Hit Enter to Continue

```

Started Task Interface

The SCHEDULER started task must be running to process scheduled items. The task can be started with the following operator command:

```
S AASTC01
```

Upon starting, The SCHEDULER started task issues a WTOR (Write To OPERATOR with Reply) that allows an operator to instruct the task to perform various functions. Below is a sample of the WTOR and the possible replies to the WTOR.

WTOR Sample

```
*44 AASTC01 ENTER VALID SSA SCHEDULE FACILITY COMMAND
```

WTOR Replies

- A Instructs the started task to archive all completed tasks to the historical file. The started task does not process any requests until the archival process is complete. When the started task archives the completed items, it produces a report detailing what was archived. The report contains all information concerning the completed items with the exception of the actual JCL or commands that were in the request. The report is put out to DD AAHSTLOG on the started task job.

When completed, the following messages are displayed:

```
AASTC50 ARCHIVAL TASK IN PROGRESS
AASTC51 ARCHIVAL TASK COMPLETED NORMALLY
```

- D** Instructs the started task to display the current WAKEUP, SCAN, and HISTORY interval. The WAKEUP value dictates at what time interval will the started task 'WAKEUP' and check if any response to its WTOR has been entered. The SCAN value dictates how often the started task scans The SCHEDULER database for scheduled items. The HISTORY interval indicates how long the started task waits before archiving a completed task. The output from the display command is as follows:

```
AASTC02 SCAN INTERVAL: 00 HRS 01 MINS 00 SECS
AASTC02 WAKEUP INTERVAL: 00 HRS 00 MINS 30 SECS
AASTC02 HISTORY RETAIN: 007 DAYS
```

- M** Instructs the started task to display all WTOR responses available. The output from the display command is as follows:

```
AASTC03 VALID SSA SCHEDULER REPLIES:
AASTC03 REPLY A TO ARCHIVE COMPLETED TASKS
AASTC03 REPLY D TO DISPLAY CURRENT OPTIONS
AASTC03 REPLY P TO PURGE ARCHIVE FILE
AASTC03 REPLY S TO START DATABASE SCAN IMMEDIATELY
AASTC03 REPLY T TO TERMINATE THE STARTED TASK
AASTC03 REPLY U TO UPDATE TASK OPTIONS
```

- P** Instructs the started task to purge the archived records from the historical database. The started task will not process any requests until the purging process is complete. When the started task purges the archived items, it produces a report detailing what was purged. The report contains all information concerning the completed items including the actual JCL or commands that were in the request. The report is put out to DD AAPRGLOG on the started task job. When the purge is completed the following messages are displayed:

```
AASTC60 HISTORY PURGE IN PROGRESS
AASTC61 HISTORY PURGE COMPLETED NORMALLY
```

- S** Instructs the started task immediately upon WAKEUP and receiving this WTOR response to scan the database regardless of the scan interval setting.
- T** Instructs the started task to terminate. This is the recommended method of shutting down the started task. If you cancel the started task, you will receive VSAM errors upon its subsequent startup. Issuing a "T" insures data integrity and a 'normalized' shutdown process. Upon a 'normal' shutdown the following message is displayed:

```
AASTC40 STARTED TASK COMPLETED NORMALLY
```

- U** Instructs the started task to update its WAKEUP, SCAN and HISTORY settings. This needs to only be done after the options have been changed through configuration option 4. It is important to note that the started task retrieves these settings only upon startup or when it is instructed to. When retrieved, the started task will display the new settings in the same format as the 'D' response to the WTOR.

The SCHEDULER Main Menu

The SCHEDULER Main Menu provides screen options to enter modify, report, or approve scheduled events. Screen options are described beneath the example of the Main Menu.

```

The SCHEDULER ----- SSA ----- The SCHEDULER

Option ==>

General User Options:

    1 Enter New Jobs or Commands to be Scheduled
    2 Modify an Existing Scheduled Entry
    3 Reschedule or Cancel an Existing Scheduled Entry
    4 Report on Scheduled or Historical Entries

Administrator Options:

    5 Approve/Deny/View Scheduled Entries

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

- Enter New Jobs or Commands to be Scheduled

This option allows a user or administrator to enter new scheduled entries consisting of either a job or commands.

- Modify an Existing Scheduled Entry

This option allows a user or administrator to modify a scheduled entry that they entered into the system. A user is only allowed to view and modify their entries.

- Reschedule or Cancel an Existing Scheduled Entry

This option allows a user or administrator to reschedule or cancel a scheduled entry that they entered into the system. A user is only allowed to view or modify their entries.

- Report on Scheduled or Historical Entries

This option allows a user or administrator to report on scheduled or historical entries that they entered into the system. A user can only report on their own entries, however, an administrator has a choice of their own entries only or all entries.

- Approve/Deny/View Scheduled Events

This option is available to administrators only and allows them to approve, deny or view those scheduled entries requiring approval, namely, those items scheduled by users who have requested that the entry run with the started tasks authority and not theirs.

Enter New Jobs or Commands to be Scheduled

This SCHEDULER option opens an edit session to enter a new entry to be scheduled. Screen fields are described beneath the example of edit screen.

[illegible]

- Commands or a Job

Indicate if the entry is a job (JCL) or commands. Commands are encapsulated in a IKJEFT01 step when they are submitted, as shown below. The JCL for the IKJEFT01 step is configured through Configuration option 4.

```
//ASTC01J JOB ( ),MSGCLASS=A,  
// CLASS=A,REGION=4096K,NOTIFY=&SYSUID  
//*  
//STEP010 EXEC PGM=IKJEFT01,DYNAMNBR=20  
//SYSTSPRT DD SYSOUT=*  
//SYSTSIN DD *  
<commands>  
//*
```

Note Press PF03 to exit the edit session after entering your item. You will then be presented with the Scheduler Input screen discussed on page 272.

Modify an Existing Scheduled Entry

This SCHEDULER option includes two screens. The first screen includes fields to enter search criteria to select commands or JCL that are current entries in the SCHEDULER. The second screen displays the results of the search, which are current scheduled commands or JCL that met your search criteria. Scheduled items can be modified after they have been selected from the search result screen.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
                          Modify an Existing Scheduled Entry

Command ==>

                          Enter your Display Criteria below:

Entry Date                ==> *                EQ
Entry Time                ==> *                EQ
JCL/Command (JCL/CMD/*)  ==> *
Execute Date              ==> *                EQ
Execute Time              ==> *                EQ
Already Approved (Yes/No/*) ==> *
Already Denied (Yes/No/*) ==> *

                          Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

There are two types of search criteria fields. The first field can contain an exact value or wildcard characters used to search for scheduled entries. The second field is the logical operator for the character based field. Below are the logical operators available.

EQ	Equal To
NE	Not Equal To
LT	Less Than
GT	Greater Than
LE	Less Than or Equal To
GE	Greater Than or Equal To

Not every character field has a logical field. Those fields are single character fields as in whether a scheduled item was already approved. That is a yes or no question. The logical operator field determines the analysis of the character field as in EQUAL TO which is represented by EQ.

It is important to keep in mind that search records must meet all search criteria to be selected. Therefore, you should not enter search criteria that could potentially eliminate all records.

After entering your search criteria, the results appear in the SCHEDULER Search Results screen. It is important to note that only those entries that are scheduled to run are displayed, not those that already have been submitted.

From the Search Result screen you can select those entries you want to modify. You will be 'paged' through the entries until you have completed or canceled all selections.

The SCHEDULER ----- SSA ----- The SCHEDULER	
Modify an Existing Scheduled Entry	
Command ==>	Scroll ==> PAGE
Select Entries You Want to Modify	
SEL	Scheduled Entries

---	OMVS SEG UPDATE WITH TASK AUTH
	Entered: 1998-08-21 - 16:18 TYPE= CMD
	Approved: NO Denied: NO

---	DCE SEG UPDATE WITH TASK AUTH
	Entered: 1998-08-22 - 11:27 TYPE= CMD
	Approved: NO Denied: NO

---	CONNECTS UPDATE WITH TASK AUTH
	Entered: 1998-08-22 - 11:51 TYPE= CMD
	Approved: NO Denied: NO

- When you select an entry for modification, you will go through the following steps:
- 1 Scheduled JCL or commands are retrieved and placed in an edit session.
 - 2 Press PF03 to exit and save your changes to the entry.
 - 3 After exiting and saving you will be presented with the scheduler input screen with the retrieved settings of that scheduled event.
 - 4 You can then change the scheduled settings for that entry.

Reschedule or Cancel an Existing Scheduled Entry

This SCHEDULER option provides screens to search and select SCHEDULER entries for rescheduling or cancellation. The first screen includes fields to enter search criteria to select commands or JCL that are current entries in the Scheduler. The second screen displays the results of the search, which are current scheduled commands or JCL that met your search criteria. Scheduled items can be cancelled or rescheduled after they have been selected from the search result screen.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
Reschedule or Cancel an Existing Scheduled Entry

Command ==>

Enter your Display Criteria below:

Entry Date           ==> *           EQ
Entry Time           ==> *           EQ
JCL/Command (JCL/CMD/*) ==> *
Execute Date         ==> *           EQ
Execute Time         ==> *           EQ
Already Approved (Yes/No/*) ==> *
Already Denied (Yes/No/*) ==> *

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Enter your search criteria and hit enter to receive the search results. Refer to page 277 for an explanation of values that can be entered on the search screen.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
Reschedule or Cancel an Existing Scheduled Entry
Command ==>                               Scroll ==> PAGE
R = Reschedule an Entry  C = Cancel an Entry

SEL      Scheduled Entries                Scheduled By      Scheduled
-----
-----
OMVS SEG UPDATE WITH TASK AUTH          USER001          1998-08-21
Entered: 1998-08-21 - 16:18  TYPE= CMD  ENDUSER, JOSEPH  15:59
Approved: NO                 Denied: NO
-----
DCE  SEG UPDATE WITH TASK AUTH          USER001          1998-08-21
Entered: 1998-08-22 - 11:27  TYPE= CMD  ENDUSER, JOSEPH  15:59
Approved: NO                 Denied: NO
-----
  
```

After entering your search criteria, you are presented with the results of the search. From this screen, you can enter C to cancel the scheduled item, or R to reschedule the event. If you choose to cancel a scheduled item, you will be asked to confirm the cancellation after viewing the commands in an edit session.

Changes made during the edit session are not honored; edit session is only made available so the user can copy the entry to another location. If you choose to reschedule an item you will go through the following sequence:

- 1 Scheduled JCL or commands are retrieved and placed in an edit session.
- 2 Press PF03 to exit and save your changes to the entry.
- 3 After exiting and saving you will be presented with the scheduler input screen with the retrieved settings of that scheduled event. You can then change the scheduled settings for that entry.

Report on Scheduled or Historical Entries

This SCHEDULER option allows users to report on entries they have scheduled or that have been archived.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
      Report on Scheduled or Historical Entries
Command ==>

      Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): S
-----

If you are an Administrator do you want all records? (Y/N): Y
Scheduled or Historical Entries? (S/H): S
Include Job or Commands Entered? (Y/N): N

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

- If your are an Administrator do you want all records?

If you are an administrator, indicate if you want just your scheduled or archived items in the report, or if you want all entries for all users reported on.

- Scheduled or Historical Entries?

Indicate if you want items still in the scheduler database, or those that have been archived to the historical database.

- Include Job or Commands Entered?

Indicate if you want the actual JCL or commands entered to be included in the report.

Note The operational mode, direct output and if run in batch sequence are identical to the reports sequence. If you require instructions on those fields or the sequence of screens to come in this selection, see ‘Report Global Conventions’ on page 60 for more information.

Approve/Deny/View Scheduled Entries

This SCHEDULER option allows administrators to approve, view, or deny a scheduled entry.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
                          Approve/Deny/View Scheduled Entries

Command ==>

                          Enter your Display Criteria below:

Userid                      ==> *                EQ
Entry Date                  ==> *                EQ
Entry Time                  ==> *                EQ
JCL/Command (JCL/CMD/*)    ==> *
Execute Date               ==> *                EQ
Execute Time               ==> *                EQ
Already Approved (Yes/No/*) ==> *
Already Denied  (Yes/No/*) ==> *

                          Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Enter your search criteria and hit enter to receive the search results. Refer to page 277 for an explanation of values that can be entered on the search screen.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
                          Approve/Deny/View Scheduled Entries
Command ==>                      Scroll ==> PAGE
                          A = Approved, D = Deny, V = View

SEL      Scheduled Entries          Scheduled      Scheduled
----- By ----- To Run On -----
-----
___ OMVS SEG UPDATE WITH TASK AUTH  USER001      1998-08-21
   Entered: 1998-08-21 - 16:18  TYPE= CMD  ENDUSER, JOSEPH  15:59
   Approved: NO      Denied: NO
-----
___ DCE  SEG UPDATE WITH TASK AUTH  USER001      1998-08-21
   Entered: 1998-08-22 - 11:27  TYPE= CMD  ENDUSER, JOSEPH  15:59
   Approved: NO      Denied: NO
-----
___ CONNECTS UPDATE WITH TASK AUTH  USER001      1998-08-21
   Entered: 1998-08-22 - 11:51  TYPE= CMD  ENDUSER, JOSEPH  15:59
   Approved: NO      Denied: NO
-----
  
```

After entering your search criteria, you are presented with the results of the search. From this screen, you can enter the following line commands for each listed entry:

A Approve the scheduled item to run. Below is the screen that will be displayed.

```
The SCHEDULER ----- SSA ----- The SCHEDULER
                          Approve/Deny/View Scheduled Entries
Command ==>
                          A = Approved, D = Deny, V = View
                          Scheduled      Scheduled
                          -----
The SCHEDULER ----- SSA ----- The SCHEDULER
                          Approve Scheduled Entry
Command ==>
                          Approve (Y/N) ==> Y
                          Reason      ==>
                          Scheduled Entries      Scheduled      Scheduled
                          -----              By      To Run On
OMVS SEG UPDATE WITH TASK AUTH      USER001      1998-08-21
Entered: 1998-08-21 - 16:18      TYPE= CMD      ENDUSER, JOSEPH      15:59
Denied: NO
                          Hit Enter to Continue
```

D Deny the scheduled item to run. The reason is optional. Below is the screen that will be displayed.

```
The SCHEDULER ----- SSA ----- The SCHEDULER
                          Approve/Deny/View Scheduled Entries
Command ==>
                          A = Approved, D = Deny, V = View
                          Scheduled      Scheduled
                          -----
The SCHEDULER ----- SSA ----- The SCHEDULER
                          Deny Scheduled Entry
Command ==>
                          Deny (Y/N) ==> N
                          Reason      ==>
                          Scheduled Entries      Scheduled      Scheduled
                          -----              By      To Run On
OMVS SEG UPDATE WITH TASK AUTH      USER001      1998-08-21
Entered: 1998-08-21 - 16:18      TYPE= CMD      ENDUSER, JOSEPH      15:59
Denied: NO
                          Hit Enter to Continue
```

- V View the scheduled item. From the browse session of the scheduled entry you can approve, deny, or bypass the selection. The same procedures apply as stated above for approval and denial.

```

The SCHEDULER ----- SSA ----- The SCHEDULER
                          View Scheduled Entry
Command ==>                               Scroll ==> CSR

Approve/Deny/Bypass (A/D/B): A Reason:

          Scheduled Entry                      Scheduled      Scheduled
          -----                      By              To Run On
OMVS SEG UPDATE WITH TASK AUTH              USER001          YYYY-MM-DD
Entered: YYYY-MM-DD - 16:18    TYPE= CMD  ENDUSER, JOSEPH          15:59

BROWSE - USER001.TSCSSA.TEMP.JCL(VIEWITEM) ---- LINE 00000000 COL 001 080
***** Top of Data *****
/*      SSA  Vv.v          */
/* ENTERED VIA AASCHED MACRO */
/* SSA VERSION Vv.v      */
CONTROL LIST ASIS
ALTUSER TSTU037 OMVS(-
  HOME('-
this is a test of blanks                                start of text-
') -
)

```




CHAPTER 7

TSO Direct Administration

SSA can administer RACF from TSO directly without granting Group SPECIAL, Global SPECIAL, or any other RACF authority that could potentially compromise security. TSO Direct Administration (referred to as SSA-TDA) allows security administrators to do the following:

- Userid Administration
- Group Administration
- Connect Administration
- Password Administration
- Dataset Administration
- Resource Administration
- Dataset Permit Administration
- Resource Permit Administration
- Resource Member Administration
- User TSO Segment Administration
- User CICS Segment Administration
- Access Simulator

It is also important to note the following operating pluses for using SSA-TDA.

- All updates and inquiries done by SSA-TDA are done live.
- SSA-TDA allows a user to use the various features without having group or global SPECIAL.

Note TSO Direct Administration produces standard SMF Type 80 audit records.

TSO Direct Administration Global Conventions

Security

Security for TSO Direct Administration functions are protected on two levels. The first level is the ‘Authority’ profile. This type of profile determines what profiles a user may affect. The table show below lists the format for a general ‘Authority’ profile, and the specific ‘Authority’ profile that protects global SPECIAL users.

Function	RACF Class	RACF Profile (Authority Profile)
Userid Administration	MAA\$RULE	MEGASOLVE-SSA.\$USER.<default group>
Group Administration	MAA\$RULE	MEGASOLVE-SSA.\$GROUP. <superior group>
Connect Administration	MAA\$RULE	MEGASOLVE-SSA.\$CONNECT.<group>
Password Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESET.<group>
Dataset Administration	MAA\$RULE	MEGASOLVE-SSA.\$DATASET.<hlq>
Resource Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE. <class>
Dataset Permit Administration	MAA\$RULE	MEGASOLVE-SSA.\$DATASET.<hlq>
Resource Permit Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE. <class>
Resource Member Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE. <class>
User TSO Segment Administration	MAA\$RULE	MEGASOLVE-SSA.\$UTSO. <default group>
User CICS Segment Administration	MAA\$RULE	MEGASOLVE-SSA.\$UCICS. <default group>
Access Simulator	MAA\$RULE	MEGASOLVE-SSA.ACCESS.SIMULATOR
Global Special User Protection	MAA\$RULE	MEGASOLVE-SSA.\$SPECIAL\$

MEGASOLVE-SSA.\$USER.<default group>

A Userid Administration user that has access to an ‘Authority’ profile may change any user that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you may use generic characters in the <default group> to cover a wide range of users.

MEGASOLVE-SSA.\$GROUP.<superior group>

A Group Administration user that has access to an ‘Authority’ profile may change any group that has that particular group as their superior group. If you have generic processing turned on for the SSA security class, you may use generic characters in the <superior group> to cover a wide range of users.

MEGASOLVE-SSA.\$RESET.<group>

A Password Administration user that has access to an ‘Authority’ profile may change any user that is connected to the <group> specified in the profile. If you have generic processing turned on for the SSA security class, you may use generic characters in the <group> to cover a wide range of users.

MEGASOLVE-SSA.\$CONNECT.<group>

A Connect Administration user that has access to an ‘Authority’ profile may change any connection for the <group> specified in the profile. If you have generic processing turned on for the SSA security class, you may use generic characters in the <group> to cover a wide range of users.

MEGASOLVE-SSA.\$DATASET.<hlq>

A Dataset Administration and Dataset Permit Administration user that has access to an ‘Authority’ profile may change any dataset profile that begins with the <hlq> specified in the profile. If you have generic processing turned on for the SSA security class, you may use generic characters in the <hlq> to cover a wide range of dataset profiles.

MEGASOLVE-SSA.\$RESRCE. <class>

A Resource Administration, Resource Permit Administration, and Resource Member Administration user that has access to an ‘Authority’ profile may change resource profiles that begins with the <class> specified in the profile. If you have generic processing turned on for the SSA security class, you may use generic characters in the <class> to cover a wide range of resource profiles.

MEGASOLVE-SSA.\$UTSO. <default group>

A User TSO Segment Administration user that has access to an ‘Authority’ profile may change any user’s TSO segment that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you may use generic characters in the <default group> to cover a wide range of users.

MEGASOLVE-SSA.\$UCICS.<default group>

A User CICS Segment Administration user that has access to an ‘Authority’ profile may change any user’s CICS segment that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you may use generic characters in the <default group> to cover a wide range of users.

SSA.ACCESS.SIMULATOR

This profile protects the access simulator which allows a user to interrogate RACF to determine a users or groups highest allowed access level to a particular resource. The Access Simulator will also determine what is the protecting profile of the resource.

MEGASOLVE-SSA.\$SPECIAL\$

This profile protects global SPECIAL users from any user that has any TSO Direct Administration function. In order to use a CICS Direct Administration function to affect a global SPECIAL user they must have access to an ‘Authority’ profile that protects the SPECIAL user and they also must have access to this profile. If you do not define this profile, then this check is bypassed for global SPECIAL users, and normal ‘Authority’ profile checking applies.

Note It is highly recommended that you define this profile. The profile should have a UACC(NONE) and no access list entries. This protects global SPECIAL users from unauthorized attempts at being updated.

Example ‘Authority’ Profile Setup

This example illustrates how to define an ‘Authority’ profile.

- Scenario: You, the security administrator, want to allow the Payroll department manager to be able to add users, connect those users to payroll groups and do Password Administration for all of the users in the Payroll Department.
- Known: The default group for the PAYROLL Department is PAYROLL. The userid for the Payroll department manager is MNGRPAY.

Profiles to build

- Add UserMEGASOLVE-SSA.\$USER.PAYROLL
- ConnectMEGASOLVE-SSA.\$CONNECT.PAYROLL
- Password AdministrationMEGASOLVE-SSA.\$RESET.PAYROLL

Command to issue

```
RDEFINE GAA$RULE CDA-PAYROLL -  
  ADDMEM(MEGASOLVE-SSA.$USER.PAYROLL -  
    MEGASOLVE-SSA.$CONNECT.PAYROLL -  
    MEGASOLVE-SSA.$RESET.PAYROLL) -  
  OWNER(SYS1) UACC(NONE)
```

The second type of security is the access level you have to the ‘Authority’ profile. The following tables list user, group, connect, and password administration functions. Each table lists the administrative functions for the authority profile and what access levels are required to perform them.

Userid Administration Function	Userid Administration ‘Authority’ Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Userid	X	X	X	X
Add Userid	X	X	X	X
Add/Change Userid Name	X	X	X	X
Add/Change Owner	X	X	X	X

Userid Administration Function	Userid Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Add/Change Password	X	X	X	X
Add/Change Userid Installation Data			X	X
Delete Userid				X

Userid Administration Function	Userid Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Userid	X	X	X	X
Add Userid	X	X	X	X
Add/Change Userid Name	X	X	X	X
Add/Change Owner	X	X	X	X
Add/Change Password	X	X	X	X
Add/Change Userid Installation Data			X	X
Delete Userid				X

Group Administration Function	Group Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Group	X	X	X	X
Add Group	X	X	X	X
Add/Change Owner	X	X	X	X
Add/Change TERMUACC	X	X	X	X
Add/Change Group Installation Data			X	X
Delete Group				X

Connect Administration Function	Connect Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List All Connect Profiles	X	X	X	X
List Specific Connect Profile	X	X	X	X
Connect User to Group	X	X	X	X
Change Group UACC	X	X	X	X

Connect Administration Function	Connect Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Resume Connect	X	X	X	X
Revoke Connect	X	X	X	X
Set/Remove TERMUACC Attribute	X	X	X	X
Set/Remove Connect Resume Date		X	X	X
Set/Remove Connect Revoke Date		X	X	X
Remove User from Group		X	X	X
Change Group Authority			X	X
Set/Remove Connect Attributes (except TERMUACC)				X

Password Administration Function	Password Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List User	X	X	X	X
Set Password for User	X	X	X	X
Resume User	X	X	X	X
Revoke User	X	X	X	X
Set/Remove a Resume Date for a User		X	X	X
Set/Remove a Revoke Date for a User		X	X	X
Update Installation Data for a User			X	X
SuperRevoke User or Resume a SuperRevoked User				X

Dataset Administration Function	Dataset Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Dataset profile	X	X	X	X
Add Dataset profile	X	X	X	X
Change Dataset profile	X	X	X	X

Dataset Administration Function	Dataset Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Update Installation Data for a Dataset Profile			X	X
Delete Dataset profile				X

Resource Administration Function	Resource Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Resource profile	X	X	X	X
Add Resource profile	X	X	X	X
Change Resource profile	X	X	X	X
Update Installation and/or Application Data for a Resource Profile			X	X
Delete Resource profile				X

Dataset Permit Administration Function	Dataset Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Permit	X	X	X	X
Add Permit	X	X	X	X
Change Permit		X	X	X
Delete Permit		X	X	X

Resource Permit Administration Function	Resource Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Permit	X	X	X	X
Add Permit	X	X	X	X
Change Permit		X	X	X
Delete Permit		X	X	X

Resource Member Administration Function	Resource Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Resource Member	X	X	X	X
Add Resource Member	X	X	X	X

Resource Member Administration Function	Resource Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Delete Resource Members		X	X	X

User TSO Segment Administration Function	TSO Segment Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Segment	X	X	X	X
Add Segment		X	X	X
Change Segment		X	X	X
Delete Segment				X

User CICS Segment Administration Function	CICS Segment Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Segment	X	X	X	X
Add Segment		X	X	X
Change Segment		X	X	X
Delete Segment				X

Example Access Level Setup

The example below illustrates how to set the access level for the ‘Authority’ profile.

Scenario:	You, the security administrator, want to allow the Payroll department manager to be able to add users, connect those users to payroll groups and do Password Administration for all of the users in the Payroll Department.
Known:	The default group for the PAYROLL Department is PAYROLL. The userid for the Payroll department manager is MNGRPAY. Profiles protecting all Payroll Department users: MEGASOLVE-SSA.\$USER.PAYROLL MEGASOLVE-SSA.\$CONNECT.PAYROLL MEGASOLVE-SSA.\$RESET.PAYROLL
Access level needed	CONTROL
Command to issue	PERMIT CDA-PAYROLL - CLASS(GAA\$RULE) ID(MNGRPAY) - ACCESS(CONTROL)

Note The authorities relate only to the RACF access the user has to the MAA\$RULE class profiles. Just because a user may have GROUP SPECIAL, it does not mean this individual has the authority to use SSA-TDA to do RACF Administration.

Function Explanations	All SSA-TDA function explanation sections will use the following sequence:
	A Associated Screens and particular function examples and descriptions

SSA-TDA Programs

You can invoke a TSO Direct function directly without using SSA ISPF panels. The table below lists the appropriate program to call.

Function	Program
Userid Administration	AACMDP03
Group Administration	AACMDP04
Connect Administration	AACMDP02
Password Administration	AACMDP01
Dataset Administration	AACMDP05
Resource Administration	AACMDP06
Dataset Permit Administration	AACMDP07
Resource Permit Administration	AACMDP15
Resource Member Administration	AACMDP14
TSO Segment Administration	AACMDP08
CICS Segment Administration	AACMDP09
Access Simulator	AAACCSIM

RACLIST vs. Non-RACLIST Classes

Whenever a TSO Direct function is performed against any general resource class that has been RACLISTed in RACF, it is recommended that a SETROPTS RACLIST(classname) REFRESH RACF command be issued in order for any normal RACF command (that is, RLIST, RALT, RDEL) to be processed successfully.

TSO Direct Administration Main Menu

The Main Menu lists SSA-TDA options:

```
Direct Administration ----- SSA ----- Direct Administration
                               Main Menu

Option ==>

      1 - Userid Administration
      2 - Group Administration
      3 - Connect Administration
      4 - Password Administration
      5 - Dataset Administration
      6 - Resource Administration
      7 - Dataset Permit Administration
      8 - Resource Permit Administration
      9 - Resource Member Administration
     10 - User TSO Segment Administration
     11 - User CICS Segment Administration

      Please Note: All Direct Administration Functions are LIVE

      Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Userid Administration Screens

This section describes TDA userid Administration screens.

Perform List User

Perform the following steps to issue the equivalency of a RACF List User command (that is, LU DEMOTEST):

- 1 Enter 'L' as the request type.
- 2 Enter the userid in the USERID field and press ENTER.

```

Userid Administration ----- SSA ----- Userid Administration
                        Administration Input

Command ==>

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> L              (A=Add,C=Change,L=List,D=Delete)
Userid            ==> DEMOTEST       User id to be Processed
Default Group     ==> _____    Default Group for New Userid
Name              ==> _____    Userid Name
Owner             ==> _____    Profile Owner
Password          ==> _____    Password
Installation Data ==> _____

<==

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

List User Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Userid Administration ----- SSA ----- Userid Administration
                        List User Output

Command ==>

  Userid      ==> DEMOTEST   Default Group   ==> DEMOUSER
  Name        ==> DEMOTEST USERID
  Owner       ==> DEMOUSER

  Password Changed ==> ****.**.**
  Last Used Date ==> 1998-06-01   Last Used Time ==> 18:24:25
  Resume Date   ==>              Revoke Date   ==>

  Installation Data ==> THIS IS DATA

<==

  Do You Want to Keep This Information
  For the Add User Screen (Y/N): N

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Always press ENTER after a List User, or to recover from a message, to return to the Userid Administration Main panel.

Add Userid

Perform the following steps to issue the equivalency of a RACF Add User command (that is, ADDUSER DEMOTEST NA('DEMONSTRATION USER') DFL(DEMOUSER) OWNER(DEMOUSER):

- 1

Enter 'A' as the request type.
- 2

Enter the userid into the USERID field.
- 3

Enter a default group that you are authorized to use in the DEFAULT GROUP field. By not entering in the owner, the owner is set to the default group entered.
- 4

Enter the name in the NAME field (optional).

----- SSA -----

Userid Administration Administration Input Userid Administration

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> A (A=Add,C=Change,L=List,D=Delete)

Userid ==> DEMOTEST User id to be Processed

Default Group ==> DEMOUSER Default Group for New Userid

Name ==> DEMONSTRATION USER__ Userid Name

Owner ==> Profile Owner

Password ==> Password

Installation Data ==>

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process adds the user to the specified default group. The name is included as part of the profile but is optional. The profile owner is also optional. If not specified the owner is set to the same value as the default group entered.

Change Password

Perform the following steps to issue the equivalency of a RACF Alter User Password Resume with a password specified (that is, ALTUSER DEMOTEST PASSWORD(<password>) RESUME):

- 1

Enter 'C' as the request type.
- 2

Enter the userid into the USERID field.
- 3

TAB to the PASSWORD field, enter the desired password (clear the rest of the field by depressing the EOF (Erase End-Of-Field key), and press ENTER. You may change the Password to the Default Group by depressing the EOF (Erase End-Of-Field) key which clears the Password field, and then press ENTER.

```

Userid Administration ----- SSA ----- Userid Administration
                        Administration Input

Command ==>

        Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> C                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> DEMOTEST              User id to be Processed
Default Group     ==> _____            Default Group for New Userid
Name              ==> _____            Userid Name
Owner             ==> _____            Profile Owner
Password          ==> NEWPASS_             Password
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process sets the PASSDATE field to zeros requiring the user to enter a new password when they signon next and updates the LAST USED DATE/TIME fields with the current date and time.

Change Various Fields

Perform the following steps to issue the equivalency of a RACF Alter User Owner Name (that is, ALTUSER DEMOTEST OWNER(DEMOUSER) NA('DEMONSTRATION USER')):

- 1 Enter 'C' as the request type.
- 2 Enter the userid into the USERID field.
- 3 Enter the owner in the OWNER field (optional).
- 4 Enter the name in the NAME field (optional).

```

Userid Administration ----- SSA ----- Userid Administration
                        Administration Input

Command ==>

        Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> C                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> DEMOTEST              User id to be Processed
Default Group     ==> _____            Default Group for New Userid
Name              ==> DEMONSTRATION USER__ Userid Name
Owner             ==> DEMOUSER             Profile Owner
Password          ==> _____            Password
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process updates the profile owner or name field.

Add/Replace User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter ‘A’ for the request type if you are adding the user or ‘C’ if you are changing the userid.
- 2 Enter the userid into the USERID field.
- 3 TAB to the Installation Data field, type in data, and press ENTER.

Userid Administration ----- SSA ----- Userid Administration
Administration Input

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> C (A=Add,C=Change,L=List,D=Delete)

Userid ==> DEMOTEST User id to be Processed

Default Group ==> _____ Default Group for New Userid

Name ==> _____ Userid Name

Owner ==> _____ Profile Owner

Password ==> _____ Password

Installation Data ==> NEW INSTALLATION DATA FOR A DEMONSTRATION USERID_____

<==

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process updates the Installation Data field.

Update Existing User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter ‘L’ as the request type to list the userid.
- 2 Enter the userid into the USERID field and press ENTER.
- 3 TAB to the Keep Installation Data field, type a ‘Y’, and press ENTER.
- 4 TAB to the Installation Data field, type in changes to data, and press ENTER.

```
Userid Administration ----- SSA ----- Userid Administration
                                List User Output

Command ==>

Userid      ==> DEMOTEST      Default Group    ==> DEMOUSER
Name        ==> DEMONSTRATION USER
Owner       ==> DEMOUSER

Password Changed ==> ****.**.*
Last Used Date ==> 1998-06-01   Last Used Time ==> 18:24:25
Resume Date   ==>              Revoke Date      ==>

Installation Data ==> NEW INSTALLATION DATA FOR A DEMONSTRATION USERID

                                <==

                                Do You Want to Keep This Information
                                For the Add User Screen (Y/N): Y

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

When you specify 'Y' to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field.

Group Administration Screens

Perform List Group

Perform the following steps to issue the equivalency of a RACF List Group command (that is, LU DEMOTEST):

- 1
- Enter ‘L’ as the request type.
- 2
- Enter the group in the GROUP field and press ENTER.

Group Administration ----- SSA ----- Group Administration

Administration Input

Command ==>

Enter the Group and Request Type. Other fields are optional.

Request Type ==> L (A=Add,C=Change,L=List,D=Delete)

Group ==> DEMOUSER Group to be Processed

Superior Group ==> Superior Group for Add

Owner ==> Profile Owner

Termuacc (Y/N) ==> Termuacc Setting

Installation Data ==>

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

List Group Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Group Administration ----- SSA ----- Group Administration

List Group Output

Command ==>

Group ==> DEMOUSER Superior Group ==> USER

Owner ==> TESTUSER TERMUACC ==> Y

Installation Data ==> DEMONSTRATION USER GROUP

<==

Do You Want to Keep This Information
For the Add Group Screen (Y/N): N

Hit Enter to Continue PF03=EXIT/PF01=HELP

Always press ENTER after a List Group, or to recover from a message, to return to the Group Administration Main panel.

Add Group

Perform the following steps to issue the equivalency of a RACF Add Group command (that is, ADDGROUP DEMOTST1 SUPGRP(DEMOUSER) OWNER(DEMOUSER)):

- 1** Enter 'A' as the request type.
- 2** Enter the group into the GROUP field.
- 3** Enter a superior group that you are authorized to use in the SUPERIOR GROUP field. By not entering in the owner, the owner is set to the superior group entered.
- 4** Determine if TERMUACC is to be on or off (optional) and hit Enter.

Group Administration ----- SSA ----- Group Administration	
Administration Input	
Command ==>	
Enter the Group and Request Type. Other fields are optional.	
Request Type	==> A (A=Add,C=Change,L=List,D=Delete)
Group	==> DEMOTST1 Group to be Processed
Superior Group	==> DEMOUSER Superior Group for Add
Owner	==> _____ Profile Owner
Termuacc (Y/N)	==> _ Termuacc Setting
Installation Data	==> _____
_____ <==	

Hit Enter to Continue PF03=EXIT/PF01=HELP	

This process adds the group to the superior group. The profile owner is also optional. If not specified the owner is set to the same value as the default group entered. The TERMUACC if not entered, defaults to 'Y'.

Change Various Fields

Perform the following steps to issue the equivalency of a RACF Alter Group Owner TERMUACC (that is, ALTGROUP DEMOTST1 OWNER(DEMOUSER) TERMUACC):

- 1** Enter 'C' as the request type.
- 2** Enter the group into the GROUP field.
- 3** Enter the owner in the OWNER field (optional).
- 4** Enter Y or 'N' in the TERMUACC field (optional).

Group Administration ----- SSA ----- Group Administration
Administration Input

Command ==>

Enter the Group and Request Type. Other fields are optional.

Request Type ==> C (A=Add,C=Change,L=List,D=Delete)

Group ==> DEMOTST1 Group to be Processed

Superior Group ==> Superior Group for Add

Owner ==> DEMOUSER Profile Owner

Termuacc (Y/N) ==> _ Termuacc Setting

Installation Data ==> _____

<==

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process updates the profile owner or TERMUACC field.

Add/Replace Group Installation Data

Perform the following steps to add or replace installation data for the specified group:

- 1 Enter ‘A’ for the request type if you are adding the group or ‘C if you are changing the group.
- 2 Enter the group into the GROUP field.
- 3 TAB to the Installation Data field, type in data, and press ENTER.

Group Administration ----- SSA ----- Group Administration
Administration Input

Command ==>

Enter the Group and Request Type. Other fields are optional.

Request Type ==> C (A=Add,C=Change,L=List,D=Delete)

Group ==> DEMOTST1 Group to be Processed

Superior Group ==> Superior Group for Add

Owner ==> Profile Owner

Termuacc (Y/N) ==> _ Termuacc Setting

Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION GROUP_____

<==

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process updates the Installation Data field.

Update Existing Group Installation Data

Perform the following steps to add or replace installation data for the specified group:

- 1 Enter ‘L’ as the request type to list the group.

- 2 Enter the group into the GROUP field and press ENTER.
- 3 TAB to the Keep Installation Data field, type a 'Y', and press ENTER.
- 4 TAB to the Installation Data field, type in changes to data, and press ENTER.

```
Group Administration ----- SSA ----- Group Administration
                          List Group Output

Command ==>

Group          ==> DEMOTST1    Superior Group    ==> DEMOUSER
Owner          ==> DEMOUSER    TERMUACC       ==> Y
Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION GROUP

                          <==

                          Do You Want to Keep This Information
                          For the Add Group Screen (Y/N): Y

                          Hit Enter to Continue          PF03=EXIT/PF01=HELP
```

When you specify 'Y' to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field.

Connect Administration Screens

List All Connects

Perform the following steps to issue the equivalency of a RACF List User command that shows only connect groups for which the user is authorized to (that is, LU DEMOTEST):

- 1
- Enter the <userid> in the USERID field, enter an 'L' in the Request Type field, and press ENTER.

```
Connect Administration ----- SSA ----- Connect Administration
                               Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> L            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> _____ Connect group
Connect Owner ==> _____ Connect owner
Resume      ==> _            Specify Y to resume the connect
Revoke      ==> _            Specify Y to revoke the connect
Resume Date ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC  ==> _____ (None,Read,Update,Control,Alter)
Group Auth  ==> _____ (None,Use,Create,Connect,Join)

                               Group Connect Attributes:
ADSP        ==> _            Auditor    ==> _            GRPACC      ==> _
Special     ==> _            Operations ==> _            TERMUACC   ==> _

                               Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

List All Connects Display

If the user has READ access to the appropriate MAA\$RULE class profile, the following screen will be displayed.

```
Connect Administration ----- SSA ----- Connect Administration
                               List a Users Connect Groups

Command ==>                               Scroll ==> CSR

                               Connects for ==> DEMOTEST

                               S = List Specific Connect, C = Connect, R = Remove Connect

SELECT      Group
-----
_____ DEMOTSTZ
_____ DEMOTST1
_____ DEMOTST2
_____ DEMOTST3
_____ DEMOUSER
***** Bottom of data *****
```

You may ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- List Specific Connect (S)

Displays a screen with specific information about the connect. See List Specific Connect for screen example.

- Connect (C)

Displays the Connect Administration Main Panel with appropriate fields filled in.

- Remove Connect (R)

Displays a confirmation panel to confirm the remove request. If the request is confirmed with a 'Y' then the user will be removed from the group.

Note This screen lists only those groups authorized to the user by SSA.\$CONNECT.<group> authority profiles.

List Specific Connect Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Connect Administration ----- SSA ----- Connect Administration
                          List Specific User Connect Output
Command ==>

      Userid              ==> DEMOTEST      Connect Group  ==> DEMOUSER

      Group Owner         ==> DEMOUSER      Connect Date    ==> 1998-05-14
      Group UACC          ==> NONE           Group Authority ==> USE
      Last Connect Date   ==>                Connect Count   ==> 00000
      Last Connect Time   ==>

                          Group Connect Attributes:

      Revoked?            ==> N              ADSP?          ==> N
      Auditor?            ==> N              GRPACC          ==> N
      Special?            ==> N              Operations?     ==> N
      TERMUACC?           ==> N

      Resume Date         ==>                Revoke Date     ==>

                          Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Connect a User to a Group

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) command.

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field, and press ENTER.

Connect Administration ----- SSA ----- Connect Administration

Administration Input

Command ==>

Enter Connect Userid and Request Type. Other fields are optional.

Userid ==> DEMOTEST

Userid to be processed

Request Type ==> C

(L=List,S=Specific,C=Connect,R=Remove)

Connect Group ==> MEGA_____

Connect group

Connect Owner ==> _____

Connect owner

Resume ==> _

Specify Y to resume the connect

Revoke ==> _

Specify Y to revoke the connect

Resume Date ==> _____

Resume date for the connect (YYYY-MM-DD)

Revoke Date ==> _____

Revoke date for the connect (YYYY-MM-DD)

Group UACC ==> _____

(None,Read,Update,Control,Alter)

Group Auth ==> _____

(None,Use,Create,Connect,Join)

Group Connect Attributes:

ADSP ==> _

Auditor ==> _

GRPACC ==> _

Special ==> _

Operations ==> _

TERMUACC ==> _

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process connects the user to the specified group.

For a new connect the following defaults will be used if not explicitly specified:

- UACC(NONE)
- NOTERMUACC
- OWNER(<group>)

For existing connects, unless explicitly specified, no fields will be changed.

Note You may request any combination of Connect Administration functions. If the user does not have the correct access level to the SSA.\$CONNECT profile to do any one of the functions the entire request is failed (no partial updates are processed).

Remove User from Group

Perform the following steps to issue the equivalency of a RACF REMOVE <userid> GROUP(<group>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'R' in the Request Type field.
- 3 Enter a <group> in the Connect Group field, and press ENTER.
- 4 Type a 'Y' in the Confirmation Pop-up Panel when prompted and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> R            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> MEGA_____ Connect group
Connect Owner ==> _____ Connect owner
Resume      ==> _            Specify Y to resume the connect
Revoke      ==> _            Specify Y to revoke the connect
Resume Date ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC  ==> _____ (None,Read,Update,Control,Alter)
Group Auth  ==> _____ (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP        ==> _            Auditor ==> _            GRPACC ==> _
Special     ==> _            Operations ==> _          TERMUACC ==> _

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      ----- SSA -----
      | Remove a Group Connect |
      | Confirm Remove Request (Y/N): Y |
      | Userid ==> DEMOTEST |
      | Group ==> MEGA |
      | Hit Enter to Continue |
      | ----- |
      | Group Auth ==> _____ | (None,Use,Create,Connect,Join)

      Group Connect Attributes:
ADSP ==> _ Auditor ==> _ GRPACC ==> _
Special ==> _ Operations ==> _ TERMUACC ==> _

      Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Resume a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) RESUME command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Type a 'Y' in the Resume field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==> _____ Connect owner
Resume       ==> Y            Specify Y to resume the connect
Revoke       ==> _            Specify Y to revoke the connect
Resume Date  ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==> _____ (None,Read,Update,Control,Alter)
Group Auth   ==> _____ (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP         ==> _           Auditor   ==> _           GRPACC     ==> _
Special      ==> _           Operations ==> _           TERMUACC  ==> _

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Revoke a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT *<userid>* GROUP(*<group>*) REVOKE command:

- 1 Enter the *<userid>* into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a *<group>* in the Connect Group field.
- 4 Type a 'Y' in the Revoke field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==> _____ Connect owner
Resume       ==> _            Specify Y to resume the connect
Revoke       ==> Y            Specify Y to revoke the connect
Resume Date  ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==> _____ (None,Read,Update,Control,Alter)
Group Auth   ==> _____ (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP         ==> _           Auditor   ==> _           GRPACC     ==> _
Special      ==> _           Operations ==> _           TERMUACC  ==> _

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Set a Resume Date on a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT *<userid>* GROUP(*<group>*) RESUME(*<date>*) command:

- 1 Enter the *<userid>* into the USERID field.

- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a Gregorian <date> in the format of YYYY-MM-DD, that is greater than the current date, in the RESUME DATE field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid           ==> DEMOTEST      Userid to be processed
Request Type     ==> C             (L=List,S=Specific,C=Connect,R=Remove)
Connect Group    ==> DEMOUSER      Connect group
Connect Owner    ==> _____    Connect owner
Resume           ==> _             Specify Y to resume the connect
Revoke           ==> _             Specify Y to revoke the connect
Resume Date      ==> 1998-12-01    Resume date for the connect (YYYY-MM-DD)
Revoke Date      ==> _____    Revoke date for the connect (YYYY-MM-DD)
Group UACC       ==> _____    (None,Read,Update,Control,Alter)
Group Auth       ==> _____    (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP             ==> _             Auditor ==> _             GRPACC ==> _
Special          ==> _             Operations ==> _          TERMUACC ==> _

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Set a Revoke Date on a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) REVOKE(<date>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a Gregorian <date> in the format of YYYY-MM-DD, that is greater than the current date, in the REVOKE DATE field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid           ==> DEMOTEST      Userid to be processed
Request Type     ==> C             (L=List,S=Specific,C=Connect,R=Remove)
Connect Group    ==> DEMOUSER      Connect group
Connect Owner    ==> _____    Connect owner
Resume           ==> _             Specify Y to resume the connect
Revoke           ==> _             Specify Y to revoke the connect
Resume Date      ==> _____    Resume date for the connect (YYYY-MM-DD)
Revoke Date      ==> 1998-12-02    Revoke date for the connect (YYYY-MM-DD)
Group UACC       ==> _____    (None,Read,Update,Control,Alter)
Group Auth       ==> _____    (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP             ==> _             Auditor ==> _             GRPACC ==> _
Special          ==> _             Operations ==> _          TERMUACC ==> _

                        Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Change Connect Authority

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) AUTH(<auth>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter ‘C in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter an <auth> value in the Group Auth field, and press ENTER.

Connect Administration ----- SSA ----- Connect Administration
Administration Input

Command ==>

Enter Connect Userid and Request Type. Other fields are optional.

Userid	==> DEMOTEST	Userid to be processed
Request Type	==> C	(L=List,S=Specific,C=Connect,R=Remove)
Connect Group	==> DEMOUSER	Connect group
Connect Owner	==> _____	Connect owner
Resume	==> _	Specify Y to resume the connect
Revoke	==> _	Specify Y to revoke the connect
Resume Date	==> _____	Resume date for the connect (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the connect (YYYY-MM-DD)
Group UACC	==> _____	(None,Read,Update,Control,Alter)
Group Auth	==> CONNECT	(None,Use,Create,Connect,Join)

Group Connect Attributes:

ADSP	==> _	Auditor	==> _	GRPACC	==> _
Special	==> _	Operations	==> _	TERMUACC	==> _

Hit Enter to ContinuePF03=EXIT/PF01=HELP

Set/Remove Connect Attributes

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) <attribute> command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter ‘C in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a ‘Y’ or ‘N’ in the appropriate <attribute> field, and press ENTER.

Note The example below will remove the SPECIAL attribute, if any, and set the AUDITOR attribute.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Command ==>

      Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==> _____ Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==> _____ (None,Read,Update,Control,Alter)
Group Auth   ==> _____ (None,Use,Create,Connect,Join)

                        Group Connect Attributes:
ADSP         ==> _           Auditor      ==> Y      GRPACC      ==> _
Special      ==> N           Operations   ==> _      TERMUACC     ==> _

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Password Administration Screens

Perform List User

Perform the following steps to issue the equivalency of a RACF List User command (that is, LU DEMOTEST):

- Enter the userid in the USERID field and press ENTER.

Password Administration ----- SSA ----- Password Administration

Administration Input

Command ==>

Enter the Userid to be Reset. All other fields are optional.

Userid ==> DEMOTEST

User id to be reset

Password ==> ???????

New password - Blank for default group

Resume ==> _

Specify Y to resume the userid

Revoke ==> _

Specify Y to revoke the userid

Resume Date ==> _____

Resume date for the userid (YYYY-MM-DD)

Revoke Date ==> _____

Revoke date for the userid (YYYY-MM-DD)

SuperRevoke ==> _

Specify Y to super-revoke the userid

Installation Data ==> _____

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

List User Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Password Administration ----- SSA ----- Password Administration

List User Output

Command ==>

Userid ==> DEMOTEST

Default Group ==> DEMOUSER

User Name ==> DEMONSTRATION USER

Password Changed ==> ****.**.*

Last Used Date ==> 1998-06-01

Last Used Time ==> 18:24:25

Revoked? ==> Y

SuperRevoked? ==> Y

Special? ==> N

Operations? ==> N

Resume Date ==> _____

Revoke Date ==> _____

Installation Data ==> NEW INSTALLATION DATA FOR A DEMONSTRATION USERID

<==

Do You Want to Keep Installation Data
For the Reset Screen (Y/N): N

Hit Enter to Continue PF03=EXIT/PF01=HELP

Always press ENTER after a List User, or to recover from a message, to return to the Password Administration Main panel.

Set Password to Default Group and Resume User

Perform the following steps to issue the equivalency of a RACF Alter User Resume Password with no password. By not specifying a password, the password is reset to the default group of the userid being reset (that is, ALTUSER DEMOTEST RESUME PASSWORD):

- 1 Enter the userid into the USERID field.
- 2 TAB to the PASSWORD field, depress the EOF (Erase End-Of-Field) key.
- 3 TAB to the RESUME field, type a 'Y', and press ENTER.

Password Administration ----- SSA ----- Password Administration	
Administration Input	
Command ==>	
Enter the Userid to be Reset. All other fields are optional.	
Userid	==> DEMOTEST User id to be reset
Password	==> New password - Blank for default group
Resume	==> Y Specify Y to resume the userid
Revoke	==> - Specify Y to revoke the userid
Resume Date	==> _____ Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____ Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> - Specify Y to super-revoke the userid
Installation Data	==> _____
_____ <==	
Hit Enter to Continue PF03=EXIT/PF01=HELP	

This process clears the REVOKE flag, the UNSUCCESSFUL LOGON ATTEMPT COUNTER field, the REVOKE and RESUME dates if any, updates the LASTUSED DATE/TIME fields with the current date and time, updates the PASSDATE field with the current Julian date, and changes the PASSWORD field to the password that is the name of the DEFAULT GROUP.

Note Password Administration handles this request as two separate functions (a Resume and a Password Change) and will produce two RACF Type 80 SMF records.

You may request any combination of Password Administration functions. If the user does not have the correct access level to the SSA.\$RESET profile to do any one of the functions the entire request is failed (no partial updates are processed).

Change Password

Perform the following steps to issue the equivalency of a RACF Alter User Password with a password specified (that is, ALTUSER DEMOTEST PASSWORD(<password>):

- 1 Enter the userid into the USERID field.
- 2 TAB to the PASSWORD field, enter the desired password (clear the rest of the field by depressing the EOF (Erase End-Of-Field) key), and press ENTER. You may change the Password to the Default Group by depressing the EOF (Erase End-Of-Field) key which clears the Password field, and then press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid          ==> DEMOTEST      User id to be reset
Password        ==> NEWPASS      New password - Blank for default group
Resume          ==> _            Specify Y to resume the userid
Revoke          ==> _            Specify Y to revoke the userid
Resume Date     ==> _____   Resume date for the userid (YYYY-MM-DD)
Revoke Date     ==> _____   Revoke date for the userid (YYYY-MM-DD)
SuperRevoke     ==> _            Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process updates the PASSDATE field with the current Julian date, changes the PASSWORD field with the specified password, and updates the LAST USED DATE/TIME fields with the current date and time.

Resume a Userid

Perform the following steps to issue the equivalency of a RACF Alter User Resume (that is, ALTUSER DEMOTEST RESUME):

- 1 Enter the userid into the USERID field.
- 2 TAB to the RESUME field and enter a Y, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid          ==> DEMOTEST      User id to be reset
Password        ==> ????????     New password - Blank for default group
Resume          ==> Y            Specify Y to resume the userid
Revoke          ==> _            Specify Y to revoke the userid
Resume Date     ==> _____   Resume date for the userid (YYYY-MM-DD)
Revoke Date     ==> _____   Revoke date for the userid (YYYY-MM-DD)
SuperRevoke     ==> _            Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process clears the REVOKE flag, the UNSUCCESSFUL LOGON ATTEMPT COUNTER field, the REVOKE and RESUME dates if any, and updates the LASTUSED DATE/TIME fields with the current date and time.

This process does not change the password of the userid.

Revoke a Userid

Perform the following steps to issue the equivalency of a RACF Alter User Revoke (that is, ALTUSER DEMOTEST REVOKE):

- 1 Enter the userid into the USERID field.
- 2 TAB to the REVOKE field and enter a Y, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid           ==> DEMOTEST      User id to be reset
Password         ==> ????????     New password - Blank for default group
Resume           ==> _             Specify Y to resume the userid
Revoke           ==> Y             Specify Y to revoke the userid
Resume Date      ==> _____    Resume date for the userid (YYYY-MM-DD)
Revoke Date      ==> _____    Revoke date for the userid (YYYY-MM-DD)
SuperRevoke      ==> _             Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

This process sets the REVOKE flag, and clears the REVOKE and RESUME dates if any. This process does not change the password of the userid.

Set a Resume Date

Perform the following steps to issue the equivalency of a RACF Alter User Resume with a date (that is, ALTUSER USERBOB RESUME(<date>):

- 1 Enter the userid into the USERID field.
- 2 TAB to the RESUME DATE field and enter a Gregorian date in the format of YYYY-MM-DD, that is greater than the current date, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid           ==> DEMOTEST      User id to be reset
Password         ==> ????????     New password - Blank for default group
Resume           ==> _             Specify Y to resume the userid
Revoke           ==> _             Specify Y to revoke the userid
Resume Date      ==> 1998-12-01    Resume date for the userid (YYYY-MM-DD)
Revoke Date      ==> _____    Revoke date for the userid (YYYY-MM-DD)
SuperRevoke      ==> _             Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

This process updates the RESUME DATE field. This process does not change the password of the userid.

If you specify both RESUME DATE and REVOKE DATE that are the same, the RESUME DATE is ignored and the REVOKE DATE is updated with the date entered.

If there is a REVOKE DATE already set on the userid, and the RESUME DATE entered is the same, the RESUME DATE is ignored and the REVOKE DATE remains the same.

Set a Revoke Date

Perform the following steps to issue the equivalency of a RACF Alter User Revoke with a date (that is, ALTUSER DEMOTEST REVOKE(<date>):

- 1 Enter the userid into the USERID field.
- 2 TAB to the REVOKE DATE field and enter a Gregorian date in the format of YYYY-MM-DD, that is greater than the current date, and press ENTER.

Password Administration ----- SSA ----- Password Administration
Administration Input

Command ==>

Enter the Userid to be Reset. All other fields are optional.

Userid	==> DEMOTEST	User id to be reset
Password	==> ????????	New password - Blank for default group
Resume	==> -	Specify Y to resume the userid
Revoke	==> -	Specify Y to revoke the userid
Resume Date	==> _____	Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> 1998-12-02	Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> -	Specify Y to super-revoke the userid
Installation Data	==> _____	

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process updates the REVOKE DATE field. This process does not change the password of the userid.

If you specify both RESUME DATE and REVOKE DATE that are the same, the RESUME DATE is ignored and the REVOKE DATE is updated with the date entered.

If there is a RESUME DATE already set on the userid, and the REVOKE DATE entered is the same, the RESUME DATE is cleared and the REVOKE DATE is updated with the date entered.

Set SuperRevoke

Perform the following steps to issue a Password Administration SuperRevoke. This will prevent users from using Password Administration functions unless they have ALTER access to the appropriate SSA.\$RESET.<group> profile or the userid is removed from the SuperRevoke group \$SREVOKE:

- 1 Enter the userid into the USERID field.
- 2 TAB to the SuperRevoke field, type a ‘Y’, and press ENTER.


```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid           ==> DEMOTEST      User id to be reset
Password         ==> ????????     New password - Blank for default group
Resume           ==> _             Specify Y to resume the userid
Revoke           ==> _             Specify Y to revoke the userid
Resume Date      ==> _____    Resume date for the userid (YYYY-MM-DD)
Revoke Date      ==> _____    Revoke date for the userid (YYYY-MM-DD)
SuperRevoke      ==> Y             Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process sets the REVOKE flag, and connects the user to the SuperRevoke group \$SREVOKE. This process does not change the password of the userid.

Add/Replace User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter the userid into the USERID field.
- 2 TAB to the Installation Data field, type in data, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Command ==>

        Enter the Userid to be Reset. All other fields are optional.

Userid           ==> DEMOTEST      User id to be reset
Password         ==> ????????     New password - Blank for default group
Resume           ==> _             Specify Y to resume the userid
Revoke           ==> _             Specify Y to revoke the userid
Resume Date      ==> _____    Resume date for the userid (YYYY-MM-DD)
Revoke Date      ==> _____    Revoke date for the userid (YYYY-MM-DD)
SuperRevoke      ==> _             Specify Y to super-revoke the userid
Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION USERID_____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process updates the Installation Data field. This process does not change the password of the userid.

Update Existing User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter the userid into the USERID field and press ENTER.
- 2 TAB to the Keep Installation Data field, type a 'Y', and press ENTER.

3 TAB to the Installation Data field, type in changes to data, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                                List User Output
Command ==>

      Userid           ==> DEMOTEST      Default Group   ==> DEMOUSER
      User Name        ==> DEMONSTRATION USER

      Password Changed ==> ****.**.**
      Last Used Date   ==> 1998-06-01    Last Used Time   ==> 18:24:25

      Revoked?         ==> Y             SuperRevoked?    ==> Y
      Special?         ==> N             Operations?      ==> N

      Resume Date      ==>              Revoke Date      ==>

      Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION USERID

                                <==

                                Do You Want to Keep Installation Data
                                For the Reset Screen (Y/N): Y

                                Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

When you specify ‘Y’ to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field. This process does not change the password of the userid.

Dataset Administration Screens

Perform List Dataset Profile

Perform the following steps to issue the equivalency of a RACF List Dataset command (that is, LD DA() GEN):

- 1 Enter 'L' in the Request Type field.
- 2 Enter the dataset profile in the Dataset Profile field and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                                Administration Input
Command ==>

      Enter the Dataset and Request Type.  Other fields are optional.

Request Type      ==> L              (A=Add,C=Change,L=List,D=Delete)
Dataset Profile   ==> USER01.*
Owner            ==> _____ Profile Owner
UACC             ==> _____ (None,Execute,Read,Update,Control,Alter)
Notify           ==> _____ Userid to Notify
Warn (Y/N)       ==> _             Activate Warn?
Level            ==> _____ Resource Level
Local Audit      ==> _____ (All,Success,Fail,None)
Success Level    ==> _____ (None,Read,Update,Control,Alter)
Failure Level    ==> _____ (None,Read,Update,Control,Alter)
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

List Dataset Profile Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Dataset Administration ----- SSA ----- Dataset Administration
                                List Dataset Output
Command ==>

Dataset Profile   ==> USER01.*

Owner            ==> TSGBAT      UACC            ==> NONE
Notify           ==> _____ Warn            ==> NO
Level            ==> 000

Local Audit      ==> FAIL
Success Level    ==> _____
Failure Level    ==> READ

Installation Data ==> _____

_____ <==

Do You Want to Keep This Information
For the Add Dataset Screen (Y/N): N

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Always press ENTER after a List Dataset Profile, or to recover from a message, to return to the Dataset Administration Main panel.

Add Dataset Profile

Perform the following steps to issue the equivalency of a RACF Add Dataset Profile command (that is, ADDSD ‘USER01.JCLCNTL’ GEN):

- 1 Enter ‘A’ into the Request Type field
- 2 TAB to the Dataset Profile field, type in the dataset profile you want to add, and press ENTER.

Dataset Administration ----- SSA ----- Dataset Administration

Administration Input

Command ==>

Enter the Dataset and Request Type. Other fields are optional.

Request Type ==> A (A=Add,C=Change,L=List,D=Delete)

Dataset Profile ==> USER01.JCL.CNTL

Owner ==> Profile Owner

UACC ==> (None,Execute,Read,Update,Control,Alter)

Notify ==> Userid to Notify

Warn (Y/N) ==> Activate Warn?

Level ==> Resource Level

Local Audit ==> (All,Success,Fail,None)

Success Level ==> (None,Read,Update,Control,Alter)

Failure Level ==> (None,Read,Update,Control,Alter)

Installation Data ==>

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process adds the specified dataset profile. All other fields are optional. The default values for optional fields if not specified are: The Owner field defaults to the Userid of person issuing the add profile, UACC defaults to None, Local Audit defaults to Fail, Failure Level defaults to Read, Warn defaults to N, Level defaults to 000, and all other fields default to blanks.

Change Dataset Profile

Perform the following steps to issue the equivalency of a RACF Alter Dataset Profile (that is, ALTDSD ‘USER01.JCLCNTL’ GEN OW(USER02) UACC(READ)):

- 1 Enter ‘C’ into the Request Type field
- 2 TAB to the Dataset Profile field, type in the dataset profile you want to change
- 3 TAB to the Owner field and type in the new owner
- 4 TAB to the UACC field and type in the new UACC level, and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                                Administration Input
Command ==>

      Enter the Dataset and Request Type.  Other fields are optional.

Request Type      ==> C              (A=Add,C=Change,L=List,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL
Owner            ==> USER02____ Profile Owner
UACC             ==> READ____ (None,Execute,Read,Update,Control,Alter)
Notify           ==> _____ Userid to Notify
Warn (Y/N)       ==> _ Activate Warn?
Level            ==> _____ Resource Level
Local Audit      ==> _____ (All,Success,Fail,None)
Success Level    ==> _____ (None,Read,Update,Control,Alter)
Failure Level    ==> _____ (None,Read,Update,Control,Alter)
Installation Data ==> _____

_____ <==

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

This process changes the specified dataset profile. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Update Existing Dataset Profile Information

Perform the following steps to update existing information for the specified dataset profile:

- 1 Enter 'L' as the request type to list the dataset profile.
- 2 TAB to the dataset profile field and Enter the dataset profile and press ENTER.
- 3 TAB to the Do You Want to Keep This Information For the Add Dataset Screen field, type a 'Y', and press ENTER.
- 4 TAB to any appropriate field, type in changes, and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                                List Dataset Output
Command ==>

Dataset Profile   ==> USER01.JCL.CNTL

Owner            ==> USER02      UACC            ==> NONE
Notify           ==> _____ Warn            ==> NO
Level            ==> 000

Local Audit      ==> FAIL
Success Level    ==> _____
Failure Level    ==> READ

Installation Data ==> THIS IS NEW INSTALLATION DATA FOR THE USER01.JCL.CNTL

_____ <==

Do You Want to Keep This Information
For the Add Dataset Screen (Y/N): Y

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

When you specify 'Y' to Do You Want to Keep This Information For the Add Dataset Screen, the Owner, UACC, Warn, Level, Local Audit, Success/Failure Audit Level, and Installation Data will be passed back to the Input Screen.

Delete Dataset Profile

Perform the following steps to issue the equivalency of a RACF Delete Dataset Profile command (that is, DELDSD ‘USER01JCLCNTL’ GEN):

- 1
- Enter ‘D’ into the Request Type field
- 2
- TAB to the Dataset Profile field, type in the dataset profile you want to delete, and press ENTER.

Dataset Administration ----- SSA ----- Dataset Administration
Administration Input
Command ==>

Enter the Dataset and Request Type. Other fields are optional.

Request Type ==> D (A=Add,C=Change,L=List,D=Delete)
Dataset Profile ==> USER01.JCL.CNTL
Owner ==> Profile Owner
UACC ==> (None,Execute,Read,Update,Control,Alter)
Notify ==> Userid to Notify
Warn (Y/N) ==> Activate Warn?
Level ==> Resource Level
Local Audit ==> (All,Success,Fail,None)
Success Level ==> (None,Read,Update,Control,Alter)
Failure Level ==> (None,Read,Update,Control,Alter)
Installation Data ==>

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process deletes the specified dataset profile. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

Confirm Delete Dataset Profile Panel

Dataset Administration ----- SSA ----- Dataset Administration
Administration Input
Command ==>

Enter the Dataset and Request Type. Other fields are optional.

Req | -----SSA-----
Dat | Delete a Dataset Profile
Own | Command ==>
UAC |
Not | Confirm Delete Request (Y/N): Y
War |
Lev | Dataset Profile ==> USER01.JCL.CNTL
Loc |
Su | Hit Enter to Continue
Fa |
Installation Data ==>

Hit Enter to Continue PF03=EXIT/PF01=HELP

Resource Administration Screens

Perform List Resource Profile

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST TSOPROC MEGA130):

- 1 Enter 'L' in the Request Type field.
- 2 TAB to the Resource Profile field and enter the resource profile.
- 3 TAB to the Class field and enter the class name, and press ENTER.

```

Resource Administration ----- SSA ----- Resource Administration
                        Administration Input
Command ==>

    Enter the Resource, Class and Request Type. Other fields are optional.
Request Type      ==> L              (A=Add,C=Change,L=List,D=Delete)
Resource Profile  ==> MEGA130_____

_____
_____
Class             ==> TSOPROC_      Resource Class of Profile
Owner            ==> _____    Profile Owner
UACC             ==> _____    (None,Execute,Read,Update,Control,Alter)
Notify           ==> _____    Userid to Notify
Warn (Y/N)       ==> -             Activate Warn?
Level            ==> _____    Resource Level
Local Audit      ==> _____    (All,Success,Fail,None)
Success Level    ==> _____    (None,Read,Update,Control,Alter)
Failure Level    ==> _____    (None,Read,Update,Control,Alter)

Process Installation or Application Data (Y/N): Y

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

List Resource Profile Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Resource Administration ----- SSA ----- Resource Administration
                        List Resource Output
Command ==>

Resource Profile ==> MEGA130

_____
_____
Class             ==> TSOPROC      Owner            ==> SYSTEM
UACC             ==> NONE          Notify          ==>
Warn             ==> NO            Level           ==> 000

Local Audit       ==> FAIL
Success Level     ==>
Failure Level     ==> READ

Do You Want to Keep This Information
For the Rdefine Screen (Y/N): N

Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

Always press ENTER after a List Resource Profile, or to recover from a message, to return to the Resource Administration Main panel.

If the Process: Inst/Appl Data field was set to ‘Y’ (on the initial screen) then the following screen will be displayed as well.

```
Resource Administration ----- SSA ----- Resource Administration
                                List Resource Output
Command ==>

Resource Profile ==> MEGA130

Class ==> TSOPROC <==

Installation Data ==>

Application Data ==>

Hit Enter to Continue PF03=EXIT/PF01=HELP
```

Add Resource Profile

Perform the following steps to issue the equivalency of a RACF Add Resource Profile command (that is, RDEFINE TSOPROC NEWPROC):

- 1 Enter ‘A’ into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile you want to add.
- 3 TAB to the Class field, type in the class name you want to add the resource profile to, and press ENTER.

```
Resource Administration ----- SSA ----- Resource Administration
                                Administration Input
Command ==>

Enter the Resource, Class and Request Type. Other fields are optional.
Request Type ==> A (A=Add,C=Change,L=List,D=Delete)
Resource Profile ==> NEWPROC_____

Class ==> TSOPROC_ <==
Owner ==> _____ Resource Class of Profile
UACC ==> _____ Profile Owner
Notify ==> _____ (None,Execute,Read,Update,Control,Alter)
Warn (Y/N) ==> _ Userid to Notify
Level ==> _ Activate Warn?
Local Audit ==> _____ Resource Level
Success Level ==> _____ (All,Success,Fail,None)
Failure Level ==> _____ (None,Read,Update,Control,Alter)

Process Installation or Application Data (Y/N): Y

Hit Enter to Continue PF03=EXIT/PF01=HELP
```


This process adds the specified resource profile. All other fields are optional. The default values for optional fields if not specified are: The Owner field defaults to the Userid of person issuing the add profile, UACC defaults to None, Local Audit defaults to Fail, Failure Level defaults to Read, Warn defaults to N, Level defaults to 000, and all other fields default to blanks.

Change Resource Profile

Perform the following steps to issue the equivalency of a RACF Alter Resource Profile (that is, RALT TSOPROC NEWPROC OW(USER02) UACC(READ)):

- 1 Enter 'C' into the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile you want to change.
- 3 TAB to the Class field, and type in the class name.
- 4 TAB to the Owner field and type in the new owner
- 5 TAB to the UACC field and type in the new UACC level, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration	
Administration Input	
Command ==>	
Enter the Resource, Class and Request Type. Other fields are optional.	
Request Type	==> C (A=Add,C=Change,L=List,D=Delete)
Resource Profile	==> NEWPROC_____

<==	
Class	==> TSOPROC_ Resource Class of Profile
Owner	==> USER02_ Profile Owner
UACC	==> READ_ (None,Execute,Read,Update,Control,Alter)
Notify	==> _____ Userid to Notify
Warn (Y/N)	==> _____ Activate Warn?
Level	==> _____ Resource Level
Local Audit	==> _____ (All,Success,Fail,None)
Success Level	==> _____ (None,Read,Update,Control,Alter)
Failure Level	==> _____ (None,Read,Update,Control,Alter)
Process Installation or Application Data (Y/N): Y	
Hit Enter to Continue PF03=EXIT/PF01=HELP	

This process changes the specified resource profile. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Change Resource Profile - Installation/Application Data

Perform the following steps to issue the equivalency of a RACF Alter Resource Profile (that is, RALT TSOPROC NEWPROC APPL("") DATA(")):

- 1 Enter 'C' into the Request Type field.
- 2 TAB to Resource Profile field, type in the resource profile you want to change.
- 3 TAB to the Class field, and type in the class name.
- 4 TAB to the Process: Inst/Appl Data field and type in 'Y', and press ENTER.

Resource Administration ----- SSA ----- Resource Administration

Administration Input

Enter the Resource, Class and Request Type. Other fields are optional.

Request Type ==> C (A=Add,C=Change,L=List,D=Delete)

Resource Profile ==> NEWPROC

<==

Class ==> TSOPROC_ Resource Class of Profile

Owner ==> Profile Owner

UACC ==> (None,Execute,Read,Update,Control,Alter)

Notify ==> Userid to Notify

Warn (Y/N) ==> Activate Warn?

Level ==> Resource Level

Local Audit ==> (All,Success,Fail,None)

Success Level ==> (None,Read,Update,Control,Alter)

Failure Level ==> (None,Read,Update,Control,Alter)

Process: Inst/Appl Data (Y/N): Y

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Enter in the data in the appropriate field as shown in the screen below, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration

Administration Input

Command ==>

Enter the Installation and/or Application Data Fields.

Installation Data ==> THIS PROC IS TO BE USED FOR INSTALLING NEW TSO BASED 3RD PARTY PRODUCTS.

<==

Application Data ==> ACCESS LIST SHOULD BE: MVS SYSTEMS AREA, END-USER TESTING TEAM, AND DATA SECURITY DEPARTMENT.

<==

Hit Enter to Continue PF03=EXIT/PF01=HELP

Update Existing Resource Profile Information

Perform the following steps to update existing information for the specified resource profile:

- 1 Enter ‘L’ as the request type to list the resource profile.
- 2 TAB to the resource profile field and Enter the resource profile.
- 3 TAB to the class field and Enter the class name. If you wish to also include the resource profile’s Installation/Application Data TAB to Process: Inst/Appl Data field and type a ‘Y’
- 4 Press ENTER.
- 5 TAB to the Do You Want to Keep This Information For the Add Resource Screen field, type a ‘Y’, and press ENTER.

- 6 TAB to any appropriate field, type in changes. If you wish to also include the resource profile's Installation/Application Data TAB to Process: Inst/Appl Data field and type a 'Y' and press ENTER. You will then be presented with the Administration Input screen. TAB to either field, type in changes.
- 7 Press ENTER.

```

Resource Administration ----- SSA ----- Resource Administration
                                List Resource Output
Command ==>

Resource Profile ==> NEWPROC

Class          ==> TSOPROC      Owner          ==> TSGBAT
UACC           ==> NONE        Notify         ==>
Warn           ==> NO          Level          ==> 000

Local Audit    ==> FAIL
Success Level  ==>
Failure Level  ==> READ

Do You Want to Keep This Information
For the Rdefine Screen (Y/N): Y

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

When you specify 'Y' to Do You Want to Keep This Information For the Add Resource Screen, the Owner, UACC, Warn, Level, Local Audit, Success/Failure Audit Level, and Installation/Application Data will be passed back to the appropriate screen.

Delete Resource Profile

Perform the following steps to issue the equivalency of a RACF Delete Resource Profile command (that is, RDEL TSOPROC NEWPROC):

- 1 Enter 'D' into the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile you want to delete, and press ENTER.

```

Resource Administration ----- SSA ----- Resource Administration
                        Administration Input
Command ==>

    Enter the Resource, Class and Request Type.  Other fields are optional.
Request Type    ==> D                (A=Add,C=Change,L=List,D=Delete)
Resource Profile ==> NEWPROC

Class           ==> TSOPROC          <==
Owner           ==> _____      Resource Class of Profile
UACC            ==> _____      Profile Owner
Notify         ==> _____      (None,Execute,Read,Update,Control,Alter)
Warn (Y/N)      ==> _____      Userid to Notify
Level           ==> _____      Activate Warn?
Local Audit     ==> _____      Resource Level
Success Level   ==> _____      (All,Success,Fail,None)
Failure Level   ==> _____      (None,Read,Update,Control,Alter)
                                   (None,Read,Update,Control,Alter)

Process Installation or Application Data (Y/N): Y

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process deletes the specified resource profile. The following screen is presented to confirm the delete. Change the N to Y and press enter:

```

Resource Administration ----- SSA ----- Resource Administra
                        Delete a Resource Profile
Command ==>

Confirm Delete Request (Y/N): Y

Profile ==> NEWPROC

Class    ==> TSOPROC

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Dataset Permit Administration Screens

Perform List Dataset Profile Permits

Perform the following steps to issue the equivalency of a RACF List Dataset command (that is, LD DA() GEN AUTHUSER):

- 1 Enter 'L' in the Request Type field.
- 2 Enter the dataset profile in the Dataset Profile field and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                        Dataset Permit Input

                        Enter the Dataset and Permit Information.

Request Type      ==> L              (L=List Std,A=Add,C=Change,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL_____
Access Entry      ==> _____      User or Group to Permit
Access Level      ==> _____      (None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

List Dataset Profile Permits Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Permit Administration ----- SSA ----- Permit Administration
                        List Standard Permits

Command ==>                                Scroll ==> CSR

Permits for ==> USER01.JCL.CNTL

A = Add Permit, D = Delete Permit, C = Change Permit

SELECT      Entry      Access Level
-----
-           MEGA        ALTER
***** Bottom of data *****
  
```

You may ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- Add Permit (A)
Displays the Dataset Permit Administration Main Panel with the appropriate fields filled in.
- Delete Permit (D)
Displays the Delete Dataset Permit confirmation panel. Type ‘Y’ to confirm the delete.
- Change Permit (C)
Displays the Dataset Permit Administration Main Panel with the appropriate fields filled in.

Note The CICS version of Dataset Permit Administration only allows the user to select one permit from the list. The TSO version allows as many selections as the user requests.

Add Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT ‘USER01JCLCNTL’ GEN ID(USER02) ACCESS(ALTER)):

- 1 Enter ‘A’ into the Request Type field.
- 2 TAB to the Dataset Profile field, type in the dataset profile.
- 3 TAB to the Access Entry field, type in a userid or group.
- 4 TAB to the Access Level field, type in the access level, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Dataset Permit Input

Command ==>

Enter the Dataset and Permit Information.

Request Type

Dataset Profile

Access Entry

Access Level

==> A

==> USER01.JCL.CNTL

==> USER02__

==> ALTER__

(L=List,A=Add,C=Change,D=Delete)

User or Group to Permit

(None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process adds the userid or group to the dataset profile with the access level specified.

Change Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT 'USER01JCLCNTL' GEN ID(USER02) ACCESS(READ)):

- 1** Enter 'C' into the Request Type field.
- 2** TAB to the Dataset Profile field, type in the dataset profile.
- 3** TAB to the Access Entry field, type in a userid or group.
- 4** TAB to the Access Level field, type in the access level you want to change to, and press ENTER.

Permit Administration	----- SSA -----	Permit Administration
Dataset Permit Input		
Command ==>		
Enter the Dataset and Permit Information.		
Request Type	==> C	(L=List,A=Add,C=Change,D=Delete)
Dataset Profile	==> USER01.JCL.CNTL	
Access Entry	==> USER02__	User or Group to Permit
Access Level	==> READ__	(None,Execute,Read,Update,Control,Alter)
Hit Enter to Continue PF03=EXIT/PF01=HELP		

This process changes the userid's or group's access level to the dataset profile specified.

Delete Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT 'USER01.JCLCNTL' GEN ID(USER02) DELETE):

- 1** Enter 'D' into the Request Type field.
- 2** TAB to the Dataset Profile field, type in the dataset profile.
- 3** TAB to the Access Entry field, type in a userid or group, and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                        Dataset Permit Input

Command ==>

                        Enter the Dataset and Permit Information.

Request Type      ==> D          (L=List,A=Add,C=Change,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL
Access Entry      ==> USER02___ User or Group to Permit
Access Level      ==> _____ (None,Execute,Read,Update,Control,Alter)

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process deletes the specified dataset profile permit. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                        Dataset Permit Input

Command ==>

Req | ----- SSA -----
Dat | Delete A Standard Permit
Acc | Command ==>
Acc |
    | Confirm Delete Request (Y/N): Y
    | Dataset Profile ==> USER01.JCL.CNTL
    | Entry           ==> USER02
    | Hit Enter to Continue
    | -----

```


Resource Permit Administration Screens

Perform List Resource Profile Permits

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST TSOPROC NEWPROC AUTHUSER):

- 1 Enter 'L' in the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name, and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                                Resource Permit Input

                                Enter the Resource Profile, Class and Permit Information.

Request Type      ==> L              (L=List,A=Add,C=Change,D=Delete)
Resource Profile  ==> NEWPROC_____

-----
Class             ==> TSOPROC_      <==
Access Entry      ==> _____    Resource Class of Profile
Access Level      ==> _____    User or Group to Permit
                                      (None,Execute,Read,Update,Control,Alter)

                                Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

List Resource Profile Permits Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Permit Administration ----- SSA ----- Permit Administration
                                List Standard Permits
Command ==>                               Scroll ==> CSR

Permits For ==> NEWPROC

                                <==
Class             ==> TSOPROC
                                A = Add Permit, D = Delete Permit, C = Change Permit

SELECT   Entry   Access Level
-----
_        USER01   ALTER
***** Bottom of data *****
  
```

You may ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- Add Permit (A)
Displays the Resource Permit Administration Main Panel with the appropriate fields filled in.
- Delete Permit (D)
Displays the Delete Resource Permit confirmation panel. Type ‘Y’ to confirm the delete.
- Change Permit (C)
Displays the Resource Permit Administration Main Panel with the appropriate fields filled in.

Add Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) ACCESS(READ)):

- 1 Enter ‘A’ into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Access Entry field, type in a userid or group
- 5 TAB to the Access Level field, type in the access level, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Resource Permit Input

Command ==>

Enter the Resource Profile, Class and Permit Information.

Request Type ==> A (L=List,A=Add,C=Change,D=Delete)

Resource Profile ==> NEWPROC

Class ==> TSOPROC Resource Class of Profile

Access Entry ==> USER02__ User or Group to Permit

Access Level ==> ALTER__ (None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process adds the userid or group to the resource profile with the access level specified.

Change Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) ACCESS(NONE)):

- 1 Enter 'C' into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Access Entry field, type in a userid or group
- 5 TAB to the Access Level field, type in the new access level, and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                                Change Permit Input

Command ==>

                                Enter the Access Level to Change to.

Request Type      ==> C              (A=Add,Change,D=Delete)
Resource Profile  ==> NEWPROC

                                <==
Class             ==> TSOPROC        Resource Class of Profile
Access Entry      ==> USER02        User or Group to Permit
Access Level      ==> NONE_____    (None,Execute,Read,Update,Control,Alter)

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

This process changes the userid's or group's access level to the resource profile specified.

Delete Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) DEL):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Access Entry field, type in a userid or group, and press ENTER.

Permit Administration ----- SSA ----- Permit Change Successful

Resource Permit Input

Command ==>

Enter the Resource Profile, Class and Permit Information.

Request Type ==> D (L=List,A=Add,C=Change,D=Delete)

Resource Profile ==> NEWPROC_____

_____<==

Class ==> TSOPROC_ Resource Class of Profile

Access Entry ==> USER02_ User or Group to Permit

Access Level ==> _____ (None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process deletes the specified resource profile permit. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Resource Permit Input

Command ==>

Req | ----- SSA -----

Res | Delete A Standard Permit

Command ==>

Confirm Delete Request (Y/N): Y

Cla | Profile ==> NEWPROC

Acc |

Acc |

Class ==> TSOPROC <==

Entry ==>

Level ==>

Hit Enter to Continue

Resource Member Administration Screens

Perform List Resource Profile Members

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST GCICSTRN CICSCAT2):

- 1 Enter 'L' in the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name, and press ENTER.

```

Member Administration ----- SSA ----- Member Administration
                        Resource Member Input
Command ==>

        Enter the Resource Profile, Class and Member Information.

Request Type      ==> L              (L=List,A=Add,D=Delete)
Resource Profile  ==> CICSCAT2

                                <==
Class            ==> GCICSTRN      Resource Class of Profile
Member          ==> _____

                                <==
                                Member To Be Processed

                                _____

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

List Resource Profile Members Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Member Administration ----- SSA ----- Member Administration
                        List Resource Members
Command ==>                                Scroll ==> CSR

Resource      ==> CICSCAT2

                                <==
Class         ==> GCICSTRN

                                A = Add Member, D = Delete Member

SELECT                                Member
-----                                -----
_____ CEMT                                -----

                                <==
                                -----
_____ CEOT                                -----

                                <==
                                -----
  
```

You may 'select and scroll' through the listing and specify, in the select column, any of the following options:

- Add Member (A)
Displays the Resource Member Administration Main Panel with the appropriate fields filled in.
- Delete Member (D)
Displays the Delete Resource Member confirmation panel. Type ‘Y’ to confirm the delete.

Add Resource Profile Member

Perform the following steps to issue the equivalency of a RACF Resource Profile Add Member command (that is, RALTER GCICSTRN CICSCAT2 ADDMEM(CEMX)):

- 1 Enter ‘A’ into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Member field, type in the new member, and press ENTER.

Member Administration ----- SSA ----- Member Administration

Resource Member Input

Command ==>

Enter the Resource Profile, Class and Member Information.

Request Type ==> A (L=List,A=Add,D=Delete)

Resource Profile ==> CICSCAT2

Class ==> GCICSTRN Resource Class of Profile

Member ==> CEMX

Member To Be Processed

Hit Enter to Continue PF03=EXIT/PF01=HELP

This process adds the member requested to the resource profile and class specified.

Delete Resource Profile Member

Perform the following steps to issue the equivalency of a RACF Resource Profile Add Member command (that is, RALTER GCICSTRN CICSCAT2 DELMEM(CEMX)):

- 1 Enter ‘D’ into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Member field, type in the member to remove, and press ENTER.

Member Administration ----- SSA ----- Member Administration	
Resource Member Input	
Command ==>	
Enter the Resource Profile, Class and Member Information.	
Request Type	==> D (L=List,A=Add,D=Delete)
Resource Profile	==> CICSCAT2
<==	
Class	==> GCICSTRN Resource Class of Profile
Member	==> CEMX
<==	
Member To Be Processed	
Hit Enter to Continue PF03=EXIT/PF01=HELP	

This process deletes the specified resource member. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

Member Administration ----- SSA ----- Member Administration	
Resource Member Input	
Comma	----- SSA -----
	Delete A Resource Member
Req	Command ==>
Res	Confirm Delete Request (Y/N): Y
	Profile ==> CICSCAT2
Clas	
Mem	Class ==> GCICSTRN <==
	Member ==> CEMX
	<==
	Hit Enter to Continue

User TSO Segment Administration Screens

Perform List User TSO Segment

Perform the following steps to issue the equivalency of a RACF List User TSO Segment command (that is, LISTUSER USER01 TSO NORACF):

- 1
- Enter ‘L’ in the Request Type field.
- 2
- TAB to the Userid field, type in the userid, and press ENTER.

TSO Segment Administration ----- SSA ----- TSO Segment Administration

Administration Input

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> L (A=Add,C=Change,L=List,D=Delete)

Userid ==> USER01

Account Number ==>

Destination ==> Unit ==>

Hold Class ==> Job Class ==>

Msg Class ==> Sysout Class ==>

Logon Procedure ==> Security Label ==>

Logon Size ==> 0000000 Max Size ==> 0000000

User Data ==> 0000

Command** ==>

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue PF03=EXIT/PF01=HELP

List User TSO Segment Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

TSO Segment Administration ----- SSA ----- TSO Segment Administration

List TSO Segment Output

Command ==>

Userid ==> USER01

Account Number ==>

Destination ==> Unit ==>

Hold Class ==> X Job Class ==>

Msg Class ==> Sysout Class ==>

Logon Procedure ==> Security Label ==>

Logon Size ==> 0000000 Max Size ==> 0000000

User Data ==> 0000

Command ==>

Do You Want to Keep This Information

For the Add/Change TSO Segment Screen (Y/N): N

Hit Enter to Continue PF03=EXIT/PF01=HELP

Always press ENTER after a List User TSO Segment, or to recover from a message, to return to the User TSO Segment Administration Main panel.

Add User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 TSO(PROC(NEWPROC) SIZE(2048) MAXSIZE(4096))

- 1 Enter 'A' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Logon Procedure field, type in the procedure.
- 4 TAB to the Logon Size field, type in the minimum size.
- 5 TAB to the Max Size field, type in the maximum size, and press ENTER.

```

TSO Segment Administration ----- SSA ----- TSO Segment Administration
                        Administration Input

Command ==>

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> A                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01
Account Number    ==> _____
Destination       ==> _____ Unit      ==> _____
Hold Class        ==> _                     Job Class      ==> _
Msg Class         ==> _                     Sysout Class     ==> _
Logon Procedure    ==> NEWPROC_             Security Label  ==> _____
Logon Size        ==> 0002048              Max Size        ==> 0004096
User Data         ==> 0000

Command**         ==> _____

                        ** = Only Valid On RACF 2.3 Or Above

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
  
```

This process adds a TSO segment for the userid specified. All other fields are optional. The default values for optional fields if not specified are: The Logon Size field defaults to all zeroes, the Max Size field defaults to all zeroes, and the User Data field defaults to all zeroes.

Note If the Max Size field is all zeroes then the userid's TSO segment has an 'unlimited' amount of size for their logon session. Also, if the Max Size field is other than all zeroes, it must be greater than the Logon Size.

Change User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 TSO(MAXSIZE(0000) MSGCLASS(X)):

- 1 Enter 'C' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Msg Class field, type in the new message class value.
- 4 TAB to the Max Size field, type in the new maximum size.
- 5 TAB to the Logon Size and press Erase-End-Of-Field key, TAB to the User Data and press Erase-End-Of-Field key, and press ENTER.

TSO Segment Administration ----- SSA ----- TSO Segment Administration
Administration Input

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type

==> C

Userid

==> USER01

Account Number

==>

Destination

==>

Unit

==>

Hold Class

==> _

Job Class

==> _

Msg Class

==> X

Sysout Class

==> _

Logon Procedure

==>

Security Label

==>

Logon Size

==>

Max Size

==> 0000000

User Data

==>

Command**

==>

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process changes the specified userid’s TSO segment. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Delete User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 NOTSO):

1 Enter ‘D’ into the Request Type field

2 TAB to the Userid field, type in the userid profile, and press ENTER.

TSO Segment Administration ----- SSA ----- TSO Segment Administration
Administration Input

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type

==> D

Userid

==> USER01

Account Number

==>

Destination

==>

Unit

==>

Hold Class

==> _

Job Class

==> _

Msg Class

==> _

Sysout Class

==> _

Logon Procedure

==>

Security Label

==>

Logon Size

==> 0000000

Max Size

==> 0000000

User Data

==> 0000

Command**

==>

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue

PF03=EXIT/PF01=HELP

This process deletes the specified userid’s TSO segment. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

Smart Security Administrator USER GUIDE

TSO Segment Administration ----- SSA ----- TSO Segment Administration
Administration Input

Command ==>

Req
Use
Acc
Des
Ho1
Msg
Log
Log
Use

----- SSA -----
Delete a TSO Segment
Command ==>
Confirm Delete Request (Y/N): Y
Userid ==> USER01
Hit Enter to Continue

ds are optional.
Change,L=List,D=Delete)

==> _
==> _
==> _
==> 0000000

Command** ==> _____

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue PF03=EXIT/PF01=HELP

User CICS Segment Administration Screens

Perform List User CICS Segment

Perform the following steps to issue the equivalency of a RACF List User CICS Segment command (that is, LISTUSER USER01 CICS NORACF):

- 1
- Enter ‘L’ in the Request Type field.
- 2
- TAB to the Userid field, type in the userid, and press ENTER.

CICS Segment Administration ----- SSA ----- CICS Segment Administration

Administration Input

Command ==>

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> L (A=Add,C=Change,L=List,D=Delete)

Userid ==> USER01

Operator ID ==> _____

Operator Priority ==> 000 (000 - 255)

XRF Takeover Force ==> NOFORCE (FORCE/NOFORCE)

Timeout ==> 00:00 (HH:MM)

Opclasses: (Y=Add,N=Delete)

01: _ 02: _ 03: _ 04: _

05: _ 06: _ 07: _ 08: _

09: _ 10: _ 11: _ 12: _

13: _ 14: _ 15: _ 16: _

17: _ 18: _ 19: _ 20: _

21: _ 22: _ 23: _ 24: _

Hit Enter to Continue PF03=EXIT/PF01=HELP

List User CICS Segment Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

CICS Segment Administration ----- SSA ----- CICS Segment Administration

List CICS Segment Output

Command ==>

Userid ==> USER01 Operator ID ==> 000

Operator Priority ==> 000 XRF Takeover Force ==> NOFORCE

Timeout ==> 00:00

Opclasses ==>

01: 02: 03: 04:

05: 06: 07: 08:

09: 10: 11: 12:

13: 14: 15: 16:

17: 18: 19: 20:

21: 22: 23: 24:

Do You Want to Keep This Information

For the Add/Change CICS Segment Screen (Y/N): N

Hit Enter to Continue PF03=EXIT/PF01=HELP

Always press ENTER after a List User CICS Segment, or to recover from a message, to return to the User CICS Segment Administration Main panel.

Add User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER USER01 CICS (OPIDENT(AB1) TIMEOUT(0130)):

- 1 Enter 'A' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Operator Identity field, type in the opid.
- 4 TAB to the Timeout field, type in the timeout value, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                                Administration Input
Command ==>

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> A                (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01
Operator ID       ==> AB1
Operator Priority  ==> 000              (000 - 255)
XRF Takeover Force ==> NOFORCE          (FORCE/NOFORCE)
Timeout           ==> 01:30            (HH:MM)

Opcodes:                                (Y=Add,N=Delete)

      01: _      02: _      03: _      04: _
      05: _      06: _      07: _      08: _
      09: _      10: _      11: _      12: _
      13: _      14: _      15: _      16: _
      17: _      18: _      19: _      20: _
      21: _      22: _      23: _      24: _

      Hit Enter to Continue          PF03=EXIT/PF01=HELP
  
```

This process adds a CICS segment for the userid specified. All other fields are optional. The default values for optional fields if not specified are: The Operator ID field defaults to all zeroes, the Operator Priority field defaults to all zeroes, the Timeout field defaults to all zeroes, XRF Takeover Force field defaults to NOFORCE.

Change User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER USER01 CICS (TIMEOUT(0415)):

- 1 Enter 'C' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Timeout field, type in the new timeout value, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Administration Input
Command ==>

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> C          (A=Add,C=Change,L=List,D=Delete)
Userid           ==> USER01
Operator ID      ==> _____
Operator Priority ==> 000        (000 - 255)
XRF Takeover Force ==> NOFORCE  (FORCE/NOFORCE)
Timeout          ==> 04:15     (HH:MM)

Opcodes:                                     (Y=Add,N=Delete)

      01: _      02: _      03: _      04: _
      05: _      06: _      07: _      08: _
      09: _      10: _     11: _      12: _
      13: _      14: _     15: _      16: _
      17: _      18: _     19: _      20: _
      21: _      22: _     23: _      24: _

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process changes the specified userid's CICS segment. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Delete User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER USER01 NOCICS):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Administration Input
Command ==>

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> D          (A=Add,C=Change,L=List,D=Delete)
Userid           ==> USER01
Operator ID      ==> _____
Operator Priority ==> 000        (000 - 255)
XRF Takeover Force ==> NOFORCE  (FORCE/NOFORCE)
Timeout          ==> 00:00     (HH:MM)

Opcodes:                                     (Y=Add,N=Delete)

      01: _      02: _      03: _      04: _
      05: _      06: _      07: _      08: _
      09: _      10: _     11: _      12: _
      13: _      14: _     15: _      16: _
      17: _      18: _     19: _      20: _
      21: _      22: _     23: _      24: _

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

This process deletes the specified userid's CICS Segment. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

CICS Segment Administration ----- SSA ----- CICS Segment Administration			
Administration Input			
Command ==>			
Enter the Request Type and Userid. Other fields are optional.			
Req	----- SSA -----		L=List,D=Delete)
Use	Delete a CICS Segment		
Ope	Command ==>		
Ope			
XRF	Confirm Delete Request (Y/N): Y		
Tim			
	Userid ==> USER01		
Opc	Hit Enter to Continue		

05: _	06: _	07: _	08: _
09: _	10: _	11: _	12: _
13: _	14: _	15: _	16: _
17: _	18: _	19: _	20: _
21: _	22: _	23: _	24: _
Hit Enter to Continue PF03=EXIT/PF01=HELP			

Access Simulator

The access simulator allows users to interrogate RACF to determine the user’s or group’s highest allowed access level to a particular resource. The Access Simulator also determines the protecting profile of the resource.

Security

You must have read access to the default profile
SSA.ACCESS.SIMULATOR in the default resource class
MAA\$RULE (See Configuration section for changing defaults).

Below is the input screen where you specify the user or group and the resource to be checked.:

Access Simulator ----- SSA ----- Access Simulator

Command ==>

Enter All Applicable Fields to Simulate an Access Attempt.

Enter Valid Userid or Group ==> IBMUSER

Resource ==> SYS1.PARMLIB

Class ==> DATASET

Volume (Optional) ==> _____

Hit Enter to Continue PF03=EXIT/PF01=HELP

- ENTER VALID
USERID OR GROUP

Enter a valid userid or group whose authority you want checked.
- RESOURCE

Enter a resource (can be dataset or general resource) that you want the user or groups authority checked against. It must be a fully qualified resource; no generic profiles.
- CLASS

Enter a valid resource class (can be dataset or general resource class).
- VOLUME

Note USER and GROUP are not valid classes.

Optional. If you specify a dataset as the resource and DATASET as the class to check, you can specify a volume. If the resource and volume combination do not match an existing discrete profile, then checking will default to the generic profile that is providing protection. When you have entered the required fields and hit enter, you will be presented with the results of the access check as shown below.

Access Simulator Results Screen

```
Access Simulator ----- SSA ----- Access Simulator
Command ==>

                                Simulation Results

                                USERID=IBMUSER,NAME=GENERAL DFLT USER

Resource                        ==> SYS1.PARMLIB

                                <==
Class                          ==> DATASET
Volume (Optional)              ==>

Protecting Profile ==> SYS1.*

                                <==

Highest Allowed Access Level ==> ALTER

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

The access simulation returns the following:

- Identification of entry. If it is a user, the users name is returned as well.
- The resource you entered originally.
- The resource class you entered originally
- The volume if entered originally
- RACF profile, if any, that is protecting the resource specified.
- Highest access level allowed by the user or group entered to the resource specified.



CHAPTER 8

System Resource Monitor

SSA monitors and reports on sensitive system resources. These resources are critical z/OS components. However, they can represent a possible impact on the integrity and security of a system.

Most resources can be related to RACF security, in which case the report shows that relationship and expands upon it. For example, it is important to monitor the status of RACF dataset profile protection for APF authorized libraries. SSA will not only report on the APF authorized libraries but will include, if you choose the options, the protecting RACF profile (if there is one), the permissions to that profile, and will expand the group permissions showing all users connected to that group.

Note All reports obtain information from in-storage currently active settings, not from datasets like SYS1.PARMLIB.

System Resource Monitor Global Conventions

Through-out the SSA product and manual there are several “global” conventions that occur. For the System Resource Monitor section the following conventions apply:

Security

All SSA system resource monitor reports are protected at both the panel dialog level and at the report execution level. The default RACF general resource class is MAASRULE and READ is the required access level. Below is a list of the system resource monitor reports and the default security profiles that a user must have access to in order to execute the options. See the Configuration section on changing the default protecting class or profiles if you want to change them.

System Resource Monitor Report	RACF Profile
System Resource Monitor Panel Dialog	MEGASOLVE-SSA.MONITOR.REPORTS
APF (Authorized Program Facility)	MEGASOLVE-SSA.MONITOR.APF
LLT (Link List Table)	MEGASOLVE-SSA.MONITOR.LLT
LPA (Link Pack Area)	MEGASOLVE-SSA.MONITOR.LPA
CDT (Class Descriptor Table)	MEGASOLVE-SSA.MONITOR.CDT
PPT (Program Properties Table)	MEGASOLVE-SSA.MONITOR.PPT
GRI (General RACF Information)	MEGASOLVE-SSA.MONITOR.RAC
EXT (RACF Installation Exits)	MEGASOLVE-SSA.MONITOR.RAC
RDS (RACF Database Datasets)	MEGASOLVE-SSA.MONITOR.RAC
RAU (RACF Authorized Caller Table)	MEGASOLVE-SSA.MONITOR.RAU
RFR (RACF Router Table)	MEGASOLVE-SSA.MONITOR.RFR
SMF (System Management Facility)	MEGASOLVE-SSA.MONITOR.SMF
STC (Started Task Table)	MEGASOLVE-SSA.MONITOR.STC
SVC (Supervisor Calls)	MEGASOLVE-SSA.MONITOR.SVC
ATT (Authorized TSO Tables)	MEGASOLVE-SSA.MONITOR.ATT
	** And PARMLIB profile in the TSOAUTH class

Batch or Online Operational Mode

BATCH mode processing generates the JCL necessary to create the report you requested based upon your selections. SSA displays the Review Generated JCL panel, as shown below.

```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'IBMUSER.SSA.TEMP.JCL(BATCH)'

OPTION ==> E

Enter E to Edit the Generated JCL
V to View the Generated JCL
S to Submit the Generated JCL
ST to Store the Generated JCL
SC to Schedule the Generated JCL

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

- E Select E if you want to be placed in an EDIT session.
- V Select V if you want to be placed in a VIEW session.
- S Select S if you want to submit the generated JCL.
- ST Select ST if you want to store the generated JCL in the SSA storage facility.
- SC Select SC if you want to schedule the generated JCL through The SCHEDULER. For details on scheduling, please see ‘The SCHEDULER’ on page 269.

ONLINE mode processing creates the report based upon your selections automatically. You are then presented with a BROWSE session as shown below. You can decide to print the report produced.

```

Print ParmS ----- SSA ----- Print ParmS
Command ==> Scroll ==> CSR

Do you want to print this display (Y/N): N

Sysout ==> A Copies ==> 01 Title ==> N
Hold (Y/N) ==> N Page Length ==> 55 Destination ==>

BROWSE - IBMUSER.TSCSSA.REPORT.OUTPUT ----- LINE 00000000 COL 001 080
***** Top of Data *****

-----
Date: MM/DD/YYYY
Time: 14:37

SSA - Version V.V
System Resource Monitor

CPU ID: 123456
CPU Model: 9672

```

Send Report Output

- S (SYSOUT) Valid for BATCH mode only. Sends the report output to SYSOUT (if the JOB is expanded through SDSF a DDNAME of AAREPORT is used).
- D (DATASET) Valid for BATCH or ONLINE modes. In either mode the output is directed to the output dataset.

System Resource Monitor Report JCL

All report generation options use the same JCL. Below is sample JCL (MNMONBTC - System Resource Monitor Reports):

```
//*
//*
//*****
//**
//**          SMART SECURITY ADMINISTRATOR      **
//**          **                                **
//**          VERSION V.V                      **
//**          **                                **
//** (C) YYYY UNICOM SYSTEMS, INC.             **
//**          ALL RIGHTS RESERVED               **
//*****
//*
//* JCL CREATED BY USER01
//* JCL CREATED ON MM/DD/YYYY
//* JCL CREATED AT 14:37
//*
//* JOB FUNCTION: SYSTEM_RESOURCE_MONITOR_REPORT
//*
//STEP010 EXEC PGM=IKJEFT01,DYNAMNBR=30,TIME=1440,REGION=4096K
//SYSPROC DD DISP=SHR,
//          DSN=SSA.ISPCLIB
//ISPPROF DD DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
//          DCB=(LRECL=80,BLKSIZE=6160,RECFM=FB),UNIT=SYSDA
//ISPPLIB DD DISP=SHR,
//          DSN=SSA.ISPPLIB
//ISPSLIB DD DISP=SHR,
//          DSN=SSA.ISPSLIB
//ISPMLIB DD DISP=SHR,
//          DSN=ISP.SISPMENU
//          DD DISP=SHR,
//          DSN=SSA.ISPMLIB
//ISPTLIB DD DISP=SHR,
//          DSN=ISP.SISPTENU
//AADBTLIB DD DISP=SHR,
//          DSN=SSA.RACFDATA.ISPTLIB
//STEPLIB DD DISP=SHR,
//          DSN=SSA.LOADLIB
//ISPCTL1 DD DSN=&CNTL1,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),SPACE=(TRK,(5,5))
//ISPCTL2 DD DSN=&CNTL2,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),SPACE=(TRK,(5,5))
//SYSTSPRT DD SYSOUT=*,DCB=(BLKSIZE=19019,LRECL=133,RECFM=FBA)
//SYSPRINT DD SYSOUT=*,DCB=(BLKSIZE=20000,LRECL=200,RECFM=FBA)
//ISPLOG DD SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
//SYSOUT DD SYSOUT=*
//TEMPWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//MNMONLIB DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//MNTMPLIB DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE),
//          DCB=(RECFM=FB,LRECL=380,BLKSIZE=23180)
//AAREPORT DD SYSOUT=*,
//          DCB=(RECFM=FBA,LRECL=133)
//*
//AACTLCDS DD *
REPORT=APF,PER(YES)
//*
//SYSTSIN DD *
ISPSTART PGM(MNMONBTC)
//*
```

JCL DD Statements

Below is a brief explanation of the JCL DD statements and what they must reference:

SYSPROC	Must reference the SSA CLIST library.
ISPPLIB	Must reference the SSA Panel library.
ISPSLIB	Must reference the SSA Skeleton library.
ISPMLIB	Must reference the ISPF system message library and the SSA ISPF message library.
ISPTLIB	Must reference the ISPF table library.
AADBTLIB	Must reference the SSA RACF information table library.
STEPLIB	Must reference the SSA APF authorized load library.
AACMDOUT	This DD must reference an output dataset with the following DCBs: RECFM=FB, LRECL=133, DSORG=PS
SYSTIN	This DD is where the start command for activation system resource monitor reporting are entered.
AACTLCDS	The DD AACTLCDS references control cards that specify the data shown in the report. The control cards must start in column 1. Also, if no control cards are entered, the APF report is activated as a default.

Refer to 'System Resource Monitor Overrides' on page 358 for a list of control cards that can override each report's default values.

System Resource Monitor Menu

This menu allows you to select system resource monitor reports and the options used to create these reports.

```
System Resource Monitor ----- SSA ----- System Resource Monitor
Command ==>

      Operational Mode (Batch/Online) ==> BATCH
-----
Direct Report Output to Sysout or Dataset (S/D): S
-----
      Default Report Settings (Y/N) N

      S   Authorized Program Facility   (APF)
      -   Link List Datasets             (LLT)
      -   Link Pack Area Datasets        (LPA)
      -   Class Descriptor Table         (CDT)
      -   Program Properties Table       (PPT)
      -   General RACF Information       (GRI)
      -   RACF Installation Exits       (EXT)
      -   RACF Database Datasets        (RDS)
      -   RACF Authorized Caller Table   (RAU)
      -   RACF Router Table              (RFR)
      -   System Management Facility     (SMF)
      -   Started Task Table             (STC)
      -   Supervisor Calls               (SVC)
      -   Authorized TSO Tables          (ATT)

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Reports and Options

Default Report Settings	Indicate if you want to use the default settings for all reports you create. If you indicate “N”, you are prompted with the override choices for each report. “Y” is the default.
Authorized Program Facility (APF)	Indicate if you want to run a report on the APF authorized libraries in your system. This report lists datasets that contain programs requiring authorization because they issue privileged instructions or restricted Sifts. As a result, these programs can bypass system security and integrity mechanisms.
Link List Table (LLT)	Indicate if you want to run a report on the LLT libraries in your system. This is a list of datasets concatenated to SYS1 .LINKLIB - allows easy access to programs and system services that are used frequently - a directory list of all programs in these datasets is created at initialization.
Link Pack Area Table (LPA)	Indicate if you want to run a report on the LPA libraries in your system. This is a list of datasets concatenated to SYS1 .LPALIB containing program modules to be shared between address spaces, including many system routines (SVCs and access methods). These program modules are loaded into storage (Pageable Link Pack Area) during initialization.

Class Descriptor table (CDT)	Indicate if you want to create a report on the CDT entries in your system. This report lists information that directs processing of general resources. It contains one entry for each class, except USER, GROUP, and DATASET. Sources are IBM supplied (ICHRRCDX) and User supplied (ICHRRCDE).
PROGRAM PROPERTIESTABLE (PPT)	Indicate if you want to create a report on the PPT entries in your system. This report lists programs with special attributes (non-swappable, non-cancelable, or special storage keys). The programs must be APF-authorized for these to take effect.
General RACF Information (GRI)	Indicate if you want to create a report on General RACF settings usually obtained through SETROPTS list as they currently are in storage.
RACF Installation Exits (EXT)	Indicate if you want to run a report on the RACF installed exits for pre and post processing and other related functions.
RACF Database Datasets (RDS)	Indicate if you want to run a report on the RACF Database Datasets on your system.
RACF Authorized Caller Table (RAU)	Indicate if you want to run a report on the RACF Authorized Caller Table. This is a list of program modules that can execute a RACINIT SVC without NEWPASSWORD or execute a RACLIST SVC.
RACF Router Table (RFR)	Indicate if you want to run a report on the RACF Router Table. This is a list of entries that control the action taken by the RACF router (ICHRFR00) when invoked by the RACROUTE macro. Sources are IBM supplied: ICHRFROX and User supplied: ICHRFRO1.
System Management Facility (SMF)	Indicate if you want to run a report on the SMF libraries and setup in your system. This is a report on the z/OS component that records audit-type records for system events as they occur.
Started Task Table (STC)	Indicate if you want to run a report on the Started Task Table. This is a list of entries that assigns userid/group and special attributes to procedures started from the operator console based on procedure name. Sources are IBM supplied: ICHRIN03 and the STARTED class in RACF.
Supervisor Call Table (SVC)	Indicate if you want to run a report on the SVC table in your system. This is a list of system and user routines that comprise many system services, such as OPEN, CLOSE, ABEND, and so on.
Authorized TSO Tables (ATT)	Indicate if you want to run a report on the Authorized TSO table in your system. This is a list of commands/programs that can run authorized under TSO - list of commands/programs that can run authorized when called through the TSO services facility.

System Resource Monitor Overrides

Listed below are control cards/overrides that can be specified with the AACTLCDS DD statement of the JCL used to produce System Resource Monitor reports.

Authorized Program Facility (APF)

Include RACF Permissions	Indicate if you want to display all the permissions to the RACF profiles that protect APF authorized datasets.
Expand Group Permissions	Indicate if you want all group permissions to be expanded showing all users connected to that particular group.
Parameters	Main Card =REPORT=APF Permissions =PER(YES) or PER(NO) Expand Groups =EGP
Sample	REPORT=APF,PER(YES),EGP

Link List Datasets (LLT)

Include RACF Permissions	Indicate if you want to display all the permissions to the RACF profiles that are protecting the Link List datasets.
Expand Group Permissions	Indicate if you want all group permissions to be expanded showing all users connected to that particular group.
Parameters	Main Card =REPORT=LLT Permissions =PER(YES) or PER(NO) Expand Groups =EGP
Sample	REPORT=LLT,PER(YES),EGP

Link Pack Area Datasets (LPA)

Include RACF Permissions	Indicate if you want to display all the permissions to the RACF profiles that are protecting the Link Pack Area datasets.
Expand Group Permissions	Indicate if you want all group permissions to be expanded showing all users connected to that particular group.
Parameters	Main Card =REPORT=LPA Permissions =PER(YES) or PER(NO) Expand Groups =EGP
Sample	REPORT=LPA,PER(YES),EGP

Class Descriptor Table (CDT)

Sort Choice	Indicate how you want the report sorted. Sort choices are:	
	01	=Report is sorted by Resource Class in Ascending order.
	02	=Report is sorted by Posit Number in Ascending order.
	03	=Report is sorted by Posit Number in Ascending order and secondarily by Resource Class in Ascending order.
Report Style Choice	Indicate the style of report you want to create. Report choices are:	
	01	=The report consists of one line per entry in the Class Descriptor Table. Because of space limitations, only key information is included. Some fields are not included. (See the report sample in Appendix A).
	02	=The report consists of one entry per page with all the available information included in the report. Although this style can produce reports that are much larger than option one, it is recommended if you want all CDT fields shown in the report.
Parameters	Main Card	=REPORT=CDT
	Sort Choice	=SORT=01
	Report Choice	=REPORT=01
Sample	REPORT=CDT,SORT=01,REPORT=01	

Program Properties Table (PPT)

Parameters	Main Card	=REPORT=PPT
Sample	REPORT=PPT	

General RACF Information (GRI)

Parameters	Main Card	=REPORT=GRI
Sample	REPORT=GRI	

RACF Installation Exits (EXT)

Parameters	Main Card	=REPORT=EXT
Sample	REPORT=EXT	

RACF Database Datasets (RDS)

Include RACF Permissions	Indicate if you want to display all the permissions to the RACF profiles that are protecting the RACF Database datasets.	
Expand Group Permissions	Indicate if you want all group permissions to be expanded showing all users connected to that particular group.	

Parameters	Main Card	=REPORT=RDS
	Permissions	=PER(YES) or PER(NO)
	Expand Groups	=EGP
Sample	REPORT=RDS,PER(YES),EGP	

RACF Authorized Caller Table (RAU)

Parameters	Main Card	=REPORT=RAU
Sample	REPORT=RAU	

RACF Router Table (RFR)

Parameters	Main Card	=REPORT=RFR
Sample	REPORT=RFR	

System Management Facility (SMF)

Include RACF Permissions	Indicate if you want to display all the permissions to the RACF profiles that are protecting the SMF datasets.	
Expand Group Permissions	Indicate if you want all group permissions to be expanded showing all users connected to that particular group.	
Parameters	Main Card	=REPORT=SMF
	Permissions	=PER(YES) or PER(NO)
	Expand Groups	=EGP
Sample	REPORT=SMF,PER(YES),EGP	

Started Task Table (STC)

Include RACF Information	Indicate if you want to include relevant RACF information concerning the users defined to the Started Task table.	
Expand Group Entries	Indicate if you want all group related entries to be expanded showing all users connected to that particular group.	
Parameters	Main Card	=REPORT=STC
	Include RACF Info	=RAC(YES) or RAC(NO)
	Expand Groups	=EGP
Sample	REPORT=STC,RAC(YES),EGP	

Supervisor Calls (SVC)

Parameters	Main Card	=REPORT=SVC
Sample	REPORT=SVC	

Authorized TSO Tables (ATT)

Parameters	Main Card	=REPORT=ATT
Sample	REPORT=ATT	



CHAPTER 9

CICS Direct Administration

Most RACF administration can be done from CICS. CICS Direct Administration (referred to as SSA-CDA) allows users to do:

- Userid administration
- Group administration
- Connect administration
- Password administration
- Dataset administration
- Resource administration
- Dataset permit administration
- Resource permit administration
- Resource member administration
- User TSO segment administration
- User CICS segment administration
- Access simulator

It is also important to note the following operating pluses for using SSA-CDA:

- All updates and inquiries done by SSA-CDA are done live.
- SSA-CDA allows for the administration of remote systems, and uses the same security and look and feel as SSA-TDA.
- SSA-CDA allows a user to use the various features without having group or global SPECIAL.

Prerequisites

To perform all of its documented functions, SSA-CDA requires the following software releases:

RACF	FMID HRF7730 or greater
CICS	CICS TS 4.2 or greater

Note CICS uses standard APIs to communicate with SSA.

If you do not meet these requirements or have a question concerning them, please call your SSA representative for clarification. It is quite possible that your current levels will allow SSA-CDA to perform all of its functions.

Note CICS Direct Administration produces standard SMF Type 80 audit records.

CICS Direct Administration Global Conventions

Security

Security for CICS Direct Administration functions are protected on two levels.

- ‘Authority’ profile.

This type of profile determines what profiles a user can affect. The table show below lists the format for a general ‘Authority’ profile, and the specific ‘Authority’ profile that protects global SPECIAL users.

Function	RACF Class	RACF Profile (Authority Profile)
Userid Administration	MAA\$RULE	MEGASOLVE-SSA.\$USER.<default group>
Group Administration	MAA\$RULE	MEGASOLVE-SSA.\$GROUP.<superior group>
Connect Administration	MAA\$RULE	MEGASOLVE-SSA.\$CONNECT.<group>
Password Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESET.<group>
Dataset Administration	MAA\$RULE	MEGASOLVE-SSA.\$DATASET.<hlq>
Resource Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE.<class>
Dataset Permit Administration	MAA\$RULE	MEGASOLVE-SSA.\$DATASET.<hlq>
Resource Permit Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE.<class>
Resource Member Administration	MAA\$RULE	MEGASOLVE-SSA.\$RESRCE.<class>
User TSO Segment Administration	MAA\$RULE	MEGASOLVE-SSA.\$UTSO.<default group>
User CICS Segment Administration	MAA\$RULE	MEGASOLVE-SSA.\$UCICS.<default group>
Access Simulator	MAA\$RULE	MEGASOLVE-SSA.ACCESS.SIMULATOR
Global Special User Protection	MAA\$RULE	MEGASOLVE-SSA.\$SPECIAL\$

MEGASOLVE-SSA.\$USER.<default group>

A Userid Administration user that has access to an ‘Authority’ profile can change any user that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you can use generic characters in the <default group> to select a range of users.

MEGASOLVE-SSA.\$GROUP.<superior group>

A Group Administration user that has access to an ‘Authority’ profile can change any group that has that particular group as their superior group. If you have generic processing turned on for the SSA security class, you can use generic characters in the <superior group> to cover a wide range of users.

MEGASOLVE-SSA.\$RESET.<group>

A Password Administration user that has access to an ‘Authority’ profile can change any user that is connected to the <group> specified in the profile. If you have generic processing turned on for the SSA security class, you can use generic characters in the <group> to cover a wide range of users.

MEGASOLVE-SSA.\$CONNECT.<group>

A Connect Administration user that has access to an ‘Authority’ profile can change any connection for the <group> specified in the profile. If you have generic processing turned on for the SSA security class, you can use generic characters in the <group> to cover a wide range of users.

MEGASOLVE-SSA.\$DATASET.<hlq>

A Dataset Administration and Dataset Permit Administration user that has access to an ‘Authority’ profile can change any dataset profile that begins with the <hlq> specified in the profile. If you have generic processing turned on for the SSA security class, you can use generic characters in the <hlq> to cover a wide range of dataset profiles.

MEGASOLVE-SSA.\$RESRCE.<class>

A Resource Administration, Resource Permit Administration, and Resource Member Administration user that has access to an ‘Authority’ profile can change resource profiles that begins with the <class> specified in the profile. If you have generic processing turned on for the SSA security class, you can use generic characters in the <class> to cover a wide range of resource profiles.

MEGASOLVE-SSA.\$UTSO.<default group>

A User TSO Segment Administration user that has access to an ‘Authority’ profile can change any user’s TSO segment that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you can use generic characters in the <default group> to cover a wide range of users.

MEGASOLVE-SSA.\$UCICS.<default group>

A User CICS Segment Administration user that has access to an ‘Authority’ profile can change any user’s CICS segment that has that particular group as their default group. If you have generic processing turned on for the SSA security class, you can use generic characters in the <default group> to cover a wide range of users.

MEGASOLVE-SSA.ACCESS.SIMULATOR

This profile protects the access simulator which allows a user to interrogate RACF to determine a users or groups highest allowed access level to a particular resource. The Access Simulator will also determine what is the protecting profile of the resource.

MEGASOLVE-SSA.\$SPECIAL\$

This profile protects global SPECIAL users from any user that has any CICS Direct Administration function. In order to use a CICS Direct Administration function to affect a global SPECIAL user they must have access to an 'Authority' profile that protects the SPECIAL user and they also must have access to this profile. If you do not define this profile, then this check is bypassed for global SPECIAL users, and normal 'Authority' profile checking applies.

Note It is highly recommended that you define this profile. The profile should have a UACC(NONE) and no access list entries. This will protect global SPECIAL users from unauthorized attempts at being updated.

Example 'Authority' Profile Setup

The example below illustrates how to define an 'Authority' profile.

Scenario: You, the security administrator, want to allow the Payroll department manager to be able to add users, connect those users to payroll groups and do Password Administration for all of the users in the Payroll Department.

Known: The default group for the PAYROLL Department is PAYROLL. The userid for the Payroll department manager is MNGRPAY.

Profiles to build:

For Add User: MEGASOLVE-SSA.\$USER.PAYROLL
For Connect: MEGASOLVE-SSA.\$CONNECT.PAYROLL
For Password Administration: MEGASOLVE-SSA.\$RESET.PAYROLL

Command to issue:

```
RDEFINE GAA$RULE CDA-PAYROLL -
  ADDMEM(MEGASOLVE-SSA.$USER.PAYROLL -
    MEGASOLVE-SSA.$CONNECT.PAYROLL -
    MEGASOLVE-SSA.$RESET.PAYROLL) - OWNER(SYS1) UACC(NONE)
```

▪ Access level security

The second type of security is the access level you have to the 'Authority' profile. Below is a separate table showing each function and what access levels are required to perform them.

Userid Administration Function	Userid Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Userid	X	X	X	X
Add Userid	X	X	X	X
Add/Change Userid Name	X	X	X	X
Add/Change Owner	X	X	X	X
Add/Change Password	X	X	X	X
Add/Change Userid Installation Data			X	X

Userid Administration Function	Userid Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Delete Userid				X
List Group	X	X	X	X
Add Group	X	X	X	X
Add/Change Owner	X	X	X	X
Add/Change TERMUACC	X	X	X	X
Add/Change Group Installation Data			X	X
Delete Group				X

Connect Administration Function	Connect Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List All Connect Profiles	X	X	X	X
List Specific Connect Profile	X	X	X	X
Connect User to Group	X	X	X	X
Change Group UACC	X	X	X	X
Resume Connect	X	X	X	X
Revoke Connect	X	X	X	X
Set/Remove TERMUACC Attribute	X	X	X	X
Set/Remove Connect Resume Date		X	X	X
Set/Remove Connect Revoke Date		X	X	X
Remove User from Group		X	X	X
Change Group Authority			X	X
Set/Remove Connect Attributes (except TERMUACC)				X

Password Administration Function	Password Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List User	X	X	X	X
Set Password for User	X	X	X	X
Resume User	X	X	X	X

Password Administration Function	Password Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Revoke User	X	X	X	X
Set/Remove a Resume Date for a User		X	X	X
Set/Remove a Revoke Date for a User		X	X	X
Update Installation Data for a User			X	X
SuperRevoke User or Resume a SuperRevoked User				X

Dataset Administration Function	Dataset Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Dataset profile	X	X	X	X
Add Dataset profile	X	X	X	X
Change Dataset profile	X	X	X	X
Update Installation Data for a Dataset Profile			X	X
Delete Dataset profile				X

Resource Administration Function	Resource Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Resource profile	X	X	X	X
Add Resource profile	X	X	X	X
Change Resource profile	X	X	X	X
Update Installation and/or Application Data for a Resource Profile			X	X
Delete Resource profile				X

Dataset Permit Administration Function	Dataset Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Permit	X	X	X	X
Add Permit	X	X	X	X
Change Permit		X	X	X

Dataset Permit Administration Function	Dataset Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
Delete Permit		X	X	X

Resource Permit Administration Function	Resource Permit Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Permit	X	X	X	X
Add Permit	X	X	X	X
Change Permit		X	X	X
Delete Permit		X	X	X

Resource Member Administration Function	Resource Member Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Resource Member	X	X	X	X
Add Resource Member	X	X	X	X
Delete Resource Members		X	X	X

User TSO Segment Administration Function	User TSO Segment Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Segment	X	X	X	X
Add Segment		X	X	X
Change Segment		X	X	X
Delete Segment				X

User CICS Segment Administration Function	User CICS Segment Administration 'Authority' Profile Access Level			
	READ	UPDATE	CONTROL	ALTER
List Segment	X	X	X	X
Add Segment		X	X	X
Change Segment		X	X	X
Delete Segment				X

Example Access Level Setup

The example below illustrates how to set the access level for the ‘Authority’ profile.

Scenario: You, the security administrator, want to allow the Payroll department manager to be able to add users, connect those users to payroll groups and do Password Administration for all of the users in the Payroll Department.

Known: The default group for the PAYROLL Department is PAYROLL. The userid for the Payroll department manager is MNGRPAY.

Profiles protecting all Payroll Department users:

```
MEGASOLVE-SSA.$USER.PAYROLL
MEGASOLVE-SSA.$CONNECT.PAYROLL
MEGASOLVE-SSA.$RESET.PAYROLL
```

Access level needed:

```
CONTROL
```

Command to issue:

```
PERMIT CDA-PAYROLL -
CLASS(GAA$RULE) ID(MNGRPAY) -
ACCESS(CONTROL)
```

Note It is important to remember that the authorities only relate to the RACF access the user has to the MAA\$RULE class profiles. Just because a user can have GROUP SPECIAL, it does not mean this individual has the authority to use SSA-CDA to do RACF Administration.

Function Explanations

All SSA-CDA function explanation sections use the following sequence:

- Associated Screens and particular function examples and descriptions
- API Invocation

Application Programming Interface

CICS Direct Administration offers two distinct ways of doing RACF administrative tasks:

- through the SSA-CDA transaction interface
- through the SSA-CDA application programming interface.

The SSA-CDA API allows a company to incorporate RACF administrative tasks into their CICS applications. The CDA API uses the same security rules and communication means as the CDA transactions. This permits programmers to create their own front-ends, or incorporate RACF processing into the application of their choice. The invoker of the API does not run authorized, does not need to know RACF command syntax, or the rules concerning fields. The contents and the API can be used for cross platform administration See ‘Cross Platform Administration’ on page 492.

Invoking the API To invoke the API, the CICS program must call the SSA-CDA client program AAZCLNT with a COMMAREA. The COMMAREA consists of a header section used by all function types being requested and the actual parameters or data for that request. The COMMAREA must always be 32760 in length regardless of the function being used. Below is an example of the EXEC CICS call to the CDA API client program:

API Call Example

```
EXEC CICS LINK PROGRAM('AAZCLNT')
      COMMAREA(COMMAREA) LENGTH(HALF)
```

Note The constant HALF is defined as:

```
HALFDC    H'32760'
```

API Header The API header section has the following fields:

Field Label	Length	Explanation	Required on Invocation?
CMMSG	0CL80	Error message from API client program. This area is broken down into the 4 character transaction code field CTRAN and FILLER.	NO
CTRAN	4	Transaction Code (SAPW, and so on.) used to look up entries in the AATCPIP table which is used to indicate what IP and PORT address to direct the request to.	NO, unless you are doing cross platform administration. See 'Cross Platform Administration' on page 492 for further explanation.
FILLER	76	Filler	NO
CTASK	12	Code indicating what function you are invoking. The following codes are valid: ADDUSER - Userid Administration ADDGROUP - Group Administration CONNECT - Connect Administration PSWADMIN - Password Administration ADDDATASET - Dataset Administration ADDRSOURCE - Resource Administration DSNPERMIT - Dataset Permit Administration RSCPERMIT - Resource Permit Administration RSCMEMBER - Resource Member Administration USERTSO - User TSO Segment Administration USERCICS - User CICS Segment Administration AUTHCHK - Access Simulator	YES. You must indicate what function you are requesting. This area on return can contain an error message.
CADMINAID	8	Userid to be used for verifying authority to do the function requested.	NO, unless you are doing cross platform administration. See 'Cross Platform Administration' on page 492 for further explanation.

Field Label	Length	Explanation	Required on Invocation?
CADMPW	8	Password to be used for verifying the userid requesting the function.	NO, unless you are doing cross platform administration. See 'Cross Platform Administration' on page 492 for further explanation.
CADMNEW	8	New Password that can be used if the requester's password expired or they wish to change it.	NO. See 'Cross Platform Administration' on page 492 for further explanation
RSTCODE	3	Decimal Error Code. See the API Error Code table.	NO. The API client program AAZCLNT fills in this code. See the API Error Code table for a complete listing.
CREQTYPE	1	Determined access level of request	NO, the API client program AAZCLNT will automatically fill this in.

API Header Example

The following Assembler layout sample can be found in member APIHEADR of the SSA install library:

```

MSG          DS      0CL80      ERROR MESSAGE FROM CLIENT
CTAN         DS      CL4        TRANSACTION CODE *THAT ROUTES *
                                REQUEST TO DESIGNATED IP AND *PORT
                                ADDRESS
*
*          DS      CL76        FILLER
CTASK        DS      CL12       FUNCTION REQUESTED
*
*          - ADDUSER - USERID ADMIN
*          - ADDGROUP - GROUP ADMIN
*          - CONNECT - CONNECT ADMIN
*          - PSWADMIN - PASSWORD ADMIN
*          - ADDDATASET - DATASET ADM.
*          - ADDRESOURCE - RESOURCE
*          - DSNPERMIT - DATASET PERM.
*          - RSCPERMIT - RESOURCE PERM
*          - RSCMEMBER - RESOURCE MEMB
*          - USERTSO - USER TSO SEG.
*          - USERCICS - USER CICS SEG.
*          - AUTHCHK - ACCESS SIMULATE
*          ** THIS AREA ON RETURN MAY
*          ** CONTAIN AN ERROR MESSAGE
ADMINID      DS      CL8        USERID TO BE USED FOR
*          VERIFYING AUTHORITY TO DO
*          THE FUNCTION REQUESTED
*          ** THIS IS ONLY REQUIRED FOR
*          ** CROSS PLATFORM ADMIN
CADMPW       DS      CL8        PASSWORD TO BE USED FOR
*          VERIFYING THE USERID
*          REQUESTING THE FUNCTION
*          ** THIS IS ONLY REQUIRED FOR
*          ** CROSS PLATFORM ADMIN

```

CADMNEW	DS	CL8	NEW PASSWORD THAT CAN BE USED
*			IF THE REQUESTER'S PASSWORD
*			EXPIRED OR THEY WISH TO
*			CHANGE IT.
*			** THIS IS ONLY REQUIRED FOR
*			** CROSS PLATFORM ADMIN AND
*			** IF THE USER WANTS TO
*			** CHANGE THEIR PASSWORD
RSTCODE	DS	CL3	DECIMAL RETURN CODE
CREQTYPE	DS	CL1	DETERMINED ACCESS LEVEL OF
*			REQUEST

General API Errors

When an error occurs utilizing the SSA-CDA API client program AAZCLNT the invoking program must perform the following sequence of error checking to insure that the error is interpreted correctly:

The invoking program must check the CTASK field. Initially this field is filled in by the invoking program determining what function is to be performed. Upon return, this field can contain an error indicator. Below are the possible error indicators and the message(s) that would be placed in the CMSG field:

CTASK Message Indicator	Message	Explanation
ADDUSER	None	Invoking program requested Userid Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
ADDGROUP	None	Invoking program requested Group Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
CONNECT	None	Invoking program requested Connect Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.

CTASK Message Indicator	Message	Explanation
PSWADMIN	None	Invoking program requested Password Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
ADDDATASET	None	Invoking program requested Dataset Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
ADDRSOURCE	None	Invoking program requested Resource Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
DSNPERMIT	None	Invoking program requested Dataset Permit Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
RSCPERMIT	None	Invoking program requested Resource Permit Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.

CTASK Message Indicator	Message	Explanation
RSCMEMBER	None	Invoking program requested Resource Member Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
USERTSO	None	Invoking program requested User TSO Segment Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
USERCICS	None	Invoking program requested User CICS Segment Administration function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
AUTHCHK	None	Invoking program requested Access Simulator function and no errors were detected in the invocation. Invoking program should now check the RSTCODE field for errors on the request itself.
TCPIP ERROR	COMMAREA error length is not correct	Invoking program specified an incorrect length on the COMMAREA. The length must always be 32760.
TCPIP ERROR	Client not authorized to get your userid	The client program retrieves and uses the userid currently invoking the program but was unable to do so. Contact your SSA representative for assistance.

CTASK Message Indicator	Message	Explanation
TCPIP ERROR	CSKE required to activate the API	SSA-CDA uses CICS Sockets. The CICS Sockets API is not activated. The default transaction to activate the CICS Sockets API is CSKE. Contact your CICS systems programmer for assistance in activating the CICS Sockets API. Details on this can be found in the CICS TCP/IP Socket Interface Guide.
TCPIP ERROR	INITAPI function failed	The SSA-CDA client program was unable to initialize the CICS Sockets API. Check your settings in the AATCPIP configuration module. See details in the Cross Platform part of this section.
TCPIP ERROR	Cannot get this host's IP address	The SSA-CDA client program was unable to obtain or reference the correct IP address for the TCP/IP started task servicing its current system.
TCPIP ERROR	SOCKET function failed (<i>nnn</i>)	A SOCKET request failed (<i>nnn</i> = return code from TCP/IP function that failed). Check that the AATCPIP configuration module settings are correct and that the destination started task is active and operating properly. Contact your SSA representative if you require assistance.

CTASK Message Indicator	Message	Explanation
TCPIP ERROR	CONNECT function failed (<i>nnn</i>)	A CONNECT request failed (<i>nnn</i> = return code from TCP/IP function that failed). Check that the AATCPIP configuration module settings are correct and that the destination started task is active and operating properly. Contact your SSA representative if you require assistance.
TCPIP ERROR	SEND function failed (<i>nnn</i>)	A SEND request failed (<i>nnn</i> = return code from TCP/IP function that failed). Check that the AATCPIP configuration module settings are correct and that the destination started task is active and operating properly. Contact your SSA representative if you require assistance.
TCPIP ERROR	RECV function failed (<i>nnn</i>)	A RECV request failed (<i>nnn</i> = return code from TCP/IP function that failed). Check that the AATCPIP configuration module settings are correct and that the destination started task is active and operating properly. Contact your SSA representative if you require assistance.
TCPIP ERROR	CLOSE function failed (<i>nnn</i>)	A CLOSE request failed (<i>nnn</i> = return code from TCP/IP function that failed). Check that the AATCPIP configuration module settings are correct and that the destination started task is active and operating properly. Contact your SSA representative if you require assistance.

CTASK Message Indicator	Message	Explanation
NEED IDENT	None	The value in the CTRAN field or the name of the invoking transaction referenced an AATCPIP site configuration that was not the local system. Thus, the invoking program must supply a RACF userid and password that is valid on the remote system where the request is being routed. See 'Cross Platform Administration' on page 492 for further explanation.
IDENT ERROR	None, however, the RSTCODE field is set to one of the following values: 904 - User Unknown 908 - Password Invalid 912 - Password Expired 916 - New Password Not Valid 920 - User Not Defined to Group 924 - Failed By Installation Exit 928 - User Is Revoked 932 - User Group Access Is Revoked 936 - Set as Invalid Userid 940 - Set as Invalid Password	The value in the CTRAN field or the name of the invoking transaction referenced an AATCPIP site configuration that was not the local system. An error was encountered using the userid and password supplied for the request being sent to the remote system.
PARM ERROR	Invalid value in CTASK parameter	An invalid request type was entered in the CTASK field. CTASK must contain either ADDUSER, ADDGROUP, CONNECT, PSWADMIN, ADDDATASET, ADDRESOURCE, DSNPERMIT, RSCPERMIT, RSCMEMBER, USERTSO, USERCICS, or AUTHCHK

If the CTASK field is not set to an error message (that is, “IDENT ERROR”, “TCPIP ERROR”, and so on.), then the invoking program must check the return code (RSTCODE field) to determine the status of the request. Below are tables detailing the function specific return codes possible.

Userid
Administration
Specific Errors

The following table details the errors and messages specific to the Userid Administration function being requested.

CTASK Message	Indicator	Message Explanation
ADDUSER	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Userid Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field.	000 - Add user performed as requested	
	004 - Userid already exists	
	008 - Not authorized	
	012 - Database update error	
	016 - Resource not protected by RACF	
	020 - AACMD003 is not authorized	
	024 - RACROUTE error extracting user data	
	028 - Not authorized for install update	
	032 - Not authorized for segments	
	036 - Invalid default group	
	040 - List user performed as requested	
	044 - Default Group = SuperRevoke	
	048 - Owner invalid	
	052 - Userid does not exist	
	056 - Userid already exists as group	
	060 - RC>8 - authority check	
	064 - Invalid parm - authority check	
	068 - Unable to verify userid - authority check	
	072 - Userid revoked - authority check	
	076 - User not authorized for delete	
	080 - User change complete	
	084 - AACMD003 is not authorized	
	088 - Dataset profiles exist for this user	
	092 - Userid deleted as requested	
	096 - Default group invalid for change	
	100 - Invalid userid	
	104 - Invalid owner	
	108 - Invalid password	
	112 - Invalid default group	
	116 - Not authorized for SPECIAL	

CTASK Message	Indicator	Message Explanation
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Default Group is Required for Add ▪ Request not 'A', 'C', 'L', or 'D' ▪ There Were No Fields to Change ▪ Userid must be specified ▪ Password Entered Contains Invalid Characters ▪ Group Entered Contains Invalid Characters ▪ Owner Entered Contains Invalid Characters ▪ Userid Entered Contains Invalid Characters	The SSA-CDA Userid Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Group Administration Specific Errors

The following table details the errors and messages specific to the Group Administration function being requested.

CTASK Message Indicator	Message	Explanation
ADDGROUP	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Group Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field.	000 - Add group performed as requested 004 - Group already exists as a user 008 - Not authorized 012 - Database update error 016 - Resource not protected by RACF 020 - AACMD004 is not authorized 024 - RACROUTE error extracting group data 028 - Not authorized for install update 032 - Not authorized for segments 036 - Invalid superior group 040 - List group ok 044 - Superior Group = SuperRevoke 048 - Owner invalid 052 - Group does not exist 056 - Group already exists as group 060 - RC>8 - authority check 064 - Invalid parm - authority check 068 - Unable to verify userid - authority check 072 - Userid revoked - authority check 076 - Not authorized for delete 080 - Group change complete 084 - AACMD004 not authorized 088 - Dataset profiles exist for this group 092 - Users exist for this group 096 - Group deleted 100 - Subgroups exist for this group 104 - Subgroup invalid for change 108 - Invalid group 112 - Invalid subgroup 116 - Invalid owner	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'C', 'L', or 'D'. ▪ There Were No Fields to Change ▪ Group and Superior Group required for add ▪ You must enter a Group to be Processed ▪ TERMUACC Setting must be 'Y', 'N', or blank ▪ Group Entered Contains Invalid Characters ▪ Owner Entered Contains Invalid Characters ▪ Superior Group Entered Contains Invalid Characters	The SSA-CDA Group Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Connect Administration Specific Errors

The following table details the errors and messages specific to the Connect Administration function being requested.

CTASK Message	Indicator	Message Explanation
CONNECT	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Connect Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field.	000 - Connect or Remove performed as requested 004 - Unable to verify userid 008 - Not authorized to list user 012 - Resume/Revoke/Reset error 016 - List of specific group ok 020 - Resource not protected by RACF 024 - AACMD002 is not authorized 028 - Not authorized for special 032 - Not authorized for super-revoke 036 - Resume/Revoke date less than today 040 - RACROUTE error extracting user data 044 - Connect group is invalid 048 - Not authorized for attributes 052 - Not authorized for authority 056 - Not authorized for revoke/resume dates 060 - Not authorized for remove 064 - User not connected to remove group 068 - No GETMAIN address for list 072 - Not authorized to list this group 076 - Attempt to remove default group 080 - Not authorized to list any connect group 084 - List-of-groups ok 088 - User not connected to this group 092 - Resume date/Revoke date invalid 096 - Unsupported date 100 - RC>8 - Authority check 104 - Invalid parm - Authority check 108 - Unable to verify userid - Authority check 112 - Userid revoked - Authority check	

CTASK Message	Indicator	Message Explanation
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Userid must be specified ▪ Request not 'L', 'S', 'C', or 'R' ▪ Connect group must be specified ▪ Resume date must look like YYYY-MM-DD ▪ Revoke date must look like YYYY-MM-DD ▪ Resume field must be 'Y' or 'N' ▪ Revoke field must be 'Y' or 'N' ▪ Resume and revoke cannot both be 'Y' ▪ ADSP field must be 'Y' or 'N' ▪ Audit field must be 'Y' or 'N' ▪ GRPACC field must be 'Y' or 'N' ▪ SPEC field must be 'Y' or 'N' ▪ OPER field must be 'Y' or 'N' ▪ TRMUACC field must be 'Y' or 'N' ▪ Group UACC field is invalid ▪ Group AUTH field is invalid	The SSA-CDA Connect Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Password Administration Specific Errors

The following table details the errors and messages specific to the Password Administration function being requested.

CTASK Message Indicator	Message	Explanation
PSWADMIN Please Note: This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	None, however, the RSTCODE field will be set to one of the following values: 000 - Reset performed as requested 004 - Unable to verify userid 008 - Not authorized to list user 012 - Resume/Revoke/Reset error 016 - List userid performed as requested 020 - Resource not protected by RACF 024 - AACMD001 is not authorized 028 - Not authorized for userid with global special 032 - Not authorized for Super-Revoke 036 - Resume/Revoke date less than today 040 - RACROUTE error extracting user data 044 - Super-Revoke group is invalid 048 - Not authorized for install update 052 - Not authorized for revoke/resume dates 056 - Invalid default group 060 - Revoke date ignored 064 - Resume/Revoke date invalid 068 - Reserved for future use 072 - RACROUTE error 076 - Invalid parm - auth check 080 - Unable to verify userid 084 - Userid revoked	The SSA-CDA Password Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Userid must be specified ▪ Resume date must look like YYYY-MM-DD ▪ Revoke date must look like YYYY-MM-DD ▪ Resume field must be 'Y' or blank ▪ Revoke field must be 'Y' or blank ▪ Resume and revoke cannot both be 'Y' ▪ Super-Revoke must be 'Y' or blank ▪ Password contains invalid characters	The SSA-CDA Password Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Dataset Administration Specific Errors

The following table details the errors and messages specific to the Dataset Administration function being requested.

Note Dataset Administration does not support Discrete RACF Dataset Profiles.

CTASK Message Indicator	Message	Explanation
ADDDATASET	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Dataset Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add dataset profile performed as requested 004 - Dataset profile already exists 008 - Not authorized 012 - Database update error 016 - Dataset not protected by RACF 020 - AACMD005 is not authorized 024 - RACROUTE error extracting Dataset data 028 - Not authorized for installation data 032 - Not authorized for permit/member data 036 - List dataset profile performed as requested 040 - Owner is invalid 044 - Dataset profile does not exist 048 - RACROUTE error - auth check 052 - Invalid Parm - auth check 056 - Unable to verify userid 060 - Userid revoked 064 - Not authorized for DELETE 068 - Change dataset profile performed as requested 072 - Delete dataset profile performed as requested 076 - Invalid dataset profile 080 - Invalid dataset profile - only 1 qualifier 084 - Invalid Owner 088 - Invalid Notify	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'C', 'L', or 'D' ▪ You must enter a dataset profile ▪ Invalid dataset profile ▪ Warn must be 'Y', 'N', or blank ▪ Invalid level number ▪ UACC must be 'LIST', 'NONE', 'EXECUTE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Failure level must be 'NONE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Success level must be 'NONE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Local audit must be 'ALL', 'SUCCESS', 'FAIL', or 'NONE' ▪ At least one field must be entered for dataset profile change	The SSA-CDA Dataset Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Resource Administration Specific Errors

The following table details the errors and messages specific to the Resource Administration function being requested.

CTASK Message	Indicator	Message Explanation
ADDRESOURCE	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Resource Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add resource profile performed as requested 004 - Resource profile already exists 008 - Not authorized 012 - Database update error 016 - Resource not protected by RACF 020 - AACMD006 is not authorized 024 - RACROUTE error extracting resource data 028 - Not authorized for installation data 032 - Not authorized for permit/member data 036 - Invalid Class 040 - List resource profile performed as requested 044 - Owner is invalid 048 - Resource profile does not exist 052 - RACROUTE error - auth check 056 - Invalid Parm - auth check 060 - Unable to verify userid 064 - Userid revoked 068 - Not authorized for DELETE 072 - Change resource profile performed as requested 076 - Delete resource profile performed as requested 080 - Profile cannot be defined due to CDT restrictions 084 - Profile too long for class 088 - Notify is invalid	

CTASK Message	Indicator	Message Explanation
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'C', 'L', or 'D' ▪ You must enter a resource profile ▪ You must enter a resource class ▪ Warn must be 'Y', 'N', or blank ▪ Invalid level number ▪ UACC must be 'LIST', 'NONE', 'EXECUTE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Failure level must be 'NONE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Success level must be 'NONE', 'READ', 'UPDATE', 'CONTROL', or 'ALTER' ▪ Local audit must be 'ALL', 'SUCCESS', 'FAIL', or 'NONE' ▪ At least one field must be entered for resource profile change	The SSA-CDA Resource Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Dataset Permit Administration Specific Errors

The following table details the errors and messages specific to the Dataset Permit Administration function being requested.

Note Dataset Permit Administration does not support RACF Conditional Access Lists.

CTASK Message Indicator	Message	Explanation
DSNPERMIT	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Dataset Permit Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add permit performed as requested 004 - Change permit performed as requested 008 - Delete permit performed as requested 012 - List permit performed as requested 016 - Reserved 020 - Unable to verify Userid/Group 024 - Resource not protected 028 - AACMD007 is not authorized 032 - RACROUTE error 036 - Not authorized for change/delete 040 - No GETMAIN address for list 044 - Not authorized to add/list permits 048 - RACROUTE error - auth check 052 - Invalid Parm - auth check 056 - Unable to verify userid 060 - Userid revoked 064 - Dataset does not exist 068 - Nothing to list 072 - Permit exists for add 076 - Permit does not exist for change/delete	
PARM ERROR	Message content in field CMSG could be one of the following: - Request not 'A', 'C', 'L', or 'D' - Dataset profile must be specified - Access Level must be 'NONE', 'EXECUTE', 'READ', 'UPDATE', 'CONTROL', 'ALTER', or blank - Access Entry and Level must be specified for add/change	The SSA-CDA Dataset Permit Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Resource Permit Administration Specific Errors

The following table details the errors and messages specific to the Resource Permit Administration function being requested.

Note Resource Permit Administration does not support RACF Conditional Access Lists.

CTASK Message Indicator	Message	Explanation
RSCPERMIT	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Resource Permit Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add permit performed as requested 004 - Change permit performed as requested 008 - Delete permit performed as requested 012 - List permit performed as requested 016 - Specified class is invalid 020 - Unable to verify Userid/Group 024 - Resource not protected 028 - AACMD015 is not authorized 032 - RACROUTE error 036 - Not authorized for change/delete 040 - No GETMAIN address for list 044 - Not authorized to add/list permits 048 - RACROUTE error - auth check 052 - Invalid Parm - auth check 056 - Unable to verify userid 060 - Userid revoked 064 - Dataset does not exist 068 - Nothing to list 072 - Permit exists for add 076 - Permit does not exist for change/delete	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'C', 'L', or 'D' ▪ Resource profile must be specified ▪ Resource Class must be specified •Access Level must be 'NONE', 'EXECUTE', 'READ', 'UPDATE', 'CONTROL', 'ALTER', or blank ▪ Access Entry and Level must be specified for add/change	The SSA-CDA Resource Permit Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Resource Member Administration Specific Errors

The following table details the errors and messages specific to the Resource Member Administration function being requested.

CTASK Message Indicator	Message	Explanation
RSCMEMBER	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA Resource Member Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add member performed as requested 004 - Member exists for add 008 - Delete member performed as requested 012 - List member performed as requested 016 - Specified class is invalid 020 - Member does not exist for delete 024 - Resource not protected 028 - AACMD014 is not authorized 032 - RACROUTE error 036 - Not authorized for delete 040 - No GETMAIN address for list 044 - Not authorized to add/list members 048 - RACROUTE error - auth check 052 - Invalid Parm - auth check 056 - Unable to verify userid 060 - Userid revoked 064 - Resource/Class does not exist 068 - Nothing to list 072 - Not a grouping class 076 - Profile too long	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'L', or 'D' ▪ Resource profile must be specified ▪ Resource Class must be specified •Member must be specified for add/delete	The SSA-CDA Resource Member Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

User TSO Segment Administration Specific Errors

The following table details the errors and messages specific to the TSO Segment Administration function being requested.

CTASK Message Indicator	Message	Explanation
USERTSO	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA TSO Segment Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field		
	000 - Add/change segment performed as requested	
	004 - Not authorized for read	
	008 - Database update error	
	012 - Resource not protected by RACF	
	016 - AACMD008 is not authorized	
	020 - RACROUTE error extracting user data	
	024 - Not authorized for update	
	028 - List segment performed as requested	
	032 - Userid does not exist	
	036 - RACROUTE error - auth check	
	040 - Invalid Parm - auth check	
	044 - Unable to verify userid	
	048 - Userid revoked	
	052 - Not authorized for delete	
	056 - Delete segment performed as requested	
	060 - Not authorized for SPECIAL	
	064 - DEST is invalid	
	068 - HOLDCLASS is invalid	
	072 - JOBCLASS is invalid	
	076 - PROC is invalid	
	080 - SIZE is invalid	
	084 - MSGCLASS is invalid	
	088 - MAXSIZE is invalid	
	092 - SYSOUTCLASS is invalid	
	096 - USERDATA is invalid	
	100 - UNIT is invalid	
	104 - SECLABEL is invalid	
	110 - COMMAND Keyword is invalid	
	112 - Segment does not exist	

CTASK Message Indicator	Message	Explanation
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'L', 'C, or 'D' ▪ DESTINATION contains invalid characters ▪ HOLDCLASS contains invalid characters ▪ JOBCLASS contains invalid characters ▪ PROC contains invalid characters ▪ SIZE contains invalid characters ▪ MSGCLASS contains invalid characters ▪ MAXSIZE contains invalid characters ▪ SYSOUTCLASS contains invalid characters ▪ USERDATA contains invalid characters ▪ UNIT contains invalid characters ▪ SECLABEL contains invalid characters ▪ At least one field must be entered for add/change	The SSA-CDA TSO Segment Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

User CICS Segment Administration Specific Errors

The following table details the errors and messages specific to the CICS Segment Administration function being requested.

CTASK Message Indicator	Message	Explanation
USERCICS	None, however, the RSTCODE field will be set to one of the following values:	The SSA-CDA CICS Segment Administration API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Add/change segment performed as requested 004 - Not authorized for read 008 - Database update error 012 - Resource not protected by RACF 016 - AACMD009 is not authorized 020 - RACROUTE error extracting user data 024 - Not authorized for update 028 - List segment performed as requested 032 - Userid does not exist 036 - RACROUTE error - auth check 040 - Invalid Parm - auth check 044 - Unable to verify userid 048 - Userid revoked 052 - Not authorized for delete 056 - Delete segment performed as requested 060 - Not authorized for SPECIAL 064 - OPPTY is invalid 068 - TIMEOUT is invalid 072 - Segment does not exist 076 - Segment exists for add	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Request not 'A', 'L', 'C', or 'D' ▪ Userid is required ▪ OPCLASS fields must be 'Y', 'N', or blank ▪ XRF Takeover Force must be 'FORCE' or 'NOFORCE' ▪ Timeout must be HH:MM or blank ▪ Minutes can not be greater than 60 ▪ Minutes can not be greater than 59 ▪ At least one field must be entered for add/change	The SSA-CDA CICS Segment Administration API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Access Simulator Specific Errors The following table details the errors and messages specific to the Access Simulator function being requested.

CTASK Message Indicator	Message	Explanation
AUTHCHK	None, however, the RSTCODE field will be set to one of the following values:	The SSA-C DA Access Simulator API call was filled in properly, and the RSTCODE contains the result of the request being processed.
Please Note:		
This is the original CTASK value. This field will contain either an error or be blank upon return. If it is blank you must check the RSTCODE field	000 - Authorization check performed as requested 004 - No profile found 008 - Access not allowed 012 - Severe RACROUTE error 016 - Invalid access 020 - Unable to verify userid/group 024 - Userid is revoked 028 - Profile is blank 032 - Class is blank	
PARM ERROR	Message content in field CMSG could be one of the following: ▪ Userid or group must be specified ▪ Resource must be specified ▪ Userid/group/class must be specified ▪ Class is not valid ▪ Volume specified - Class must be DATASET	The SSA-C DA Access Simulator API call was not filled in properly. Syntax errors must be corrected before invoking the API again.

Samples supplied To facilitate usage of the SSA-CDA API program samples for API invocations and menus, maps and other jobs have been provided. Below is a list of the members in the SSA install library and a brief explanation of their content:

Install Library Member	Description
\$ALMAPS	JCL to assemble CICS maps
\$ALPGM	JCL to assemble a CICS program
\$RDO	JCL for CICS resource definitions
AATCPIP	Sample TCPIP routing table
AAZAUT	Map definitions used by the AAZAUT01 Access Simulator program
AAZCON	Map definitions used by the AAZCON01 Connect Administration program
AAZDSA	Map definitions used by the AAZDSA01 Dataset Administration program
AAZDSP	Map definitions used by the AAZDSP01 Dataset Permit Administration program
AAZGRP	Map definitions used by the AAZGRP01 Group Administration program

Install Library Member	Description
AAZMBA	Map definitions used by the AAZMBA01 Resource Member Administration program
AAZMN	Map Definitions used by the AAZMN01 Standard Menu program
AAZMN01	Sample CICS Menu Program for remote processing.
AAZMNU	Map definitions used by the AAZMNU01 Sample Basic Menu program
AAZMNU01	Sample CICS Basic Menu Program
AAZPWA	Map definitions used by the AAZPWA01 Password Administration program
AAZPWS	Map definitions used by the AAZPWS01 Sample Basic Password Admin Program
AAZPWS01	Sample CICS Basic Password Administration program
AAZRSA	Map definitions used by the AAZRSA01 Resource Administration program
AAZRSP	Map definitions used by the AAZRSP01 Resource Permit Administration program
AAZUID	Map definitions used by the AAZUID01 Userid / Password Prompting program
AAZUSR	Map definitions used by the AAZUSR01 Userid Administration program
AAZUTC	Map definitions used by the AAZUTC01 CICS Segment Administration program
AAZUTP	Map definitions used by the AAZUTP01 TSO Segment Administration program
CPYAUT	Copylib statements for COMMAREA used by the Access Simulator program
CPYCON	Copylib statements for COMMAREA used by the Connect Administration program
CPYDSA	Copylib statements for COMMAREA used by the Dataset Administration program
CPYDSP	Copylib statements for COMMAREA used by the Dataset Permit Administration program
CPYGRP	Copylib statements for COMMAREA used by the Group Administration program
CPYMBA	Copylib statements for COMMAREA used by the Resource Member Administration
CPYPWA	Copylib statements for COMMAREA used by the Password Administration program

Install Library Member	Description
CPYRSA	Copylib statements for COMMAREA used by the Resource Administration program
CPYRSP	Copylib statements for COMMAREA used by the Resource Permit Administration program
CPYUSR	Copylib statements for COMMAREA used by the Userid Administration program
CPYUTC	Copylib statements for COMMAREA used by the CICS Segment Administration program
CPYUTP	Copylib statements for COMMAREA used by the TSO Segment Administration program
REGISTER	Copylib statements for register equates used by AAZPWS01

Note All programmers wishing to use the SSA-CDA API should review the sample program AAZPWS01 to get a good understanding by example of what is required to properly invoke the SSA-CDA API.

RACLIST vs. Non-RACLIST Classes Whenever a CICS Direct function is performed against any general resource class that has been RACLISTed in RACF, it is recommended that a SETROPTS RACLIST(classname) REFRESH RACF command be issued in order for any normal RACF command (that is, RLIST, RALT, RDEL) to be processed successfully.

CICS DIRECT Administration Main Menu

CICS Direct Administration functions can be invoked from the SSA-CDA Main Menu. The Main Menu is accessible by executing transaction SAMN, which brings up the Main Menu.

```
CICS Direct Administration ----- SSA ----- CICS Direct Administration
                               Main Menu

Selection ==> _                OPTION

Userid Administration          1
Group Administration           2
Connect Administration         3
Password Administration        4
Dataset Administration         5
Resource Administration        6
Dataset Permit Administration   7
Resource Permit Administration  8
Resource Member Administration  9
User TSO Segment Administration A
User CICS Segment Administration B
Access Simulator               C

Technologic Software Concepts
(949) 509-5000 Fax (949) 509-5015
www.technologic.com

Select one of the above and hit Enter key to Continue.      PF03 or Clear=EXIT
```

It is important to note that the different functions can be invoked by executing their individual transactions as well as choosing them off the Main Menu. Below is a table showing the transactions and the programs they execute:

Transaction Table

Function	Transaction	Program
Main Menu	SAMN	AAZMN01
Userid Administration	SAUR	AAZUSR01
Group Administration	SAGP	AAZGRP01
Connect Administration	SACN	AAZCON01
Password Administration	SAPW	AAZPWA01
Dataset Administration	SADS	AAZDSA01
Resource Administration	SARS	AAZRSA01
Dataset Permit Administration	SASP	AAZDSP01
Resource Permit Administration	SARP	AAZRSP01
Resource Member Administration	SAMA	AAZMBA01
TSO Segment Administration	SAUT	AAZUTP01
CICS Segment Administration	SAUC	AAZUTC01
Access Simulator	SAAU	AAZAUT01
Sample Menu for remote processing	SAMD	AAZMNU01

Function	Transaction	Program
Sample Password Administration API call	SAPR	AAZPWS01

USERID Administration Screens

Perform List User

Perform the following steps to issue the equivalency of a RACF List User command (that is, LU DEMOTEST):

- 1 Enter ‘L’ as the request type.
- 2 Enter the userid in the USERID field and press ENTER.

Userid Administration ----- SSA ----- Userid Administration

Administration Input

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> L (A=Add,C=Change,L=List,D=Delete)

Userid ==> DEMOTEST Userid to be Processed

Default Group ==> _____ Default Group for New Userid

Name ==> _____ Userid Name

Owner ==> _____ Profile Owner

Password ==> _____ Password

Installation Data ==> _____

<==

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

List User Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Userid Administration ----- SSA ----- Userid Administration

List User Output

Userid ==> DEMOTEST Default Group ==> DEMOUSER

Name ==> DEMOTEST USERID

Owner ==> DEMOUSER

Password Changed ==> ****.**. **

Last Used Date ==> 1998-06-01 Last Used Time ==> 18:24:25

Resume Date ==> _____ Revoke Date ==> _____

Installation Data ==> THIS IS DATA

<==

Do You Want to Keep This Information
For the Add User Screen (Y/N): N

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Always press ENTER after a List User, or to recover from a message, to return to the Userid Administration Main panel.

Add Userid

Perform the following steps to issue the equivalency of a RACF Add User command (that is, ADDUSER DEMOTEST NA('DEMONSTRATION USER') DFL(DEMOUSER) OWNER(DEMOUSER):

- 1 Enter 'A' as the request type.
- 2 Enter the userid into the USERID field.
- 3 Enter a default group that you are authorized to use in the DEFAULT GROUP field. By not entering in the owner, the owner is set to the default group entered.
- 4 Enter the name in the NAME field (optional).

```

Userid Administration ----- SSA ----- Userid Administration
                        Administration Input

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> A                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> DEMOTEST                Userid to be Processed
Default Group     ==> DEMOUSER                Default Group for New Userid
Name              ==> DEMONSTRATION USER___  Userid Name
Owner             ==> _____             Profile Owner
Password          ==> _____             Password
Installation Data ==> _____

_____
_____
_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process adds the user to the specified default group. The name is included as part of the profile but is optional. The profile owner is also optional. If not specified the owner is set to the same value as the default group entered.

Change Password

Perform the following steps to issue the equivalency of a RACF Alter User Password Resume with a password specified (that is, ALTUSER DEMOTEST PASSWORD(<password>) RESUME:

- 1 Enter 'C' as the request type.
- 2 Enter the userid into the USERID field.
- 3 TAB to the PASSWORD field, enter the desired password (clear the rest of the field by depressing the EOF (Erase End-Of-Field key), and press ENTER. You can change the Password to the Default Group by depressing the EOF (Erase End-Of-Field) key which clears the Password field, and then press ENTER.

Userid Administration

SSA

Userid Administration

Administration Input

Enter the Request Type and Userid. Other fields are optional.

Request Type

==> C

(A=Add,C=Change,L=List,D=Delete)

Userid

==> DEMOTEST

Userid to be Processed

Default Group

==>

Default Group for New Userid

Name

==>

Userid Name

Owner

==>

Profile Owner

Password

==> NEWPASS_

Password

Installation Data

==>

<==

Hit Enter to ContinuePF03 or Clear=EXIT/PF01=HELP

This process sets the PASSDATE field to zeros requiring the user to enter a new password when they signon next and updates the LAST USED DATE/TIME fields with the current date and time.

Change the User’s Name or Owner

Perform the following steps to issue the equivalency of a RACF Alter User Owner Name (that is, ALTUSER DEMOTEST OWNER(DEMOUSER) NA(‘DEMONSTRATION USER’):

- 1 Enter ‘C as the request type.
- 2 Enter the userid into the USERID field.
- 3 Enter the owner in the OWNER field (optional).
- 4 Enter the name in the NAME field (optional).

Userid Administration

SSA

Userid Administration

Administration Input

Enter the Request Type and Userid. Other fields are optional.

Request Type

==> C

(A=Add,C=Change,L=List,D=Delete)

Userid

==> DEMOTEST

Userid to be Processed

Default Group

==>

Default Group for New Userid

Name

==> DEMONSTRATION USER__

Userid Name

Owner

==> DEMOUSER

Profile Owner

Password

==>

Password

Installation Data

==>

<==

Hit Enter to ContinuePF03 or Clear=EXIT/PF01=HELP

This process updates the profile owner or name field.

Add/Replace User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1** Enter 'A' for the request type if you are adding the user or 'C' if you are changing the userid.
- 2** Enter the userid into the USERID field.
- 3** TAB to the Installation Data field, type in data, and press ENTER.

```

Userid Administration ----- SSA ----- Userid Administration
                        Administration Input

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> C                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> DEMOTEST                Userid to be Processed
Default Group     ==> _____             Default Group for New Userid
Name              ==> _____             Userid Name
Owner             ==> _____             Profile Owner
Password          ==> _____             Password
Installation Data ==> NEW INSTALLATION DATA FOR A DEMONSTRATION USERID_____

_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process updates the Installation Data field.

Update Existing User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1** Enter 'L' as the request type to list the userid.
- 2** Enter the userid into the USERID field and press ENTER.
- 3** TAB to the Keep Installation Data field, type a 'Y', and press ENTER.
- 4** TAB to the Installation Data field, type in changes to data, and press ENTER.

```

Userid Administration ----- SSA ----- Userid Administration
                                List User Output

Userid          ==> DEMOTEST      Default Group    ==> DEMOUSER
Name            ==> DEMONSTRATION USER
Owner           ==> TSGPA0
Installation Data ==> NEW INSTALLATION DATA FOR A DEMONSTRATION USERID

                                <==

                                Do You Want to Keep This Information
                                For the Add User Screen (Y/N): Y

                                Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

When you specify ‘Y’ to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field.

Userid Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Userid Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List A = Add C = Change D = Delete	YES
CUSERID	8	Userid to be affected.	YES
CDFLTGP	8	Default group to be used if the request is an add.	NO, only when adding the userid.
CNAME	20	Data to be used in updating the name field on the userid specified.	NO
COWNER	8	User or group to be made the owner of the userid specified when the request is an add or change.	NO
CPSWD	8	Password to reset the userid specified with when the request is an add or change.	NO
CINSTL	255	Data to update installation data field on userid specified when the request is an add or change.	NO
CTSOFLG	1	Flag reserved for TSO segment	NO
CCICFLG	1	Flag reserved for CICS segment	NO
CDFPFLG	1	Flag reserved for DFP segment	NO
LUSERID	8	Output field indicating userid that was listed	NO
LDFLTGP	8	Output field showing the default group of the userid that was listed	NO
LNAME	20	Output field showing name of the userid that was listed.	NO
LOWNER	8	Output field showing the profile owner of the userid that was listed.	NO
LLCHGDT	10	Output field showing the password last changed date of the userid that was listed.	NO

Field Label	Length	Explanation	Required on Invocation?
LLACCDT	10	Output field showing the last used date of the userid that was listed.	NO
LLACCTM	8	Output field showing the last used time of the userid that was listed.	NO
LRESDT	10	Output field showing the resume date of the userid that was listed.	NO
LREVDT	10	Output field showing the revoke date of the userid that was listed.	NO
LINSTL	255	Output field containing the installation data of the userid listed.	NO
LTSOFLG	1	Reserved	NO
LCICFLG	1	Reserved	NO
LDFPFLG	1	Reserved	NO
LUSRSAV	1	Reserved	NO

Userid Administration API Example

The following Assembler layout sample can be found in member CPYUSR in the SSA install library:

```

**** API HEADER ****
CACTION   DS    CL1    ACTION REQUESTED
CUSERID   DS    CL8    USERID
CDFLTGP   DS    CL8    CURRENT DEFAULT GROUP
CNAME     DS    CL20   CURRENT NAME
COWNER    DS    CL8    OWNER
CPSWD     DS    CL8    NEW PASSWORD
CINSTL    DS    CL255  NEW INSTALLATION DATA
CTSOFLG   DS    CL1    TSO SEGMENT?
CCICFLG   DS    CL1    CICS SEGMENT?
CDFPFLG   DS    CL1    DFP SEGMENT?

LUSERID   DS    CL8    USERID

LDFLTGP   DS    CL8    CURRENT DEFAULT GROUP
LNAME     DS    CL20   CURRENT NAME
LOWNER    DS    CL8    OWNER
LLCHGDT   DS    CL10   PW CHANGE DATE
LLACCDT   DS    CL10   LAST USE DATE
LLACCTM   DS    CL8    LAST USE TIME
LRESDT    DS    CL10   RESUME DATE
LREVDT    DS    CL10   REVOKE DATE
LINSTL    DS    CL255  NEW INSTALLATION DATA
LTSOFLG   DS    CL1    TSO SEGMENT?
LCICFLG   DS    CL1    CICS SEGMENT?
LDFPFLG   DS    CL1    DFP SEGMENT?
LUSRSAV   DS    CL1    SAVE INFO FROM LIST SCREEN?

ORG      COMMAREA+32760

```


Always press ENTER after a List Group, or to recover from a message, to return to the Group Administration Main panel.

Add Group

Perform the following steps to issue the equivalency of a RACF Add Group command (that is, ADDGROUP DEMOTST1 SUPGRP(DEMOUSER) OWNER(DEMOUSER):

- 1 Enter ‘A’ as the request type.
- 2 Enter the group into the GROUP field.
- 3 Enter a superior group that you are authorized to use in the SUPERIOR GROUP field. By not entering in the owner, the owner is set to the superior group entered.
- 4 Determine if TERMUACC is to be on or off (optional) and hit Enter.

Group Administration ----- SSA ----- Group Administration
Administration Input

Enter the Group and Request Type. Other fields are optional.

Request Type	==> A	(A=Add,C=Change,L=List,D=Delete)
Group	==> DEMOTST1	Group to be Processed
Superior Group	==> DEMOUSER	Superior Group for Add
Owner	==> _____	Profile Owner
Termuacc (Y/N)	==> _	Termuacc Setting
Installation Data	==> _____	

<==

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process adds the group to the superior group. The profile owner is also optional. If not specified the owner is set to the same value as the default group entered. The TERMUACC if not entered, defaults to ‘Y’.

Change the Group’s Owner or TERMUACC

Perform the following steps to issue the equivalency of a RACF Alter Group Owner TERMUACC (that is, ALTGROUP DEMOTST1 OWNER(DEMOUSER) TERMUACC):

- 1 Enter ‘C’ as the request type.
- 2 Enter the group into the GROUP field.
- 3 Enter the owner in the OWNER field (optional).
- 4 Enter Y or ‘N’ in the TERMUACC field (optional).

```

Group Administration ----- SSA ----- Group Administration
                        Administration Input

      Enter the Group and Request Type.  Other fields are optional.

Request Type      ==> C                      (A=Add,C=Change,L=List,D=Delete)
Group            ==> DEMOTST1                Group to be Processed
Superior Group   ==> _____              Superior Group for Add
Owner           ==> DEMOUSER                 Profile Owner
Termuacc (Y/N)   ==> _                      Termuacc Setting
Installation Data ==> _____

_____
_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process updates the profile owner or TERMUACC field.

Add/Replace Group Installation Data

Perform the following steps to add or replace installation data for the specified group:

- 1** Enter 'A' for the request type if you are adding the group or 'C' if you are changing the group.
- 2** Enter the group into the GROUP field.
- 3** TAB to the Installation Data field, type in data, and press ENTER.

```

Group Administration ----- SSA ----- Group Administration
                        Administration Input

      Enter the Group and Request Type.  Other fields are optional.

Request Type      ==> C                      (A=Add,C=Change,L=List,D=Delete)
Group            ==> DEMOTST1                Group to be Processed
Superior Group   ==> _____              Superior Group for Add
Owner           ==> _____                 Profile Owner
Termuacc (Y/N)   ==> _                      Termuacc Setting
Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION GROUP_____

_____
_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process updates the Installation Data field.

Update Existing Group Installation Data

Perform the following steps to add or replace installation data for the specified group:

- 1** Enter 'L' as the request type to list the group.
- 2** Enter the group into the GROUP field and press ENTER.
- 3** TAB to the Keep Installation Data field, type a 'Y', and press ENTER.
- 4** TAB to the Installation Data field, type in changes to data, and press ENTER.

```

Group Administration ----- SSA ----- Group Administration
                          List Group Output

Group          ==> DEMOTST1    Superior Group    ==> DEMOUSER
Owner          ==> DEMOUSER    TERMUACC         ==> Y
Installation Data ==> NEW INSTALLATION DATA FOR THE DEMONSTRATION GROUP

                                <==

Do You Want to Keep This Information
For the Add Group Screen (Y/N): Y

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP

```

When you specify 'Y' to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field.

Group Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (See API details at the beginning of this chapter). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Group Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List A = Add C = Change D = Delete	YES
CGROUP	8	Group to be affected	YES
CSUPGRP	8	Superior group to be used on an add request.	NO, only when adding a group.
COWNER	8	User or group to be made the owner of the group specified when the request is an add or change.	NO
CTRMUAC	1	Indicator specifying if TERMUACC is to be ON or OFF when the request is an add or change.	NO
CINSTL	255	Data to update installation data field on group specified when the request is an add or change.	NO
CMVSFLG	1	Flag reserved for OMVS segment	NO
CDFPFLG	1	Flag reserved for DFP segment	NO
LGROUP	8	Output field indicating group that was listed	NO
LSUPGRP	8	Output field showing the superior group of the group that was listed	NO
LOWNER	8	Output field showing the profile owner of the group that was listed.	NO
LTRMUAC	1	Output field showing if TERMUACC is ON or OFF.	NO
LINSTL	255	Output field containing the installation data of the group listed.	NO
LMVSFLG	1	Reserved output field for the OMVS segment	NO
LDFPFLG	1	Reserved output field for the DFP segment	NO

Field Label	Length	Explanation	Required on Invocation?
LGRPSAV	1	RESERVED	NO

Group Administration API Example

The following Assembler layout sample can be found in member CPYGRP of the SSA install library:

```

**** API HEADER ****
CACTION      DS      CL1      ACTION REQUESTED
CGROUP       DS      CL8      GROUP
CSUPGRP      DS      CL8      CURRENT SUPERIOR GROUP
COWNER       DS      CL8      OWNER
CTRMUAC      DS      CL1      TERMUACC
CINSTL       DS      CL255    NEW INSTALLATION DATA
CMVSFLG      DS      CL1      RESERVED FOR FUTURE USE
CDFPFLG      DS      CL1      RESERVED FOR FUTURE USE

LGROUP       DS      CL8      GROUP

LSUPGRP      DS      CL8      CURRENT SUPERIOR GROUP
LOWNER       DS      CL8      OWNER
LTRMUAC      DS      CL1      TERMUACC
LINSTL       DS      CL255    INSTALLATION DATA
LMVSFLG      DS      CL1      RESERVED FOR FUTURE USE
LDFPFLG      DS      CL1      RESERVED FOR FUTURE USE
LGRPSAV      DS      CL1      RESERVED

ORG          COMMAREA+32760

```


Connect Administration Screens

List All Connects

Perform the following steps to issue the equivalency of a RACF List User command that shows only connect groups for which the user is authorized to (that is, LU DEMOTEST):

- Enter the <userid> in the USERID field, enter an 'L' in the Request Type field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                                Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid           ==> DEMOTEST      Userid to be processed
Request Type     ==> L             (L=List,S=Specific,C=Connect,R=Remove)
Connect Group    ==> _____   Connect group
Connect Owner    ==> _____   Connect owner
Resume          ==> _             Specify Y to resume the connect
Revoke          ==> _             Specify Y to revoke the connect
Resume Date     ==> _____   Resume date for the connect (YYYY-MM-DD)
Revoke Date     ==> _____   Revoke date for the connect (YYYY-MM-DD)
Group UACC       ==> _____   (None,Read,Update,Control,Alter)
Group Auth      ==> _____   (None,Use,Create,Connect,Join)

                                Group Connect Attributes:
ADSP            ==> _             Auditor      ==> _             GRPACC       ==> _
Special         ==> _             Operations  ==> _             TERMUACC     ==> _

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP
  
```

List All Connects Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Connect Administration ----- SSA ----- Connect Administration
                                List a User's Connect Groups

Connects for ==> DEMOTEST

S = List Specific Connect, C = Connect, R = Remove Connect

SELECT   Group      (Select an option for ONE group or PF7/PF8)
-----
_        DEMOTST1
_        DEMOUSER
_        TSTADDG
_        TSTGBATX
_        TSTGCON
_        TSTGCONX
_        TSTGEXTL
_        TSTGGLBL
_        TSTGJOE
_        TSTGOUT
_        TSTGPAOX
_        TSTGS01
_        TSTGS02
_        TSTGS03
  
```

You can ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- List Specific Connect (S)
Displays a screen with specific information about the connect. See List Specific Connect for screen example.
- Connect (C)
Displays the Connect Administration Main Panel with appropriate fields filled in.
- Remove Connect (R)
Displays a confirmation panel to confirm the remove request. If the request is confirmed with a ‘Y’ then the user will be removed from the group.

Notes

- 1 This display only lists those groups that the user is authorized to through SSA.\$CONNECT.<group> authority profiles.
- 2 The CICS version of Connect Administration only allows the user to select one connection from the list. The TSO version allows as many selections as the user requests.

List Specific Connect Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Connect Administration ----- SSA ----- Connect Administration

List Specific User Connect Output

Userid ==> DEMOTEST

Connect Group ==> DEMOUSER

Group Owner ==> DEMOUSER

Connect Date ==> 1998-01-20

Group UACC ==> NONE

Group Authority ==> USE

Last Connect Date ==> 1998-02-24

Connect Count ==> 00000

Last Connect Time ==> 15:36:52

Group Connect Attributes:

Revoked? ==> N

ADSP? ==> N

Auditor? ==> N

GRPACC ==> N

Special? ==> N

Operations? ==> N

TERMUACC? ==> N

Resume Date ==>

Revoke Date ==>

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

Connect a User to a Group

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) command.

- 1 Enter the <userid> into the USERID field.

- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> MEGA_____ Connect group
Connect Owner ==> _____ Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==> _____ (None,Read,Update,Control,Alter)
Group Auth   ==> _____ (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP      ==> _   Auditor ==> _   GRPACC ==> _
Special   ==> _   Operations ==> _   TERMUACC ==> _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process will connect the user to the specified group.

For a new connect the following defaults will be used if not explicitly specified:

- UACC(NONE)
- NOTERMUACC
- OWNER(<group>)

For existing connects, unless explicitly specified, no fields will be changed.

Note You can request any combination of Connect Administration functions. If the user does not have the correct access level to the SSA.\$CONNECT profile to do any one of the functions the entire request is failed (no partial updates are processed).

Remove User from Group

Perform the following steps to issue the equivalency of a RACF REMOVE <userid> GROUP(<group>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'R' in the Request Type field.
- 3 Enter a <group> in the Connect Group field, and press ENTER.
- 4 Type a 'Y' in the Confirmation Pop-up Panel when prompted and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type.  Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> R            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> MEGA_____ Connect group
Connect Owner ==> _____ Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==> _____ Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> _____ Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==> _____ (None,Read,Update,Control,Alter)
Group Auth   ==> _____ (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP         ==> _           Auditor ==> _           GRPACC ==> _
Special      ==> _           Operations ==> _         TERMUACC ==> _

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP

```

```

Connect Administration ----- SSA ----- Connect Administration
                        Remove a Group Connect

Confirm Remove Request (Y/N): Y

Userid ==> DEMOTEST
Group  ==> MEGA

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP

```

Resume a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT *<userid>* GROUP(*<group>*) RESUME command:

- 1** Enter the *<userid>* into the USERID field.
- 2** Enter 'C' in the Request Type field.
- 3** Enter a *<group>* in the Connect Group field.
- 4** Type a 'Y' in the Resume field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==>           Connect owner
Resume       ==> Y           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==>           Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==>           Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==>           (None,Read,Update,Control,Alter)
Group Auth   ==>           (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP         ==> _      Auditor ==> _      GRPACC ==> _
Special      ==> _      Operations ==> _    TERMUACC ==> _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Revoke a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) REVOKE command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Type a 'Y' in the Revoke field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==>           Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> Y           Specify Y to revoke the connect
Resume Date  ==>           Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==>           Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==>           (None,Read,Update,Control,Alter)
Group Auth   ==>           (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP         ==> _      Auditor ==> _      GRPACC ==> _
Special      ==> _      Operations ==> _    TERMUACC ==> _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Set a Resume Date on a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) RESUME(<date>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a Gregorian <date> in the format of YYYY-MM-DD, that is greater than the current date, in the RESUME DATE field, and press ENTER.

Connect Administration ----- SSA ----- Connect Administration

Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid	==> DEMOTEST	Userid to be processed
Request Type	==> C	(L=List,S=Specific,C=Connect,R=Remove)
Connect Group	==> DEMOUSER	Connect group
Connect Owner	==> _____	Connect owner
Resume	==> _	Specify Y to resume the connect
Revoke	==> _	Specify Y to revoke the connect
Resume Date	==> 1998-05-06	Resume date for the connect (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the connect (YYYY-MM-DD)
Group UACC	==> _____	(None,Read,Update,Control,Alter)
Group Auth	==> _____	(None,Use,Create,Connect,Join)

Group Connect Attributes:

ADSP	==> _	Auditor	==> _	GRPACC	==> _
Special	==> _	Operations	==> _	TERMUACC	==> _

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Set a Revoke Date on a Connect

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) REVOKE(<date>) command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a Gregorian <date> in the format of YYYY-MM-DD, that is greater than the current date, in the REVOKE DATE field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==>           Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==>           Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==> 1998-05-07 Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==>           (None,Read,Update,Control,Alter)
Group Auth   ==>           (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP         ==> _ Auditor ==> _ GRPACC ==> _
Special      ==> _ Operations ==> _ TERMUACC ==> _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Change Connect Authority

Perform the following steps to issue the equivalency of a RACF CONNECT *<userid>* GROUP(*<group>*) AUTH(*<auth>*) command:

- 1 Enter the *<userid>* into the USERID field.
- 2 Enter 'C' in the Request Type field.
- 3 Enter a *<group>* in the Connect Group field.
- 4 Enter an *<auth>* value in the Group Auth field, and press ENTER.

```

Connect Administration ----- SSA ----- Connect Administration
                        Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid      ==> DEMOTEST      Userid to be processed
Request Type ==> C            (L=List,S=Specific,C=Connect,R=Remove)
Connect Group ==> DEMOUSER    Connect group
Connect Owner ==>           Connect owner
Resume       ==> _           Specify Y to resume the connect
Revoke       ==> _           Specify Y to revoke the connect
Resume Date  ==>           Resume date for the connect (YYYY-MM-DD)
Revoke Date  ==>           Revoke date for the connect (YYYY-MM-DD)
Group UACC   ==>           (None,Read,Update,Control,Alter)
Group Auth   ==> CONNECT     (None,Use,Create,Connect,Join)

Group Connect Attributes:
ADSP         ==> _ Auditor ==> _ GRPACC ==> _
Special      ==> _ Operations ==> _ TERMUACC ==> _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Set/Remove Connect Attributes

Perform the following steps to issue the equivalency of a RACF CONNECT <userid> GROUP(<group>) <attribute> command:

- 1 Enter the <userid> into the USERID field.
- 2 Enter 'C in the Request Type field.
- 3 Enter a <group> in the Connect Group field.
- 4 Enter a 'Y' or 'N' in the appropriate <attribute> field, and press ENTER.

Note The example below will remove the SPECIAL attribute, if any, and set the AUDITOR attribute.

Connect Administration ----- SSA ----- Connect Administration
Administration Input

Enter Connect Userid and Request Type. Other fields are optional.

Userid	==> DEMOTEST	Userid to be processed
Request Type	==> C	(L=List,S=Specific,C=Connect,R=Remove)
Connect Group	==> DEMOUSER	Connect group
Connect Owner	==> _____	Connect owner
Resume	==> _	Specify Y to resume the connect
Revoke	==> _	Specify Y to revoke the connect
Resume Date	==> _____	Resume date for the connect (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the connect (YYYY-MM-DD)
Group UACC	==> _____	(None,Read,Update,Control,Alter)
Group Auth	==> _____	(None,Use,Create,Connect,Join)

Group Connect Attributes:

ADSP	==> _	Auditor	==> _	GRPACC	==> _
Special	==> _	Operations	==> Y	TERMUACC	==> _

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Connect Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Connect Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List of connects S = Specific connect list C = Connect R = Remove	YES
LISTADDR	4	Reserved Field	NO
CUSERID	8	Userid whose connect you are affecting	YES
CGROUP	8	Group whose connection will be affected.	NO, however, if you doing a specific list, connect or remove you must enter this field. It is not required for the list of groups function.
COWNER	8	Userid or group to be made the owner of the connect specified when the request is an add or change.	NO
CUACC	7	UACC level to put on the connect in question. The only acceptable values are: NONE READ UPDATE CONTROL ALTER	NO. The default value is NONE.
CADSP	1	Indicator of request to add the ADSP attribute to the connect when the request is an add or change. Must be ‘Y’ or ‘N’.	NO

Field Label	Length	Explanation	Required on Invocation?
CSPEC	1	Indicator of request to add the SPECIAL attribute to the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
COPER	1	Indicator of request to add the OPERATIONS attribute to the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
CREVOKE	1	Indicator of request to add the REVOKE attribute to the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
CRESUME	1	Indicator of request to resume the connection. This is only valid for the change request. Must be 'Y' or 'N'.	NO
CGRPACC	1	Indicator of request to add the GRPACC attribute to the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
CTRMUAC	1	Indicator of request to have TERMUACC or NOTERMUACC on the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
CAUDIT	1	Indicator of request to add the AUDIT attribute to the connect when the request is an add or change. Must be 'Y' or 'N'.	NO
CREVDT	10	Revoke date. Format must be YYYY-MM-DD.	NO
CRESDT	10	Resume date. Format must be YYYY-MM-DD.	NO
CAUTH	7	Authority level to put on the connect in question. The only acceptable values are: NONE USE CREATE CONNECT JOIN	NO. The default value is USE.
LUSERID	8	Output field containing the userid whose connect was listed.	NO
LGROUP	8	Output field showing the group whose connect was listed	NO

Field Label	Length	Explanation	Required on Invocation?
LDATE	10	Output field showing the connection date. Format is YYYY-MM-DD.	NO
LOWNER	8	Output field showing the profile owner of the connect that was listed.	NO
LLJTIME	8	Output field showing the last connect time of the connect that was listed.	NO
LLJDATE	10	Output field showing the last connect date of the connect that was listed. Format is YYYY-MM-DD.	NO
LUACC	7	Output field showing the UACC level on the connect that was listed.	NO
LINITCT	5	Output field showing the init count on the connect that was listed.	NO
LADSP	1	Output field indicating if the ADSP attribute was on for the connect that was listed.	NO
LSPEC	1	Output field indicating if the SPECIAL attribute was on for the connect that was listed.	NO
LOPER	1	Output field indicating if the OPERATIONS attribute was on for the connect that was listed.	NO
LREVOKE	1	Output field indicating if the REVOKE attribute was on for the connect that was listed.	NO
LRESUME	1	Reserved	NO
LGRPACC	1	Output field indicating if the GRPACC attribute was on for the connect that was listed.	NO
LTRMUAC	1	Output field indicating if the TERMUACC attribute was on for the connect that was listed.	NO
LAUDIT	1	Output field indicating if the AUDITOR attribute was on for the connect that was listed.	NO
LREVDT	10	Output field showing the revoke date on the connect that was listed. Format is YYYY-MM-DD.	NO
LRESDT	10	Output field showing the resume date on the connect that was listed. Format is YYYY-MM-DD.	NO

Field Label	Length	Explanation	Required on Invocation?
LAUTH	7	Output field showing the Authority level on the connect that was listed.	NO
LARRAY	Remainder of 32760	If the request was to list the connects a userid has, the list of groups is returned in this area. The groups are returned in 8 character fields with the last entry followed by a single HEX 00.	NO

Connect Administration API Example

The following Assembler layout sample can be found in member CPYCON in the SSA install library:

```

**** API HEADER ****
CACTION      DS      CL1      ACTION REQUESTED
LISTADDR     DS      XL4      LIST-OF-GROUPS GETMAIN'D AREA
CUSERID      DS      CL8      USERID
CGROUP       DS      CL8      GROUP
COWNER       DS      CL8      OWNER
CUACC        DS      CL7      UACC
CADSP        DS      CL1      ADSP?
CSPEC        DS      CL1      SPECIAL?
COPER        DS      CL1      OPER?
CREVOKE      DS      CL1      REVOKE?
CRESUME      DS      CL1      RESUME?
CGRPACC      DS      CL1      GRPACC?
CTRMUAC      DS      CL1      TRMUAC?
CAUDIT       DS      CL1      AUDITOR?
CREVDI       DS      CL10     REVOKE DATE?
CRESDI       DS      CL10     RESUME DATE?
CAUTH        DS      CL7      AUTH DATE?
*
* STORAGE AREAS FOR LIST GROUP OUTPUT
*
LISTINFO     DS      0CL99
LUSERID      DS      CL8      USERID
LGROUP       DS      CL8      GROUP
LDATE        DS      CL10     CONNECT DATE
LOWNER       DS      CL8      CONNECT OWNER
LLJTIME      DS      CL8      LAST CONNECT TIME
LLJDATE      DS      CL10     LAST CONNECT DATE
LUACC        DS      CL7      UACC
LINITCT      DS      CL5      INIT COUNT
LADSP        DS      CL1      ADSP?
LSPEC        DS      CL1      SPECIAL?
LOPER        DS      CL1      OPER?
LREVOKE      DS      CL1      REVOKE?
LRESUME      DS      CL1      RESERVED
LGRPACC      DS      CL1      GRPACC?
LTRMUAC      DS      CL1      TRMUAC?
LAUDIT       DS      CL1      AUDITOR?
LREVDI       DS      CL10     REVOKE DATE?
LRESDI       DS      CL10     RESUME DATE?

```

```
LAUTH      DS      CL7      AUTH
*
LARRAY     EQU      *      RETURNED LIST OF 8-BYTE GRPS
* THESE WILL BE UNSORTED, FOLLOWED BY A SINGLE X'00' CHAR
*
          ORG      COMMAREA+32760
```

Password Administration Screens

Perform List User

Perform the following steps to issue the equivalency of a RACF List User command (that is, LU DEMOTEST):

Password Administration ----- SSA ----- Password Administration

Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid ==> DEMOTEST

Password ==> ????????

Resume ==> _

Revoke ==> _

Resume Date ==> _____

Revoke Date ==> _____

SuperRevoke ==> _

Installation Data ==> _____

Userid to be reset

New password - Blank for default group

Specify Y to resume the userid

Specify Y to revoke the userid

Resume date for the userid (YYYY-MM-DD)

Revoke date for the userid (YYYY-MM-DD)

Specify Y to super-revoke the userid

<==

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

List User Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Password Administration ----- SSA ----- Password Administration

List User Output

Userid ==> DEMOTEST

User Name ==> DEMO TEST ID

Default Group ==> DEMOUSER

Password Changed ==> ****.*.*.*

Last Used Date ==> 1998-03-24

Last Used Time ==> 06:49:50

Revoked? ==> N

Special? ==> N

SuperRevoked? ==> N

Operations? ==> N

Resume Date ==>

Revoke Date ==>

Installation Data ==> NEW DATA

<==

Do You Want to Keep Installation Data

For the Reset Screen (Y/N): N

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

Always press ENTER after a List User, or to recover from a message, to return to the Password Administration Main panel.

Set Password to Default Group and Resume User

Perform the following steps to issue the equivalency of a RACF Alter User Resume Password with no password. By not specifying a password, the password is reset to the default group of the userid being reset (that is, ALTUSER DEMOTEST RESUME PASSWORD):

- 1 Enter the userid into the USERID field.
- 2 TAB to the PASSWORD field, depress the EOF (Erase End-Of-Field) key.
- 3 TAB to the RESUME field, type a 'Y', and press ENTER.

Password Administration ----- SSA ----- Password Administration	
Administration Input	
Enter the Userid to be Reset. All other fields are optional.	
Userid	==> DEMOTEST Userid to be reset
Password	==> New password - Blank for default group
Resume	==> y Specify Y to resume the userid
Revoke	==> - Specify Y to revoke the userid
Resume Date	==> _____ Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____ Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> - Specify Y to super-revoke the userid
Installation Data	==> _____
_____ <==	
Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP	

This process clears the REVOKE flag, the UNSUCCESSFUL LOGON ATTEMPT COUNTER field, the REVOKE and RESUME dates if any, updates the LASTUSED DATE/TIME fields with the current date and time, updates the PASSDATE field with the current Julian date, and changes the PASSWORD field to the password that is the name of the DEFAULT GROUP.

Note Password Administration handles this request as two separate functions (a Resume and a Password Change) and will produce two RACF Type 80 SMF records.

You can request any combination of Password Administration functions. If the user does not have the correct access level to the SSA.\$RESET profile to do any one of the functions the entire request is failed (no partial updates are processed).

Change Password

Perform the following steps to issue the equivalency of a RACF Alter User Password with a password specified (that is, ALTUSER DEMOTEST PASSWORD(<password>)):

- 1 Enter the userid into the USERID field.
- 2 TAB to the PASSWORD field, enter the desired password (clear the rest of the field by depressing the EOF (Erase End-Of-Field) key), and press ENTER. You can change the Password to the Default Group by depressing the EOF (Erase End-Of-Field) key which clears the Password field, and then press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid          ==> DEMOTEST      Userid to be reset
Password        ==> NEWPASS      New password - Blank for default group
Resume          ==> _            Specify Y to resume the userid
Revoke          ==> _            Specify Y to revoke the userid
Resume Date     ==> _            Resume date for the userid (YYYY-MM-DD)
Revoke Date     ==> _            Revoke date for the userid (YYYY-MM-DD)
SuperRevoke     ==> _            Specify Y to super-revoke the userid
Installation Data ==> _

=====
=====
===== <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process updates the PASSDATE field with the current Julian date, changes the PASSWORD field with the specified password, and updates the LAST USED DATE/TIME fields with the current date and time.

Resume a Userid

Perform the following steps to issue the equivalency of a RACF Alter User Resume (that is, ALTUSER DEMOTEST RESUME):

- 1 Enter the userid into the USERID field.
- 2 TAB to the RESUME field and enter a Y, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid          ==> DEMOTEST      Userid to be reset
Password        ==> ???????      New password - Blank for default group
Resume          ==> Y            Specify Y to resume the userid
Revoke          ==> _            Specify Y to revoke the userid
Resume Date     ==> _            Resume date for the userid (YYYY-MM-DD)
Revoke Date     ==> _            Revoke date for the userid (YYYY-MM-DD)
SuperRevoke     ==> _            Specify Y to super-revoke the userid
Installation Data ==> _

=====
=====
===== <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process clears the REVOKE flag, the UNSUCCESSFUL LOGON ATTEMPT COUNTER field, the REVOKE and RESUME dates if any, and updates the LASTUSED DATE/TIME fields with the current date and time.

This process does not change the password of the userid.

Revoke a Userid

Perform the following steps to issue the equivalency of a RACF Alter User Revoke (that is, ALTUSER DEMOTEST REVOKE):

- 1 Enter the userid into the USERID field.
- 2 TAB to the REVOKE field and enter a Y, and press ENTER.

Password Administration ----- SSA ----- Password Administration	
Administration Input	
Enter the Userid to be Reset. All other fields are optional.	
Userid	==> DEMOTEST Userid to be reset
Password	==> ??????? New password - Blank for default group
Resume	==> _ Specify Y to resume the userid
Revoke	==> Y Specify Y to revoke the userid
Resume Date	==> _____ Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____ Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> _ Specify Y to super-revoke the userid
Installation Data	==> _____
_____ <==	
Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP	

- 3 This process sets the REVOKE flag, and clears the REVOKE and RESUME dates if any. This process does not change the password of the userid

Set a Resume Date

Perform the following steps to issue the equivalency of a RACF Alter User Resume with a date (that is, ALTUSER USERBOB RESUME(<date>):

- 1 Enter the userid into the USERID field.
- 2 TAB to the RESUME DATE field and enter a Gregorian date in the format of YYYY-MM-DD, that is greater than the current date, and press ENTER.

Password Administration
SSA
Password Administration

Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid	==> DEMOTEST	Userid to be reset
Password	==> ????????	New password - Blank for default group
Resume	==> _	Specify Y to resume the userid
Revoke	==> _	Specify Y to revoke the userid
Resume Date	==> 1998-05-07	Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> _	Specify Y to super-revoke the userid
Installation Data	==> _____	

<==

Hit Enter to ContinuePF03 or Clear=EXIT/PF01=HELP

This process updates the RESUME DATE field. This process does not change the password of the userid.

If you specify both RESUME DATE and REVOKE DATE that are the same, the RESUME DATE is ignored and the REVOKE DATE is updated with the date entered.

If there is a REVOKE DATE already set on the userid, and the RESUME DATE entered is the same, the RESUME DATE is ignored and the REVOKE DATE remains the same.

Set a Revoke Date

Perform the following steps to issue the equivalency of a RACF Alter User Revoke with a date (that is, ALTUSER DEMOTEST REVOKE(<date>):

- 1
2
- Enter the userid into the USERID field.
TAB to the REVOKE DATE field and enter a Gregorian date in the format of YYYY-MM-DD, that is greater than the current date, and press ENTER.

Password Administration ----- SSA ----- Password Administration	
Administration Input	
Enter the Userid to be Reset. All other fields are optional.	
Userid	==> DEMOTEST Userid to be reset
Password	==> ??????? New password - Blank for default group
Resume	==> - Specify Y to resume the userid
Revoke	==> - Specify Y to revoke the userid
Resume Date	==> _____ Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> 1998-06-21 Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> - Specify Y to super-revoke the userid
Installation Data	==> _____
_____ <==	
Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP	

This process updates the REVOKE DATE field. This process does not change the password of the userid.

If you specify both RESUME DATE and REVOKE DATE that are the same, the RESUME DATE is ignored and the REVOKE DATE is updated with the date entered.

If there is a RESUME DATE already set on the userid, and the REVOKE DATE entered is the same, the RESUME DATE is cleared and the REVOKE DATE is updated with the date entered.

Set SuperRevoke

Perform the following steps to issue a Password Administration SuperRevoke. This will prevent users from using Password Administration functions unless they have ALTER access to the appropriate SSA.\$RESET.<group> profile or the userid is removed from the SuperRevoke group \$SREVOKE:

- 1 Enter the userid into the USERID field.
- 2 TAB to the SuperRevoke field, type a 'Y', and press ENTER.

Password Administration
SSA
Password Administration

Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid	==> DEMOTEST	Userid to be reset
Password	==> ????????	New password - Blank for default group
Resume	==> _	Specify Y to resume the userid
Revoke	==> _	Specify Y to revoke the userid
Resume Date	==> _____	Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> Y	Specify Y to super-revoke the userid
Installation Data	==> _____	

<==

Hit Enter to ContinuePF03 or Clear=EXIT/PF01=HELP

This process sets the REVOKE flag, and connects the user to the SuperRevoke group \$SREVOKE. This process does not change the password of the userid.

Add/Replace User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter the userid into the USERID field.
- 2 TAB to the Installation Data field, type in data, and press ENTER.

Password Administration
SSA
Password Administration

Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid	==> DEMOTEST	Userid to be reset
Password	==> ????????	New password - Blank for default group
Resume	==> _	Specify Y to resume the userid
Revoke	==> _	Specify Y to revoke the userid
Resume Date	==> _____	Resume date for the userid (YYYY-MM-DD)
Revoke Date	==> _____	Revoke date for the userid (YYYY-MM-DD)
SuperRevoke	==> _	Specify Y to super-revoke the userid
Installation Data	==> NEW INSTALLATION DATA FOR THE DEMONSTRATION USERID_____	

<==

Hit Enter to ContinuePF03 or Clear=EXIT/PF01=HELP

This process updates the Installation Data field. This process does not change the password of the userid

Update Existing User Installation Data

Perform the following steps to add or replace installation data for the specified user:

- 1 Enter the userid into the USERID field and press ENTER.
- 2 TAB to the Keep Installation Data field, type a 'Y', and press ENTER.
- 3 TAB to the Installation Data field, type in changes to data, and press ENTER.

```

Password Administration ----- SSA ----- Password Administration
                          List User Output

Userid          ==> DEMOTEST      Default Group  ==> DEMOUSER
User Name       ==> DEMO TEST ID

Password Changed ==> ****.**.**
Last Used Date  ==> 1998-03-24   Last Used Time ==> 06:49:50

Revoked?        ==> N           SuperRevoked? ==> N
Special?        ==> N           Operations?  ==> N

Resume Date     ==>             Revoke Date     ==>

Installation Data ==> NEW DATA

                                <==

                        Do You Want to Keep Installation Data
                        For the Reset Screen (Y/N): Y

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

When you specify 'Y' to Keep Installation Data, the installation data will be passed back to the Input Screen.

This process updates the Installation Data field. This process does not change the password of the userid.

Password Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Password Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CUSERID	8	Userid to be affected.	YES
CPSWD	8	Value to reset password on userid specified.	NO
CRESUME	1	Decision to issue RESUME on userid specified. Must be ‘Y’ or ‘N’. Can not be ‘Y’ if CREVOKE is ‘Y’.	NO
CREVOKE	1	Decision to issue REVOKE on userid specified. Must be ‘Y’ or ‘N’. Can not be ‘Y’ if CRESUME is ‘Y’.	NO
CRESDT	10	Resume date. Format must be YYYY-MM-DD and must be a date that is in the future.	NO
CREVDT	10	Revoke date. Format must be YYYY-MM-DD and must be a date that is in the future.	NO
CSUPRV	1	Request to SuperRevoke the userid specified.	NO
CINSTL	255	Data to update installation data field on userid specified.	NO
LUSERID	8	Output field indicating userid that was listed	NO
LNAME	20	Output field showing name of userid that was listed	NO
LDFLTGP	8	Output field showing the default group of the userid that was listed	NO
LLCHGDT	10	Output field showing the date the password was updated on the userid that was listed. Format is YYYY-MM-DD.	NO
LLACCDT	10	Output field showing the last accessed date on the userid that was listed. Format is YYYY-MM-DD.	NO
LLACCTM	8	Output field showing the last accessed time on the userid that was listed. Format is HH:MM.SS	NO

Field Label	Length	Explanation	Required on Invocation?
LREVOKE	1	Output field indicating whether or not the listed userid is revoked	NO
LSPEC	1	Output field indicating whether or not the listed userid has global special	NO
LOPER	1	Output field indicating whether or not the listed userid has global operation.	NO
LRESDT	10	Output field showing the resume date if any that is set on the userid listed	NO
LREVDT	10	Output field showing the revoke date if any that is set on the userid listed.	NO
LSUPRV	1	Output field indicating whether or not the userid listed is SuperRevoked	NO
LINSTL	255	Output field containing the installation data of the userid listed.	NO
LQINST	1	Reserved	NO

Password Administration API Example

The following Assembler layout sample can be found in member CPYPWA of the SSA install library:

```

**** API HEADER ****
CUSERID      DS      CL8      USERID
CPSWD        DS      CL8      NEW PASSWORD
CRESUME       DS      CL1      RESUME?
CREVOKE       DS      CL1      REVOKE?
CRESDT        DS      CL10     RESUME DATE?
CREVDT        DS      CL10     REVOKE DATE?
CSUPRV        DS      CL1      SUPER-REVOKE?
CINSTL        DS      CL255    NEW INSTALLATION DATA
*
* LIST USER OUTPUT FIELDS
*
LUSERID      DS      CL8      CURRENT USERID
LNAME        DS      CL20     CURRENT NAME
LDFLTGP      DS      CL8      CURRENT DEFAULT GROUP
LLCHGDT      DS      CL10     CURRENT PASSWORD DATE CHANGE
LLACCDT      DS      CL10     CURRENT LAST ACCESS DATE
LLACCTM      DS      CL8      CURRENT LAST ACCESS TIME
LREVOKE       DS      CL1      REVOKED = Y OR N
LSPEC        DS      CL1      SPECIAL= Y OR N
LOPER        DS      CL1      OPERATIONS = Y OR N
LRESDT        DS      CL10     CURRENT RESUME DATE
LREVDT        DS      CL10     CURRENT REVOKE DATE
LSUPRV        DS      CL1      SUPER-REVOKE
LINSTL        DS      CL255    CURRENT INSTALLATION DATA
LQINST        DS      CL1      RESERVED
ORG          COMMAREA+32760

```

Dataset Administration Screens

Perform List Dataset Profile

Perform the following steps to issue the equivalency of a RACF List Dataset command (that is, LD DA() GEN):

- 1
- Enter ‘L’ in the Request Type field.
- 2
- Enter the dataset profile in the Dataset Profile field and press ENTER.

Dataset Administration ----- SSA ----- Dataset Administration

Administration Input

Enter the Dataset and Request Type. Other fields are optional.

Request Type

==> L

(A=Add,C=Change,L=List,D=Delete)

Dataset Profile

==> USER01.*

Owner

==> _____

Profile Owner

UACC

==> _____

(None,Execute,Read,Update,Control,Alter)

Notify

==> _____

Userid to Notify

Warn (Y/N)

==> _

Activate Warn?

Level

==> _____

Resource Level

Local Audit

==> _____

(All,Success,Fail,None)

Success Level

==> _____

(None,Read,Update,Control,Alter)

Failure Level

==> _____

(None,Read,Update,Control,Alter)

Installation Data

==> _____

<==

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

List Dataset Profile Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Dataset Administration ----- SSA ----- Dataset Administration

List Dataset Output

Dataset Profile

==> USER01.*

Owner

==> GRP001

UACC

==> NONE

Notify

==> _____

Warn

==> N

Level

==> 000

Local Audit

==> FAIL

Success Level

==> _____

Failure Level

==> READ

Installation Data

==> _____

<==

Do You Want to Keep This Information
For the Add Dataset Screen (Y/N): N

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Always press ENTER after a List Dataset Profile, or to recover from a message, to return to the Dataset Administration Main panel.

Add Dataset Profile

Perform the following steps to issue the equivalency of a RACF Add Dataset Profile command (that is, ADDSD 'USER01.JCLCNTL' GEN):

- 1 Enter 'A' into the Request Type field
- 2 TAB to the Dataset Profile field, type in the dataset profile you want to add, and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                        Administration Input

Enter the Dataset and Request Type. Other fields are optional.

Request Type      ==> A              (A=Add,C=Change,L=List,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL
Owner             ==> _____ Profile Owner
UACC              ==> _____ (None,Execute,Read,Update,Control,Alter)
Notify           ==> _____ Userid to Notify
Warn (Y/N)       ==> _             Activate Warn?
Level            ==> _____ Resource Level
Local Audit      ==> _____ (All,Success,Fail,None)
Success Level    ==> _____ (None,Read,Update,Control,Alter)
Failure Level    ==> _____ (None,Read,Update,Control,Alter)
Installation Data ==> _____

_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process adds the specified dataset profile. All other fields are optional. The default values for optional fields if not specified are: The Owner field defaults to the Userid of person issuing the add profile, UACC defaults to None, Local Audit defaults to Fail, Failure Level defaults to Read, Warn defaults to N, Level defaults to 000, and all other fields default to blanks.

Change Dataset Profile

Perform the following steps to issue the equivalency of a RACF Alter Dataset Profile (that is, ALTDSD 'USER01.JCLCNTL' GEN OW(USER02) UACC(READ)):

- 1 Enter 'C' into the Request Type field
- 2 TAB to the Dataset Profile field, type in the dataset profile you want to change
- 3 TAB to the Owner field and type in the new owner
- 4 TAB to the UACC field and type in the new UACC level, and press ENTER.

Dataset Administration ----- SSA ----- Dataset Administration

Administration Input

Enter the Dataset and Request Type. Other fields are optional.

Request Type ==> C (A=Add,C=Change,L=List,D=Delete)

Dataset Profile ==> USER01.JCL.CNTL

Owner ==> USER02 Profile Owner

UACC ==> READ (None,Execute,Read,Update,Control,Alter)

Notify ==> Userid to Notify

Warn (Y/N) ==> _ Activate Warn?

Level ==> Resource Level

Local Audit ==> (All,Success,Fail,None)

Success Level ==> (None,Read,Update,Control,Alter)

Failure Level ==> (None,Read,Update,Control,Alter)

Installation Data ==>

<==

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process changes the specified dataset profile. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Update Existing Dataset Profile Information

Perform the following steps to update existing information for the specified dataset profile:

- 1 Enter 'L' as the request type to list the dataset profile.
- 2 TAB to the dataset profile field and Enter the dataset profile and press ENTER.
- 3 TAB to the Do You Want to Keep This Information For the Add Dataset Screen field, type a 'Y', and press ENTER.
- 4 TAB to any appropriate field, type in changes, and press ENTER.

Dataset Administration ----- SSA ----- Dataset Administration

List Dataset Output

Dataset Profile ==> USER01.JCL.CNTL

Owner ==> USER01 UACC ==> NONE

Notify ==> Warn ==> N

Level ==> 000

Local Audit ==> FAIL

Success Level ==>

Failure Level ==> READ

Installation Data ==> THIS IS NEW INSTALLATION DATA FOR THE TEST01.REPORT.OUTPUT DATASET PROFILE.

<==

Do You Want to Keep This Information
For the Add Dataset Screen (Y/N): Y

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

When you specify 'Y' to Do You Want to Keep This Information For the Add Dataset Screen, the Owner, UACC, Warn, Level, Local Audit, Success/Failure Audit Level, and Installation Data will be passed back to the Input Screen.

Delete Dataset Profile

Perform the following steps to issue the equivalency of a RACF Delete Dataset Profile command (that is, DELDSD 'USER01JCLCNTL' GEN):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Dataset Profile field, type in the dataset profile you want to delete, and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                        Administration Input

Enter the Dataset and Request Type.  Other fields are optional.

Request Type      ==> D              (A=Add,C=Change,L=List,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL_____
Owner             ==> _____ Profile Owner
UACC              ==> _____ (None,Execute,Read,Update,Control,Alter)
Notify            ==> _____ Userid to Notify
Warn (Y/N)        ==> _____ Activate Warn?
Level             ==> _____ Resource Level
Local Audit       ==> _____ (All,Success,Fail,None)
Success Level     ==> _____ (None,Read,Update,Control,Alter)
Failure Level     ==> _____ (None,Read,Update,Control,Alter)
Installation Data ==> _____

_____
_____ <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process deletes the specified dataset profile. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```

Dataset Administration ----- SSA ----- Dataset Administration
                        Delete a Dataset Profile

Confirm Delete Request (Y/N): Y

Dataset Profile   ==> USER01.JCL.CNTL_____

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

Dataset Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Dataset Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List Profile A = Add Profile C = Change Profile D = Delete Profile	YES
CDSNAM	44	Dataset profile to be affected	YES
COWNER	8	User or group to be made the owner of the dataset profile specified when the request is an add or change.	NO. On add request the default is the Userid issuing request if not specified.
CUACC	8	UACC level for the profile specified when request is add or change. The only acceptable values are: NONE EXECUTE READ UPDATE CONTROL ALTER	NO. The default value is NONE.
CNOTIFY	8	Userid to be notified whenever RACF uses this profile to deny access to a data set.	NO
CWARN	1	Indicator of request to add the WARNING flag that will issue a warning message and allow access to the resource even if access is insufficient. Must be ‘Y’ or ‘N’.	NO
CLEVEL	3	Level value for profile specified. The value must be between 000 and 099. The default is 000	NO. The default value is 000.

Field Label	Length	Explanation	Required on Invocation?
CAUDIT	7	Indicates what access attempts you want to log on the SMF data set. The only acceptable values are: NONE ALL SUCCESS FAIL	NO. The default value is FAIL.
CAUDOK	7	Indicates what access level you want logged for SUCCESS audit levels. The only acceptable values are: NONE READ UPDATE CONTROL ALTER	NO
CAUDNG	7	Indicates what access level you want logged for FAIL audit levels. The only acceptable values are: NONE READ UPDATE CONTROL ALTER	NO
CPERADD	1	RESERVED	NO
CINSTAD	1	RESERVED	NO
CDFPADD	1	RESERVED	NO
CINSTL	255	Data to update installation data field on the dataset profile specified when the request is an add or change.	NO
LDSNAM	44	Output field profile that was listed	NO
LOWNER	8	Output field showing the owner of the profile that was listed	NO
LUACC	8	Output field showing UACC of the profile that was listed.	NO
LNOTIFY	8	Output field showing the Userid to be notified whenever RACF uses the profile to deny access to a data set.	NO
LWARN	3	Output field indicating whether the Warning flag for the profile is in effect.	NO
LLEVEL	3	Output field showing the level of the profile that was listed	NO

Field Label	Length	Explanation	Required on Invocation?
LAUDIT	7	Output field showing what type of auditing is to be in effect for the profile that was listed.	NO
LAUDOK	7	Output field showing what access level will be used for successful auditing.	NO
LAUDNG	7	Output field showing what access level will be used for failure auditing.	NO
LPERADD	1	RESERVED	NO
LINSTAD	1	RESERVED	NO
LDFPADD	1	RESERVED	NO
LINSTL	255	Output field showing installation data for the profile that was listed.	NO
LDSNSAV	1	RESERVED	NO

Dataset Administration API Example

The following Assembler layout sample can be found in member CPYDSA of the SSA install library:

```

**** API HEADER ****
CACTION      DS      CL1      ACTION REQUIRED
CDSNAM       DS      CL44     DATASET PROFILE
COWNER       DS      CL8      OWNER
CUACC        DS      CL8      UACC
CNOTIFY      DS      CL8      NOTIFY
CWARN        DS      CL1      WARN
CLEVEL       DS      CL3      LEVEL
CAUDIT       DS      CL7      AUDIT LEVEL
CAUDOK       DS      CL7      AUDIT SUCCESS ACCESS
CAUDNG       DS      CL7      AUDIT FAIL ACCESS LEV
CPERADD      DS      CL3      RESERVED
CINSTL       DS      CL255    NEW INSTALLATION DATA
*
LDSNAM       DS      CL44     DATASET
LOWNER       DS      CL8      OWNER
LUACC        DS      CL8      UACC
LNOTIFY      DS      CL8      NOTIFY
LWARN        DS      CL3      WARN
LLEVEL       DS      CL3      LEVEL
LAUDIT       DS      CL7      AUDIT
LAUDOK       DS      CL7      AUDOK
LAUDNG       DS      CL7      AUDNG
LPERADD      DS      CL3      RESERVED
LINSTL       DS      CL255    NEW INSTALLATION DATA
LDSNSAV      DS      CL1      RESERVED
ORG          COMMAREA+32760

```

Resource Administration Screens

Perform List Resource Profile

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST TSOPROC SSA130):

- 1 Enter 'L' in the Request Type field.
- 2 TAB to the Resource Profile field and enter the resource profile.
- 3 TAB to the Class field and enter the class name, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration
Administration Input

Enter the Resource, Class and Request Type. Other fields are optional.
Request Type ==> L (A=Add,C=Change,L=List,D=Delete)
Resource Profile ==> MEGA130

Class ==> TSOPROC_

Owner ==>

UACC ==>

Notify ==>

Warn (Y/N) ==> _

Level ==>

Local Audit ==>

Success Level ==>

Failure Level ==>

<==

Resource Class of Profile

Profile Owner

(None,Execute,Read,Update,Control,Alter)

Userid to Notify

Activate Warn?

Resource Level

(All,Success,Fail,None)

(None,Read,Update,Control,Alter)

(None,Read,Update,Control,Alter)

Process: Inst/Appl Data (Y/N): N

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

List Resource Profile Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Resource Administration ----- SSA ----- Resource Administration
                          List Resource Output

Resource Profile ==> MEGA130

Class          ==> TSOPROC      Owner          ==> SYSTEM
UACC           ==> NONE        Notify         ==>
Warn           ==> N           Level          ==> 000

Local Audit    ==> FAIL
Success Level  ==>
Failure Level  ==> READ

Do You Want to Keep This Information
For the Rdefine Screen (Y/N): N

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Always press ENTER after a List Resource Profile, or to recover from a message, to return to the Resource Administration Main panel.

If the Process: Inst/Apl Data field was set to 'Y' (on the initial screen) then the following screen will be displayed as well.

```

Resource Administration ----- SSA ----- Resource Administration
                          List Resource Output

Resource Profile ==> NEWPROC

Class          ==> TSOPROC

Installation Data ==>

Application Data ==>

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

Add Resource Profile

Perform the following steps to issue the equivalency of a RACF Add Resource Profile command (that is, RDEFINE TSOPROC NEWPROC):

- 1** Enter 'A' into the Request Type field
- 2** TAB to the Resource Profile field, type in the resource profile you want to add.
- 3** TAB to the Class field, type in the class name you want to add the resource profile to, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration		
Administration Input		
Enter the Resource, Class and Request Type. Other fields are optional.		
Request Type	==> A	(A=Add,C=Change,L=List,D=Delete)
Resource Profile	==> NEWPROC_____	
		<==
Class	==> TSOPROC_	Resource Class of Profile
Owner	==> _____	Profile Owner
UACC	==> _____	(None,Execute,Read,Update,Control,Alter)
Notify	==> _____	Userid to Notify
Warn (Y/N)	==> -	Activate Warn?
Level	==> _____	Resource Level
Local Audit	==> _____	(All,Success,Fail,None)
Success Level	==> _____	(None,Read,Update,Control,Alter)
Failure Level	==> _____	(None,Read,Update,Control,Alter)
Process: Inst/Appl Data (Y/N): N		
Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP		

This process adds the specified resource profile. All other fields are optional. The default values for optional fields if not specified are: The Owner field defaults to the Userid of person issuing the add profile, UACC defaults to None, Local Audit defaults to Fail, Failure Level defaults to Read, Warn defaults to N, Level defaults to 000, and all other fields default to blanks.

Change Resource Profile

Perform the following steps to issue the equivalency of a RACF Alter Resource Profile (that is, RALT TSOPROC NEWPROC OW(USER02) UACC(READ)):

- 1 Enter 'C' into the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile you want to change.
- 3 TAB to the Class field, and type in the class name.
- 4 TAB to the Owner field and type in the new owner
- 5 TAB to the UACC field and type in the new UACC level, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration
Administration Input

Enter the Resource, Class and Request Type. Other fields are optional.
Request Type ==> C (A=Add,C=Change,L=List,D=Delete)
Resource Profile ==> NEWPROC_____

<==

Class	==> TSOPROC_	Resource Class of Profile
Owner	==> USER02_	Profile Owner
UACC	==> READ_	(None,Execute,Read,Update,Control,Alter)
Notify	==> _____	Userid to Notify
Warn (Y/N)	==> _	Activate Warn?
Level	==> _____	Resource Level
Local Audit	==> _____	(All,Success,Fail,None)
Success Level	==> _____	(None,Read,Update,Control,Alter)
Failure Level	==> _____	(None,Read,Update,Control,Alter)

Process: Inst/Appl Data (Y/N): N

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process changes the specified resource profile. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Change Resource Profile - Installation/Application Data

Perform the following steps to issue the equivalency of a RACF Alter Resource Profile (that is, RALT TSOPROC NEWPROC APPL("") DATA(")):

- 1 Enter ‘C’ into the Request Type field.
- 2 TAB to Resource Profile field, type in the resource profile you want to change.
- 3 TAB to the Class field, and type in the class name.
- 4 TAB to the Process: Inst/Appl Data field and type in ‘Y’, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration
Administration Input

Enter the Resource, Class and Request Type. Other fields are optional.
Request Type ==> C (A=Add,C=Change,L=List,D=Delete)
Resource Profile ==> NEWPROC_____

<==

Class	==> TSOPROC_	Resource Class of Profile
Owner	==> _____	Profile Owner
UACC	==> _____	(None,Execute,Read,Update,Control,Alter)
Notify	==> _____	Userid to Notify
Warn (Y/N)	==> _	Activate Warn?
Level	==> _____	Resource Level
Local Audit	==> _____	(All,Success,Fail,None)
Success Level	==> _____	(None,Read,Update,Control,Alter)
Failure Level	==> _____	(None,Read,Update,Control,Alter)

Process: Inst/Appl Data (Y/N): Y

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Enter in the data in the appropriate field as shown in the screen below, and press ENTER.

```

Resource Administration ----- SSA ----- Resource Administration
                        Administration Input

Enter the Installation and/or Application Data Fields.

Installation Data ==> THIS PROC IS TO BE USED FOR INSTALLING NEW TSO BASED 3R
D PARTY PRODUCTS._____
_____ <==

Application Data ==> ACCESS LIST SHOULD BE: MVS SYSTEMS AREA, END-USER TESTI
NG TEAM, AND DATA SECURITY DEPARTMENT._____
_____ <==

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP

```

Update Existing Resource Profile Information

Perform the following steps to update existing information for the specified resource profile:

- 1** Enter 'L' as the request type to list the resource profile.
- 2** TAB to the resource profile field and Enter the resource profile.
- 3** TAB to the class field and Enter the class name. If you wish to also include the resource profile's Installation/Application Data TAB to Process: Inst/Appl Data field and type a 'Y'
- 4** Press ENTER.
- 5** TAB to the Do You Want to Keep This Information For the Add Resource Screen field, type a 'Y', and press ENTER.
- 6** TAB to any appropriate field, type in changes. If you wish to also include the resource profile's Installation/Application Data TAB to Process: Inst/Appl Data field and type a 'Y' and press ENTER. You will then be presented with the Administration Input screen. TAB to either field, type in changes.
- 7** Press ENTER.

Resource Administration ----- SSA ----- Resource Administration

List Resource Output

Resource Profile ==> NEWPROC

<==

Class	==> TSOPROC	Owner	==> TEST02
UACC	==> READ	Notify	==>
Warn	==> N	Level	==> 000

Local Audit	==> FAIL
Success Level	==>
Failure Level	==> READ

Do You Want to Keep This Information
For the Rdefine Screen (Y/N): Y

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

When you specify ‘Y’ to Do You Want to Keep This Information For the Add Resource Screen, the Owner, UACC, Warn, Level, Local Audit, Success/Failure Audit Level, and Installation/Application Data will be passed back to the appropriate screen.

Delete Resource Profile

Perform the following steps to issue the equivalency of a RACF Delete Resource Profile command (that is, RDEL TSOPROC NEWPROC):

- 1 Enter ‘D’ into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile you want to delete, and press ENTER.

Resource Administration ----- SSA ----- Resource Administration

Administration Input

Enter the Resource, Class and Request Type. Other fields are optional.

Request Type	==> D	(A=Add,C=Change,L=List,D=Delete)
Resource Profile	==> NEWPROC	

<==

Class	==> TSOPROC_	Resource Class of Profile
Owner	==>	Profile Owner
UACC	==>	(None,Execute,Read,Update,Control,Alter)
Notify	==>	Userid to Notify
Warn (Y/N)	==> _	Activate Warn?
Level	==> _	Resource Level
Local Audit	==>	(All,Success,Fail,None)
Success Level	==>	(None,Read,Update,Control,Alter)
Failure Level	==>	(None,Read,Update,Control,Alter)

Process: Inst/App1 Data (Y/N): Y

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process deletes the specified resource profile. The following screen is presented to confirm the delete. Change the N to Y and press enter.

```
Resource Administration ----- SSA ----- Resource Administration
                        Delete a Resource Profile

                        Confirm Delete Request (Y/N): N

Profile==> NEWPROC

                                <==

Class ==> TSOPROC

Hit Enter to Continue          PF03 or Clear=EXIT/PF01=HELP
```

Resource Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Resource Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List Profile A = Add Profile C = Change Profile D = Delete Profile	YES
CRESRCE	246	Resource profile to be affected	YES
CCLASS	8	RACF Class that the profile belongs to	YES
COWNER	8	User or group to be made the owner of the resource profile specified when the request is an add or change.	NO. On add request the default is the Userid issuing request if not specified.
CUACC	8	UACC level for the profile specified when request is add or change. The only acceptable values are: NONE EXECUTE READ UPDATE CONTROL ALTER	NO. The default value is NONE.
CNOTIFY	8	Userid to be notified whenever RACF uses this profile to deny access to a resource	NO
CWARN	1	Indicator of request to add the WARNING flag that will issue a warning message and allow access to the resource even if access is insufficient. Must be ‘Y’ or ‘N’.	NO
CLEVEL	3	Level value for profile specified. The value must be between 000 and 099. The default is 000	NO. The default value is 000.

Field Label	Length	Explanation	Required on Invocation?
CAUDIT	7	Indicates what access attempts you want to log on the SMF data set. The only acceptable values are: NONE ALL SUCCESS FAIL	NO. The default value is FAIL.
CAUDOK	7	Indicates what access level you want logged for SUCCESS audit levels. The only acceptable values are: NONE READ UPDATE CONTROL ALTER	NO
CAUDNG	7	Indicates what access level you want logged for FAIL audit levels. The only acceptable values are: NONE READ UPDATE CONTROL ALTER	NO
CPERADD	1	RESERVED	NO
CMEMADD	1	RESERVED	NO
CINAPAD	1	RESERVED	NO
CINSTL	255	Data to update installation data field on the resource profile specified when the request is an add or change.	NO
CAPPL	255	Data to update application data field on the resource profile specified when the request is an add or change.	NO
LRESRCE	246	Output field profile that was listed	NO
LCLASS	8	Output field of class of profile that was listed	NO
LOWNER	8	Output field showing the owner of the profile that was listed	NO
LUACC	8	Output field showing UACC of the profile that was listed.	NO
LNOTIFY	8	Output field showing the Userid to be notified whenever RACF uses the profile to deny access to a data set.	NO

Field Label	Length	Explanation	Required on Invocation?
LWARN	3	Output field indicating whether the Warning flag for the profile is in effect.	NO
LLEVEL	3	Output field showing the level of the profile that was listed	NO
LAUDIT	7	Output field showing what type of auditing is to be in effect for the profile that was listed.	NO
LAUDOK	7	Output field showing what access level will be used for successful auditing.	NO
LAUDNG	7	Output field showing what access level will be used for failure auditing.	NO
LPERADD	1	RESERVED	NO
LMEMADD	1	RESERVED	NO
LINAPAD	1	RESERVED	NO
LINSTL	255	Output field showing installation data for the profile that was listed.	NO
LAP PL	255	Output field showing application data for the profile that was listed.	NO
LRSCSAV	1	RESERVED	NO

Resource Administration API Example

The following Assembler layout sample can be found in member CPYRSA in the SSA install library:

```

**** API HEADER ****
CACTION      DC      CL1' '    ACTION REQUIRED
CRESRCE      DC      CL246     RESOURCE
CCLASS       DC      CL8' '    CLASS
COWNER       DC      CL8' '    OWNER
CUACC        DC      CL8' '    UACC
CNOTIFY      DC      CL8' '    NOTIFY
CWARN        DC      CL1' '    WARN
CLEVEL       DC      CL3' '    LEVEL
CAUDIT       DC      CL7' '    AUDIT
CAUDOK       DC      CL7' '    AUDOK
CAUDNG       DC      CL7' '    AUDNG
CPERADD      DC      CL1' '    RESERVED
CMEMADD      DC      CL1' '    RESERVED
CINAPAD      DC      CL1' '    RESERVED
CINSTL       DC      CL255' '  NEW INSTALLATION DATA
CAPPL        DC      CL255' '  NEW APPLICATION DATA
*
LRESRCE      DC      CL246' '  RESOURCE

```


LCLASS	DC	CL8' '	CLASS
LOWNER	DC	CL8' '	OWNER
LUACC	DC	CL8' '	UACC
LNOTIFY	DC	CL8' '	NOTIFY
LWARN	DC	CL3' '	WARN
LLEVEL	DC	CL3' '	LEVEL
LAUDIT	DC	CL7' '	AUDIT
LAUDOK	DC	CL7' '	AUDOK
LAUDNG	DC	CL7' '	AUDNG
LPERADD	DC	CL1' '	RESERVED
LMEMADD	DC	CL1' '	RESERVED
LINAPAD	DC	CL1' '	RESERVED
LINSTL	DC	CL255' '	NEW INSTALLATION DATA
LAPPL	DC	CL255' '	NEW APPLICATION DATA
LRSCSAV	DC	CL1' '	RESERVED
ORG		COMMAREA+32760	

Dataset Permit Administration Screens

Perform List Dataset Profile Permits

Perform the following steps to issue the equivalency of a RACF List Dataset command (that is, LD DA() GEN AUTHUSER):

- 1 Enter ‘L’ in the Request Type field.
- 2 Enter the dataset profile in the Dataset Profile field and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Dataset Permit Input

Enter the Dataset and Permit Information.

Request Type

Dataset Profile

Access Entry

Access Level

==> L

==> USER01.JCL.CNTL

==> _____

==> _____

(L=List Std,A=Add,C=Change,D=Delete)

User or Group to Permit

(None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

List Dataset Profile Permits Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

Permit Administration ----- SSA ----- Permit Administration

List Standard Permits

Permits for ==> USER01.JCL.CNTL

A = Add Permit, D = Delete Permit, C = Change Permit

SELECT

Entry

Access Level

_

MEGA

ALTER

You can ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- Add Permit (A)

Displays the Dataset Permit Administration Main Panel with the appropriate fields filled in.

- Delete Permit (D)

Displays the Delete Dataset Permit confirmation panel. Type ‘Y’ to confirm the delete.

- Change Permit (C)

Displays the Dataset Permit Administration Main Panel with the appropriate fields filled in.

Note The CICS version of Dataset Permit Administration only allows the user to select one permit from the list. The TSO version allows as many selections as the user requests.

Add Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT ‘USER01JCLCNTL’ GEN ID(USER02) ACCESS(ALTER)):

- 1 Enter ‘A’ into the Request Type field.
- 2 TAB to the Dataset Profile field, type in the dataset profile.
- 3 TAB to the Access Entry field, type in a userid or group.
- 4 TAB to the Access Level field, type in the access level, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration	Dataset Permit Input
Enter the Dataset and Permit Information.	
Request Type	==> A (L=List Std,A=Add,C=Change,D=Delete)
Dataset Profile	==> USER01.JCL.CNTL_____
Access Entry	==> USER02__ User or Group to Permit
Access Level	==> ALTER__ (None,Execute,Read,Update,Control,Alter)
Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP	

This process adds the userid or group to the dataset profile with the access level specified.

Change Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT ‘USER01JCLCNTL’ GEN ID(USER02) ACCESS(READ)):

- 1 Enter ‘C’ into the Request Type field.
- 2 TAB to the Dataset Profile field, type in the dataset profile.
- 3 TAB to the Access Entry field, type in a userid or group.
- 4 TAB to the Access Level field, type in the access level you want to change to, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Dataset Permit Input

Enter the Dataset and Permit Information.

Request Type

Dataset Profile

Access Entry

Access Level

==> C

==> USER01.JCL.CNTL

==> USER02

==> READ

(L=List Std,A=Add,C=Change,D=Delete)

User or Group to Permit

(None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

This process changes the userid’s or group’s access level to the dataset profile specified.

Delete Dataset Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Dataset Profile command (that is, PERMIT ‘USER01.JCLCNTL’ GEN ID(USER02) DELETE):

- 1 Enter ‘D’ into the Request Type field.
- 2 TAB to the Dataset Profile field, type in the dataset profile.
- 3 TAB to the Access Entry field, type in a userid or group, and press ENTER.

```
Permit Administration ----- SSA ----- Permit Administration
                          Dataset Permit Input

                          Enter the Dataset and Permit Information.

Request Type      ==> D              (L=List Std,A=Add,C=Change,D=Delete)
Dataset Profile   ==> USER01.JCL.CNTL_____
Access Entry      ==> USER02__      User or Group to Permit
Access Level      ==> _____    (None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

This process deletes the specified dataset profile permit. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```
Permit Administration ----- SSA ----- Permit Administration
                          Delete A Standard Permit

                          Confirm Delete Request (Y/N): Y

Dataset Profile ==> TEST01.JCL.CNTL
Entry           ==> TEST02

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

Dataset Permit Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Dataset Permit Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List Standard Access List A = Add Permit C = Change Permit D = Delete Permit	YES
LISTADDR	4	RESERVED	NO
CDSNAM	44	Dataset profile to be affected	YES
CPERENT	8	User or group to permit to the profile specified.	YES. (NO, if request is a list standard permits).
CPERLVL	8	Indicates what access level. The only acceptable values are: NONE EXECUTE READ UPDATE CONTROL ALTER	YES. (NO, if request is a list standard permits).
LARRAY	Remainder of 32760	If the request was to list standard permits, the list of permits is returned in this area. The permits are returned in 16 character fields (8 Character Userid/Group and 8 Character Access Level), with the last entry followed by a single HEX 00.	NO

Dataset Permit Administration API Example

The following Assembler layout sample can be found in member CPYDSP in the SSA install library:

```

CACTION    DS      CL1    A(DD), D(DELETE), C(HANGE), L(IST STD)
LISTADDR   DS      XL4    PERMITS GETMAIN'D AREA
CDSNAM     DS      CL44   DATASET NAME
CPERENT    DS      CL8    PERMIT USER
CPERLVL    DS      CL8    PERMIT LEVEL
*
```

LARRAY	EQU	COMMAREA+184	RETURNED LIST OF 16-BYTE ENTRIES
	ORG	COMMAREA+32760	

Resource Permit Administration Screens

Perform List Resource Profile Permits

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST TSOPROC NEWPROC AUTHUSER):

- 1 Enter ‘L’ in the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration
Resource Permit Input

Enter the Resource Profile, Class and Permit Information.

Request Type ==> L (L=List,A=Add,C=Change,D=Delete)

Resource Profile ==> NEWPROC_____

_____ <==

Class ==> TSOPROC_

Access Entry ==> _____

Access Level ==> _____

Resource Class of Profile

User or Group to Permit

(None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue

PF03 or Clear=EXIT/PF01=HELP

List Resource Profile Permits Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.


```

Permit Administration ----- SSA ----- Permit Administration
                               List Standard Permits

Permits For ==> NEWPROC

Class      ==> TSOPROC      <==

          A = Add Permit, D = Delete Permit, C = Change Permit

SELECT      Entry      Access Level
-----
-          USER01      READ

```

You can ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- Add Permit (A)

Displays the Resource Permit Administration Main Panel with the appropriate fields filled in.

- Delete Permit (D)

Displays the Delete Resource Permit confirmation panel. Type ‘Y’ to confirm the delete.

- Change Permit (C)

Displays the Resource Permit Administration Main Panel with the appropriate fields filled in.

Note The CICS version of Resource Permit Administration only allows the user to select one permit from the list. The TSO version allows as many selections as the user requests.

Add Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) ACCESS(READ)):

- 1** Enter ‘A’ into the Request Type field.
- 2** TAB to the Resource Profile field, type in the resource profile.
- 3** TAB to the Class field, type in the class name.
- 4** TAB to the Access Entry field, type in a userid or group
- 5** TAB to the Access Level field, type in the access level, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Add Permit Input

Enter The Permit Information.

Request Type ==> A (A=Add,C=Change,D=Delete)

Resource Profile ==> NEWPROC

Class ==> TSOPROC

Access Entry ==> USER02

Access Level ==> READ

<==

Resource Class of Profile

User or Group to Permit

(None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process adds the userid or group to the resource profile with the access level specified.

Change Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) ACCESS(NONE)):

- 1 Enter 'C into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Access Entry field, type in a userid or group
- 5 TAB to the Access Level field, type in the new access level, and press ENTER.

Permit Administration ----- SSA ----- Permit Administration

Dataset Permit Input

Enter the Dataset and Permit Information.

Request Type ==> C (L=List Std,A=Add,C=Change,D=Delete)

Dataset Profile ==> USER01.JCL.CNTL_____

Access Entry ==> USER02__ User or Group to Permit

Access Level ==> NONE_____ (None,Execute,Read,Update,Control,Alter)

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process changes the userid's or group's access level to the resource profile specified.

Delete Resource Profile Permit

Perform the following steps to issue the equivalency of a RACF Permit to Resource Profile command (that is, PERMIT NEWPROC CLASS(TSOPROC) ID(USER02) DELETE):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Access Entry field, type in a userid or group, and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                                Resource Permit Input

                                Enter the Resource Profile, Class and Permit Information.

Request Type      ==> D              (L=List,A=Add,C=Change,D=Delete)
Resource Profile  ==> NEWPROC_____

-----
Class             ==> TSOPROC_      <==
Access Entry      ==> USER02_      Resource Class of Profile
Access Level      ==> _____    User or Group to Permit
                                      (None,Execute,Read,Update,Control,Alter)

                                Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process deletes the specified resource profile permit. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```

Permit Administration ----- SSA ----- Permit Administration
                                Delete A Standard Permit

                                Confirm Delete Request (Y/N): N

Profile ==> NEWPROC

-----
Class      ==> TSOPROC      <==
Entry      ==> TEST02
Level      ==>

                                Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

Resource Permit Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Resource Permit Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List Standard Permits A = Add Permit C = Change Permit D = Delete Permit	YES
LISTADDR	4	RESERVED	NO
CRESRCE	246	Resource profile to be affected	YES
CCLASS	8	RACF Class of the profile to be affected	YES
CPERENT	8	User or group to permit to the profile specified.	YES. (NO, if request is a list standard permits).
CPERLVL	8	Indicates what access level. The only acceptable values are: NONE EXECUTE READ UPDATE CONTROL ALTER	YES. (NO, if request is a list standard permits).
LARRAY	Remainder of 32760	If the request was to list standard permits, the list of permits is returned in this area. The permits are returned in 16 character fields (8 Character Userid/Group and 8 Character Access Level), with the last entry followed by a single HEX 00.	NO

Resource Permit Administration API Example

The following Assembler layout sample can be found in member CPYRSP in the SSA install library:

```
CACTION      DS      CL1      ACTION REQUIRED
LISTADDR     DS      XL4      PERMITS GETMAIN'D AREA
CRESRCE      DS      CL246    RESOURCE
```

CCLASS	DS	CL8	CLASS
CPERENT	DS	CL8	PERMIT USER
CPERLVL	DS	CL8	PERMIT LEVEL
*			
LARRAY	EQU	COMMAREA+406	RETURNED LIST
	ORG	COMMAREA+32760	

Resource Member Administration Screens

Perform List Resource Profile Members

Perform the following steps to issue the equivalency of a RACF List Resource command (that is, RLIST GCICSTRN CICSCAT2):

- 1 Enter ‘L’ in the Request Type field.
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name, and press ENTER.

Member Administration ----- SSA ----- Member Administration

Resource Member Input

Enter the Resource Profile, Class and Member Information.

Request Type ==> L (L=List,A=Add,D=Delete)

Resource Profile ==> CICSCAT2

Class ==> GCICSTRN Resource Class of Profile

Member ==>

Member To Be Processed

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

List Resource Profile Members Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

Member Administration ----- SSA ----- Member Administration
                                List Resource Members

Resource  ==>  CICSCAT2

Class      ==>  GCICSTRN      <==
                                A = Add Member, D = Delete Member

SELECT    Member
-----
-         CEMT

-         CEOT      <==

-         <==

```

You can ‘select and scroll’ through the listing and specify, in the select column, any of the following options:

- Add Member (A)

Displays the Resource Member Administration Main Panel with the appropriate fields filled in.

- Delete Member (D)

Displays the Delete Resource Member confirmation panel. Type ‘Y’ to confirm the delete.

Note The CICS version of Resource Member Administration only allows the user to select one member from the list. The TSO version allows as many selections as the user requests.

Add Resource Profile Member

Perform the following steps to issue the equivalency of a RACF Resource Profile Add Member command (that is, RALTER GCICSTRN CICSCAT2 ADDMEM(CEMX)):

- 1** Enter ‘A’ into the Request Type field
- 2** TAB to the Resource Profile field, type in the resource profile.
- 3** TAB to the Class field, type in the class name.
- 4** TAB to the Member field, type in the new member, and press ENTER.

```

Member Administration ----- SSA ----- Member Administration
                          Resource Member Input

      Enter the Resource Profile, Class and Member Information.

Request Type      ==> A              (L=List,A=Add,D=Delete)
Resource Profile ==> CICSCAT2_____

-----
Class             ==> GCICSTRN      <==
Member           ==> CEMX_____   Resource Class of Profile
-----

----- <== Member To Be Processed -----

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process adds the member requested to the resource profile and class specified.

Delete Resource Profile Member

Perform the following steps to issue the equivalency of a RACF Resource Profile Add Member command (that is, `RALTER GCICSTRN CICSCAT2 DELMEM(CEMX)`):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Resource Profile field, type in the resource profile.
- 3 TAB to the Class field, type in the class name.
- 4 TAB to the Member field, type in the member to remove, and press ENTER.

```

Member Administration ----- SSA ----- Member Administration
                          Resource Member Input

      Enter the Resource Profile, Class and Member Information.

Request Type      ==> D              (L=List,A=Add,D=Delete)
Resource Profile ==> CICSCAT2_____

-----
Class             ==> GCICSTRN      <==
Member           ==> CEMX_____   Resource Class of Profile
-----

----- <== Member To Be Processed -----

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process deletes the specified resource member. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.


```
Member Administration ----- SSA ----- Member Administration
                          Delete A Resource Member

                          Confirm Delete Request (Y/N): Y

Profile ==> CICSCAT2

Class   ==> GCICSTRN          <==
Entry   ==>

                          <==

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

Resource Member Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Resource Member Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List Members A = Add Member D = Delete Member	YES
LISTADDR	4	RESERVED	NO
CRESRCE	246	Resource profile to be affected	YES
CCLASS	8	RACF Class of the profile to be affected	YES
CMEMBER	246	Member to add/delete to the resource profile specified.	YES. (NO, if request is a list standard permits).
LARRAY	Remainder of 32760	If the request was to list members, the list of members is returned in this area. The members are returned in 246 character fields, with the last entry followed by a single HEX 00.	NO

Resource Member Administration API Example

The following Assembler layout sample can be found in member CPYMBA in the SSA install library:

```

CACTION  DS      CL1      ACTION REQUIRED
LISTADDR DS      XL4      MEMBERS GETMAIN'D AREA
CRESRCE  DS      CL246    RESOURCE
CCLASS   DS      CL8      CLASS
CMEMBER  DS      CL246    MEMBER
*
          ORG      COMMAREA+642RETURNED LIST
LARRAY   EQU      *
          ORG      COMMAREA+32760

```

User TSO Segment Administration Screens

Perform List User TSO Segment

Perform the following steps to issue the equivalency of a RACF List User TSO Segment command (that is, LISTUSER USER01 TSO NORACF):

- 1 Enter 'L' in the Request Type field.
- 2 TAB to the Userid field, type in the userid, and press ENTER.

```

TSO Segment Administration ----- SSA ----- TSO Segment Administration
                        Administration Input

Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> L                      (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01__
Account Number    ==>
Destination       ==>                      Unit            ==>
Hold Class        ==>                      Job Class        ==>
Msg Class         ==>                      Sysout Class     ==>
Logon Procedure    ==>                      Security Label    ==>
Logon Size        ==>                      Max Size         ==>
User Data         ==>
Command**         ==>
                  ** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

List User TSO Segment Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```

TSO Segment Administration ----- SSA ----- TSO Segment Administration
                        List TSO Segment Output

Userid            ==> USER01
Account Number    ==>
Destination       ==>                      Unit            ==>
Hold Class        ==>                      Job Class        ==>
Msg Class         ==>                      Sysout Class     ==>
Logon Procedure    ==> NEWPROC              Security Label    ==>
Logon Size        ==> 0002048              Max Size         ==> 0004096
User Data         ==> 0000

Command          ==>
                  <==

Do You Want to Keep This Information
For the Add/Change TSO Segment Screen (Y/N): N

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

Always press ENTER after a List User TSO Segment, or to recover from a message, to return to the Main panel.

Add User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 TSO(PROC(NEWPROC) SIZE(2048) MAXSIZE(4096))

- 1 Enter ‘A’ into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Logon Procedure field, type in the procedure.
- 4 TAB to the Logon Size field, type in the minimum size.
- 5 TAB to the Max Size field, type in the maximum size, and press ENTER.

TSO Segment Administration ----- SSA ----- TSO Segment Administration
Administration Input

Enter the Request Type and Userid. Other fields are optional.

Request Type	==> A	(A=Add,C=Change,L=List,D=Delete)	
Userid	==> USER01__		
Account Number	==> _____		
Destination	==> _____	Unit	==> _____
Hold Class	==> _	Job Class	==> _
Msg Class	==> _	Sysout Class	==> _
Logon Procedure	==> NEWPROC_	Security Label	==> _____
Logon Size	==> 0002048	Max Size	==> 0004096
User Data	==> _____		
Command**	==> _____		

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

This process adds a TSO segment for the userid specified. All other fields are optional. The default values for optional fields if not specified are: The Logon Size field defaults to all zeroes, the Max Size field defaults to all zeroes, and the User Data field defaults to all zeroes.

Note If the Max Size field is all zeroes then the userid’s TSO segment has an ‘unlimited’ amount of size for their logon session. Also, if the Max Size field is other than all zeroes, it must be greater than the Logon Size.

Change User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 TSO(MAXSIZE(0000) MSGCLASS(X)):

- 1 Enter ‘C into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Msg Class field, type in the new message class value.

- 4 TAB to the Max Size field, type in the new maximum size, and press ENTER.

```

TSO Segment Administration ----- SSA ----- TSO Segment Administration
                        Administration Input

Enter the Request Type and Userid.  Other fields are optional.

Request Type    ==> C                      (A=Add,C=Change,L=List,D=Delete)
Userid          ==> USER01__
Account Number  ==> _____
Destination     ==> _____ Unit        ==> _____
Hold Class     ==> _ Job Class              ==> _
Msg Class       ==> X Sysout Class           ==> _
Logon Procedure ==> _____ Security Label ==> _____
Logon Size      ==> _____ Max Size      ==> 0000000
User Data       ==> _____

Command**      ==> _____

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process changes the specified userid's TSO segment. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Delete User TSO Segment

Perform the following steps to issue the equivalency of a RACF Alter User TSO Segment command (that is, ALTUSER USER01 NOTSO):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile, and press ENTER.

```

TSO Segment Administration ----- SSA ----- TSO Segment Administration
                        Administration Input

Enter the Request Type and Userid.  Other fields are optional.

Request Type    ==> D                      (A=Add,C=Change,L=List,D=Delete)
Userid          ==> USER01__
Account Number  ==> _____
Destination     ==> _____ Unit        ==> _____
Hold Class     ==> _ Job Class              ==> _
Msg Class       ==> _ Sysout Class           ==> _
Logon Procedure ==> _____ Security Label ==> _____
Logon Size      ==> _____ Max Size      ==> _____
User Data       ==> _____

Command**      ==> _____

** = Only Valid On RACF 2.3 Or Above

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process deletes the specified userid's TSO segment. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```
TSO Segment Administration ----- SSA ----- TSO Segment Administration
                                Delete a TSO Segment
```

```
                                Confirm Delete Request (Y/N): Y
```

```
Userid                      ==> USER01
```

```
Hit Enter to Continue
```

```
PF03 or Clear=EXIT/PF01=HELP
```

User TSO Segment Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the User TSO Segment Administration SSA-CDA API call:

Field Label	Length	Explanation	Required
CACTION	1	Action requested. The valid values are: L = List A = Add C = Change D = Delete	YES
CUSERID	8	Userid to be affected.	YES
CTACCT	40	Account number to be used if request is an add or change.	NO
CTCMD	80	Default command at logon if request is an add or change.	NO
CTDEST	8	Destination to be used if request is an add or change.	NO
CTHCLAS	1	Default hold class to be used if request is an add or change.	NO
CTJCLAS	1	Default job class to be used if request is an add or change.	NO
CTLPROC	8	Default logon procedure to be used if request is an add or change.	NO
CTLSIZE	7	Logon size to be used if request is an add or change.	NO
CTMCLAS	1	Default message class to be used if request is an add or change.	NO
CTMSIZE	7	Maximum logon size to be used if request is an add or change.	NO
CTSCLAS	1	Default SYSOUT class to be used if request is an add or change.	NO
CTUDATA	4	User data to be used if request is an add or change.	NO
CTUNIT	8	Default UNIT to be used if request is an add or change.	NO
CTSLABL	8	Default logon security label to be used if request is an add or change.	NO

Field Label	Length	Explanation	Required
LUSERID	8	Output field indicating userid that was listed	NO
LTACCT	40	Output field showing the default account number of the userid that was listed	NO
LTCMD	80	Output field showing the default command at logon of the userid that was listed.	NO
LTDEST	8	Output field showing the default destination of the userid that was listed.	NO
LTHCLAS	1	Output field showing the default hold class of the userid that was listed	NO
LTJCLAS	1	Output field showing the default job class of the userid that was listed	NO
LTLPROC	8	Output field showing the default logon procedure of the userid that was listed	NO
LTLSIZE	7	Output field showing the default logon size of the userid that was listed	NO
LTMCLAS	1	Output field showing the default message class of the userid that was listed	NO
LTMSIZE	7	Output field showing the maximum logon size of the userid that was listed	NO
LTSCLAS	1	Output field showing the default SYSOUT class of the userid that was listed	NO
LTUDATA	4	Output field showing the user data of the userid that was listed	NO
LTUNIT	8	Output field showing the default unit of the userid that was listed	NO
LTSLABL	8	Output field showing the default logon security label of the userid that was listed	NO
LTSOSAV	1	RESERVED	NO

User TSO Segment Administration API Example

The following Assembler layout sample can be found in member CPYUTP in the SSA install library:

```
CACTION  DS      CL1      ACTION REQUESTED
CUSERID  DS      CL8      USERID
```


CTACCT	DS	CL40	ACCOUNT NUMBERS
CTCMD	DS	CL80	DEFAULT CMD AT LOGON
CTDEST	DS	CL8	DESTINATION
CTHCLAS	DS	CL1	DEFAULT HOLD CLASS
CTJCLAS	DS	CL1	DEFAULT JOB CLASS
CTLPROC	DS	CL8	DEFAULT LOGON PROC
CTLSIZE	DS	CL7	LOGON SIZE
CTMCLAS	DS	CL1	DEFAULT MESSAGE CLASS
CTMSIZE	DS	CL7	MAXIMUM REGION SIZE
CTSCLAS	DS	CL1	DEFAULT SYSOUT CLASS
CTUDATA	DS	CL4	USER DATA
CTUNIT	DS	CL8	DEFAULT UNIT NAME
CTSLABL	DS	CL8	DEFAULT LOGON SECLABEL
*			
LUSERID	DS	CL8	USERID
LTACCT	DS	CL40	ACCOUNT NUMBERS
LTCMD	DS	CL80	DEFAULT CMD AT LOGON
LTDEST	DS	CL8	DESTINATION
LTHCLAS	DS	CL1	DEFAULT HOLD CLASS
LTJCLAS	DS	CL1	DEFAULT JOB CLASS
LTLPROC	DS	CL8	DEFAULT LOGON PROC
LTLSIZE	DS	CL7	LOGON SIZE
LTMCLAS	DS	CL1	DEFAULT MESSAGE CLASS
LTMSIZE	DS	CL7	MAXIMUM REGION SIZE
LTSCCLAS	DS	CL1	DEFAULT SYSOUT CLASS
LTUDATA	DS	CL4	USER DATA
LTUNIT	DS	CL8	DEFAULT UNIT NAME
LTSLABL	DS	CL8	DEFAULT LOGON SECLABEL
LTSOSAV	DS	CL1	SAVE INFO FROM LIST SCREEN?
ORG			COMMAREA+32760

User CICS Segment Administration Screens

Perform List User CICS Segment

Perform the following steps to issue the equivalency of a RACF List User CICS Segment command (that is, LISTUSER USER01 CICS NORACF):

- 1
- Enter ‘L’ in the Request Type field.
- 2
- TAB to the Userid field, type in the userid, and press ENTER.

CICS Segment Administration ----- SSA ----- CICS Segment Administration

Administration Input

Enter the Request Type and Userid. Other fields are optional.

Request Type ==> L (A=Add,C=Change,L=List,D=Delete)

Userid ==> USER01__

Operator ID ==> _____

Operator Priority ==> 000 (000 - 255)

XRF Takeover Force ==> NOFORCE (FORCE/NOFORCE)

Timeout ==> 00:00 (HH:MM)

Opcodes:

01: _ 02: _ 03: _ 04: _

05: _ 06: _ 07: _ 08: _

09: _ 10: _ 11: _ 12: _

13: _ 14: _ 15: _ 16: _

17: _ 18: _ 19: _ 20: _

21: _ 22: _ 23: _ 24: _

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

List User CICS Segment Display

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

CICS Segment Administration ----- SSA ----- CICS Segment Administration

List CICS Segment Output

Userid ==> USER01 Operator ID ==> AB1

Operator Priority ==> 000 XRF Takeover Force ==> NOFORCE

Timeout ==> 00:00

Opcodes

01: 02: 03: 04:

05: 06: 07: 08:

09: 10: 11: 12:

13: 14: 15: 16:

17: 18: 19: 20:

21: 22: 23: 24:

Do You Want to Keep This Information

For the Add/Change CICS Segment Screen (Y/N): N

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

Always press ENTER after a List User CICS Segment, or to recover from a message, to return to the User CICS Segment Administration Main panel.

Add User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER USER01 CICS (OPIDENT(AB1) TIMEOUT(0130))):

- 1 Enter 'A' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Operator Identity field, type in the opid.
- 4 TAB to the Timeout field, type in the timeout value, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Administration Input

Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> A              (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01__
Operator ID       ==> AB1
Operator Priority  ==> 000            (000 - 255)
XRF Takeover Force ==> NOFORCE       (FORCE/NOFORCE)
Timeout           ==> 01:30         (HH:MM)

Opclasses:
01: _            02: _            03: _            04: _
05: _            06: _            07: _            08: _
09: _            10: _            11: _            12: _
13: _            14: _            15: _            16: _
17: _            18: _            19: _            20: _
21: _            22: _            23: _            24: _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
  
```

This process adds a CICS segment for the userid specified. All other fields are optional. The default values for optional fields if not specified are: The Operator ID field defaults to all zeroes, the Operator Priority field defaults to all zeroes, the Timeout field defaults to all zeroes, XRF Takeover Force field defaults to NOFORCE.

Change User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER USER01 CICS (TIMEOUT(0415))):

- 1 Enter 'C' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile.
- 3 TAB to the Timeout field, type in the new timeout value, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Administration Input

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> C          (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01___
Operator ID       ==> _____
Operator Priority  ==> 000        (000 - 255)
XRF Takeover Force ==> NOFORCE   (FORCE/NOFORCE)
Timeout           ==> 04:15     (HH:MM)

Opclasses:
    01: _      02: _      03: _      04: _
    05: _      06: _      07: _      08: _
    09: _      10: _      11: _      12: _
    13: _      14: _      15: _      16: _
    17: _      18: _      19: _      20: _
    21: _      22: _      23: _      24: _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process changes the specified userid's CICS segment. At least one of the other fields is required. All other fields are optional. No fields are updated unless specified.

Delete User CICS Segment

Perform the following steps to issue the equivalency of a RACF Alter User CICS Segment command (that is, ALTUSER NOCICS):

- 1 Enter 'D' into the Request Type field
- 2 TAB to the Userid field, type in the userid profile, and press ENTER.

```

CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Administration Input

      Enter the Request Type and Userid.  Other fields are optional.

Request Type      ==> D          (A=Add,C=Change,L=List,D=Delete)
Userid            ==> USER01___
Operator ID       ==> _____
Operator Priority  ==> 000        (000 - 255)
XRF Takeover Force ==> NOFORCE   (FORCE/NOFORCE)
Timeout           ==> 00:00     (HH:MM)

Opclasses:
    01: _      02: _      03: _      04: _
    05: _      06: _      07: _      08: _
    09: _      10: _      11: _      12: _
    13: _      14: _      15: _      16: _
    17: _      18: _      19: _      20: _
    21: _      22: _      23: _      24: _

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP

```

This process deletes the specified userid's CICS Segment. The following screen is presented to confirm the delete. Change the N to Y and press ENTER.

```
CICS Segment Administration ----- SSA ----- CICS Segment Administration
                        Delete a CICS Segment

                        Confirm Delete Request (Y/N): Y

Userid                ==> USER01

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

User CICS Segment Administration API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (See API details at the beginning of this chapter). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the User CICS Segment Administration SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
CACTION	1	Action requested. The valid values are: L = List A = Add C = Change D = Delete	YES
CUSERID	8	Userid to be affected.	YES
COPID	3	Operator identifier to be used if request is an add or change.	NO
COPPRTY	3	Operator priority to be used if request is an add or change.	NO
CXRFS	7	XRFORCE indicator if request is an add or change. The valid values are: FORCE NOFORCE	NO
CTIME	6	Timeout value to be used if request is an add or change. The format of the value must be HH:MM	NO
COPCL01		Indicator to add operator class 01 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL02		Indicator to add operator class 02 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL03		Indicator to add operator class 03 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL04		Indicator to add operator class 04 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL05		Indicator to add operator class 05 if the request is an add or change. Must be 'Y' or 'N'.	NO

Field Label	Length	Explanation	Required on Invocation?
COPCL06		Indicator to add operator class 06 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL07		Indicator to add operator class 07 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL08		Indicator to add operator class 08 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL09		Indicator to add operator class 09 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL10		Indicator to add operator class 10 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL11		Indicator to add operator class 11 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL12		Indicator to add operator class 12 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL13		Indicator to add operator class 13 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL14		Indicator to add operator class 14 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL15		Indicator to add operator class 15 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL16		Indicator to add operator class 16 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL17		Indicator to add operator class 17 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL18		Indicator to add operator class 18 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL19		Indicator to add operator class 19 if the request is an add or change. Must be 'Y' or 'N'.	NO

Field Label	Length	Explanation	Required on Invocation?
COPCL20		Indicator to add operator class 20 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL21		Indicator to add operator class 21 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL22		Indicator to add operator class 22 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL23		Indicator to add operator class 23 if the request is an add or change. Must be 'Y' or 'N'.	NO
COPCL24		Indicator to add operator class 24 if the request is an add or change. Must be 'Y' or 'N'.	NO
LUSERID	8	Output field indicating userid that was listed	YES
LOPID	3	Output field showing the opid of the userid that was listed	NO
LOPPRTY	3	Output field showing the operator priority of the userid that was listed.	NO
LXRFS	7	Output field showing the XRFORCE of the userid that was listed. The valid values are FORCE NOFORCE	NO
LTIME	6	Output field showing the timeout value of the userid that was listed.	NO
LOPCL01	1	Output filed indicating that the userid listed has operator class 01.	NO
LOPCL02	1	Output filed indicating that the userid listed has operator class 02.	NO
LOPCL03	1	Output filed indicating that the userid listed has operator class 03.	NO
LOPCL04		Output filed indicating that the userid listed has operator class 04.	NO
LOPCL05		Output filed indicating that the userid listed has operator class 05.	NO
LOPCL06		Output filed indicating that the userid listed has operator class 06.	NO

Field Label	Length	Explanation	Required on Invocation?
LOPCL07		Output filed indicating that the userid listed has operator class 07.	NO
LOPCL08		Output filed indicating that the userid listed has operator class 08.	NO
LOPCL09		Output filed indicating that the userid listed has operator class 09.	NO
LOPCL10		Output filed indicating that the userid listed has operator class 10.	NO
LOPCL11		Output filed indicating that the userid listed has operator class 11.	NO
LOPCL12		Output filed indicating that the userid listed has operator class 12.	NO
LOPCL13		Output filed indicating that the userid listed has operator class 13.	NO
LCOPCL14		Output filed indicating that the userid listed has operator class 14.	NO
LCOPCL15		Output filed indicating that the userid listed has operator class 15.	NO
LCOPCL16		Output filed indicating that the userid listed has operator class 16.	NO
LCOPCL17		Output filed indicating that the userid listed has operator class 17.	NO
LCOPCL18		Output filed indicating that the userid listed has operator class 18.	NO
LCOPCL19		Output filed indicating that the userid listed has operator class 19.	NO
LCOPCL20		Output filed indicating that the userid listed has operator class 20.	NO
LOPCL21		Output filed indicating that the userid listed has operator class 21.	NO
LCOPCL22		Output filed indicating that the userid listed has operator class 22.	NO
LOPCL23		Output filed indicating that the userid listed has operator class 23.	NO
LOPCL24		Output filed indicating that the userid listed has operator class 24.	NO

User CICS Segment Administration API Example

The following Assembler layout sample can be found in member CPYUTC in the SSA install library:

CACTION	DS	CL1	ACTION REQUESTED
CUSERID	DS	CL8	USERID
COPID	DS	CL3	OPERATOR ID
COPPTY	DS	CL3	OPERATOR PRIORITY
CXRFS	DS	CL7	XRF FORCE
CTIME	DS	CL5	TIMEOUT
COPCL01	DS	C	OPERATOR CLASSES
COPCL02	DS	C	
COPCL03	DS	C	
COPCL04	DS	C	
COPCL05	DS	C	
COPCL06	DS	C	
COPCL07	DS	C	
COPCL08	DS	C	
COPCL09	DS	C	
COPCL10	DS	C	
COPCL11	DS	C	
COPCL12	DS	C	
COPCL13	DS	C	
COPCL14	DS	C	
COPCL15	DS	C	
COPCL16	DS	C	
COPCL17	DS	C	
COPCL18	DS	C	
COPCL19	DS	C	
COPCL20	DS	C	
COPCL21	DS	C	
COPCL22	DS	C	
COPCL23	DS	C	
COPCL24	DS	C	
*			
LUSERID	DS	CL8	USERID
LOPID	DS	CL3	OPERATOR ID
LOPPPTY	DS	CL3	OPERATOR PRIORITY
LXRFS	DS	CL7	XRFS FORCE
LTIME	DS	CL5	TIMEOUT
LOPCL01	DS	C	OPERATOR CLASS
LOPCL02	DS	C	
LOPCL03	DS	C	
LOPCL04	DS	C	
LOPCL05	DS	C	
LOPCL06	DS	C	
LOPCL07	DS	C	
LOPCL08	DS	C	
LOPCL09	DS	C	
LOPCL10	DS	C	
LOPCL11	DS	C	
LOPCL12	DS	C	
LOPCL13	DS	C	
LOPCL14	DS	C	
LOPCL15	DS	C	
LOPCL16	DS	C	
LOPCL17	DS	C	
LOPCL18	DS	C	
LOPCL19	DS	C	

LOPCL20	DS	C
LOPCL21	DS	C
LOPCL22	DS	C
LOPCL23	DS	C
LOPCL24	DS	C
	ORG	COMMAREA+32760

Access Simulator Screens

Perform Access Simulation

Perform the following steps to issue an actual check against RACF on behalf of the specified Userid or Group.

- 1 Enter a valid Userid or Group.
- 2 TAB to the Resource field, type in a fully qualified resource.
- 3 TAB to the Class field, type in the class name, and press ENTER.

```
Access Simulator ----- SSA ----- Access Simulator

      Enter All Applicable Fields to Simulate an Access Attempt.

      Enter Valid Userid or Group ==> USER02__

Resource      ==> NEWPROC_____
_____
_____
Class         ==> TSOPROC_<==
Volume (Optional) ==> _____

      Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

Simulation Results

If the user has READ access to the appropriate MAA\$RULE class profile the following screen will be displayed.

```
Access Simulator ----- SSA ----- Access Simulator

                                Simulation Results
                                USER=USER02 ,NAME=GENERAL USER 02

Resource                        ==> NEWPROC

                                <==
Class                          ==> TSOPROC
Volume (Optional)              ==>

Protecting Profile ==> NEWPROC

                                <==

Highest Allowed Access Level ==> READ

                                Hit Enter| to Continue      PF03 or Clear=EXIT/PF01=HELP
```

Always press ENTER after a Simulation Results screen, or to recover from a message, to return to the Access Simulator Main panel.

Access Simulator API Invocation

All calls to the SSA-CDA API involve calling the API program AAZCLNT with a COMMAREA that is always 32760 in length (see ‘Application Programming Interface’ on page 371). The COMMAREA consists of a header that is used for all invocations of the API and then the data for the actual requested function. Below is a table detailing the fields and formats for the Access Simulator SSA-CDA API call:

Field Label	Length	Explanation	Required on Invocation?
AUTTYPE	3	Access check type. The valid values are: RSC = General resource profile DSN = Dataset profile	YES
AUTATTR	8	Output field that shows the access level that the access entity has to the specified resource/class or dataset profile.	NO
AUTENT	8	Userid or Group to check against specified resource/class or dataset profile	YES
AUTCLAS	8	Class to check for specified dataset or resource profile. USER and GROUP are not valid for this field. The valid values are: DATASET = Any General Resource Class name	NO
AUTVOL	6	Volume to check for specified dataset profile. This is only valid when the class field is DATASET.	NO
AUTPROF	246	Resource/Dataset profile to check.	YES
AUTNAME	20	Output field for the name of a userid. This field will be filled in.	NO
AUTSTAT	1	Output field that indicates if the AUTENT is a userid or a group. The valid values are: G = group U = userid	NO
AUTPROT	246	Output field that shows the profile from RACF that protects the specified resource/class or dataset profile.	NO

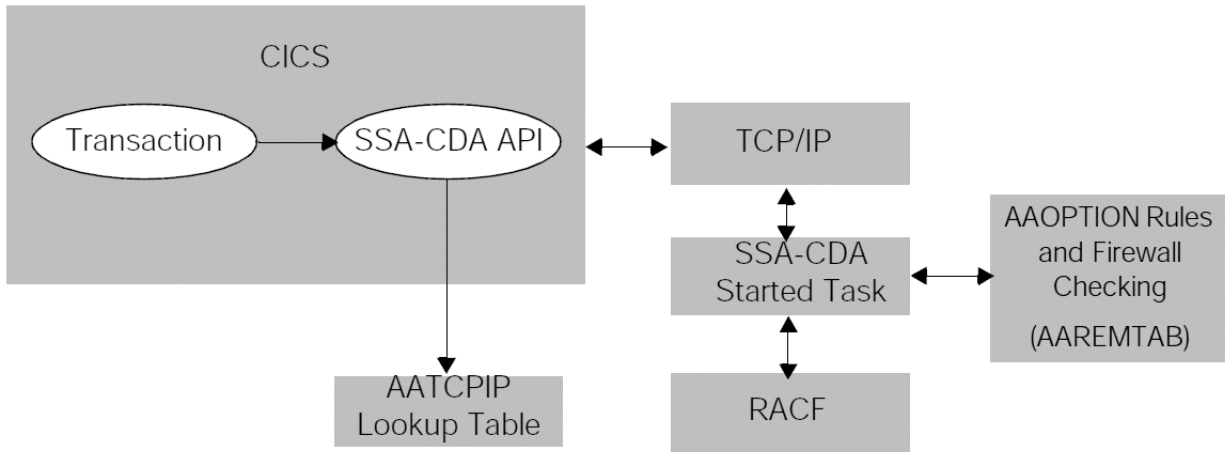
Access Simulator API Example

The following Assembler layout sample can be found in member CPYAUT in the SSA install library:

```
AUTTYPE      DS      CL3      WILL AUTOMATICALLY BE SET BY
*
AUTATTR      DS      CL8      RETURNED ACCESS TYPE
AUTENT       DS      CL8      USERID OR GROUP
AUTCLAS      DS      CL8      CLASS
AUTVOL       DS      CL6      VOLUME (OPTIONAL)
AUTPROF      DS      CL246    RESOURCE
AUTNAME      DS      CL20     RETURNED NAME (IF STAT=G)
AUTSTAT      DS      CL1      RETURNED G (GROUP) OR U (USE
AUTPROT      DS      CL246    RETURNED PROTECTING PROFILE
ORG          COMMAREA+32760
```

Cross Platform Administration

CICS Direct Administration uses TCP/IP to communicate its requests from a CICS based application to a started task that processes those requests. Those requests can be initiated from one distinct system to another as long as SSA-CDA is setup properly on each system. This allows an administrator or user to perform SSA-CDA functions on multiple distinct systems from one CICS region. It is important to understand the request flow so that all the components and settings involved will make sense. Below is a flow chart to show how a request is routed and handled:



The request takes the following steps:

- 1** A transaction or program is initiated to invoke the SSA-CDA API.
- 2** The SSA-CDA API receives the request and does the following:
 - Checks the incoming request for syntax errors.
 - Retrieves the associated IP address and port from the AATCPIP module.
 - Upon syntax validation, the API initiates a conversation with the SSA-CDA started task.
 - Upon establishing the conversation, the API encrypts the request and sends it to the SSA-CDA started task.
- 3** The started task receives the request and does the following:
 - Decrypts the request.
 - Checks the incoming request for syntax errors.
 - Loads the security syntax rules established for SSA from the AAOPTION module.
 - Loads and checks the table of allowed IP addresses from AAREMTAB module.
 - If the request is a remote system request, the task validates userid and password supplied.
 - Verifies requesters authority to perform the requested function.
 - Upon verification of the requesters authority, the started task performs the function requested and communicates the results back to the requester through TCP/IP.

- 4 The SSA-CDA API receives the results back from the started task and returns those results back to the originating transaction or program

Setup Cross Platform Administration

To setup SSA-CDA to do cross platform administration you must do the following:

Note To help clarify the explanation below, the documentation will refer to two systems - SYSTEMA and SYSTEMB. SYSTEMA is the system through SSA-CDA sending RACF requests to SYSTEMB. SYSTEMA has the following settings:

TCP/IP Task Name	=TCPIPSYA
TCP/IP Task IP ADDRESS	=205.185.254.2
CICS Task	=SYSACICS
CICS Task PORT	=3500

SYSTEMB is the system with the started task receiving and processing the requests. SYSTEMB has the following settings:

TCP/IP Task Name	=TCPIPSYB
TCP/IP Task IP ADDRESS	=205.185.254.3
SSA-CDA Started Task PORT	=4500

Changes to Be Made On SYSTEMA

A full base installation must be done. It is important to note that if you do not require certain features on this system (that is, The SCHEDULER) or you are not licensed for that module on the remote system you do not need to perform those steps directly related to those modules. You must do the CICS Direct Administration step.

Edit member AATCPIP in the SSA install library and create an entry that directs the requests for a particular transaction to SYSTEMB. AATCPIP is a table that contains a reference to the transaction that is executing the SSA-CDA API. The reference contains the IP address, port and other important fields that tell the API where to route the request. Below is a complete explanation of AATCPIP and the significance of the fields and values involved:

AATCPIP Entry Sample

```
* THIS FIRST ENTRY IS REQUIRED. IT IS THE DEFAULT DATA
* THAT WILL BE USED IF YOUR TRANSACTION NAME DOES NOT MATCH
* ONE IN THIS TABLE.
*
DFLT_TRANS      DC  CL4'DFLT'          REQUIRED - DEFAULT TRANSACTION
DFLT_TCPIP      DC  CL8'TCIPMVS'      TCPIP JOB NAME
DFLT_CICS       DC  CL8'SENTCICS'     CICS JOB NAME
DFLT_DISPLAY    DC  C'N'              N=DO NOT DISPLAY,Y=DISPLAY
DFLT_IP_ADDR    DC  CL15'205.185.254.3'
DFLT_PORT       DC  H'3500'          TCPIP PORT NUMBER
DFLT_DESC       DC  CL40'DEFAULT SYSTEM'
```

Field Label	Length	Content	Explanation
DFLT_TRANS	4	Transaction that is invoking the SSA-CDA API	The transaction or program that invokes the API if not supplied to the API is retrieved and used as the lookup in the AATCPIP table. If the transaction or program wants to route to another system based on that value it can supply a different value to the API and have it routed accordingly.
DFLT_TCPIP	8	Name of the TCP/IP started task.	The name of the TCP/IP started task for the system the CICS component is running on must be supplied.
DFLT_CICS	8	Name of the CICS region.	The name of the CICS region the SSA-CDA module is installed in must be supplied.
DFLT_DISPLAY	1	'Y' or 'N'	The default display flag tells the API and the invoking transaction or program to either display or not display the connecting system information. The information displayed is IP address, PORT and the 40 character description field. This is helpful in letting the invoking user know what system the request is being routed to.
DFLT_IP_ADDR	15	IP address of the TCP/IP started task on SYSTEMB	The IP address of the TCP/IP started task on the destination system must be supplied. The request is routed based on this IP address and the PORT too.
DFLT_PORT	2 (Half word)	PORT assigned to the SSA-CDA started task on the SYSTEMB (Binary number)	The PORT assigned to the SSA-CDA started task on the destination system must be supplied. The request is first routed to the TCP/IP started task based on the IP address supplied and then TCP/IP routes the request to the SSA-CDA started task based on PORT assignment.
DFLT_DESC	40	Comments	If you set the display flag to 'Y', the 40 character description field is displayed on the invoking transactions initial screen. This is useful in that a plain English explanation or description can be assigned to the routing that is being done.

Sample AATCPIP Entry Addition

The following entry is a sample addition to AATCPIP based on the SYSTEMA to SYSTEMB scenario. The entry added indicates that transaction SAPB will route its requests to SYSTEMB.

```
**** Default Entry (must be in table) ****
**
** AATCPIP ADDITION FOR SYSTEMB
**
SYSTEMB_TRANS  DC  CL4'SAPB'          PASSWORD ADMIN FOR SYSTEMB
SYSTEMA_TCPIP   DC  CL8'TCPIPSYA'      SYSTEMA TCPIP JOB NAME
SYSTEMA_CICS    DC  CL8'SYSACICS'      SYSTEMA CICS JOB NAME
SYSTEMB_DISPLAY DC  C'Y'              N=DO NOT DISPLAY,Y=DISPLAY
SYSTEMB_IP_ADDR DC  CL15'205.185.254.3' SYSTEMB TCPIP TASK ADDR
SYSTEMB_PORT    DC  H'4500'           SYSTEMB CICS PORT NUMBER
SYSTEMB_DESC    DC  CL40'SYSTEMB'     DESCRIPTION OF DESTINATION
```

When you have made your addition to the AATCPIP table you must assemble it. You can use the supplied ASSEMBLE member in the SSA install library.

- Define the new transaction to SYSTEMA. If the invoking transaction uses the same SSA-CDA program as the default Password Administration transaction SAPW, then all you have to do is define the new transaction with the same attributes as SAPW. You can do this in batch using the DFCS DUP program or by executing transaction CEDA in the CICS region you are installing the software. Below is an example of that definition being done with CEDA:

CEDA Define Sample

```
CEDA DEFINE TRANS(SAPB) GROUP(SSA)
DESCRIPTION(REMOTE PASSWORD ADMINISTRATION ON SYSTEMB)
PROGRAM(AAZPWA01)
```

SYSTEMA installation is complete. You must now proceed to configure SYSTEMB to receive and process the requests from SYSTEMA.

Below is an example of what the Password Administration screen would look like with the remote IP, PORT and description displayed:

```

Password Administration ----- SSA ----- Password Administration
                        Administration Input

Enter the Userid to be Reset. All other fields are optional.

Userid      ==> _____ Userid to be reset
Password    ==> ???????? New password - Blank for default group
Resume      ==> - Specify Y to resume the userid
Revoke      ==> - Specify Y to revoke the userid
Resume Date ==> _____ Resume date for the userid (YYYY-MM-DD)
Revoke Date ==> _____ Revoke date for the userid (YYYY-MM-DD)
SuperRevoke ==> - Specify Y to super-revoke the userid
Installation Data ==> _____

_____ <==

CONNECTING TO: SYSTEMB
IP: 205.185.254.3 PORT: 4500

Hit Enter to Continue PF03 or Clear=EXIT/PF01=HELP

```

Changes to Be Made On SYSTEMB

- A full base installation must be done. It is important to note that if you do not require certain features on this system (that is, The SCHEDULER) or you are not licensed for that module on the remote system you do not need to perform those steps directly related to those modules. You must do the CICS Direct Administration step.
- Define the security rules you want established to govern the requests received. See ‘Security’ on page 365.
- Edit member AAREMTAB in the SSA install library and create an entry that allows requests from SYSTEMA to be honored. The table in AAREMTAB is used by the SSA-CDA started task to do a secondary check on the request validating if the IP address of the requestor is to be honored. The entries in AAREMTAB can use generic masking. The generic masking can use the conventions described below.

Generic Masking in AAREMTAB: Asterisk (*)

- By itself indicates all entries are honored. This is the default entry in AAREMTAB.
- At the end of a string indicates that the string must match and all other characters following are honored.
- At the beginning of a string and simultaneous at the end of that string indicates that the characters of the string specified will be searched for throughout the IP of the incoming request. For example you could specify ‘*205.185*’. In this case, the SSA-CDA started task would search the entire IP address of the incoming request for 205.185. If found, the request is honored.
- In any other position in the string, the asterisk is not honored as a generic character. Specifying the asterisk in this fashion is invalid.

Percent Sign (%)

- The percent sign can be used anywhere and as often as required in the search string as a single character generic masking character, however, it is not honored if you are using the asterisk at beginning and end of string masking scheme.

- Obviously you can specify exact IP addresses in the table to be honored. Below is the default layout for AAREMTAB and an example addition for honoring requests from SYSTEMA.

AAREMTAB Example

```
*****
**                                     **
**   AUTHORIZED REMOTE IP ADDRESSES   **
**                                     **
*****
SYSTEMA_ENTRY   DC   CL15'205.185.254.2'
END_OF_TABLE    DC   CL15'#####'
```

The sample above contains the explicit IP address of SYSTEMA. SYSTEMB will honor all requests that come from that IP address. Also displayed is the mandatory END_OF_TABLE entry that must be the last entry in the table of entries. When you have made your addition to the AATCPIP table you must assemble it. You can use the supplied ASSEMBLE member in the SSA install library.

SYSTEMB is now setup to receive the requests from SYSTEMA. You must make sure that the SSA-CDA started task AASTC02 on the SYSTEMB has started successfully.

Cross Platform Request Validation

If a SSA-CDA request is sent to a remote system, the invoker must supply a valid userid and password for the remote system. Of course, the userid must be permitted to perform the option requested as well. Below is an example of the userid and password prompting screen. It is important to note that the screen allows a user to not only enter in their password but also enter in a new password if they wish to change it. The started task does a RACROUTE=VERIFY with the userid and password supplied, therefore, all the conditions of a signon apply. For example, if the userid's password is expired, the SSA-CDA dialog will come back with a notification of that status. SSA-CDA Userid and Password Prompt:

```
Authentication ----- SSA ----- Authentication
                Administrator's ID Information is Required
Please enter your Userid and Password.

Enter your Userid and Password for the System that you want to administrate.

Userid           ==> _____ Your Userid on the Other System
Password         ==> _____ Your Password on the Other System
New Password     ==> _____ Your NEW Password on the Other System

Hit Enter to Continue      PF03 or Clear=EXIT/PF01=HELP
```

Cross Platform Administration API Requirements

If the SSA-CDA request is being sent across platforms, the request must have a valid userid/password combination; valid on the remote system. When the API is used for cross platform administration the userid must be put in the CADMINID field in the API header and the valid password for that userid must be placed in the CADMPW field (see API header part of this section). If the user needs to or wants to change their password, the new password must be placed in the CADMNEW field. The userid's password will be updated only if all three fields are correct.

**CHAPTER 10****Configuration**

The chapter describes the following configuration topics:

- Screen Configuration Options
- Setting Up SSA users and administrators
- AAOPTION Configuration Module - System Level Configuration Options

Configuration Main Menu

The Configuration Main Menu includes two groups of options for general users and SSA administrators. General users can select options to edit their personal configuration and store new configuration values. SSA Administrators can view and change SSA configuration settings.

```
Configuration ----- SSA ----- Configuration
                          Main Menu

Option ==>

General User Options:

1 Edit Stored Configuration Values
2 Choose New Stored Configuration

Administrator Options:

3 Manipulate Stored Configurations
4 Change The SCHEDULER Task Settings
5 Display a User or Groups SSA Authorities
6 Run Extract Job

Current Configuration in Use ==> AACONFIG-DEFAULT

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Edit Stored Configuration Values	This option allows an administrator or user to change configuration values stored in their personal ISPF profile.
Choose New Stored Configuration	This option allows users or administrators to select another stored configuration to use with SSA.
Manipulate Stored Configurations	This option is restricted to administrators. This function allows an administrator to retrieve and manipulate stored configurations.
Change the Scheduler Task Settings	This option is restricted to administrators. This feature allows an administrator to change the settings of the SCHEDULER started task.
Display a Users or Groups SSA Authorities	This option is restricted to administrators. This function displays all SSA secured functions and user or group access to those functions.
Run Extract Jobs	This option is restricted to administrators. This function will assist the administrator in creating the extract jobs that retrieve and store their RACF information.
Current Configuration in Use	The current configuration is displayed for informational purposes only.

Edit Stored Configuration Values

The Edit Stored Configuration Values is a scrollable screen that allows users to change their personal configuration settings. Descriptions of screen fields follow the example shown below.

```

Configuration ----- SSA ----- Configuration
                                Edit Stored Configuration Values
Command ==>

                                Enter Configuration Values

                                More:      +

SSA Job Statement Information:
==> //IBMUSER JOB (ACCOUNT),'NAME',NOTIFY=&SYSUID
==> /*
==> /*
==> /*

SSA Libraries:
RACF/ISPF Tables           ==> SSA.RACFDATA.ISPTLIB
The SCHEDULER Database     ==> SSA.SCHED.DATABASE
The SCHEDULER Historical   ==> SSA.SCHED.HISTORY
*Load Library              ==> SSA.LOADLIB
*ISPF Panel Library        ==> SSA.ISPPLIB
*ISPF Message Library      ==> SSA.ISPMLIB
*ISPF Skeleton JCL Library ==> SSA.ISPSLIB
*ISPF CLIST Library        ==> SSA.ISPCLIB

* = Entries only used for JCL, not for panel operations

Users Libraries:
Report Output              ==> IBMUSER.TSCSSA.REPORT.OUTPUT
Adhoc Command Output      ==> IBMUSER.TSCSSA.ADHOC.OUTPUT
Command Generation Output ==> IBMUSER.TSCSSA.COMMAND.OUTPUT

Allocation Units:
Permanent Datasets        ==> SYSDA
Sort or Work Areas        ==> SYSDA
Temporary Datasets        ==> SYSDA
Allocation Prefix         ==> IBMUSER

Operational Information:
Lines Per Page (Print Parm) ==> 55
Report Menu Format (Long/Short) ==> SHORT
Prompt for Print After Browse (Y/N) ==> Y
Clear Select Fields After Processing (Y/N) ==> N
Execute Command Generation Commands
Immediately after Creation in Batch (Y/N) ==> N

System Libraries:
ISPF Table Library        ==> SYS1.SISPTENU
ISPF Message Library      ==> SYS1.SISPMENU
Sort Library              ==> _____
Steplib Sort library (Y/N): N

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Job Statement	Specify a jobcard that is valid to run in your shop.
RACF/ISPF Tables	This value cannot be changed through this screen. You must choose a stored configuration that has the SSA RACF/ISPF table dataset you want to use.
The SCHEDULER Database	This value can not be changed through this screen. You must choose a stored configuration that has the SSA scheduler database you desire to use.
The SCHEDULER Historical	This value can not be changed through this screen. You must choose a stored configuration that has the SSA scheduler historical database you desire to use.

Load Library	Specify the SSA APF-authorized load library.
ISPF Panel Library	Specify the SSA ISPF panel library.
ISPF Message Library	Specify the SSA ISPF message library.
ISPF Skeleton JCL Library	Specify the SSA ISPF skeleton JCL library.
ISPF CLIST Library	Specify the SSA ISPF CLIST library.
Report Output	Specify a report output dataset that has the following DCBs: RECFM=FB, LRECL=133. SSA will allocate this dataset for you if it does not exist when you perform a reporting function. Also, SSA will construct the dataset name using the allocation prefix in your configuration and the set suffix SSA.REPORT.OUTPUT, therefore, if you manually allocate the file, you must use these naming conventions.
Adhoc Command Output	Specify an adhoc command output dataset that has the following DCBs: RECFM=FB, LRECL=80. SSA will allocate this dataset for you if it does not exist when you perform a adhoc command generation function. Also, SSA will construct the dataset name using the allocation prefix in your configuration and the set suffix SSA.ADHOC.OUTPUT, therefore, if you manually allocate the file, you must use these naming conventions.
Command Generation Output	Specify a command generation output dataset that has the following DCBs: RECFM=FB, LRECL=80. SSA will allocate this dataset for you if it does not exist when you perform a command generation function. Also, SSA will construct the dataset name using the allocation prefix in your configuration and the set suffix SSA.COMMAND.OUTPUT, therefore, if you manually allocate the file, you must use these naming conventions.
Permanent Datasets	Specify an esoteric device name for allocation of permanent datasets.
Sort or Work Areas	Specify an esoteric device name for the allocation of sort or temporary areas.
Temporary Datasets	Specify an esoteric device name for the allocation of temporary datasets.
Allocation Prefix	The allocation prefix allows the user to specify the first two qualifiers of datasets that SSA uses for report and command generation output. The entry can be up to 17 characters in length and must contain a value that is going to be unique to each user. Generally, this is the userid of the user, however, some shops do not allow the use of the userid as the first qualifier. To allow for dynamic substitution of the userid, you can enter \$USERID\$ as either of the qualifiers. SSA will substitute the userid of the user where ever it finds the \$USERID\$ value. You can also enter \$SID\$ to dynamically substitute the system id the userid is currently logged on to.

Lines Per Page	Specify a value between 10 and 99 to signify how many lines per page you want on a report.
Report Menu Format	The Report Main Menu and all online generic search result screens have the ability to show a long or short format. 'Reports Main Menu' on page 65 has greater descriptions and feature lists of the various reports. The Online Generic Searches result screens in LONG form will display more of the information available from that particular ISPF table. Specify LONG for the long format or SHORT for the shorter displays. Also, you can change this setting from anywhere in ISPF by executing CLIST AALONG to make the displays use the LONG format or CLIST AASHORT to make the displays use the SHORT format.
Prompt for Print After Browse	When the Online Generic Searches, in various mode, page through screen displays of information, you can specify whether or not you want to be prompted to print that output. Specify "Y" if you wish to always be prompted or "N" if you do not want prompting.
Clear Select Fields After Processing	Numerous SSA displays of information are table based and a user can select one or multiple rows. This option will instruct SSA to either clear those selections when the function has been performed or to leave the selections after the function has been performed. Specify "Y" if you want the selections cleared or "N" if you want the selections to remain.
Execute Command Generation Commands Immediately after Creation in Batch	When you initiate the Command Generation functions in batch, the generated JCL causes the commands to be stored in your command output dataset but does not automatically execute those generated commands. This option allows the user to indicate if they want the commands executed immediately after generation or not. Specify "Y" if you want the commands executed immediately or "N" if you do not want the commands executed immediately. Below is a sample of the IKJEFT01 step that is appended to the command generation step to execute the generated commands. <pre> //* //* COMMANDS WILL BE EXECUTED AFTER CREATION //* //STEP020 EXEC PGM=IKJEFT01,DYNAMNBR=20,REGION=4096K //SYSTSPRT DD SYSOUT=* //SYSTSIN DD DISP=SHR, // DSN=IBMUSER.SSA.COMMAND.OUTPUT //*</pre>
ISPF Table Library	Specify the ISPF system table library in use on your system. This is required for batch execution of programs using ISPF services. The correct library will have two members in it ISPPROF and ISPSPROF.
ISPF Message Library	Specify the ISPF system message library in use on your system. This is required for batch execution of programs using ISPF services. The correct library will have at least one member: ISPV01.

SORT Library	Specify the library containing your system sort modules. This is required for JCL generation if your sort library is not link-listed on your system. If that is the case, enter YES on the “Steplib Sort Library” question.

Choose New Stored Configuration

Users can select a new stored configuration from the Choose New Stored Configuration screen. The Select a New Configuration option does a number of operations before displaying the stored configurations available to a user. Those operations are:

- The classes where the configurations are stored is retrieved from the AAOPTION configuration module.
- The stored configuration profile prefix is retrieved from the AAOPTION configuration module.
- The stored configurations meeting the profile prefix naming standard are extracted.
- Only those profiles that the user has READ access to will be displayed.

Note Users must be granted access to the stored configuration for it to be displayed and selectable. the display of stored configurations can be different for every user.

```

Configuration ----- SSA ----- Configuration
                        Choose New Stored Configuration
Command ==>
                                Scroll ==> CSR

Group Class in Use ==> GAA$RULE
Member Class in Use ==> MAA$RULE

                        Select One Configuration to Switch To

SELECT                                Stored Configurations
-----                                -----
_____ AACONFIG-DEFAULT
_____ AACONFIG-DEMO
_____ AACONFIG-SSA
_____ AACONFIG-TESTOUT
***** Bottom of data *****

```

A user can select one configuration to switch to. The switching process will prompt you before actually updating your ISPF profile as shown below. When you have chosen a configuration to switch to, SSA will purge your 'old' variables and replace them with the stored values. More importantly, SSA will free the SSA RACF/ISPF table library and allocate the new stored configuration library specified. This enables a user to switch to a different SSA offload file and operational settings dynamically as well. The change is immediate, therefore, the user does not have to exit the screens for the values to take effect.

Switch Prompt Sample

```
Configuration ----- SSA ----- SSA -----
Configuration

                        Choose New Stored Configuration

Command ==>

                        Use These Stored Variables (Y/N): N

                                                More:      +

SSA Libraries:
  RACF/ISPF Tables           ==> SSA.V130A.RACFDATA.ISPTLIB
  *The SCHEDULER Database    ==> SSA.SCHED.DATABASE
  *The SCHEDULER Historical  ==> SSA.SCHED.HISTORY
  *Load Library              ==> SSA.V130A.LOADLIB
  *ISPF Panel Library        ==> SSA.V130A.ISPPLIB
  *ISPF Message Library      ==> SSA.V130A.ISPMLIB
  *ISPF Skeleton JCL Library ==> SSA.V130A.ISPSLIB
  *ISPF CLIST Library        ==> SSA.V130A.ISPCLIB

  * = Entries only used for JCL, not for panel operations

Users Libraries:
  Report Output              ==> IBMUSER.TSCSSA.REPORT.OUTPUT
  Adhoc Command Output       ==> IBMUSER.TSCSSA.ADHOC.OUTPUT
  Command Generation Output  ==> IBMUSER.TSCSSA.COMMAND.OUTPUT

                        Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

Update Stored Configurations

```

Configuration ----- SSA ----- Configuration
                        Manipulate Stored Configurations
Command ==>
                                Scroll ==> CSR

Group Class in Use ==>GAA$RULE
Member Class in Use ==>MAA$RULE

                        Select the Configurations You Want to Manipulate

SELECT                                Stored Configurations
-----
_____ AACONFIG-DEFAULT
_____ AACONFIG-DEMO
_____ AACONFIG-SSA
_____ AACONFIG-TESTOUT
***** Bottom of data *****

```

```

Configuration ----- SSA ----- Configuration
Command ==>
                        Enter All Values for a Complete Stored Configuration.

Storage Profile ==> AACONFIG-DEFAULT

                                Use Your Changes (Y/N): N
                                                                More:  +

SSA Libraries:
RACF/ISPF Tables           ==> SSA.V130A.RACFDATA.ISPTLIB
The SCHEDULER Database     ==> SSA.SCHED.DATABASE
The SCHEDULER Historical   ==> SSA.SCHED.HISTORY
*Load Library              ==> SSA.V130A.LOADLIB
*ISPF Panel Library        ==> SSA.V130A.ISPPLIB
*ISPF Message Library      ==> SSA.V130A.ISPMLIB
*ISPF Skeleton JCL Library ==> SSA.V130A.ISPSLIB
*ISPF CLIST Library        ==> SSA.V130A.ISPCLIB

* = Entries only used for JCL, not for panel operations

Allocation Units:
Permanent Datasets         ==> SYSALLDA

                                Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

Use Your Changes Indicate if you want to use the changes you have made. When you indicate you want the changes, SSA will generate the RACF commands necessary to implement those changes. You must have either Global-Special or CLAUTH authority to the SSA classes to execute these commands. Below is a sample of the edit session you will be presented with. The first command is an RALTER command using the DELMEM (delete member) parameter to purge the old values. The second command is an RALTER command with the ADDMEM(add member) parameter to add the new values you have specified.

Process Generated Commands Screen

```
Process Generated Commands ----- SSA ----- Process Generated Commands
Command ==>                               Scroll ==> CSR
      Action Command                      Action Taken
      -----
      AAEXEC                            Execute Commands Immediately
      AABATCH                          Place Commands in Batch JCL
      AASCHED                          Schedule Commands
      AASTORE                          Store or Retrieve Commands

EDIT ----- TSGPA0.SSA.TEMP.JCL(CHNGCNFG) - 01.00----- COLUMNS 00001 00072
***** ***** Top of Data *****
=NOTE= COMMANDS ARE READY FOR EXECUTION
000001 /* MEMBER DELETE COMMANDS FOR OLD DEFINITIONS */
000002 RALTER GAA$RULE -
000003   AACONFIG-DEFAULT DELMEM(-
000004   AA_DATABASE=SSA.V130A.RACFDATA.ISPTLIB -
000005   PERM_ALLOC_UNIT=SYSALLDA -
000006   TEMP_ALLOC_UNIT=SYSALLDA -
000007   SORT_ALLOC_UNIT=SYSALLDA -
000008   ISPF_SYS_MLIB=SYS1.SISPMENU -
000009   ISPF_SYS_TLIB=SYS1.SISPTENU -
000010   AA_ISPCLIB=SSA.V130A.ISPCLIB -
000011   AA_ISPMLIB=SSA.V130A.ISPMLIB -
000012   AA_ISPPLIB=SSA.V130A.ISPPLIB -
```

Stored Configuration Parameters

The following table describes the parameters that can be defined to an SSA stored configuration:

Parameter	Explanation
AA_DATABASE=	Specify the SSA RACF/ISPF table dataset.
AA_ISPMLIB=	Specify the SSA ISPF message library.
AA_ISPPLIB=	Specify the SSA ISPF panel library.
AA_ISPSLIB=	Specify the SSA ISPF skeleton JCL library
AA_LOADLIB=	Specify the SSA APF authorized load library.
ALLOCATION_PREFIX=	The allocation prefix allows the user to control the first two qualifiers of datasets that SSA uses for report and command generation output. The entry can be up to 17 characters in length and must contain a value that is unique for each user. General this is the userid of the user, however, some shops do not allow the use of the userid as the first qualifier. To allow for dynamic substitution of the userid, you can enter \$USERID\$ as either of the qualifiers. SSA will substitute the userid of the user where ever it finds the \$USERID\$ value.

Parameter	Explanation
CLEAR_SELECTIONS=	Numerous SSA displays of information are table based and a user can select one or multiple rows. This option will instruct SSA to either clear those selections when the function has been performed or to leave the selections after the function has been performed. Specify “Y” if you want the selections cleared or “N” if you want the selections to remain.
EXECUTE_COMMAND S=	When you initiate the Command Generation functions in batch, the JCL generated causes the commands to be stored in your command output dataset but does not automatically execute those generated commands. This option allows the user to indicate if they want the commands executed immediately after generation or not. Specify “Y” if you want the commands executed immediately or “N” if you do not want the commands executed immediately.
ISPF_SYS_MLIB=	Specify the ISPF system message library in use on your system. This is required for batch execution of programs using ISPF services. The correct library will have at least one member: ISPV01.
ISPF_SYS_TLIB=	Specify the ISPF system table library in use on your system. This is required for batch execution of programs using ISPF services. The correct library will have two members in it: ISPPROF and ISPSPROF.
LINES_PER_PAGE=	Specify a value between 10 and 99 to signify how many lines per page you want on a report.
MENU_FORMAT=	The Report main menu and all online generic search result screens have the ability to show a long or short format. ‘Reports Main Menu’ on page 65 has greater descriptions and feature lists of the various reports. The Online Generic Searches result screens in LONG form will display more of the information available from that particular ISPF table. Specify LONG for the long format or SHORT for the shorter displays.
PERM_ALLOC_UNIT=	Specify an esoteric device name for allocation of permanent datasets.
PRINT_PROMPT=	When the Online Generic Searches, in various mode, page through screen displays of information, you can specify whether or not you want to be prompted to print that output. Specify “Y” if you wish to always be prompted or “N” if you do not want prompting

Parameter	Explanation
SCHED_DB=	Specify the SSA SCHEDULER database dataset (cluster name).
SCHED_HIST=	Specify the SSA SCHEDULER historical database dataset (cluster name).
SORT_ALLOC_UNIT=	Specify an esoteric device name for the allocation of sort or temporary areas.
STEPLIB_SORTLIB=	If you need to specify your sort library because it is not link-listed, enter “Y”.
SYSTEM_SORTLIB=	Specify the library containing your system sort modules. This is required for JCL generation if your sort library is not link-listed on your system.
TEMP_ALLOC_UNIT=	Specify an esoteric device name for the allocation of temporary datasets.

Below is an example of defining a new stored configuration using the default prefix AACONFIG-.

```
RDEFINE GAA$RULE AACONFIG-NEW-CONFIG-SAMPLE OWNER(SYS1) -
UACC(NONE) DATA('NEW CONFIGURATION SAMPLE DEFINITION') -
ADDMEM( -
AA_DATABASE=SSA.RACFDATA.ISPTLIB -
AA_ISPCLIB=SSA.ISPCLIB -
AA_ISPMLIB=SSA.ISPMLIB -
AA_ISPPLIB=SSA.ISPPLIB -
AA_ISPSLIB=SSA.ISPSLIB -
AA_LOADLIB=SSA.LOADLIB -
ALLOCATION_PREFIX=$USERID$ -
CLEAR_SELECTIONS=Y -
EXECUTE_COMMANDS=Y -
ISPF_SYS_MLIB=SYS1.SISPMENU -
ISPF_SYS_TLIB=SYS1.SISPTENU -
LINES_PER_PAGE=55 -
MENU_FORMAT=SHORT -
PERM_ALLOC_UNIT=SYSDA -
PRINT_PROMPT=Y -
SCHED_DB=SSA.SCHED.DATABASE -
SCHED_HIST=SSA.SCHED.HISTORY -
SORT_ALLOC_UNIT=SYSDA -
STEPLIB_SORTLIB=Y -
SYSTEM_SORTLIB=SYS1.SORTLIB -
TEMP_ALLOC_UNIT=SYSDA)
```

Notes

- 1 This is just a sample. You must insure that you put in the correct values.
- 2 You must permit a user to reference that configuration. Read access is required.

Change The SCHEDULER Task Settings

This option allows an administrator to change the settings being used by the SCHEDULER started task. This option is available to defined SSA administrators

```

Configuration ----- SSA ----- Configuration
                          Change The SCHEDULER Task Settings
Command ==>

Scan Interval:
Hour   (HH)   ==> 00
Minute (MM)   ==> 01
Second (MM)   ==> 00

Wakeup Interval:
Hour   (HH)   ==> 00
Minute (MM)   ==> 00
Second (MM)   ==> 30

History Retention ==> 007

SCHEDULER Jobcard and Comment Lines:
==> //AASTC01J JOB ( ),MSGCLASS=A,
==> // CLASS=A,REGION=4096,NOTIFY=&SYSUID
==> //*
==> //STEP010 EXEC PGM=IKJEFT01,DYNAMBR=20
==> //SYSTSPRT DD SYSOUT=*

Hit Enter to Continue      PF03=EXIT/PF01=HELP
More:      +

```

Scan Interval

The SCAN value specifies how often the started task scans The SCHEDULER database for scheduled items. Enter the amount of time in hours, minutes and seconds. The setting uses military time specifications, therefore, the hours can go up to 24 hours. It is recommended that you set the scanning interval to less than an hour. If you set a large scanning interval, then requests may not be done near their scheduled time, unless you instruct The SCHEDULER started task to scan the database immediately. See ‘Started Task Interface’ on page 273 for more details. The default scan interval is 1 minute.

Wakeup Interval

The WAKEUP interval dictates at what time interval will the started task ‘WAKEUP’ and check if any response to its WTOR (Write To Operator with Response) has been entered. It is recommended that this interval be set to a low value. A low value allows the started task to respond quickly to operator responses. For example, if the operator wants to terminate the task quickly and use the standard shutdown procedure, he/she would issue “T” for terminate to the WTOR from the started task. If the started task is set to WAKEUP at a large interval, the task may not shutdown for the length of time set in the WAKEUP interval. The default WAKEUP interval is 30 seconds.

History Retention The HISTORY interval indicates how long will the started task wait before archiving a completed task. It is recommended that the setting be set in proportion to the activity in The SCHEDULER. If you have a lot of activity, set the history retention period lower to archive the completed tasks more quickly. The default history retention period is 7 days.

SCHEDULER Jobcard and Comment Lines When a user enters commands as an event into The SCHEDULER, the started task submits those commands encapsulated in a IKJEFT01 step. The 20 lines available here are to code the encapsulation JCL. The JCL pictured above is the default JCL the task will use.

Note The last ‘actual’ line entered must be the DD SYSTSIN with DD * so that the commands encapsulated will be submitted successfully.

Last Line Example

```
//SYSTSIN DD *
```

Note Although this function will update the options records in The SCHEDULER database, the started task, if running, will not be aware of the changes until you tell it to refresh those settings. You must issue a “U” to the WTOR of the started task to update the settings. See ‘Started Task Interface’ on page 273. The settings can also be updated by recycling the started task.

Display SSA User or Group Authority

This option allows an administrator to display user or group access to SSA functions.

```

Configuration ----- SSA ----- Configuration
                          Main Menu

Option ==> 5

      ----- SSA -----
      Display a User or Groups SSA Authorities
      Command ==>

      Enter the user or group you want analyzed below.

      ==> IBMUSER

      Hit Enter to Continue          PF03=EXIT/PF01=HELP
    
```

```

6 Run Extract Job

      Current Configuration in Use ==> AACONFIG-DEFAULT

      Hit Enter to Continue          PF03=EXIT/PF01=HELP
    
```

Enter the user or group you want analyzed below Enter a valid userid or group whose access to secured SSA functions you want analyzed. Upon analyzing the entries authority, SSA displays a table of all the functions checked.

```

Configuration ----- SSA ----- Configuration
                          Display a User or Groups SSA Authorities
      Command ==>

                          Userid/Group ==> IBMUSER
                          -----

                          Group/Member Class in Use ==> GAA$RULE/MAA$RULE

                          Select Entries to Display Details

      Select      Function Description      Access
      -----
      _____ Access Report for Userids      ALLOWED
      _____ Access Report for Groups      ALLOWED
      _____ Dataset Profile Permission Report      ALLOWED
      _____ Ownership Report      ALLOWED
      _____ Group Connect Report      ALLOWED
      _____ Default Group Report      ALLOWED
      _____ Clauth/Group Special Report      ALLOWED
      _____ Never Logged On Report      ALLOWED
      _____ Global Attribute Report      ALLOWED
      _____ Non-Expiring Password Report      ALLOWED
      _____ True Dataset Authority Report      ALLOWED
      _____ Notify Report      ALLOWED
    
```

The analysis result display shows the title of the function and whether or not access is allowed or denied. Select as many functions as you like to view further details on the actual protection of the function. The details include the profile checked (retrieved from AAOPTION configuration module), the protecting RACF profile and the highest level of access allowed. Below is a sample of that display.

```
Configuration ----- SSA ----- Configuration
      Display a User or Groups SSA Authorities
Command ==>                               Scroll ==> CSR
                               Userid/Group ==> IBMUSER
                               -----
|
|----- SSA -----|
|      Display a User or Groups SSA Authorities      |
|  Function   - Access Report for Userids            |
|  Profiles:                                     |
|  Checked    - MEGASOLVE-SSA.REPORT001              |
|  Protecting - MEGASOLVE-SSA.REPORT*                |
|  Highest Access Allowed - ALTER                    |
|  Hit Enter to Continue          PF03=EXIT/PF01=HELP  |
|-----|
|  _____ Never Logged On Report                ALLOWED |
|  _____ Global Attribute Report                ALLOWED |
|  _____ Non-Expiring Password Report            ALLOWED |
|  _____ True Dataset Authority Report            ALLOWED |
|  _____ Notify Report                          ALLOWED |
```

Run Extract Job

This option allows an administrator to create the JCL to extract RACF information.

```

Configuration ----- SSA ----- Configuration
                          Main Menu

Option ==> 6

Run Extract Job ----- SSA ----- Run Extract Job
Command ==>

Do you want to use SSA's offload process or
the IBM offload process (A/I) I

Hit Enter to Continue          PF03=EXIT/PF01=HELP

4 Change The SCHEDULER Task Settings
5 Display a User or Groups SSA Authorities
6 Run Extract Job

Current Configuration in Use ==> AACONFIG-DEFAULT

Hit Enter to Continue          PF03=EXIT/PF01=HELP

```

Do you want to use
SSA's offload process or
the IBM offload process

Indicate if you want to use the SSA extract (AADBU00) or the IBM extract (IRRDBU00 program). Although both extract programs will produce the same result as far as SSA is concerned, you must choose which extract is appropriate for your shop. Below is a table showing the operating differences between the two extracts.

Function/Process	SSA Offload (AADBU00)	IBM Offload (IRRDBU00)
Access Necessary to Database	Access is only governed by SSA security rules	Must have UPDATE authority to database being offloaded
Screen Records Offloaded According to Security Rules	All profiles can be subjected to a security check allowing individualized and specialized offloads	Dumps all records
Offload Secondary or Backup Databases	No, only offloads live database	Can offload secondary or backup databases
Details Offload Status	Gives detailed totals of profiles and information offloaded	Gives limited totals

SSA Extract Sequence

Below is a demonstration of the SSA extract sequence.

- 1 Indicate you want the SSA extract process.

When you have chosen the SSA offload process, you will be presented with the Review Generated JCL screen from which you can Edit, View, Submit, Store and Schedule the JCL.

```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'IBMUSER.SSA.TEMP.JCL(BATCH)'

OPTION ==> E

Enter E to Edit the Generated JCL
V to View the Generated JCL
S to Submit the Generated JCL
ST to Store the Generated JCL
SC to Schedule the Generated JCL

Hit Enter to Continue PF03=EXIT/PF01=HELP

```

2 Submit the job to extract your RACF information.

It is important to note that all library references are taken from your current configuration settings, therefore, it is recommended that you edit the JCL and verify that the library references are appropriate. Also, remember that the SSA extract process directly extracts from the active database, therefore, you will never see a JCL reference to your RACF database. Below is a sample of the JCL generated and an detailed explanation.

```

//***** PLACE YOUR JOBCARD HERE *****/
//*
//*****
//**
//**          SMART SECURITY ADMINISTRATOR          **
//**
//**          VERSION V.V                          **
//**
//** (C) YYYY UNICOM SYSTEMS, INC.                  **
//**          ALL RIGHTS RESERVED                   **
//*****
//*
//* JCL CREATED BY USER01
//* JCL CREATED ON MM/DD/YYYY
//* JCL CREATED AT 14:37
//*
//* JOB FUNCTION: RUN_EXTRACT_JOBS
//*
//STEP010 EXEC PGM=AADBU00,REGION=4M
//STEPLIB DD DISP=SHR,
//          DSN=SSA.LOADLIB
//TEMPWK01 DD DSN=&TEMPWK01,DISP=(,PASS),
//          UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE),
//          DCB=(RECFM=VB,LRECL=4096,BLKSIZE=20480)
//TEMPWK02 DD DSN=&TEMPWK02,DISP=(,PASS),
//          UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE),
//          DCB=(RECFM=VB,LRECL=4096,BLKSIZE=20480)
//AAOUTPUT DD SYSOUT=*,DCB=(RECFM=FB,LRECL=133)
//*
//STEP020 EXEC PGM=IKJEFT01,DYNAMNBR=30,TIME=1440,REGION=0M
//SYSPROC DD DISP=SHR,

```



```

//          DSN=SSA.ISPCLIB
//ISPPROF DD DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
//          DCB=(LRECL=80,BLKSIZE=6160,RECFM=FB),UNIT=SYSDA
//ISPPLIB DD DISP=SHR,
//          DSN=SSA.ISPPLIB
//ISPSLIB DD DISP=SHR,
//          DSN=SSA.ISPSLIB
//ISPMLIB DD DISP=SHR,
//          DSN=SYS1.SISPMENU
//          DD DISP=SHR,
//          DSN=SSA.ISPMLIB
//ISPTLIB DD DISP=SHR,
//          DSN=SYS1.SISPTENU
//AADBTLIB DD DISP=SHR,
//          DSN=SSA.RACFDATA.ISPTLIB
//STEPLIB DD DISP=SHR,
//          DSN=SSA.LOADLIB
//ISPCTL1 DD DSN=&CNTL1,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//ISPCTL2 DD DSN=&CNTL2,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//SYSTSPRT DD SYSOUT=*,DCB=(BLKSIZE=19019,LRECL=133,RECFM=FBA)
//SYSPRINT DD SYSOUT=*,DCB=(BLKSIZE=20000,LRECL=200,RECFM=FBA)
//ISPLOG DD SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
//SYSOUT DD SYSOUT=*
//TEMPWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK03 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//MNTMLIB DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//IRRDBU00 DD DSN=&TEMPWK02,DISP=(OLD,DELETE)
//AASATM DD SYSOUT=*
//SYSTSIN DD *
ISPSTART PGM(AAMAINLD)
//*

```

Below is a brief explanation of the DDs and what they must reference:

STEP010

STEPLIB	Must reference the SSA APF Authorized load library.
TEMPWK01	Temporary - must have the following DCBs: RECFM=VB,LRECL=4096,BLKSIZE=20480
TEMPWK02	Temporary - Final output of extract program. The output from TEMPWK02 can be directed to a dataset if desired. It must have the following DCBs: RECFM=VB,LRECL=4096,BLKSIZE=20480. The output from TEMPWK02 is passed as a temporary to STEP020 where program AAMAINLD processes it.
AAOUTPUT	SYSOUT - SSA extract report output. The output from AAOUTPUT can be directed to a dataset if desired. It must have the following DCBs: RECFM=FB,LRECL=133.

STEP020

SYSPROC	Must reference the SSA CLIST library.
ISPPLIB	Must reference the SSA ISPF panel library.
ISPSLIB	Must reference the SSA skeleton JCL library.
ISPMLIB	Must reference the SSA ISPF message library and ISPF system message library.
ISPTLIB	Must reference the ISPF system table library.
AADBTLIB	Must reference the SSA RACF information table library.
STEPLIB	Must reference the SSA APF Authorized load library.
IRRDBU00	Must reference the output from STEP010 TEMPWK02. This is usually a temporary, however, if you decide to change STEP010 and direct TEMPWK02 to a dataset, you must change DD IRRDBU00 in STEP020 to reference the same dataset.
SYSTSIN	Must reference the control card in which the ISPF start program initiates the SSA program AAMAINLD. AAMAINLD loads the DBU00 output into ISPF tables.

RACF Extract Sequence

Below is a demonstration of the RACF extract sequence.

- 1
- You indicate you want the RACF process.
- 2
- When you have chosen the RACF offload process, you will be presented with a table display of your RACF Databases as shown below.

You must keep the following in mind:

- You must choose at least one database.
- You can only choose databases of the same status (that is, primary, secondary).

RACF Database Selection Display

```
Run Extract Job ----- SSA ----- Run Extract Job
Command ==> Scroll ==> CSR

Select the Datasets You Want to Utilize

SEL          RACF Database Dataset          Primary  Master  Active
-----
___  SYS1.RACF          YES          YES      YES
-----
___  SYS1.RACF.BACKUP   NO          YES      YES
-----
***** Bottom of data *****
```

- 3
- When you have selected the database(s) you want to be included as part of the extract process, you will be presented with the Review Generated JCL screen from which you can Edit, View, Submit, Store and Schedule the JCL.

You now can submit the job to extract your RACF information. It is important to note that all library references are taken from your current configuration settings, therefore, it is recommended that you edit the JCL and verify that the library references are appropriate. Also, remember that the SSA extract process directly extracts from the active database, therefore, you will never see a JCL reference to your RACF database. Below is a sample of the JCL generated and an detailed explanation.

```
//***** PLACE YOUR JOBCARD HERE *****/
//*
//*****
//**
//**          SMART SECURITY ADMINISTRATOR          **
//**
//**          VERSION V.V                          **
//**
//** (C) YYYY UNICOM SYSTEMS, INC.                  **
//**          ALL RIGHTS RESERVED                   **
//*****
//*
//* JCL CREATED BY USER01
//* JCL CREATED ON MM/DD/YYYY
//* JCL CREATED AT 14:37
//*
//* JOB FUNCTION: RUN_EXTRACT_JOBS
//*
//STEP010 EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT DD SYSOUT=*
//INDD1 DD DISP=SHR,
//          DSN=SYS1.RACF
//OUTDD DD DSN=&TEMPWK02,DISP=(,PASS),
//          UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE),
//          DCB=(RECFM=VB,LRECL=4096,BLKSIZE=20480)
//*
//STEP020 EXEC PGM=IKJEFT01,DYNAMNBR=30,TIME=1440,REGION=0M
//SYSPROC DD DISP=SHR,
//          DSN=SSA.ISPCLIB
//ISPPROF DD DSN=&PROFILE,DISP=(,PASS),SPACE=(TRK,(1,1,1)),
//          DCB=(LRECL=80,BLKSIZE=6160,RECFM=FB),UNIT=SYSDA
//ISPPLIB DD DISP=SHR,
//          DSN=SSA.ISPPLIB
//ISPSLIB DD DISP=SHR,
//          DSN=SSA.ISPSLIB
//ISPMLIB DD DISP=SHR,
//          DSN=SYS1.SISPMENU
//          DD DISP=SHR,
//          DSN=SSA.ISPMLIB
//ISPTLIB DD DISP=SHR,
//          DSN=SYS1.SISPTENU
//AADBTLIB DD DISP=SHR,
//          DSN=SSA.RACFDATA.ISPTLIB
//STEPLIB DD DISP=SHR,
//          DSN=SSA.LOADLIB
//ISPCTL1 DD DSN=&CNTL1,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//ISPCTL2 DD DSN=&CNTL2,DISP=(,PASS),UNIT=SYSDA,
//          DCB=(LRECL=80,BLKSIZE=800,RECFM=FB),
//          SPACE=(TRK,(5,5))
//SYSTSPRT DD SYSOUT=*,DCB=(BLKSIZE=19019,LRECL=133,RECFM=FBA)
```

```
//SYSPRINT DD SYSOUT=*,DCB=(BLKSIZE=20000,LRECL=200,RECFM=FBA)
//ISPLOG DD SYSOUT=*,DCB=(BLKSIZE=129,LRECL=125,RECFM=VA)
//SYSOUT DD SYSOUT=*
//TEMPWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//TEMPWK03 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//MNTMPLIB DD UNIT=SYSDA,SPACE=(CYL,(5,5),RLSE)
//IRRDBU00 DD DSN=&TEMPWK02,DISP=(OLD,DELETE)
//AASATM DD SYSOUT=*
//SYSTSIN DD *
ISPSTART PGM(AAMAINLD)
//*
```

Below is a brief explanation of the DDs and what they must reference:

STEP010

INDD1 INDD1 must reference a RACF Database Dataset. Please note the following information taken from the RACF Security Administration Manual - Section 7.1 The RACF Database Unload Utility (IRRDBU00):

IRRDBU00 processes either a copy of the RACF database, a backup RACF database, or the active RACF database. You must have UPDATE authority to the database. It is recommended that you run the utility against a recent copy of your RACF database using the NOLOCKINPUT parameter. While processing, IRRDBU00 serializes on one profile at a time (this is also the case in IRRUT100 processing). When IRRDBU00 has finished copying a profile, it releases the serialization. Consider this possible impact to performance if you select your active RACF database as input. Running IRRDBU00 against a copy of the database causes the least impact to system performance.

INDDn DD defines the RACF input data set that makes up the RACF database. The input data sets must have all of the characteristics of a RACF database; that is, they must be contiguous single-extent data sets, non-VIO, with a logical record length (LRECL) of 4096 and a record format (RECFM) of fixed (F). The n in INDDn refers to the location of the database name in the database name table (ICHRDSNT). If you have not split your RACF database, you only have to specify INDD1. If you have split your RACF database, you can unload each part with a separate utility invocation and specify INDD1 for the input data set, or you can unload all of the parts with one utility invocation.”

OUTDD Temporary - Final output of the RACF extract program. The output from TEMPWK02 can be directed to a dataset if desired. It must have the following DCBs:
RECFM=VB,LRECL=4096,BLKSIZE=20480. The output from TEMPWK02 is passed as a temporary to STEP020 where program AAMAINLD processes it.

STEP020

SYSPROC	Must reference the SSA CLIST library.
ISPPLIB	Must reference the SSA ISPF panel library.
ISPSLIB	Must reference the SSA skeleton JCL library.
ISPMLIB	Must reference the SSA ISPF message library and ISPF system message library.
ISPTLIB	Must reference the ISPF system table library.
AADBTLIB	Must reference the SSA RACF information table library.
STEPLIB	Must reference the SSA APF Authorized load library.
IRRDBU00	Must reference the output from STEP010 OUTDD. This is usually a temporary, however, if you decide to change STEP010 and direct OUTDD to a dataset, you must change DD IRRDBU00 in STEP020 to reference the same dataset.
SYSTSIN	Must reference the control card in which the ISPF start program initiates the SSA program AAMAINLD. AAMAINLD loads the DBU00 output into ISPF tables. rence the SSA ISPF panel library.

Unload Security

SSA allows an administrator to subjugate each profile being off-loaded to security rules that determine which profiles are off-loaded and stored in the SSA RACF/ISPF tables. The default, set in module AAOPTION, is for no security checking to be done except for the initial invocation of the process. The default profile checked is SSA.DATABASE.UNLOAD.

To activate profile security checking, which is done by either AADBU00 (SSA IRRDBU00-like program) or AAMAINLD (ISPF Table Loader), the administrator must change the UNLOAD_SECURITY field in the AAOPTION module to “NORMAL”. When this setting is changed, security checking is done distinctly by profile type. Below are examples of the security checking performed:

Groups	Group records are checked by the group. The default security profile checked is MEGASOLVE-SSA.UNLOAD.GROUP.<group>. If the user running the offload has READ access to that profile, the record is processed and stored.
Users	User records are checked by the user. The default security profile checked is MEGASOLVE-SSA.UNLOAD.USERID.<userid>. If the user running the offload has READ access to that profile, the record is processed and stored.
Dataset	Dataset records are checked by the HLQ (High Level Qualifier). The default security profile checked is MEGASOLVE-SSA.UNLOAD.DATASET.<hlq>. If the user running the offload has READ access to that profile, the record is processed and stored.
General Resources	General Resource records are checked by the resource class the profile is defined to. The default security profile checked is MEGASOLVE-SSA.UNLOAD.GENRSCE.<class>. If the user running the offload has READ access to that profile, the record is processed and stored.

Note Activating profile security checking can increase the load time.

Setting Up SSA Users And Administrators

The authority to perform certain functions in SSA is based on a users status. A SSA user can be classified as either a user or an administrator. Below is a list of the differences between a user and an administrator:

- An administrator can approve or deny entries put in The SCHEDULER that require approval.
- An administrator can enter entries into The SCHEDULER to run with the started tasks authority without approval.
- An administrator can run reports on all entries in The SCHEDULER.
- An administrator can manipulate the stored configurations for SSA users given they have the proper RACF authority to change the RACF profiles holding the stored configurations.
- An administrator can change the operational settings of The SCHEDULER started task.
- An administrator can display a users or groups authority to the many SSA features.
- An administrator can create the extract jobs and given they have the correct access to the profiles protecting the offload process, they can submit them.

A user's status is set by defining their userid as a member to the appropriate grouping profile. The default profile (defaults set in module AAOPTION - see 'AAOPTION Parameter Descriptions' on page 528 to change if desired) for users is MEGASOLVE-SSA.Users and the default profile for administrators is SSA.administrators. Below is a sample of the command to define user profiles and the addition of IBMUSER as a user of SSA.

Important security note

Be sure to define yourself (the installer) as an administrator. The administrator level of authority will be necessary to complete the installation. You must have either Global Special authority or CLAUTH authority to the SSA classes to issue these commands.

RACF Command Sample

```
RDEFINE GAA$RULE MEGASOLVE-SSA.USERS UACC(NONE) OWNER(SYS1) -
  DATA('GROUP PROFILE DEFINING THE USERS OF SSA') -
  ADDMEM(IBMUSER)

RDEFINE GAA$RULE MEGASOLVE-SSA.ADMINISTRATORS UACC(NONE) OWNER(SYS1) -
  DATA('GROUP PROFILE DEFINING THE ADMINISTRATORS OF SSA') -
  ADDMEM(IBMUSER)
```

Important security note

Remember that an administrator can submit commands and jobs to the SCHEDULER to run with the started tasks authority without approval. Thus, if the started task has a higher authority than the user with administrator status, that user can use the higher authority of the started task to run commands and jobs.

AAOPTION Configuration Module

SSA allows you to customize key security and operational settings at the software system level by modifying an Assembler CSECT - AAOPTION. Customization includes:

- RACF security classes used for configuration and security rule storage.
- Configuration storage naming conventions.
- Naming conventions for:
 - Security rules governing the definitions of users and administrators.
 - Security rules protecting the usage of the Userid Administration function.
 - Security rules protecting the usage of the Group Administration function.
 - Security rules protecting the usage of the Password Administration function.
 - Security rules protecting the usage of the Connect Administration function.
 - Security rules protecting the usage of the Dataset Profile Administration function.
 - Security rules protecting the usage of the Dataset Profile Permit Administration function.
 - Security rules protecting the usage of the General Resource Profile Administration function.
 - Security rules protecting the usage of the General Resource Profile Permit Administration function.
 - Security rules protecting the usage of the General Resource Profile Member Administration function.
 - Security rules protecting the usage of the User TSO and CICS Segment Administration functions.
 - Security rules protecting the usage of the Database offload function.
 - Security rules protecting the usage of the Reporting functions.
 - Security rules protecting the usage of the Online Generic Search functions.
 - Security rules protecting the usage of the Command Generation functions.
 - Security rules protecting the usage of The SCHEDULER function.
 - Security rules protecting the usage of the System Resource Monitor function.
 - Security rules protecting the usage of the Access Simulator function.
- Settings for CICS Direct Administration TCP/IP connection.
- Settings for panel dialog workings.

A copy of the source is in member AAOPTION of the SSA install library and an assembler job is in member ASSEMBLE (uses high-level assembler).

Parameter Rules

Below are the rules governing the syntax and format of the parameters in the AAOPTION module:

- No parameters can be deleted.
- All parameters must remain in the same order as shown below and in the sample provided.
- All parameter lengths must remain the same as shown below and in the sample provided.
- You can change some or all of the parameters.
- Check the explanation for the parameter you want to change before changing it to insure you are aware of the ramifications.

Below is a sample of the AAOPTION source. Following the source is a detailed explanation of all parameters.

```

AAOPTION CSECT
*****
**
**          SMART SECURITY ADMINISTRATOR
**
**          VERSION V.V
**
** (C) YYYY UNICOM SYSTEMS, INC.
**      ALL RIGHTS RESERVED
*****
**
*****
**          GENERAL SSA SETTINGS
**
*****
GROUP_CLASS      DC CL8 'GAA$RULE'          RULES AND SETTING GROUP CLASS
MEMBER_CLASS     DC CL8 'MAA$RULE'          RULES AND SETTING MEMBER CLASS
DEFAULT_CONFIG   DS 0CL50                   DEFAULT CONFIGURATION SET
CONFIG_PREFIX    DC CL9 'AACONFIG-'         CONFIGURATION PREFIX
                DC CL41 'DEFAULT'          CONFIGURATION NAME
ADMINISTRATORS   DC CL50 'MEGASOLVE-SSA.ADMINISTRATORS'
*
*                                     GROUP PROFILE WHERE EVERY USER
*                                     DEFINED AS A MEMBER IS GIVEN
*                                     PRODUCT ADMINISTRATIVE POWERS
USERS            DC CL50 'MEGASOLVE-SSA.USERS'
*
*                                     GROUP PROFILE WHERE EVERY USER
*                                     DEFINED AS A MEMBER IS NOTED AS
*                                     A VALID SSA USER
*****
**
**          GENERAL ADMINISTRATION SETTINGS
**
*****
COMMAND_CLASS    DS          0CL9          RESOURCE CLASS
                DC          XL1 '08'       CLASS LENGTH
                DC          CL8 'MAA$RULE'  SSA RESOURCE CLASS
COMMAND_SPECIALDC CL50 'MEGASOLVE-SSA.$SPECIAL$' PROF FOR SPECIAL
COMMAND_SREVOKE  DC          CL8 '$SREVOKE' GROUP FOR SUPER-REVOKE
*****
**
**          COMMAND PROFILES
**
*****
PSWCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$RESET'      PASSWORD ADMIN
CONCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$CONNECT'    CONNECT ADMIN
USRCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$USER'       USER ADMIN
GRPCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$GROUP'      GROUP ADMIN
DSNCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$DATASET'    DATASET ADMIN
RSCCMD_PROFILE   DC          CL50 'MEGASOLVE-SSA.$RESRCE'     RESOURCE ADMIN
UTSOCMD_PROFILE  DC          CL50 'MEGASOLVE-SSA.$UTSO'       USER TSO SEG ADMIN
UCICSCMD_PROFILE DC          CL50 'MEGASOLVE-SSA.$UCICS'      USER CICS SEG ADMIN
SPAREPROFILE1    DC          CL50 'MEGASOLVE-SSA.SPARE1'      RESERVED

```

```

SPAREPROFILE2 DC CL50'MEGASOLVE-SSA.SPARE2' RESERVED
SPAREPROFILE3 DC CL50'MEGASOLVE-SSA.SPARE3' RESERVED
SPAREPROFILE4 DC CL50'MEGASOLVE-SSA.SPARE4' RESERVED
SPAREPROFILE5 DC CL50'MEGASOLVE-SSA.SPARE5' RESERVED
*****
** **
** TCPIP CONSTANTS **
** **
*****
TCPIP_NAME DC CL8'TCIPIMVS'
DEFAULT_STC_IP DC CL15'205.185.254.3' DEFAULT IP ADDRESS
DEFAULT_STC_PT DC H'3500' DEFAULT PORT ADDRESS
SPARE1_STC_IP DC CL15'205.185.254.3 ' RESERVED
SPARE1_STC_PT DC H'3500' RESERVED
SPARE2_STC_IP DC CL15'205.185.254.3' RESERVED
SPARE2_STC_PT DC H'3500' RESERVED
SPARE3_STC_IP DC CL15'205.185.254.3 ' RESERVED
SPARE3_STC_PT DC H'3500' RESERVED
SPARE4_STC_IP DC CL15'205.185.254.3 ' RESERVED
SPARE4_STC_PT DC H'3500' RESERVED
SPARE5_STC_IP DC CL15'205.185.254.3 ' RESERVED
SPARE5_STC_PT DC H'3500' RESERVED
*****
** **
** DATABASE OFFLOAD SEGREGATION RULES **
** **
*****
UNLOAD_PROFILE DC CL50'MEGASOLVE-SSA.DATABASE.UNLOAD'
* PROFILE TO RUN DB UNLOAD PGMS
UNLOAD_SECURITY DC CL8'NOCHECK ' *SECURITY LEVEL FOR UNLOADING
* RACF DATABASE:
* NOCHECK = NO SECURITY CHECKING
* NORMAL = USER - CHECK BY USER
* NORMAL = GROUP - CHECK BY GROUP
* NORMAL = DATASET - CHECK BY HLQ
* NORMAL = GENERAL RESOURCE - CHECK BY CLASS
GROUP_UNLOAD_CHK DC CL50'MEGASOLVE-SSA.UNLOAD.GROUP'
USERID_UNLOAD_CHK DC CL50'MEGASOLVE-SSA.UNLOAD.USERID'
DATASET_UNLOAD_CHKDC CL50'MEGASOLVE-SSA.UNLOAD.DATASET'
GENRSCE_UNLOAD_CHKDC CL50'MEGASOLVE-SSA.UNLOAD.GENRSCE'
*****
** **
** REPORT SECURITY PROFILES **
** **
*****
REPORT001 DC CL50'MEGASOLVE-SSA.REPORT001'
REPORT002 DC CL50'MEGASOLVE-SSA.REPORT002'
REPORT003 DC CL50'MEGASOLVE-SSA.REPORT003'
REPORT004 DC CL50'MEGASOLVE-SSA.REPORT004'
REPORT005 DC CL50'MEGASOLVE-SSA.REPORT005'
REPORT006 DC CL50'MEGASOLVE-SSA.REPORT006'
REPORT007 DC CL50'MEGASOLVE-SSA.REPORT007'
REPORT008 DC CL50'MEGASOLVE-SSA.REPORT008'
REPORT009 DC CL50'MEGASOLVE-SSA.REPORT009'
REPORT010 DC CL50'MEGASOLVE-SSA.REPORT010'
REPORT011 DC CL50'MEGASOLVE-SSA.REPORT011'
REPORT012 DC CL50'MEGASOLVE-SSA.REPORT012'
REPORT013 DC CL50'MEGASOLVE-SSA.REPORT013'
REPORT014 DC CL50'MEGASOLVE-SSA.REPORT014'
REPORT015 DC CL50'MEGASOLVE-SSA.REPORT015'
REPORT016 DC CL50'MEGASOLVE-SSA.REPORT016'
REPORT017 DC CL50'MEGASOLVE-SSA.REPORT017'
REPORT018 DC CL50'MEGASOLVE-SSA.REPORT018'
REPORT019 DC CL50'MEGASOLVE-SSA.REPORT019'
REPORT020 DC CL50'MEGASOLVE-SSA.REPORT020'
REPORT021 DC CL50'MEGASOLVE-SSA.REPORT021'
REPORT022 DC CL50'MEGASOLVE-SSA.REPORT022'
REPORT023 DC CL50'MEGASOLVE-SSA.REPORT023'
REPORT024 DC CL50'MEGASOLVE-SSA.REPORT024'
REPORT025 DC CL50'MEGASOLVE-SSA.REPORT025'
SPAREREPORT1 DC CL50'MEGASOLVE-SSA.SPARE1'
SPAREREPORT2 DC CL50'MEGASOLVE-SSA.SPARE2'
SPAREREPORT3 DC CL50'MEGASOLVE-SSA.SPARE3'
SPAREREPORT4 DC CL50'MEGASOLVE-SSA.SPARE4'
SPAREREPORT5 DC CL50'MEGASOLVE-SSA.SPARE5'
*****
** **
** ONLINE GENERIC SEARCH SECURITY PROFILES **

```

```

**
*****
GENERALUSER      DC      CL50'MEGASOLVE-SSA.ONLGEN.USER'
USERTSO          DC      CL50'MEGASOLVE-SSA.ONLGEN.USERTSO'
USERCICS         DC      CL50'MEGASOLVE-SSA.ONLGEN.USERCICS'
USERDFP          DC      CL50'MEGASOLVE-SSA.ONLGEN.USERDFP'
USERLANGUAGE     DC      CL50'MEGASOLVE-SSA.ONLGEN.USERLANGUAGE'
USERPERPARM      DC      CL50'MEGASOLVE-SSA.ONLGEN.USERPERPARM'
USERWORKATTR     DC      CL50'MEGASOLVE-SSA.ONLGEN.USERWORKATTR'
USERNETVIEW      DC      CL50'MEGASOLVE-SSA.ONLGEN.USERNETVIEW'
USEROMVS         DC      CL50'MEGASOLVE-SSA.ONLGEN.USEROMVS'
USERDCE          DC      CL50'MEGASOLVE-SSA.ONLGEN.USERDCE'
USERRRSF         DC      CL50'MEGASOLVE-SSA.ONLGEN.USERRRSF'
USERCONNECTS     DC      CL50'MEGASOLVE-SSA.ONLGEN.USERCONNECTS'
USERCLAUTH       DC      CL50'MEGASOLVE-SSA.ONLGEN.USERCLAUTH'
USERSECCATS      DC      CL50'MEGASOLVE-SSA.ONLGEN.USERSECCATS'
GENERALGROUP     DC      CL50'MEGASOLVE-SSA.ONLGEN.GROUP'
GROUPDFP         DC      CL50'MEGASOLVE-SSA.ONLGEN.GROUPDFP'
GROUPOMVS        DC      CL50'MEGASOLVE-SSA.ONLGEN.GROUPOMVS'
GENERALDATASET   DC      CL50'MEGASOLVE-SSA.ONLGEN.DATASET'
DATASETPERMS     DC      CL50'MEGASOLVE-SSA.ONLGEN.DATASETPERMS'
DATASETSECCATS   DC      CL50'MEGASOLVE-SSA.ONLGEN.DATASETSECCATS'
GENERALRSC       DC      CL50'MEGASOLVE-SSA.ONLGEN.RSC'
RSCPERMS         DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCPERMS'
RSCMEMBERS       DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCMEMBERS'
RSCSESSION       DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCSESSION'
RSCDLF           DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCDLF'
RSCSTC           DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCSTC'
RSCSYSVIEW       DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCSYSVIEW'
RSCSECCATS       DC      CL50'MEGASOLVE-SSA.ONLGEN.RSCSECCATS'
SPAREGENERIC1    DC      CL50'MEGASOLVE-SSA.ONLGEN.SPARE1'
SPAREGENERIC2    DC      CL50'MEGASOLVE-SSA.ONLGEN.SPARE2'
SPAREGENERIC3    DC      CL50'MEGASOLVE-SSA.ONLGEN.SPARE3'
SPAREGENERIC4    DC      CL50'MEGASOLVE-SSA.ONLGEN.SPARE4'
SPAREGENERIC5    DC      CL50'MEGASOLVE-SSA.ONLGEN.SPARE5'
*****
**
**  COMMAND GENERATION SECURITY PROFILES
**
*****
REPUSERID        DC      CL50'MEGASOLVE-SSA.REPLICATE.USERID'
REPGROUP         DC      CL50'MEGASOLVE-SSA.REPLICATE.GROUP'
REPDSNPROF       DC      CL50'MEGASOLVE-SSA.REPLICATE.DSNPROF'
REPRSCPROF       DC      CL50'MEGASOLVE-SSA.REPLICATE.RSCPROF'
REPRSCCLAS       DC      CL50'MEGASOLVE-SSA.REPLICATE.RSCCLAS'
TRNUSERID        DC      CL50'MEGASOLVE-SSA.TRANSFER.USERID'
TRNGROUP         DC      CL50'MEGASOLVE-SSA.TRANSFER.GROUP'
TRNDSNPROF       DC      CL50'MEGASOLVE-SSA.TRANSFER.DSNPROF'
TRNRSCPROF       DC      CL50'MEGASOLVE-SSA.TRANSFER.RSCPROF'
TRNRSCCLAS       DC      CL50'MEGASOLVE-SSA.TRANSFER.RSCCLAS'
TRNOWNER         DC      CL50'MEGASOLVE-SSA.TRANSFER.OWNER'
TRNNOTIFY        DC      CL50'MEGASOLVE-SSA.TRANSFER.NOTIFY'
REMUSER          DC      CL50'MEGASOLVE-SSA.REMOVE.USERID'
REMGROUP         DC      CL50'MEGASOLVE-SSA.REMOVE.GROUP'
REMOBSOLETE      DC      CL50'MEGASOLVE-SSA.REMOVE.OBSOLETE'
SPARECOMMAND1    DC      CL50'MEGASOLVE-SSA.SPARE1'
SPARECOMMAND2    DC      CL50'MEGASOLVE-SSA.SPARE2'
SPARECOMMAND3    DC      CL50'MEGASOLVE-SSA.SPARE3'
SPARECOMMAND4    DC      CL50'MEGASOLVE-SSA.SPARE4'
SPARECOMMAND5    DC      CL50'MEGASOLVE-SSA.SPARE5'
*****
**
**  THE SCHEDULER SECURITY PROFILES
**
*****
SCHEDGENERAL     DC      CL50'MEGASOLVE-SSA.SCHEDULE.GENERAL'
*****
**
**  SYSTEM RESOURCEMONITOR SECURITY PROFILES
**
*****
MONITORGENERAL   DC      CL50'MEGASOLVE-SSA.MONITOR.REPORTS'
MONAPF           DC      CL50'MEGASOLVE-SSA.MONITOR.APF'
MONLLT           DC      CL50'MEGASOLVE-SSA.MONITOR.LLT'
MONLPA           DC      CL50'MEGASOLVE-SSA.MONITOR.LPA'
MONCDT           DC      CL50'MEGASOLVE-SSA.MONITOR.CDT'
MONPPT           DC      CL50'MEGASOLVE-SSA.MONITOR.PPT'
MONGRI           DC      CL50'MEGASOLVE-SSA.MONITOR.RAC'

```

```

MONEXT          DC          CL50 'MEGASOLVE-SSA.MONITOR.RAC'
MONRDS          DC          CL50 'MEGASOLVE-SSA.MONITOR.RAC'
MONRAU          DC          CL50 'MEGASOLVE-SSA.MONITOR.RAU'
MONRFR          DC          CL50 'MEGASOLVE-SSA.MONITOR.RFR'
MONSMF          DC          CL50 'MEGASOLVE-SSA.MONITOR.SMF'
MONSTC          DC          CL50 'MEGASOLVE-SSA.MONITOR.STC'
MONSVC          DC          CL50 'MEGASOLVE-SSA.MONITOR.SVC'
MONATT          DC          CL50 'MEGASOLVE-SSA.MONITOR.ATT'
*****
**
**  ACCESS SIMULATOR SECURITY PROFILES
**
*****
ACCSIMGENERAL   DC          CL50 'MEGASOLVE-SSA.ACCESS.SIMULATOR'
*****
**
**  PANEL DIALOG CONTROL FLAGS
**
*****
NOPOP_IN_MAIN_START  DC      CL1 'N'  TURNS OFF POPUP PANELS IN AASTART
NO_CONTROL_ERRORS_RETURNDC  CL1 'N'  TURNS OFF CONTROL ERRORS RETURN
*****
**
**  MISCELLANEOUS CONTROL FLAGS
**
*****
STC_SCAN_MESSAGES   DC      CL1 'Y'  TURNS OFF SCAN START/END MSGS
EUROPE_DATE          DC      CL1 'N'  SETS EUROPEAN DATE FORMAT
**
AA_VERSION            DC      C'Vv.v'
AA_COPY_RITE          DC      C'COPYRIGHT YYYY UNICOM SYSTEMS,INC.'
END

```

AAOPTION Parameter Descriptions

Below is a table detailing each parameter. Be sure to read the parameter rules before changing any.

Label	Change Notes
GROUP_CLASS	Must reference the grouping class defined for SSA (See installation 'Step 7: Define RACF Classes for SSA Security' on page 40).
MEMBER_CLASS	Must reference the member class defined for SSA (See installation 'Step 7: Define RACF Classes for SSA Security' on page 40).
DEFAULT_CONFIG	References the default SSA configuration profile. Profile is defined to the grouping class. DEFAULT_CONFIG is a construct of the Config_Prefix and the configuration name. Must be defined to RACF for new users (See 'Update Stored Configurations' on page 507 for details on defined stored configurations).
CONFIG_PREFIX	Prefix for all configuration profiles. Used by SSA configuration options 2 and 3 to determine actual stored configurations (See 'Update Stored Configurations' on page 507 for details on defined stored configurations).

Label	Change Notes
ADMINISTRATORS	Grouping profile whose members are RACF userids noted as administrators in SSA.
USERS	Grouping profile whose members are RACF userids noted as users in SSA.
COMMAND_CLASS	Resource class used for SSA internal security, TSO Direct Administration, and CICS Direct Administration security. Change the XL1'08' to the character length of the class name specified. DO NOT change the length specified on the class (CL8). Highly recommended that the class remain the member class defined for SSA.
COMMAND_SPECIAL	Profile protecting the use of TSO Direct Administration and CICS Direct Administration functions against userids who have Global-Special (see TSO Direct Administration -Security or CICS Direct Administration - Security).
COMMAND_SREVOKE	Defined RACF group for the Password Administration and Connect Administration SuperRevoke function (see TSO or CICS Direct Administration chapters).
PSWCMD_PROFILE	Profile prefix used for Password Administration rule construction (see TSO or CICS Direct Administration Security sections).
CONCMD_PROFILE	Profile prefix used for Connect Administration rule construction (see TSO or CICS Direct Administration Security sections.).
USRCMD_PROFILE	Profile prefix used for Userid Administration rule construction (see TSO or CICS Direct Administration Security sections).
GRPCMD_PROFILE	Profile prefix used for Group Administration rule construction (see TSO or CICS Direct Administration Security sections).
DSNCMD_PROFILE	Profile prefix used for Dataset Profile and Dataset Permit Administration rule construction (see TSO or CICS Direct Administration Section Security).
RSCCMD_PROFILE	Profile prefix used for General Resource Profile, Permit and Member Administration rule construction (see TSO or CICS Direct Administration Section Security).
UTSOCMD_PROFILE	Profile prefix used for User TSO Segment rule construction (see TSO or CICS Direct Administration Section Security).

Label	Change Notes
UCICSCMD_PROFILE	Profile prefix used for User CICS Segment rule construction (see TSO or CICS Direct Administration Section Security).
SPAREPROFILE1 through SPAREPROFILE5	Reserved for future SSA-CDA or SSA-TDA functions
TCPIP_NAME	Name of the TCP/IP started task on the local system.
DEFAULT_STC_IP	IP address of the TCP/IP started task on the local system.
DEFAULT_STC_PT	PORT address assigned to the SSA-CDA started task (AASTC02).
SPARE1_STC_PT through SPARE5_STC_PT	Reserved for future TCP/IP connections
UNLOAD_PROFILE	Profile protecting the SSA database unload function. User must have access to this profile to use the unload function
UNLOAD_SECURITY	Setting that activates or deactivates security checking during the extract loading process. NOCHECK turns off checking NORMAL activates checking The checking, if active, is done as follows: USERS by userid GROUPS by group DATASET by HLQ GENERAL RESOURCE by class
GROUP_UNLOAD_CHK	Prefix for profile built to check a users access to group profiles. The group is added as a suffix to the prefix before checking takes place.
USERID_UNLOAD_CHK	Prefix for profile built to check a users access to user profiles. The userid is added as a suffix to the prefix before checking takes place.
DATASET_UNLOAD_CHK	Prefix for profile built to check a users access to dataset profiles. The HLQ of the dataset profile is added as a suffix to the prefix before checking takes place.

Label	Change Notes
GENRSCE_UNLOAD_CHK	Prefix for profile built to check a users access to general resource profiles. The resource class is added as a suffix to the prefix before checking takes place.
REPORT001	Profile protecting report 1 on menu. Report: Access Report for Userids
REPORT002	Profile protecting report 2 on menu. Report: Access Report for Groups
REPORT003	Profile protecting report 3 on menu. Report: Dataset Profile Permission Report
REPORT004	Profile protecting report 4 on menu. Report: Ownership Report
REPORT005	Profile protecting report 5 on menu. Report: Group Connect Report
REPORT006	Profile protecting report 6 on menu. Report: Default Group Report
REPORT007	Profile protecting report 7 on menu. Report: Clauth/Group Special Report
REPORT008	Profile protecting report 8 on menu. Report: Never Logged On Report
REPORT009	Profile protecting report 9 on menu. Report: Global Attribute Report
REPORT010	Profile protecting report 10 on menu. Report: Non-Expiring Password Report
REPORT011	Profile protecting report 11 on menu. Report: True Dataset Authority Report
REPORT012	Profile protecting report 12 on menu. Report: Notify Report
REPORT013	Profile protecting report 13 on menu. Report: Break in Ownership Report
REPORT014	Profile protecting report 14 on menu. Report: User/Group Repetitive Permits Report
REPORT015	Profile protecting report 15 on menu. Report: Group Statistics Report
REPORT016	Profile protecting report 16 on menu. Report: Obsolete Entry Report
REPORT017	Profile protecting report 17 on menu. Report: Where a User/Group Is Not in an Access List Report

Label	Change Notes
REPORT018	Profile protecting report 18 on menu. Report: General Resource Class Permission Report
REPORT019	Profile protecting report 19 on menu. Report: Userid Statistics Report
REPORT020	Profile protecting report 20 on menu. Report: Dataset Profile and Permission Report
REPORT021	Profile protecting report 21 on menu. Report: RACF to Master Catalog Comparison Report
REPORT022	Profile not currently in use
REPORT023	Profile not currently in use
REPORT024	Profile not currently in use
REPORT025	Profile not currently in use
SPAREREPORT1 through SPAREREPORT5	Reserved for future reports
GENERALUSER	Profile protecting Online Generic Searches option: General Userid
USERTSO	Profile protecting Online Generic Searches option: Userid TSO Segment
USERCICS	Profile protecting Online Generic Searches option: Userid CICS Segment
USERDFP	Profile protecting Online Generic Searches option: Userid DFP Segment
USERLANGUAGE	Profile protecting Online Generic Searches option: Userid Language Segment
USEROPERPARM	Profile protecting Online Generic Searches option: Userid OPERPARM Segment
USERWORKATTR	Profile protecting Online Generic Searches option: Userid WORKATTR Segment
USERNETVIEW	Profile protecting Online Generic Searches option: Userid NETVIEW Segment
USEROMVS	Profile protecting Online Generic Searches option: Userid OMVS Segment
USERDCE	Profile protecting Online Generic Searches option: Userid DCE Segment
USERRRSF	Profile protecting Online Generic Searches option: RRSF Associations
USERCONNECTS	Profile protecting Online Generic Searches option: Connects

Label	Change Notes
USERCLAUTH	Profile protecting Online Generic Searches option: CLAUTH Authorities
USERSECCATS	Profile protecting Online Generic Searches option: Userid Security Categories
GENERALGROUP	Profile protecting Online Generic Searches option: General Group
GROUPDFP	Profile protecting Online Generic Searches option: Group DFP Segment
GROUPOMVS	Profile protecting Online Generic Searches option: Group OMVS Segment
GENERALDATASET	Profile protecting Online Generic Searches option: General Dataset
DATASETPERMS	Profile protecting Online Generic Searches option: Dataset Permissions
DATASETSECCATS	Profile protecting Online Generic Searches option: Dataset Security Categories
GENERALRSCE	Profile protecting Online Generic Searches option: General Resource
RSCEPERMS	Profile protecting Online Generic Searches option: General Resource Permissions
RSCEMEMBERS	Profile protecting Online Generic Searches option: General Resource Members
RSCSESSION	Profile protecting Online Generic Searches option: General Resource Session Segment
RSCEDLF	Profile protecting Online Generic Searches option: General Resource DLFDATA Segment
RSCESTC	Profile protecting Online Generic Searches option: General Resource STDATA Segment
RSCSYSVIEW	Profile protecting Online Generic Searches option: General Resource SystemView Segment
RSCSECCATS	Profile protecting Online Generic Searches option: General Resource Security Categories
SPAREGENERIC1 through SPAREGENERIC5	Reserved for future Online Generic Search functions
REPUSEID	Profile protecting Command Generation option: Replicate Userid Profile
REPGROUP	Profile protecting Command Generation option: Replicate Group Profile
REPDSNPROF	Profile protecting Command Generation option: Replicate Dataset Profile

Label	Change Notes
REPRSCPROF	Profile protecting Command Generation option: Replicate General Resource Profile
REPRSCCLAS	Profile protecting Command Generation option: Replicate General Resource Class
TRNUSERID	Profile protecting Command Generation option: Transfer Userid Profile
TRNGROUP	Profile protecting Command Generation option: Transfer Group Profile
TRNDSNPROF	Profile protecting Command Generation option: Transfer Dataset Profile
TRNRSCPROF	Profile protecting Command Generation option: Transfer General Resource Profile
TRNRSCCLAS	Profile protecting Command Generation option: Transfer General Resource Class
TRNOWNER	Profile protecting Command Generation option: Transfer Ownership
TRNNOTIFY	Profile protecting Command Generation option: Transfer Notifications
REMUSER	Profile protecting Command Generation option: Remove All References to a Userid
REMGROUP	Profile protecting Command Generation option: Remove All References to a Group
REMOBSOLETE	Profile protecting Command Generation option: Remove Obsolete Entries
SPARECOMMAND1 through SPARECOMMAND5	Reserved for future Command Generation functions
SCHEDGENERAL	Profile protecting The SCHEDULER function. Users must be permitted to this profile to enter requests into The SCHEDULER.
MONITORGENERAL	Profile protecting the initiating of the System Resource Monitor screen dialog. This profile does not restrict execution of the System Resource Monitor reporting programs.
MONAPF	Profile protecting System Resource Monitor option: APF -Authorized Program Facility
MONLLT	Profile protecting System Resource Monitor option: LLT -Link List Table
MONLPA	Profile protecting System Resource Monitor option: LPA -Link Pack Area

Label	Change Notes
MONCDT	Profile protecting System Resource Monitor option: CDT -Class Descriptor Table
MONPPT	Profile protecting System Resource Monitor option: PPT -Program Properties Table
MONGRI	Profile protecting System Resource Monitor option: GRI -General RACF Information
MONEXT	Profile protecting System Resource Monitor option: EXT -RACF Installation Exits
MONRDS	Profile protecting System Resource Monitor option: RDS -RACF Database Datasets
MONRAU	Profile protecting System Resource Monitor option: RAU -RACF Authorized Caller Table
MONRFR	Profile protecting System Resource Monitor option: RFR -RACF Router Table
MONSMF	Profile protecting System Resource Monitor option: SMF -System Management Facility
MONSTC	Profile protecting System Resource Monitor option: STC -Started Task Table
MO N SVC	Profile protecting System Resource Monitor option: SVC -Supervisor Calls
MONATT	Profile protecting System Resource Monitor option: ATT -Authorized TSO Tables
ACCSIMGENERAL	Profile protecting the Access Simulator function
NOPOP_IN_MAIN_START	Setting activates or deactivates the popup notifications when AASTART is started. This enables jump functions to work (that is, =a;2;1 to jump to Online Generic Searches option - General Userid Information).
NO_CONTROL_ERRORS_RETURN	Setting activates or deactivates the invocation of “CONTROL ERRORS RETURN” within SSA ISPF dialog programs. This is only used for debugging purposes.
STC_SCAN_MESSAGES	Setting activates or deactivates the Start Scan messages produced by The SCHEDULER started task. It is recommended that the messaging be left on (default is on - “Y”) unless you are concerned about taking up spool space.
EUROPE-DATE	Not currently used. Setting will activate the reformatting of the full Gregorian dates from MM-DD-YYYY to DD-MM-YYYY. All Gregorian dates with the format YYYY-MM-DD will not change.
AA-VERSION	SSA version - should not be changed by user.
AA_COPY_RITE	Copyright notice - Do not change



APPENDIX A

SSA Report Examples

This appendix provides samples of each SSA report available from Option 1 of the Main Menu.

SSA release and dates in figures and code examples

In the report examples in this appendix, the SSA release number is indicated by V.V. Similarly, dates are indicated by the formats MM/DD/YYYY, MM/DD/YYYY, YYYY-MM-DD, YY.DDD, and so on.

Access Report for UserIDs - AAREP001

1

Date: MM/DD/YYYY

Time: 09:09

Page: 1

SSA Version V.V

User Access Report for IBMUSER

UserID: IBMUSER

Name: GENERAL DFLT USER

Default Group: SYS1

Owner: IBMUSER

Create-Date: MM/DD/YYYY

Last-Used-Date: MM/DD/YYYY

Passdate: MM/DD/YYYY

Global Attributes

Special: Yes

Operations: Yes

Auditor: Yes

Revoke: No

Grpacc: No

Uaudit: No

Oidcard: No

ADSP: No

Connect Groups

Group: SYSCTLG

Owner: IBMUSER

Authority: JOIN

UACC: READ

Special: No

Operations: No

Revoke: No

Group: SYS1

Owner: SYS1

Authority: JOIN

UACC: READ

Special: No

Operations: No

Revoke: No

Group: VSAMDSET

Owner: IBMUSER

Authority: JOIN

UACC: READ

Special: No

Operations: No

Revoke: No

1

Date: MM/DD/YYYY

Time: 09:09

Page: 2

SSA Version V.V

User Access Report for IBMUSER

Permission Access -- Conditional --

Class Profile

Type

Volume

Reason

Access Entry

Type

Level

Class Entity

ACCTNUM ACCT#

* PERMIT

*

Standard

READ

ACICSPCT **

USER

IBMUSER

Standard

ALTER

APPL IMSP

* PERMIT

*

Standard

READ

CCICSCMD *.*

USER

IBMUSER

Standard

ALTER

Access Report for Groups - AAREP002

Date: MM/DD/YYYY

Time: 09:10

SSA Version V.V

Group Access Report for SYS1

Group: SYS1

Superior Group:

Owner: IBMUSER

Connected Users

User: AASTC01

Owner: SYS1

Authority: USE

UACC: NONE

Special: No

Operations: No

Revoke: No

Sub-Groups

DEVL

NONIBM

OTHERS

PROD

SYSTEM

TEST

TESTREM2 USERS

1

Date: MM/DD/YYYY

Time: 09:10

SSA Version V.V

Group Access Report for SYS1

Class

Profile

Type

Volume

Reason

Access Entry

Permission Type

Access Level

Conditional Class Entity

ACCTNUM

ACCT#

* PERMIT

*

Standard

READ

ACICSPCT

**

* PERMIT

*

Standard

ALTER

APPL

IMSP

* PERMIT

*

Standard

READ

CCICSCMD

.

* PERMIT

*

Standard

READ

CCICSCMD

.

Generic

OWNER

CCICSCMD

..*

* PERMIT

*

Standard

READ

CCICSCMD

..*

Generic

OWNER

CCICSCMD

**

* PERMIT

*

Standard

READ

CCICSCMD

**

Generic

OWNER

CONNECT

AASTC01

(STARTED TASK

)

OWNER

SYS1

CONNECT

APPC

(STARTED TASK

)

OWNER

SYS1

Page: 1

Page: 2

Dataset Profile Permission Report - AAREP003

1							Page: 1	
Date: MM/DD/YYYY								
Time: 09:11								
SSA Version V.V								
Dataset Profile Permission Report for HLQ - SYS1								
Dataset Profile		Type	Volume	Access Entry	Access Level	Access Type	Name (If User)	Conditional Class Entity
-----								-----
SYS1.TESTOUT.THE.MASTER.*		Generic		USER01	ALTER	USER	ENDUSER, JOSEPH	
SYS1.*		Generic		BMLTD	READ	GROUP		
SYS1.*		Generic		ABC	READ	GROUP		
SYS1.*		Generic		WALK	READ	GROUP		
SYS1.*		Generic		MEGA	ALTER	GROUP		
SYS1.*		Generic		STARTASK	ALTER	GROUP		
SYS1.*		Generic		NEWMEGA	ALTER	GROUP		

Ownership Report - AAREP004

1

Date: MM/DD/YYYY|
Time: 09:13

Page: 1

SSA Version V.V
Ownership Report for USER01

Class	Profile	Type	Volume	Create Date	UACC	Is There a Break in Ownership?
CONNECT	TSTU011 STRICTLY TEST USERS		GRP-TSTG005			Yes, Group - TSTG005
DATASET	BACKUP.SENT01.G0001V00	Discrete	B00001	MM/DD/YY	NONE	Yes, HLQ - BACKUP
DATASET	SYS1.TESTOUT.THE.MASTER.*	Generic		MM/DD/YY	NONE	Yes, HLQ - SYS1
DATASET	TSTADDG.V421A.LOADLIB	Generic		MM/DD/YY	NONE	Yes, HLQ - TSTADDG
DATASET	TSTADDG.*	Generic		MM/DD/YY	NONE	Yes, HLQ - TSTADDG
DATASET	TSTGS31.*	Generic		MM/DD/YY	NONE	Yes, HLQ - TSTGS31
TERMINAL	TESTTEST	Discrete		MM/DD/YY	NONE	-- Not Applicable --
DLFCLASS	TESTDLF9	Discrete		MM/DD/YY	NONE	-- Not Applicable --

Group Connect Report - AAREP005

1					Date: MM/DD/YYYY			Page: 1	
					Time: 09:13				
					SSA Version V.V				
					Group Connect Report for SYS1				
RACF		Profile		Revoke		Resume			
UserID	Name	Owner	Authority	UACC	Date	Date	----- Group Attributes -----		

AASTC01	STARTED TASK	SYS1	USE	NONE					
APPC	STARTED TASK	SYS1	USE	NONE					
ASCH	STARTED TASK	SYS1	USE	NONE					
ASCHINT	STARTED TASK	SYS1	USE	NONE					
BLSJPRMI	#####	SYS1	USE	NONE					
CICSTART	#####	SYS1	USE	NONE					
CICSUSER	#####	SYS1	USE	NONE					
DSN3UR00	STARTED TASK	SYS1	USE	NONE					
DUMPSRV	STARTED TASK	SYS1	USE	NONE					
EZAFTPAP	#####	SYS1	USE	NONE					

Default Group Report - AAREP006

1									
Date: MM/DD/YYYY							Page:		1
Time: 09:14									
SSA Version V.V									
Default Group Report for STARTASK									
RACF		Profile	Create	Last-Used		Password	Userid		
UserID	Name	Owner	Date	Date	Passdate	Interval	Status	-----	Connect Groups -----
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
AASTC01	STARTED TASK	STARTASK	MM/DD/YY	MM/DD/YY	*****	180		SYS1	
APPC	STARTED TASK	STARTASK	MM/DD/YY	MM/DD/YY	*****	180		SYS1	
ASCH	STARTED TASK	STARTASK	MM/DD/YY	MM/DD/YY	*****	180		SYS1	
BLSJPRMI	#####	STARTASK	MM/DD/YY	MM/DD/YY	*****	180		SYS1	
CICSTART	#####	STARTASK	MM/DD/YY	MM/DD/YY	*****	180		SYS1	
DCEKERN	#####	STARTASK	MM/DD/YY	*****	*****	180		DCEGRP	

Clauth/Group Special Report - AAREP007

1

Date: MM/DD/YYYY

Time: 9:15

Page: 1

SSA - Version V.V

Clauth/Group Special Report

User	Name	Class	Group	Owner	Authority	Spec	Oper	Audt	Grpa	ADSP
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
USER01	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA0	ENDUSER, JOSEPH TEST	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA02	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA04	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA05	NEW NAME FIELD	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				

Never Logged On Report - AAREP008

1

Date: MM/DD/YYYY

Time: 9:15

Page: 1

SSA - Version V.V

Clauth/Group Special Report

User	Name	Class	Group	Owner	Authority	Spec	Oper	Audt	Grpa	ADSP
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
USER01	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA0	ENDUSER, JOSEPH TEST	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA02	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA04	ENDUSER, JOSEPH	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				
TSTPA05	NEW NAME FIELD	USER	MEGA	MEGA	USE	Yes				
			NEWMEGA	MEGA	USE	Yes				

Global Attribute Report - AAREP009

1									
Date: MM/DD/YYYY						Page: 1			
Time: 09:16									
SSA Version V.V									
Users Who Never Logged On Report									
RACF		Default		Create	Password				
UserID	Name	Group	Owner	Date	Interval	----- Global Attributes -----			
-----	-----	-----	-----	-----	-----	-----			
AASTC01	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	180	SPECIAL	OPERATIONS		
APPC	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	180				
ASCH	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	180				
ASCHINT	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	180				
USR001	ENDUSER, JOSEPH	BADGRP	BADGRP	MM/DD/YY	180	SPECIAL	OPERATIONS	AUDITOR	
BLSJPRMI	#####	STARTASK	STARTASK	MM/DD/YY	180				
CICSTART	#####	STARTASK	STARTASK	MM/DD/YY	180				
CICSUSER	#####	CICS	CICS	MM/DD/YY	180		OPERATIONS		
DUMPSRV	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	180		OPERATIONS		

Non-Expiring Password Report - AAREP010

1											
Date: MM/DD/YYYY						Page: 1					
Time: 09:17											
SSA Version V.V											
Non-Expiring Password Report											
RACF		Default		Create	LastUsed						
UserID	Name	Group	Owner	Date	Date	----- Global Attributes -----					

GTF	STARTED TASK	STARTASK	STARTASK	MM/DD/YY	MM/DD/YY						
USER03	BILL GENUSERID	MEGA	MEGA	MM/DD/YY	MM/DD/YY	SPECIAL OPERATIONS AUDITOR					
TSTU004	STRICTLY TEST USERS	TSTG001	TSTG001	MM/DD/YY	*****	REVOKE	SPECIAL	OPERATIONS	AUDITOR	UAUDIT	ADSP
TSTU042	STRICTLY TEST USERS	TSTG001	TSTG001	MM/DD/YY	*****						
TSTU045	STRICTLY TEST USERS	TSTG001	TSTG001	MM/DD/YY	*****	REVOKE	SPECIAL	OPERATIONS	AUDITOR	UAUDIT	ADSP
TSTU047	STRICTLY TEST USERS	TSTG001	TSTG001	MM/DD/YY	*****	REVOKE	SPECIAL	OPERATIONS	AUDITOR	UAUDIT	ADSP
TSTU061	THIS IS NEW NAME C	TSTG001	TSTG001	MM/DD/YY	*****	SPECIAL OPERATIONS AUDITOR UAUDIT ADSP					

True Dataset Authority Report - AAREP011

1				Date: MM/DD/YYYY	Page: 1
				Time: 9:18	
				SSA - Version V.V	
				True Dataset Access Report For IBMUSER	
Dataset Name	Volume	Protecting RACF Profile	Access		
ADMIN.SCHED.DATABASE	SENT01	ADMIN.*	ALTER		
ADMIN.SCHED.HISTORY	SENT01	ADMIN.*	ALTER		
ADMIN.V416K.ASM	SENT01	ADMIN.V*.ASM	EXECUTE		
ADMIN.V416K.COBOL	SENT01	ADMIN.V*.COBOL	ALTER		
ADMIN.V416K.DISPLAY.ISPTLIB	SENT01	ADMIN.*	ALTER		
ADMIN.V416K.ISPCLIB	SENT01	ADMIN.*	ALTER		
ADMIN.V416K.ISPMLIB	SENT01	ADMIN.*	ALTER		
ADMIN.V416K.ISPPLIB	SENT01	ADMIN.*	ALTER		
ADMIN.V416K.ISPSLIB	SENT01	ADMIN.*	ALTER		

Notify Report - AAREP012

1										Date: MM/DD/YYYY	Page: 1
										Time: 09:20	
										SSA Version V.V	
										Notify Report	
Notify	Class	Profile	Type	Volume	UACC	Create Date	Warning	Profile Owner	Valid Notify		
SNOOPER	DATASET	USER01.*	Generic		NONE	MM/DD/YY	No	SNOOPER	No		
USER02	HCICSFCT	2TESTGXX	Discrete		NONE	MM/DD/YY	No	USER02	Yes		
USER02	HCICSFCT	2TSGBXX	Discrete		NONE	MM/DD/YY	No	ABCSR	Yes		
ABCSR	HCICSFCT	2TSGXXX	Discrete		NONE	MM/DD/YY	No	ABCSR	Yes		
ABCNP	HCICSFCT	2TSTU072	Discrete		NONE	MM/DD/YY	No	ABCNP	Yes		
ABCNP	HCICSFCT	2TSTU090	Discrete		NONE	MM/DD/YY	No	ABCNP	Yes		
USER02	HCICSFCT	2TSTXXXX	Discrete		NONE	MM/DD/YY	No	USER02	Yes		
USER001	SURROGAT	*.*	Generic		NONE	MM/DD/YY	Yes	SYS1	Yes		
SNOOPER	SURROGAT	SUBMIT.SNOOPER	Discrete		NONE	MM/DD/YY	No	SNOOPER	No		

Break in Ownership Report - AAREP013

1

Date: MM/DD/YYYY

Time: 09:20

Page: 1

SSA Version V.V

Breaks In Ownership Report

Class	Profile	Type	Volume	Default Group	Superior Group	HLQ	Group	Profile Owner
USER	IBMUSER (GENERAL DFLT USER)			SYS1				IBMUSER
USER	WEBSRV (#####)			IMWEB				TSTU025
CONNECT	DCEKERN (#####)						DCEGRP	TSTU025
CONNECT	IBMUSER (GENERAL DFLT USER)						SYSCTLG	IBMUSER
GROUP	TESTREM2				SYS1			IBMUSER
GROUP	TSTG001				TEST			SNOOPER
DATASET	TSTBAT1.*.DA1*	Generic				TSTBAT		TEST
DATASET	TSTBAT1.*.DA*	Generic				TSTBAT		TEST

User/Group Repetitive Permits Report - AAREP014

1

Date: MM/DD/YYYY

Time: 9:22

Page: 1

SSA - Version V.V :

User/Group Repetitive Permits Report

Userid	Name	Profile	Type	Access Level	Conditional Class Entity
USER02	BILL GENUSERID	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- MEGA	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- NEWMEGA	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- SYS1	ADMIN.V*.ASM	- GENERIC	STD	ALTER
TSTBAT1	NEW NAME FOR BILL ID	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- MEGA	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- NEWMEGA	ADMIN.V*.ASM	- GENERIC	STD	ALTER
	GROUP- SYS1	ADMIN.V*.ASM	- GENERIC	STD	ALTER
USER02	BILL GENUSERID	ADMIN.V*.ISPTLIB	- GENERIC	STD	ALTER
	GROUP- MEGA	ADMIN.V*.ISPTLIB	- GENERIC	STD	ALTER

Group Statistics Report - AAREP015

1

Date: MM/DD/YYYY

Time: 09:23

Page: 1

SSA Version V.V

Group Statistics Report

RACF Group	Installation Data (30 Chars.)	Sub Groups	Connects	Std. Permits	Cnd. Permits	Dataset Profiles	Owned Users	Owned Groups	Owned DSN Prof.	Owned Gen. Res.
\$SREVOKE	SUPER REVOKE GROUP WITH DATA T	1	2	0	0	0	0	1	0	0
ADMIN	PRISTINE HLQ FOR SSA	1	24	10	0	5	0	1	5	20
ADMINAID		0	26	7	0	0	0	0	0	0
ADMINX		0	0	0	0	0	0	0	0	0
BACKUP	THIS IS THE HLQ FOR BACKUPS	0	0	0	0	2	0	0	2	0
BADGRP	ACCESS GROUP FOR SSA	0	2	14	0	0	2	0	0	0
CICDZN		0	0	0	0	1	0	0	1	0
CICS		0	1	0	0	1	1	0	1	4

Obsolete Entry Report - AAREP016

1

Date: MM/DD/YYYY

Time: 9:24

Page: 1

SSA - Version V.V

Obsolete Entries Report

Reason	Class	Profile	Obsolete Entry	Type	Access Level	Conditional Class	Entity
PERMIT	RACFVARS	&ABC	SNOOPER	STD	ALTER		
PERMIT	RACFVARS	&TESTIT	SNOOPER	STD	ALTER		
PERMIT	RACFVARS	&XYZ	SNOOPER	STD	ALTER		
PERMIT	TAPEVOL	ABCDEF	SNOOPER	STD	ALTER		
PERMIT	PCICSPSB	**	SNOOPER	STD	ALTER		
PERMIT	PCICSPSB	**	SNOOPER	CND	READ	CONSOLE	CONS01
PERMIT	GLOBAL	DATASET	SNOOPER	STD	ALTER		
PERMIT	FACILITY	\$RESET.*	SNOOPER	STD	CONTROL		
PERMIT	FACILITY	MEGASOLVE-SSA.*	SNOOPER	STD	ALTER		

Where a User/Group Is Not in an Access List Report - AAREP017

1

Date: MM/DD/YYYY

Time: 9:25

Page: 1

SSA - Version V.V

Where a User/Group is Not in an Access List

Entry	Name or Supgroup	Profile	Class	UACC	Owner	Warn
MEGAMO	MIKE ONADA	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
MEGAPXO	ENDUSER, JOSEPH	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
\$SREVOKE	SUPGROUP-DEVL	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
ADMIN	SUPGROUP-DEVL	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
ADMINAID	SUPGROUP-ADMIN	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
ADMINX	SUPGROUP-\$SREVOKE	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
BACKUP	SUPGROUP-PROD	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
BADGRP	SUPGROUP-TEST	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N
BMLTD	SUPGROUP-USERS	ADMIN.V*.ASM	- GENERIC	DATASET	NONE	ADMIN N

General Resource Class Permission Report - AAREP018

1

Date: MM/DD/YYYY

Time: 16:26

Page: 1

SSA Version V.V

General Resource Class Permission Report for Class - GAA\$RULE

General Resource Profile	Class	Access Entry	Access Level	Access Type	Name (If User)	-- Conditional -- Class Entity
AACONFIG-DEFAULT	GAA\$RULE	USER01	ALTER	USER	ENDUSER, JOSEPH	
AACONFIG-DEFAULT	GAA\$RULE	USER02	READ	USER	BILL GENUSERID	
AACONFIG-DEFAULT	GAA\$RULE	TSTREPUR	ALTER	USER	ENDUSER, JOSEPH	
AACONFIG-DEFAULT	GAA\$RULE	TSTPA0	ALTER	USER	ENDUSER, JOSEPH TEST	
AACONFIG-DEFAULT	GAA\$RULE	TSTPA02	ALTER	USER	ENDUSER, JOSEPH	

Userid Statistics Report - AAREP019

1

Date: MM/DD/YYYY

Time: 09:43

Page: 1

SSA Version V.V

Userid Statistics Report

RACF Userid	Name	Default Group	Profile Owner	Connects	Std. Permits	Cnd. Permits	DSN Profiles	Owned Users	Owned Groups	Owned DSN Prof.	Owned Gen. Res.
AASTC01	STARTED TASK	STARTASK	STARTASK	2	19	0	0	0	0	0	0
APPC	STARTED TASK	STARTASK	STARTASK	2	0	0	0	0	0	0	0
ASCH	STARTED TASK	STARTASK	STARTASK	2	0	0	0	0	0	0	0
ASCHINT	STARTED TASK	STARTASK	STARTASK	2	0	0	0	0	0	0	0
USR002	GENUSERID, BILL	BADGRP	BADGRP	1	1	0	1	0	0	1	0
USR001	ENDUSER, JOSEPH	BADGRP	BADGRP	1	0	0	1	0	0	1	0
BLSJPRMI	#####	STARTASK	STARTASK	2	0	0	0	0	0	0	0
CICSTART	#####	STARTASK	STARTASK	2	0	0	0	0	0	0	0
CICSUSER	#####	CICS	CICS	2	1	0	0	0	0	0	0
DCEKERN	#####	STARTASK	STARTASK	2	0	0	0	0	0	0	0

Dataset Profile and Permission Report - AAREP020

1

Date: MM/DD/YYYY

Time: 09:44

Page: 1

SSA Version V.V

Dataset Profile and Permission Report for HLQ - SYS1

Dataset Profile	Type	Volume	UACC	Warn	EOS	Notify	LastChgd Date	Access Entry	Access Level	Conditional Class Entity
SYS1.TESTOUT.THE.MASTER.*	Genr		NONE	No	No		N/A	USER01 TSTPA0 TESTP0	ALTER ALTER ALTER	
SYS1.*	Genr		NONE	No	No		N/A	BMLTD ABC WALK MEGA STARTASK NEWMEGA	READ READ READ ALTER ALTER ALTER	

RACF to Master Catalog Comparison Report - AAREP021

1

Date: MM/DD/YYYY

Time: 09:46

Page: 1

SSA Version V.V

Master Catalog vs RACF Comparison Report

Entry Type	Reason	Profile	Volume	Type	UACC	Profile Owner	Create Date
Catalog	No RACF Profiles Exist - HLQ-CAT	\$SREVOKE					
Catalog	No RACF Profiles Exist - HLQ-CAT	@READ					
Catalog	No RACF Profiles Exist - HLQ-CAT	ADMINAID					
Catalog	No RACF Profiles Exist - HLQ-CAT	ADMINX					
Catalog	No RACF Profiles Exist - HLQ-CAT	ADSM					
RACF	No Alias or Dataset(s) Exist	CICSMPE.*		Generic	NONE	CICSMP	MM/DD/YY
RACF	No Alias or Dataset(s) Exist	IBM.*		Generic	NONE	IBM	MM/DD/YY
RACF	No Alias or Dataset(s) Exist	IBMBK.*		Generic	NONE	IBMBK	MM/DD/YY
RACF	No Alias or Dataset(s) Exist	MEGA.*		Generic	NONE	MEGA	MM/DD/YY
RACF	No Alias or Dataset(s) Exist	MEGA.U.*		Generic	NONE	MEGA	MM/DD/YY
RACF	No Alias or Dataset(s) Exist	MEGA.V.*		Generic	NONE	MEGA	MM/DD/YY

Online Generic Searches

The following are samples for those reports produced from Online Generic Search print requests.

Generic Search - General User Information

1

Date: MM/DD/YYYY

Time: 13:17

Page: 1

SSA Version V.V

Online Generic Searches - General User Information Report

RACF UserID	Name	Default Group	Profile Owner	Create Date	Last-Used Date	PassDate	Password Interval	Spec	Oper	Audt	Revo	Grpa	Uaud	Adsp
TBOB	SMITHERNS, ROBERT	TSOADMN	TSOADMN	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	Yes	Yes	Yes	No	No	Yes	No
TBBL	LOGAN, BRYAN	SYSTEMS	SYSTEMS	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	No	No	No	No	No	Yes	No
TBHP	PRICE, ROBERT	SYSTEMS	SYSTEMS	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	No	No	No	No	No	Yes	No
TBRH	HANSMA, BRIAN	SYSTEMS	SYSTEMS	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	No	No	No	Yes	No	Yes	No
TBXL	LOGAN, BRYAN	SYSTEMS	SYSTEMS	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	No	No	No	No	No	Yes	No
TBXT	SMITHERNS, BILL	TSOADMN	TSOADMN	YYYY-MM-DD	YYYY-MM-DD	YYYY-MM-DD	045	Yes	Yes	Yes	No	No	Yes	No

Generic Search - Userid TSO Segment

1

Date: MM/DD/YYYY

Page: 1

Time: 13:18

SSA Version V.V

Online Generic Searches - Userid TSO Segment Report

RACF	Logon		User-	-- Classes --							
UserID	Procedure	Unit	Data	Size	Maxsize	Hold	Job	Message	Sysout	Destination	Account Number
TBOB	TTSOTBOB	TTSO	0000	0004096	0004096					TTSO	
TBOB01	TTSO	PTSO	0000	0002048	0004096					TTSO	
TBBL	TTSO	TTSO	0000	0002048	0004096					TTSO	
TBHP	TTSO	TTSO	0000	0004096	0008192					TTSO	
TBRH	TTSO	TTSO	0000	0002048	0004096					TTSO	
TBXP	TTSO	TTSO	0000	0004096	0008192					TTSO	
TBXT	TTSOTBOB	TTSO	0000	0004096	0004096					TTSO	

Generic Search - Userid CICS Segment

1

Date: MM/DD/YYYY

Time: 13:34

Page: 1

SSA Version V.V

Online Generic Searches - Userid CICS Segment Report

RACF UserID	Operator Priority	Operator Identity	Timeout	XRFSOFF	----- OPCLASSES -----																							
					01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	22	22	23	24
TCONT000	255	TOX	060	Noforce	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	
TCONT001	000	TIW	060	Noforce	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
TCONT002	000	TA5	060	Noforce	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
TCONT003	255	TEL	060	Noforce	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	
TCONT004	000	TBE	060	Noforce	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
TCONT005	000	TCN	060	Noforce	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	
TCONT006	000	T1M	060	Noforce	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	
TCONT007	000	T9N	060	Noforce	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	
TCONT009	000	T9V	030	Noforce	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	

Generic Search - Userid DFP Segment

1

Date: MM/DD/YYYY

Time: 13:37

Page: 1

SSA Version V.V

Online Generic Searches - Userid DFP Segment Report

RACF Userid	Name	Management Class	Storage Class	Data Class	Data Application
USER01	ENDUSER, JOSEPH	TESTMGMT			
TSTPA0	ENDUSER, JOSEPH TEST	TESTMGMT			
TSTPA02	ENDUSER, JOSEPH	TESTMGMT			
TSTPA04	ENDUSER, JOSEPH	TESTMGMT			
TSTPA05	NEW NAME FIELD	TESTMGMT			
TSTPA06	ENDUSER, JOSEPH	TESTMGMT			

Generic Search - Userid Language Segment

1

Date: MM/DD/YYYY

Page: 1

Time:

SSA Version V.V

Online Generic Searches - Userid LANGUAGE Segment Report

RACF Userid	Name	Primary Language	Secondary Language
-----	-----	-----	-----
MEGAMO	MIKE ONADA	ENU	
MEGAPX0	ENDUSER, JOSEPH	ENU	ESP
TESTP0	JOSEPH ENDUSER	ENU	ESP
TESTP03	JOSEPH ENDUSER	ENU	ESP
USER02	BILL GENUSERID	ENU	ESP
USER03	BILL GENUSERID	ENU	ESP
TSTPA05	NEW NAME FIELD	ENU	ESP
TSTU053	NEWID	ENU	

Generic Search - Userid Operparm Segment

1

Date: MM/DD/YYYY

Time: 13:42

Page: 1

SSA Version V.V

Online Generic Searches - Userid OPERPARM Segment Report

RACF			-- Auth --						-- Level --						-- Mform --					-- Delete --				
UserID	Storage	Key	Master	All	Info	Cons	Io	Sys	NB	All	R	I	CE	E	IN	J	M	S	T	X	Operator	Message	Migid	UD
MEGAPX0	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
MEGAPY0	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
USER02	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
USER03	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
TSGMCT	00000		N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N				N
USER01	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
TSTBAT1	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
TSTPA0	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N
TSTPA02	02000	ZZZZ	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	NORMAL		Y	N

Generic Search - Userid Workattr Segment

1

Date: MM/DD/YYYY

Time: 13:45

Page: 1

SSA Version V.V

Online Generic Searches - Userid WORKATTR Segment Report

RACF Userid	Field Label	WorkattrField
USER02	Name	123456789012345678901234567890NAME FLD FILLED OUT5
	Building	123456789012345678901234567890BUILDING FILLED OUT5
	Department	123456789012345678901234567890DEPARTMN FILLED OUT5
	Room	123456789012345678901234567890ROOM FLD FILLED OUT5
	Address 1	123456789012345678901234567890ADDRESS 1 FILLED OUT
	Address 2	123456789012345678901234567890ADDRESS 2 FILLED OUT
	Address 3	123456789012345678901234567890ADDRESS 3 FILLED OUT
	Address 4	123456789012345678901234567890ADDRESS 4 FILLED OUT
	Account	12345678901234567890123456789012345678901234567890

Generic Search - Userid NetView Segment

1

Date: MM/DD/YYYY

Time: 13:49

Page: 1

SSA Version V.V

Online Generic Searches - Userid NETVIEW Segment Report

RACF UserID	Name	CTL Security	Console Name	Receive Messages	Graphic Monitoring	Command list executed at Logon											
USER02	BILL GENUSERID	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
USER01	ENDUSER, JOSEPH	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
TSTBAT1	NEW NAME FOR BILL ID	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
TSTPA0	ENDUSER, JOSEPH TEST	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
TSTPA02	ENDUSER, JOSEPH	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
TSTPA04	ENDUSER, JOSEPH	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU
TSTPA05	NEW NAME FIELD	SPECIFIC	CNSOLE01	Yes	No	NETVIEW	IC	COMMAND	FIELD	THAT	IS	REALLY	LONG	SO	AGAIN	I	MU

Generic Search - Userid OMVS Segment

1				
Date: MM/DD/YYYY			Page: 1	
Time:				
SSA Version V.V				
Online Generic Searches - Userid OMVS Segment Report				
RACF Userid	Name	UID	Home Path	Default Program
DCEKERN	#####	0000000000		
EZAFTPAP	#####	0000000000		
IBMUSER	GENERAL DFLT USER	0000000000	/	/bin/sh
IMWEBSRV	STARTED TASK	0000000000		
OMVS	STARTED TASK	0000000000	/	/bin/sh
OMVSKERN	#####	0000000000	/	
OPEN1	STRICTLY TEST USERID	0000000000	/	/bin/sh
OPEN2	STRICTLY TEST USERID	0000000000	/	/bin/sh
OPEN3	STRICTLY TEST USERID	0000000000	/	/bin/sh

Generic Search - Userid DCE Segment

1

Date: MM/DD/YYYY

Time: 13:53

Page: 1

SSA Version V.V

Online Generic Searches - Userid DCE Segment Report

RACF Userid	Name	Field Name	Field	Automatic Logon
USER02	BILL GENUSERID	UUID	87654321-1234-1234-1234-123456789012	Yes
		Principal Name	start of the hmenme	
		Home Cell Name	/.../test	
		Home Cell UUID	12345678-1234-1234-1234-123456789012	
USER01	ENDUSER, JOSEPH	UUID	87654321-1234-1234-1234-123456789012	Yes
		Principal Name	start of the hmenme	
		Home Cell Name	/.../test	
		Home Cell UUID	12345678-1234-1234-1234-123456789012	

Generic Search - Userid RRSF Information

1

Date: MM/DD/YYYY
Time: 13:56

Page: 1

SSA Version V.V
Online Generic Searches - RRSF Report

RACF UserID	Name	Node	Target Userid	Peer	Manager User/Remote		Pending Local/Remote		Password Sync	Date Defined	Time Defined	Defining Userid
USER02	BILL GENUSERID	TSGNJE	USER03	Yes	No	No	No	No	Yes	YYYY-MM-DD	11:25:09.891446	USER02
USER02	BILL GENUSERID	TSGNJE	WALK02	No	Yes	No	No	No	No	YYYY-MM-DD	10:14:21.477369	USER02
USER03	BILL GENUSERID	TSGNJE	USER02	Yes	No	No	No	No	Yes	YYYY-MM-DD	11:25:10.397979	USER02
TSTU009	STRICTLY TEST USERS	TSGNJE	WALK02	Yes	No	No	No	Yes	No	YYYY-MM-DD	-9:54:03.893967	USER01

Generic Search - Userid Connect Information

1

Date: MM/DD/YYYY
Time: 13:59

Page: 1

SSA Version V.V

Online Generic Searches - Connect Information Report

RACF UserID	Name	RACF Group	Profile Owner	UACC	Auth	SPEC	OPER	AUDT	GRPA	ADSP	REVK	Revoke Date	Resume Date
AASTC01	STARTED TASK	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
AASTC01	STARTED TASK	SYS1	SYS1	NONE	USE	No	No	No	No	No	No		
APPC	STARTED TASK	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
APPC	STARTED TASK	SYS1	SYS1	NONE	USE	No	No	No	No	No	No		
ASCH	STARTED TASK	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
ASCHINT	STARTED TASK	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
ASCHINT	STARTED TASK	SYS1	SYS1	NONE	USE	No	No	No	No	No	No		
USR002	GENUSERID, BILL	BADGRP	BADGRP	NONE	USE	No	No	No	No	No	No		
USR001	ENDUSER, JOSEPH	BADGRP	BADGRP	NONE	USE	No	No	No	No	No	No		
BLSJPRMI	#####	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
TCPIPMVS	#####	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		
TCPIPMVS	#####	SYS1	SYS1	NONE	USE	No	No	No	No	No	No		
TCPIPOE	#####	STARTASK	STARTASK	NONE	USE	No	No	No	No	No	No		

Generic Search - Userid Clauth Authority

1

Date: MM/DD/YYYY

Time: 14:01

Page: 1

SSA Version V.V

Online Generic Searches - Clauth Authorities Report

RACF Userid	Name	CLASS
-----	-----	-----
SENTCICS	STARTED TASK	TCICSTRN
USER01	ENDUSER, JOSEPH	USER
TSTPA0	ENDUSER, JOSEPH TEST	USER
TSTPA02	ENDUSER, JOSEPH	USER
TSTPA04	ENDUSER, JOSEPH	USER
TSTPA05	NEW NAME FIELD	USER
TSTPA06	ENDUSER, JOSEPH	USER
TSTPA07	ENDUSER, JOSEPH	USER
TSTREPUR	ENDUSER, JOSEPH	USER
TSTU004	STRICTLY TEST USERS	USER

Generic Search - Userid Security Categories

1

Date: MM/DD/YYYY

Time: 14:03

Page: 1

SSA Version V.V

Online Generic Searches - Userid Security Categories Report

RACF Userid	Name	Security Categories	Number Value
-----	-----	-----	-----
USER03	BILL GENUSERID	TESTCAT	00003
USER03	BILL GENUSERID	BOB	00004
USER01	ENDUSER, JOSEPH	TESTCAT	00003
USER01	ENDUSER, JOSEPH	BOB	00004

Generic Search - General Group Information

1

Date: MM/DD/YYYY

Time: 14:04

Page: 1

SSA Version V.V

Online Generic Searches - General Group Information Report

RACF Group	Superior Group	Profile Owner	TERMUACC	Has Users	Has Subgroups	Model Dataset
\$SREVOKE	DEVL	DEVL	Yes	Yes	Yes	
ADMIN	DEVL	DEVL	No	Yes	Yes	
ADMINAID	ADMIN	ADMIN	No	Yes	No	
ADMINX	\$SREVOKE	\$SREVOKE	No	No	No	
BACKUP	PROD	PROD	No	No	No	
BADGRP	TEST	TEST	No	Yes	No	
BMLTD	USERS	USERS	Yes	Yes	No	
CICDZN	SYSTEM	SYSTEM	No	No	No	
CICS	SYSTEM	SYSTEM	No	Yes	No	
CICSMPE	SYSTEM	SYSTEM	No	No	No	
CICTZN	SYSTEM	SYSTEM	No	No	No	
VSAMDSET	SYSTEM	SYSTEM	No	Yes	No	

Generic Search - Group DFP Segment

1

Date: MM/DD/YYYY
Time: 14:06

Page: 1

SSA Version V.V
Online Generic Searches - Group DFP Segment Report

RACF Group	Management Class	Storage Class	Data Class	Data Application
BMLTD	USERMGMT	USERSTOR	USERCLAS	USERAPPL
MEGA	USERMGMT	USERSTOR	USERCLAS	USERAPPL
NEWMEGA	USERMGMT	USERSTOR	USERCLAS	USERAPPL
ABC	USERMGMT	USERSTOR	USERCLAS	USERAPPL
SYS1	PRODMGMT	PRODSTOR	PRODCLAS	PRODAPPL
TESTREM2	PRODMGMT	PRODSTOR	PRODCLAS	PRODAPPL
TSTG003	TESTMGMT	TESTSTOR	TESTCLAS	TESTAPPL

Generic Search - Group OMVS Segment

1

Date: MM/DD/YYYY

Time: 14:07

Page: 1

SSA Version V.V

Online Generic Searches - Group OMVS Segment Report

RACF Group	OMVS GID
-----	-----
DCEGRP	0000000002
IMWEB	0000000205
MEGA	0000000000
NEWGRP1	0000000002
NEWMEGA	0000000000
OMVSGRP	0000000001
SPECIAL	0000000255

Generic Search - General Dataset Information

1

Date: MM/DD/YYYY

Page: 1

Time: 14:09

SSA Version V.V

Online Generic Searches - General Dataset Information Report

Dataset Profile	Type	Profile Owner	Volume	UACC	Warn	Notify	Create Date	Last-Used Date	Resowner
ADMIN.V*.ASM	Generic	ADMIN		NONE	No		YYYY-MM-DD	YYYY-MM-DD	
ADMIN.V*.COBOL	Generic	ADMIN		NONE	No		YYYY-MM-DD	YYYY-MM-DD	
ADMIN.V*.ISPTLIB	Generic	ADMIN		NONE	No		YYYY-MM-DD	YYYY-MM-DD	
ADMIN.*.DATA.*	Generic	USER001		NONE	No		YYYY-MM-DD	YYYY-MM-DD	
ADMIN.*	Generic	ADMIN		NONE	No		YYYY-MM-DD	YYYY-MM-DD	USER01
BACKUP.*	Generic	BACKUP		NONE	No		YYYY-MM-DD	YYYY-MM-DD	
BACKUP.SENT01.G0001V00	Discrete	USER01	B00001	NONE	No		YYYY-MM-DD	YYYY-MM-DD	
MEGA.*	Generic	MEGA		NONE	No		YYYY-MM-DD	YYYY-MM-DD	MEGA

Generic Search - Dataset Permissions

1

Date: MM/DD/YYYY

Time: 14:12

Page: 1

SSA Version V.V

Online Generic Searches - Dataset Profile Permissions Report

Dataset Profile	Type	Volume	Access Entry	Access Level	Access Type	Name (If User)	Conditional Class	Entity
ADMIN.V*.ASM	Generic		MEGA	ALTER	GROUP		CONSOLE	02
ADMIN.V*.ASM	Generic		NEWMEGA	ALTER	GROUP		CONSOLE	02
ADMIN.V*.ASM	Generic		USER02	ALTER	USER	BILL GENUSERID		
ADMIN.V*.ASM	Generic		MEGA	ALTER	GROUP			
ADMIN.V*.ASM	Generic		*	NONE	GENERAL			
ADMIN.V*.ASM	Generic		TSTBAT1	ALTER	USER	NEW NAME FOR BILL ID		

Generic Search - Dataset Security Categories

1

Date: MM/DD/YYYY

Time: 14:14

Page: 1

SSA Version V.V

Online Generic Searches - Dataset Profile Security Categories Report

Dataset Profile	Type	Volume	Security Category	Numeric Value
ADMIN.*	Generic		BOB	00004
BACKUP.SENT01.G0001V00	Discrete	B00001	BOB	00004

Generic Search - General Resource Information

1

Date: MM/DD/YYYY

Time: 14:24

Page: 1

SSA Version V.V

Online Generic Searches - General Resource Profile Information Report

Class	Resource Profile	Profile Owner	UACC	Warn	Notify	Level	Create Date	Last Reference Date
GAA\$RULE	AACONFIG-DEFAULT	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	ADMIN-AIDE.ADMINISTRATORS	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	ADMIN-AIDE.PASSWORDS	USER001	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	ADMIN-AIDE.USERS	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	GENERAL-CA	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	GENERAL-PA	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	SPECIAL-PA	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	SPECIFIC-AUTHORITY	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD
GAA\$RULE	UNLOAD-SECURITY	ADMIN	NONE	No		00	YYYY-MM-DD	YYYY-MM-DD

Generic Search - General Resource Permissions

1

Date: MM/DD/YYYY

Time: 14:33

Page: 1

SSA Version V.V

Online Generic Searches - General Resource Profile Permissions

General Resource Profile	Class	Access Entry	Access Level	Access Type	Name (If User)	-- Conditional -- Class Entity
AACONFIG-DEFAULT	GAA\$RULE	USER01	ALTER	USER	ENDUSER, JOSEPH	
AACONFIG-DEFAULT	GAA\$RULE	USER02	READ	USER	BILL GENUSERID	
ADMIN-AIDE.ADMINISTRATORS	GAA\$RULE	USER01	ALTER	USER	ENDUSER, JOSEPH	
ADMIN-AIDE.ADMINISTRATORS	GAA\$RULE	TESTPO	ALTER	USER	JOSEPH ENDUSER	
ADMIN-AIDE.PASSWORDS	GAA\$RULE	USER02	ALTER	USER	BILL GENUSERID	
GENERAL-CA	GAA\$RULE	NEWMEGA	ALTER	GROUP		
SPECIAL-PA	GAA\$RULE	MEGA	ALTER	GROUP		
SPECIFIC-AUTHORITY	GAA\$RULE	TSTPA06	ALTER	USER	ENDUSER, JOSEPH	
SPECIFIC-AUTHORITY	GAA\$RULE	TSTBAT1	ALTER	USER	NEW NAME FOR BILL ID	

Generic Search - General Resource Members

1

Date: MM/DD/YYYY

Time: 14:55

Page: 1

SSA Version V.V

Online Generic Searches - General Resource Profile Members Report

Class	Resource Profile	Member	Profile Type
GAA\$RULE	AACONFIG-DEFAULT	ALLOCATION_PREFIX-\$USERID\$.TEST	Discrete
GAA\$RULE	AACONFIG-DEFAULT	AA_LOADLIB-ADMIN.V510A.LOADLIB	Discrete
GAA\$RULE	AACONFIG-DEFAULT	LINES_PER_PAGE-57	Discrete

Generic Search - General Resource Session Segment

1		Page: 1						
Date: MM/DD/YYYY Time: 15:07								
		SSA Version V.V Online Generic Searches - General Resource Session Segment Report						
Class	Resource Profile	Profile Key	Lock	Security Checking	Number of Days Key is Valid	Failed Attempts	Before Lockout	Last Date Key Was Changed
APPCLU	TEST-SESS		No		00001	00000	00000	
APPCLU	XXXXSESS		Yes		00005	00000	00000	YYYY-MM-DD

Generic Search - General Resource DLF Segment

1		Page: 1						
Date: MM/DD/YYYY Time: 15:09								
		SSA Version V.V Online Generic Searches - DLFDATA Segment Report						
Class	Resource Profile	Resource is Retained						
DLFCLASS	TESTDLF	No						

Generic Search - General Resource Started Task Segment

1		Page: 1						
Date: MM/DD/YYYY Time: 15:11								
		SSA Version V.V Online Generic Searches - Started Task Segment Report						
Class	Resource Profile	Userid	Group	Privileged	Trusted	Trace		
STARTED	AASTC01.*	AASTC01	STARTASK	Yes	No	No		
STARTED	APPC.*	APPC	STARTASK	Yes	No	No		
STARTED	ASCH.*	ASCH	STARTASK	No	No	No		

Generic Search - General Resource SystemView Segment

1

Date: MM/DD/YYYY

Page: 1

Time: 15:12

SSA Version V.V

Online Generic Searches - General Resource SystemView Segment Report

Class	Resource Profile	Script Name	Parm Name
SYSMVIEW	TESTSCRIPT	SCRNAME	PARNAME
SYSMVIEW	TESTVIEW	SCRPTER	PARMER

Generic Search - General Resource Security Categories

1

Date: MM/DD/YYYY

Page: 1

Time: 15:13

SSA Version V.V

Online Generic Searches - General Resource Security Categories

Class	Resource Profile	Security Category	Numeric Value
GCICSTRN	TEST	BOB	00004
\$TSTCLAS	TESTXXXXXX	TESTCAT	00003

System Resource Monitor

The following are sample reports produced from System Resource Monitor print requests.

System Resource Monitor - Report Banner Page

1	
Date: MM/DD/YYYY	Page: 1
Time: 15:16	
SSA - Version V.V	
System Resource Monitor	
CPU ID: 123456	
CPU Model: 9672	
SMF-ID: A90B	
System Residence Volume: OS39R1	
Operating System Level: SP5.3.0	
Operating System FMID: HBB6601	
RACF Version: 2.02	

System Resource Monitor - Authorized Program Facility

1

Date: MM/DD/YYYY
Time: 15:16

Page: 1

SSA - Version V.V
Authorized Program Facility Report

Dataset/RACF Protecting Profile		Volume	Type	Uacc	Warn	Entry	RACF Name		Level	Conditional Entry Class	
APF	SYS1.LINKLIB SYS1.*	OS39R1	GENR	NONE	NO	BMLTD MEGA	>----- >-----	GROUP GROUP	-----< -----<	READ ALTER	
APF	SYS1.SVCLIB SYS1.*	OS39R1	GENR	NONE	NO	BMLTD MEGA	>----- >-----	GROUP GROUP	-----< -----<	READ ALTER	

System Resource Monitor - Link List Datasets

1									
Date: MM/DD/YYYY Time: 15:16								Page: 1	
SSA - Version V.V Link List Datasets Report									
Conditional									
Dataset/RACF Protecting Profile		Volume	Type	Uacc	Warn	Entry	RACF Name	Level	Entry Class

LLT	SYS1.LINKLIB	OS39R1							
	SYS1.*		GENR	NONE	NO	BMLTD	>----- GROUP -----<	READ	
						MEGA	>----- GROUP -----<	ALTER	
LLT	SYS1.MIGLIB	OS39R1							
	SYS1.*		GENR	NONE	NO	BMLTD	>----- GROUP -----<	READ	
						MEGA	>----- GROUP -----<	ALTER	

System Resource Monitor - Link Pack Area Datasets

1									
Date: MM/DD/YYYY							Page: 1		
Time: 15:16									
SSA - Version V.V									
Link Pack Area Datasets Report									
Dataset/RACF Protecting Profile		Volume	Type	Uacc	Warn	Entry	RACF Name	Level	Conditional Entry Class

LPA	SYS1.LPALIB	OS39R1							
	SYS1.*		GENR	NONE	NO	BMLTD	>----- GROUP -----<	READ	
						MEGA	>----- GROUP -----<	ALTER	
LPA	SYS1.SISFLPA	OS39R1							
	SYS1.*		GENR	NONE	NO	BMLTD	>----- GROUP -----<	READ	
						MEGA	>----- GROUP -----<	ALTER	

System Resource Monitor - Class Descriptor Table (Report 01)

1

Date: MM/DD/YYYY

Time: 15:16

Page: 1

SSA - Version V.V

Class Descriptor Table Report

Class Name	Group/Member Class	Posit Number	Class ID	Maximum Mbr Lngth	- Name Syntax Rules -				--- Allowed ---			----- Options -----				
					First Character	Other Characters	Max Length	Default UACC	Oper	Rac1	Gen1	Active?	Genprf	Gencmd	Rac1	Gen1
\$TSTCLAS		0030	128	246	ALPHA	ANY	246	NONE	NO	YES	NO	YES	YES	YES	YES	NO
ACCTNUM		0126	046	039	ANY	ANY	039	NONE	NO	YES	NO	YES	YES	YES	YES	NO
ACICSPCT	BCICSPCT	0005	037	013	ANY	ANY	013	NONE	NO	NO	NO	YES	YES	YES	NO	NO
AIMS		0004	011	008	ALPHA	ALPHANUM	008	NONE	NO	NO	NO	NO	YES	YES	NO	NO
ALCSAUTH		0548	001	062	ANY	ANY	062	NONE	YES	YES	NO	NO	NO	NO	NO	NO
APPCLU		0118	057	035	ALPHA	ANY	035	NONE	NO	NO	NO	NO	YES	YES	NO	NO
APPCPORT		0087	098	008	ALPHA	ALPHANUM	008	NONE	NO	YES	NO	NO	YES	YES	NO	NO
APPCSERV		0084	105	073	ALPHANUM	ANY	073	NONE	NO	YES	NO	NO	YES	YES	NO	NO
APPCSI		0088	097	026	ALPHANUM	ANY	026	READ	NO	YES	NO	NO	YES	YES	NO	NO
BCICSPCT	ACICSPCT	0005	038	013	ANY	ANY	013	NONE	NO	NO	NO	YES	NO	NO	NO	NO
CCICSCMD	VCICSCMD	0005	052	021	ANY	ANY	021	NONE	NO	NO	NO	YES	YES	YES	NO	NO

System Resource Monitor - Class Descriptor Table (Report 02)

1

Date: MM/DD/YYYY

Time: 15:57

Page: 1

SSA - Version V.V

Class Descriptor Table Report

CLASS: \$TSTCLAS

Class Number: 128

Posit Number: 0030

Member/Group Class:

Active: YES

Genlisted: NO

Raclisted: YES

Generic Profiles Allowed: YES

Generic Commands Allowed: YES

Maximum Member Length: 246

Syntax First Character: ALPHA

Syntax of Remaining Characters: ANY

Default UACC: NONE

Resource Class: NO

Use UACC from ACEE: NO

Operations Allowed: NO

Raclist Allowed: YES

Genlist allowed: NO

Default Return Code: 004

Raclist Required: NO

Profiles Can be Defined: YES

Seclabel Required: NO

Reverse MAC Checking: NO

Characters 1-4 to Prior Class: NO

Number of Significant Qualifiers: 000

Original Maximum Member Length: 246

CDT-Raclisted: YES

CDT-Genlisted: NO

Global: NO

Auditing: NO

Statistics: NO

Log-Always: NO

Log-Never: NO

Log-Successes: NO

Log-Failures: NO

System Resource Monitor - Program Properties Table

1

Date: MM/DD/YYYY
Time: 15:16

Page: 1

SSA - Version V.V
Program Properties Table Report

Program	Non-Cancelable	- Protect Key - Required	NON Key Swappable	Privileged	SYSTEM Task	Data Set Integrity	Bypass Pwd Protection	Level Preferred Usage	CPU Affinity (FFFF If No)	Origin
IEDQTCAM	NO	YES	06	YES	NO	NO	NO	NOT2	FFFF	IBM
ISTINM01	YES	YES	06	YES	NO	YES	YES	NOT2	FFFF	IBM
IKTCAS00	YES	YES	06	NO	YES	YES	NO	NONE	FFFF	IBM
AHLGTF	YES	YES	00	YES	NO	YES	NO	NOT2	FFFF	IBM
HHLGTF	YES	YES	00	YES	NO	YES	NO	NOT2	FFFF	IBM
IHLGTF	YES	YES	00	YES	NO	YES	NO	NOT2	FFFF	IBM

System Resource Monitor - General RACF Information

1		Page: 1	
Date: MM/DD/YYYY			
Time: 15:16			
SSA - Version V.V			
General RACF Information Report			
Bypass Racinit Statistics:	NO		
Bypass Dataset Statistics:	YES		
Bypass TAPEVOL Statistics:	YES		
Bypass DASDVOL Statistics:	YES		
BYPASS TERMINAL Statistics:	YES		
ADSP Protection:	NO		
Enhanced Generic Naming in Effect:	NO		
Tape Volume Protection in Effect:	NO		
Dasd Protection in Effect:	NO		
Dataset Generic Profile Check:	YES		
Dataset Generic Command Check:	YES		
I/P Dataset Used (LOG/MSG):	NO		
JES-XBMALLRACF in Effect:	NO		
JES-EARLYVERIFY in Effect:	NO		

System Resource Monitor - RACF Installation Exits

1				Page: 1	
Date: MM/DD/YYYY					
Time: 15:16					
SSA - Version V.V					
RACF Installation Exits Report					
Exit Name	Exit Description	Active	Entry Address		
ICHRIX01	RACROUTE REQUEST-VERIFY (PRE-PROCESS)	NO			
ICHRIX02	RACROUTE REQUEST-VERIFY (POST-PROCESS)	NO			
ICHRCX01	RACROUTE REQUEST-AUTH (PRE-PROCESS)	NO			
ICHRCX02	RACROUTE REQUEST-AUTH (POST-PROCESS)	NO			
ICHRDX01	RACROUTE REQUEST-DEFINE (PRE-PROCESS)	NO			
ICHRDX02	RACROUTE REQUEST-DEFINE (POST-PROCESS)	NO			
ICHRLX01	RACROUTE REQUEST-LIST (PRE-PROCESS)	NO			
ICHPWX01	NEW PASSWORD	NO			
ICHDEX01	PASSWORD AUTHENTICATION	NO			
ICHCNV00	NAMING CONVENTION TABLE (BUILD)	NO			
ICHCNV01	NAMING CONVENTION TABLE (DELETE)	NO			
ICHRFX01	RACROUTE REQUEST-FASTAUTH (PRE-PROCESS)	NO			
ICHRFX02	RACROUTE REQUEST-FASTAUTH (POST-PROCESS)	NO			
ICHRFX03	RACROUTE REQUEST-FASTAUTH (PRE-PROCESS)	NO			

System Resource Monitor - RACF Database Datasets

1

Date: MM/DD/YYYY
Time: 15:16

Page: 1

SSA - Version V.V
RACF Database Datasets Report

Dataset/RACF Protecting Profile		Volume	Type	Uacc	Warn	Entry	RACF Name	Level	Conditional Entry	Class
RDS	SYS1.RACF SYS1.*						<PRIMARY,RESTRUCTURED,IPL-PRIMARY,ACTIVE,MASTER,SHARED> GENR NONE NO BMLTD >----- GROUP -----< READ MEGA >----- GROUP -----< ALTER			
RDS	SYS1.RACF.BACKUP SYS1.*						<BACKUP,RESTRUCTURED,IPL-BACKUP ,ACTIVE,MASTER,SHARED> GENR NONE NO BMLTD >----- GROUP -----< READ MEGA >----- GROUP -----< ALTER			

System Resource Monitor - RACF Authorized Caller Table

1		
Date: MM/DD/YYYY Time: 15:16		Page: 1
SSA - Version V.V RACF Authorized Caller Report		
Program Name	Can Program Issue Raclist	Can Program Issue Racinit
MTSPGM	YES	YES
BATPGM	NO	YES
PAOPGM	YES	NO

System Resource Monitor - RACF Router Table

1

Date: MM/DD/YYYY

Time: 8:51

Page: 2

SSA Version V.V

RACF Router Table Report

Requestor Name	Resource Class	SubSystem Name	Defined to RACF
-----	-----	-----	-----
	DATASET		YES
	USER		YES
	GROUP		YES
	CONNECT		YES
	DASDVOL		YES
	GDASDVOL		YES
	TAPEVOL		YES
	TERMINAL		YES

System Resource Monitor - System Management Facility (Report 01)

1

Date: MM/DD/YYYY

Time: 15:16

Page: 1

SSA - Version V.V

System Management Facility Report

Dataset/RACF Protecting Profile		Volume	Type	Uacc	Warn	Entry	RACF Name	Level	Conditional Entry	Class
-----		-----	-----	-----	-----	-----	-----	-----	-----	-----
SMF	SYS1.MAN1	SCPMV5	<ACTIVE,NO	DUMP	REQUIRED,PERCENT-USED=	70%>				
	SYS1.*		GENR NONE	NO	BMLTD	>-----	GROUP	-----<	READ	
					MEGA	>-----	GROUP	-----<	ALTER	
SMF	SYS1.MAN2	SCPMV5	<BACKUP,NO	DUMP	REQUIRED,PERCENT-USED=	0%>				
	SYS1.*		GENR NONE	NO	BMLTD	>-----	GROUP	-----<	READ	
					MEGA	>-----	GROUP	-----<	ALTER	

System Resource Monitor - System Management Facility (Report 02)

1

Date: MM/DD/YYYY

Time: 15:57

Page: 1

SSA - Version V.V

System Management Facility Report

System ID	SMF Dataset	Volume	Active	Dump Required	Percent Used	Job Wait Time	Max Dorm Time
A90B	SYS1.MAN1	SCPMV5	YES	NO	70%	0400	3000
A90B	SYS1.MAN2	SCPMV5	NO	NO	0%	0400	3000
A90B	SYS1.MAN3	SCPMV5	NO	NO	0%	0400	3000
A90B	SYS1.MAN4	SCPMV5	NO	NO	0%	0400	3000
ACTIVE SMF TYPES: 014:015,017,030,080:081,083,110							

System Resource Monitor - Started Task Table

1

Date: MM/DD/YYYY

Time: 15:16

Page: 1

SSA - Version V.V

Started Task Table Report

Procedure Name	Associated User	Associated Group	Privileged	Trusted	RACF Name	Default Group	OWNER	Racinit Date	--- Attributes -			
									Oper	Spec	Audt	Revk
*	-	SYS1	NO	NO								
>TEST	JOB	GRP	NO	NO	* INVALID *							
>AASTC01	AASTC01	STARTASK	YES	NO	STARTED TASK	STARTASK	STARTASK	10/02/97	YES	YES	NO	NO
>ASCHINT	ASCHINT	STARTASK	NO	NO	STARTED TASK	STARTASK	STARTASK	09/22/97	NO	NO	NO	NO

Note The '>' indicates that the entry is from the RACF STARTED class.

System Resource Monitor - Supervisor Calls

1

Date: MM/DD/YYYY

Time: 15:16

Page: 1

SSA - Version V.V

Supervisor Calls Report

SVC #000 X('000') Description: EXCP/XDAP

ESR Number: Module Name: IGC000

Entry Point: 00FDD5F0 Entry Point Name: IECVEXCP

Location: NUCLEUS AMODE-31: NO

Type: 1 Authorized: NO

ESR: NO Non-Preemptive: NO

Can Be Assigned: NO AR Mode OK: NO

Local Lock: YES CMS Lock: NO

OPT Lock: NO ALLOC Lock: NO

DISP Lock: NO New Entry Point Address:

Call Return Addr: Update Date:

New EP Name: Parmlib Suffix Via Parmlib:

Number of Updates:

System Resource Monitor - Authorized TSO Tables

1

Date: MM/DD/YYYY

Time: 15:16

Page: 1

SSA - Version V.V

Authorized TSO Tables Report

Parmlib	Tso Auth	Member List					
Member	Table						
IKJTS000	AUTHTSF	IKJEFT01	AACMD001	AACMD002	AACNG001	AACNG002	AACNG003
		AAATHCHK	AAATHDSN	AAATHRSC	AAATHUSR	AAPSWCHK	AAGRPUSR
		AAREP011	MNAPFPRC	MNGRPPRC	MNCDTPRC	MNCD2PRC	MNLLTPRC
		MNLPAPRC	MNPPTPRC	MNRACPRC	MNRAUPRC	MNRFRPRC	MNSMFPRC
		MNSM4PRC	MNSTCPRC	MNSVCPRC	MNAUTHRX	IEBCOPY	ICQASLIO
		IKJEFF76					

TSO Direct Administration and CICS Direct Administration

SSA-TDA and SSA-CDA produce standard RACF Type 80 SMF records. The format of the command will show on the report as if a user had entered the actual RACF COMMAND. Below are examples of TSO Direct Password Administration and TSO Direct Connect Administration SMF records as produced by the RACF Report Writer.

RACF Report Writer Example

The report shown below and on the following pages are examples of RACF Report Writer reports for all possible Password Administration functions. Please note the following about Password Administration SMF records:

- If a security administrator attempts to use a Password Administration function against a userid that has global SPECIAL and they do not have access to the SSA.\$RESET.\$SPECIAL\$ profile an SMF record is NOT produced.
- If a security administrator attempts to use a Password Administration function against a UserID that is SuperRevoked only one SMF record is produced; a Failure to connect the user to the SuperRevoke group (EVENT=14 QUAL=1). See the SuperRevoke UserID Success and Failure example.
- All Password Administration functions are considered separate requests. This means that if multiple functions are requested, a separate SMF record is produced for each function. See 'Change Password and Resume Success and Failure' on page 577.

TSO Direct Password Administration

Change Password Success and Failure

YY.DDD 19:07:07
PAGE 1

RACF REPORT - LISTING OF PROCESS RECORDS

DATE	TIME	SYSID	*JOB/USER NAME	*STEP/ GROUP	--TERMINAL-- ID	LVL	T	L	
YY.DDD 18:58:44	A90B		USER02X BOB SMITH	SYS1	CLNT01L2	0	13	0	JOBID=(USER02X YY.DDD 18:58:44),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 PASSWORD(****)
YY.DDD 18:59:35	A90B		USER02X BOB SMITH	SYS1	CLNT01L2	0	13	1	JOBID=(USER02X YY.DDD 18:59:35),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COM- MAND),VIOL=(USER-AUTHORITY, PASSWORD) ALTUSER USER03 PASSWORD(****)

Resume UserID Success and Failure

YY.DDD 18:58:54	A90B		USER02X BOB SMITH	SYS1	CLNT01L2	0	13	0	JOBID=(USER02X YY.DDD 18:58:54),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 RESUME
YY.DDD 18:59:40	A90B		USER02X BOB SMITH	SYS1	CLNT01L2	0	13	1	JOBID=(USER02X YY.DDD 18:59:40),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, RESUME) ALTUSER USER03 RESUME

Change Password and Resume Success and Failure

Command: ALU USERID PASSWORD RESUME

Note Password Administration will produce two SMF records for each Success and each Failure in this example.

YY.DDD 18:58:48 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 0	JOBID=(USER02X YY.DDD 18:58:48),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 RESUME
YY.DDD 18:58:48 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 0	JOBID=(USER02X YY.DDD 18:58:48),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 PASSWORD(****)
YY.DDD 18:59:40 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 1	JOBID=(USER02X YY.DDD 18:57:45),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, RESUME) ALTUSER USER03 RESUME
YY.DDD 18:59:40 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 1	JOBID=(USER02X YY.DDD 18:57:45),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, PASSWORD) ALTUSER USER03 PASSWORD(****)

Revoke UserID Success and Failure

YY.DDD 18:58:57 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 0	JOBID=(USER02X YY.DDD 18:58:57),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 REVOKE
YY.DDD 18:59:45 A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0 13 1	JOBID=(USER02X YY.DDD 18:59:45),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, REVOKE) ALTUSER USER03 REVOKE

Set Resume Date on UserID Success and Failure

YY.DDD 19:00:04	A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0	13	0	JOBID=(USER02X YY.DDD 19:00:04),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 RESUME(MM/DD/YY)
YY.DDD 19:01:51	A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0	13	1	JOBID=(USER02X YY.DDD 19:01:51),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, RESUME) ALTUSER USER03 RESUME(MM/DD/YY)

Set Revoke Date on UserID Success and Failure

YY.DDD 19:00:22	A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0	13	0	JOBID=(USER02X YY.DDD 19:00:22),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND) ALTUSER USER03 REVOKE(MM/DD/YY)
YY.DDD 19:01:56	A90B	USER02X BOB SMITH	SYS1	CLNT01L2	0	13	1	JOBID=(USER02X YY.DDD 19:01:56),USERDATA=(USRADMIN) AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY, REVOKE) ALTUSER USER03 REVOKE(MM/DD/YY)

SuperRevoke UserID Success and Failure

Note Password Administration will produce two SMF records for each Success and one SMF record for each Failure.

```
YY.DDD 19:01:55 A90B  USER02X  SYS1      CLNT01L2   0 13  0  JOBID=(USER02X YY.DDD 19:01:55),USERDATA=(USRADMIN)
                        BOB SMITH      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                      ALTUSER USER03 REVOKE

YY.DDD 19:01:55 A90B  USER02X  SYS1      CLNT01L2   0 14  0  JOBID=(USER02X YY.DDD 19:01:55),USERDATA=(USRADMIN),OWNER=$SREVOKE
                        BOB SMITH      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                      CONNECT USER03 GROUP($SREVOKE) UACC(NONE) AUTHORITY(USE) OWNER(
                                      $SREVOKE)

YY.DDD 19:01:55 A90B  USER02X  SYS1      CLNT01L2   0 14  1  JOBID=(USER02X YY.DDD 19:01:59),USERDATA=(USRADMIN),OWNER=$SREVOKE
                        BOB SMITH      AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,UACC,
                                      AUTHORITY,OWNER)
                                      CONNECT USER03 GROUP($SREVOKE) UACC(NONE) AUTHORITY(USE) OWNER(
                                      $SREVOKE)
```

Remove SuperRevoke from UserID Success

Note Password Administration will produce two SMF records for each Success.

```
YY.DDD 19:06:02 A90B  USER020   SYS1      CLNT01L2   0 13  0  JOBID=(USER02X YY.DDD 19:06:02),USERDATA=(USRADMIN)
                        BOB SMITH      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                      ALTUSER USER03 RESUME

YY.DDD 19:06:02 A90B  USER02X   SYS1      CLNT01L2   0 23  0  JOBID=(USER02X YY.DDD 19:06:02),USERDATA=(USRADMIN),OWNER=$SREVOKE
                        BOB SMITH      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                      REMOVE USER03 GROUP($SREVOKE)
```

Change UserID Installation Data Field Success and Failure

```

YY.DDD 19:01:29 A90B  USER02X  SYS1  CLNT01L2  0 13  0  JOBID=(USER02X YY.DDD 19:01:29),USERDATA=(USRADMIN)
                        BOB SMITH                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                                ALTUSER USER03 DATA('SECURITY ADMINISTRATOR')

YY.DDD 19:02:04 A90B  USER02X  SYS1  CLNT01L2  0 13  1  JOBID=(USER02X YY.DDD 19:02:04),USERDATA=(USRADMIN)
                        BOB SMITH                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(USER-AUTHORITY,DATA)
                                                ALTUSER USER03 DATA('')

```

TSO Direct Connect Administration**Connect Success/Failure**

```

YY.DDD 17:42:41                                RACF REPORT - LISTING OF PROCESS RECORDS                                PAGE      5
                                                CA COMMAND REPORT
                                                E
                                                V Q
                                                E U
                                                --TERMINAL-- N A
DATE    TIME  SYSID  *JOB/USER *STEP/  ID  LVL T L
YY.DDD 17:14:01 A90B  TSGMCT  MEGA    YYYYY01L1  0 14  0  JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG
                        MARY LAZARS                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                                CONNECT TESTCAU GROUP(TESTCAG) OWNER(TESTCAG)

YY.DDD 17:14:01 A90B  TSGMCT  MEGA    YYYYY01L1  0 14  1  JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG
                        MARY LAZARS                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP)
                                                CONNECT TESTCAU GROUP(TESTCAG)

```

Remove Success/Failure

```

YY.DDD 17:39:01 A90B  TSGMCT  MEGA    YYYYY01L1  0 23  0  JOBID=(TSGMCT YY.DDD 17:39:01),USERDATA=(CONADMIN),OWNER=ADMIN
                        MARY LAZARS                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND)
                                                REMOVE TESTCAU GROUP(ADMIN)

YY.DDD 17:39:01 A90B  TSGMCT  MEGA    YYYYY01L1  0 23  1  JOBID=(TSGMCT YY.DDD 17:39:01),USERDATA=(CONADMIN),OWNER=ADMIN
                        MARY LAZARS                      AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP)
                                                REMOVE TESTCAU GROUP(ADMIN)

```


Connect with Revoke Success/Failure

YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(TESTCAG) REVOKE
YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,REVOKE) CONNECT TESTCAU GROUP(TESTCAG) REVOKE

Connect with Resume Success/Failure

YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(TESTCAG) RESUME
YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,RESUME) CONNECT TESTCAU GROUP(TESTCAG) RESUME

Connect with Revoke Date Success/Failure

YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(TESTCAG) REVOKE(MM/DD/YY)
YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,REVOKE) CONNECT TESTCAU GROUP(TESTCAG) REVOKE(MM/DD/YY)

Connect with Resume Date Success/Failure

YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(TESTCAG) RESUME(MM/DD/YY)
YY.DDD 17:14:01	A90B	TSGMCT MARY LAZARS	MEGA	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:01),USERDATA=(CONADMIN),OWNER=TESTCAG AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,RESUME) CONNECT TESTCAU GROUP(TESTCAG) RESUME(MM/DD/YY)

Connect with Group UACC Success/Failure

YY.DDD 17:14:25 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:25),USERDATA=(CONADMIN),OWNER=TESTCAX AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(TESTCAX) UACC(READ)
YY.DDD 17:14:25 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:25),USERDATA=(CONADMIN),OWNER=TESTCAX AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,UACC) CONNECT TESTCAU GROUP(TESTCAX) UACC(ALTER)

Connect with Group Authority Success/Failure

YY.DDD 17:14:43 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:43),USERDATA=(CONADMIN),OWNER=ADMIN AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(ADMIN) AUTH(CONNECT)
YY.DDD 17:14:43 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:43),USERDATA=(CONADMIN),OWNER=ADMIN AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,AUTHORITY) CONNECT TESTCAU GROUP(ADMIN) AUTHORITY(CONNECT)

Connect with Attribute Success/Failure

YY.DDD 17:14:43 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	0	JOBID=(TSGMCT YY.DDD 17:14:43),USERDATA=(CONADMIN),OWNER=ADMIN AUTH=(INSTALLATION EXIT),REASON=(COMMAND) CONNECT TESTCAU GROUP(ADMIN) SPECIAL
YY.DDD 17:14:43 A90B	TSGMCT MEGA MARY LAZARS	YYYY01L1	0 14	1	JOBID=(TSGMCT YY.DDD 17:14:43),USERDATA=(CONADMIN),OWNER=ADMIN AUTH=(INSTALLATION EXIT),REASON=(COMMAND),VIOL=(GROUP,SPECIAL)



APPENDIX B

SSA ISPF Tables

SSA stores extracted RACF information in ISPF tables. This appendix describes each SSA table. The description includes the name of table fields, formats, content, and the IRRDBU00 record(s) that provide information stored in the tables. Users are welcome to use the information stored in the SSA ISPF tables for report or command generation.

Note SSA ISPF tables should be updated only with the SSA offload process to ensure data integrity.

Adhoc Field Substitution

SSA provides the ability to create adhoc reports that use literal substitution and the power of the Online Generic Search facilities. Refer to ‘Online Generic Searches’ on page 101 for more information about building a substitution mask.

Literal substitution means the mask or value indicator must be the same length as the field whose value will be substituted for it. For example, if you are using the General User Information Online Generic Search, and wish to create an adhoc mask to create reports, you more than likely would want the userid to be part of your mask/report. The SSA mask value is the same name as the ISPF variable name you see below - AAUSER. Therefore, you would have to put the variable name in the position you wanted the userid to be placed while padding it with two blanks.

In the ISPF table layout descriptions below, a new column has been included that documents what value must be used as the mask for the variable in question. IF THE VALUE FOR SUBSTITUTION IS THE SAME LENGTH NO VALUE WILL BE NOTED IN THE NEW COLUMN.

Note Some variables are not eligible for substitution and are noted with a N/A. In most cases, single character variables are (that is, Y/N) are translated to a 3-character value to be used for substitution (that is, YES, NO).

Some variables are long. Those variables deemed too long for single level substitution are broken up into sections. The variable names and the amount of characters that variable cover are documented. It is important to note that the separate variables are sequential pieces of the whole original variable/value. For example, the user installation data field is 255 possible characters long. The installation data field is broken up into 5 substitution masks (AAUSINDT1 through AAUSINDT5) each of which covers 51 characters of the total field. Thus, if you wanted to have characters 52 through 102 displayed on your report, you would use mask variable AAUSINDT2 with 42 blanks following it.

Only the main tables that correspond to the Online Generic Search options are available for adhoc reporting. For example, the main OPERPARM segment table is available for adhoc reporting, however, the MSCOPE table is not.

Generic Search Table Usage

All programming statements (Assembler) necessary to access the SSA ISPF tables are available in the install library. The name of the table is the name of the member where those definitions are stored. The following table shows which SSA ISPF table provides data to conduct a specific Online Generic Search.

Online Generic Search Option	SSA ISPF Table
General Userid	AATBLE01
Userid TSO Segment	AATBLE05
Userid CICS Segment	AATBLE07
Userid DFP Segment	AATBLE08
Userid Language Segment	AATBLE09
Userid OPERPARM Segment	AATBLE10

Online Generic Search Option	SSA ISPF Table
Userid WORKATTR Segment	AATBLE29
Userid NETVIEW Segment	AATBLE30
Userid OMVS Segment	AATBLE11
Userid DCE Segment	AATBLE33
RRSF Associations	AATBLE34
Connects	AATBLE12
CLAUTH Authorities	AATBLE04
Userid Security Categories	AATBLE03
General Group	AATBLE13
Group DFP Segment	AATBLE15
Group OMVS Segment	AATBLE02
General Dataset	AATBLE17
Dataset Permissions	AATBLE20
Dataset Security Categories	AATBLE27
General Resource	AATBLE22
General Resource Permissions	AATBLE26
General Resource Members	AATBLE25
General Resource Session Segment	AATBLE18
General Resource DLFDATA Segment	AATBLE21
General Resource STDATA Segment	AATBLE24
General Resource SystemView Segment	AATBLE35
General Resource Security Categories	AATBLE16

USERID Profile Related Tables

This section describes SSA ISPF tables that provide RACF user ID information.

AATBLE01 Table

Information:General User Information

Main Feed:0200

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAUSER	8	Char	Userid	
AAUSNAME	20	Char	Name	
AAUSDFLG	8	Char	Default Group	
AAUSOWNR	8	Char	Profile Owner	
AAUSCRDT	10	1900-01-01	Creation Date	
AAUSLSDT	10	1900-01-01	Last Used Date	
AAUSLSTM	8	HH:MM:SS	Last Used Time	
AAUSPSDT	10	1900-01-01	PassDate	
AAUSNVLG	1	Y/N	Never Logged On	@NV
AAUSPSWI	3	Numeric	Password Interval (000 = N/A)	@PS
AAUSMODS	44	Char	Model Dataset	
AAUSSPEC	1	Y/N	Special?	@SP
AAUSOPER	1	Y/N	Operations?	@OP
AAUSAUDI	1	Y/N	Auditor?	@AU
AAUSGRPA	1	Y/N	GRPACC?	@GR
AAUSUAUD	1	Y/N	UAUDIT?	@UA
AAUSADSP	1	Y/N	ADSP?	@AD
AAUSOIDC	1	Y/N	OIDCARD?	@OI
AAUSREVO	1	Y/N	Revoked?	@RV
AAUSRVDT	10	1900-01-01	Revoke Date	
AAUSRSDT	10	1900-01-01	Resume Date	
AAUSLGMO	1	Y/N	Logon - Monday?	@LM
AAUSLGTU	1	Y/N	Logon - Tuesday?	@LT
AAUSLGWE	1	Y/N	Logon - Wednesday	@LW
AAUSLGTH	1	Y/N	Logon - Thursday	@LH

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAUSLGFR	1	Y/N	Logon - Friday	@LF
AAUSLGSA	1	Y/N	Logon - Saturday	@LS
AAUSLGSU	1	Y/N	Logon - Sunday	@LU
AAUSLGST	4	HHMM	Logon - Start Time	@LGS
AAUSLGET	4	HHMM	Logon - End Time	@LGE
AAUSPHDT	10	1900-01-01	PhraseDate	
AAUSINDT	255	Char	Installation Data	AAUSINDT1 (51 CHARS) AAUSINDT2 (51 CHARS) AAUSINDT3 (51 CHARS) AAUSINDT4 (51 CHARS) AAUSINDT5 (51 CHARS)
AAUSSLVN	3	Numeric	Security Level (numeric value)	@SL
AAUSSCLV	39	Char	Character value of Security Level	
AAUSLACT	3	Numeric	Number of Unsuccessful logon attempts	@LA
AAUSPWDG	3	Numeric	Current Password Generation number	@PG
AAUSNOPW	3	Y/N/PRO	Logon without a Password	@NO
AAUSSCLB	8	Char	Default Security Label	
AAUSHTSO	1	Y/N	Does user have TSO Segment?	@TS
AAUSHCCS	1	Y/N	Does user have CICS Segment?	@CS
AAUSHDFP	1	Y/N	Does user have DFP Segment?	@DF
AAUSHOPR	1	Y/N	Does user have OPERPARM Segment?	@OE
AAUSHDCE	1	Y/N	Does user have DCE Segment?	@DC

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAUSHNTV	1	Y/N	Does user have NETVIEW Segment?	@NE
AAUSHOMV	1	Y/N	Does user have OMVS Segment?	@OM
AAUSHLAN	1	Y/N	Does user have LANGUAGE Segment?	@LN
AAUSHWRK	1	Y/N	Does user have WORKATTR Segment?	@WK
AAUSHRRF	1	Y/N	Does user have RRSF associations?	@RR
AAUSHSCC	1	Y/N	Does user have security categories?	@SC
AAUSHCLT	1	Y/N	Does user have clauth authorities?	@CL
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE05 Table

Information:Userid - TSO Segment

Main Feed:0220

Field Name	Length	Content	Description	Adhoc Substitution Mask
AATSUSER	8	Char	Userid	
AATSNAME	20	Char	Name	
AATSPROC	8	Char	Logon Procedure	
AATSUNIT	8	Char	Unit	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AATSUSDT	4	Char	UserData	@USD
AATSSIZE	7	Numeric	Size	@TSSIZE
AATSMSZE	7	Numeric	Max Size	@TMSIZE
AATSHCLS	1	Char	Hold Class	@H
AATSJCLS	1	Char	Job Class	@J
AATSMCLS	1	Char	Message Class	@M
AATSSCLS	1	Char	Sysout Class	@S
AATSDEST	8	Char	Destination	
AATSACCT	40	Char	Account	
AATSLCMD	80	Char	Command issued at LOGON	
AATSPRFG	10	Numeric	Performance group associated with the user	
AATSSCLB	8	Char	Default logon security label	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE07 Table

Information:Userid - CICS Segment

Main Feed:0230, 231

Field Name	Length	Content	Description	Adhoc Substitution Mask
AACIUSER	8	Char	Userid	
AACINAME	20	Char	Name	
AACIOP01	1	Y/N	CICS OPCLASS - 01	@01
AACIOP02	1	Y/N	CICS OPCLASS - 02	@02
AACIOP03	1	Y/N	CICS OPCLASS - 03	@03

Field Name	Length	Content	Description	Adhoc Substitution Mask
AACIOP04	1	Y/N	CICS OPCLASS - 04	@04
AACIOP05	1	Y/N	CICS OPCLASS - 05	@05
AACIOP06	1	Y/N	CICS OPCLASS - 06	@06
AACIOP07	1	Y/N	CICS OPCLASS - 07	@07
AACIOP08	1	Y/N	CICS OPCLASS - 08	@08
AACIOP09	1	Y/N	CICS OPCLASS - 09	@09
AACIOP10	1	Y/N	CICS OPCLASS - 10	@10
AACIOP11	1	Y/N	CICS OPCLASS - 11	@11
AACIOP12	1	Y/N	CICS OPCLASS - 12	@12
AACIOP13	1	Y/N	CICS OPCLASS - 13	@13
AACIOP14	1	Y/N	CICS OPCLASS - 14	@14
AACIOP15	1	Y/N	CICS OPCLASS - 15	@15
AACIOP16	1	Y/N	CICS OPCLASS - 16	@16
AACIOP17	1	Y/N	CICS OPCLASS - 17	@17
AACIOP18	1	Y/N	CICS OPCLASS - 18	@18
AACIOP19	1	Y/N	CICS OPCLASS - 19	@19
AACIOP20	1	Y/N	CICS OPCLASS - 20	@20
AACIOP21	1	Y/N	CICS OPCLASS - 21	@21
AACIOP22	1	Y/N	CICS OPCLASS - 22	@22
AACIOP23	1	Y/N	CICS OPCLASS - 23	@23
AACIOP24	1	Y/N	CICS OPCLASS - 24	@24
AACIOPRT	5	Numeric	Operator priority	@OPRT
AACITIME	5	HH:MM	Terminal time-out value	@TIME
AACIOPID	3	Char	Operator identifier	@OI
AACIFRCE	1	Y/N	Is the extended recovery facility (XRF) NOFORCE option in effect?	@FR
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE08 Table

Information:Userid - DFP Segment

Main Feed:0210

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADFUSER	8	Char	Userid	
AADFNAME	20	Char	Name	
AADFDCLS	8	Char	Data Class	
AADFMCLS	8	Char	Management Class	
AADFSCLS	8	Char	Storage Class	
AADFDAPL	8	Char	Data Application	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE09 Table

Information:Userid - Language Segment

Main Feed:0240

Field Name	Length	Content	Description	Adhoc Substitution Mask
AALNUSER	8	Char	Userid	
AALNNAME	20	Char	Name	
AALNPRIM	3	Char	Primary Language	@PR
AALNSECD	3	Char	Secondary Language	@SC

Field Name	Length	Content	Description	Adhoc Substitution Mask
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE10 Table

Information:Userid - OPERPARM Segment

Main Feed:0250

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPUSER	8	Char	Userid	
AAOPNAME	20	Char	Userid name	
AAOPAUMS	1	Y/N	Console authority = MASTER?	@AM
AAOPAUAL	1	Y/N	Console authority = ALL?	@AL
AAOPAUIN	1	Y/N	Console authority = INFO?	@AN
AAOPAUCO	1	Y/N	Console authority = CONS?	@AO
AAOPAUIO	1	Y/N	Console authority = I/O?	@AI
AAOPAUSY	1	Y/N	Console authority = SYSAUTH?	@AY
AAOPAUCM	8	Char	CMDSYS - The name of the system that the extended operator is connected to for command processing.	
AAOPDOM	6	Char	Delete operator messages NORMAL ALL NONE	@OPDOM

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPKEY	8	Char	KEY - Retrieval key used for searching (a null value is indicated by NONE)	
AAOPLVNB	1	Y/N	LEVEL = NB - Broadcast messages to this console are suppressed	@LB
AAOPLVAL	1	Y/N	LEVEL = ALL - Console receives all messages	@LL
AAOPLVR	1	Y/N	LEVEL = R - Console receives WTOR messages	@LR
AAOPLVI	1	Y/N	LEVEL = I - Console receives immediate messages	@LI
AAOPLVCE	1	Y/N	LEVEL = CE - Console receives critical event messages	@LC
AAOPLVE	1	Y/N	LEVEL = E - Console receives eventual event messages	@LE
AAOPLVIN	1	Y/N	LEVEL = IN - Console receives informational messages	@LV
AAOPLGCM	6	Char	LOGCMDRESP - Logging option of command responses received by the extended console SYSTEM NO	OPLGCM
AAOPMF MJ	1	Y/N	MFORM = J - Console messages contain a job ID	@MJ
AAOPMFMM	1	Y/N	MFORM = M - Console messages contain a message ID	@MM
AAOPMFMS	1	Y/N	MFORM = S - Console messages contain a system ID	@MS

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPMFMT	1	Y/N	MFORM = T - Console messages contain a timestamp	@MT
AAOPMFMX	1	Y/N	MFORM = X - Job name and system are to be suppressed for messages issued from the JES3 global processor	@MX
AAOPMGID	1	Y/N	MIGID = YES - Extended operator will receive a migration ID	@MG
AAOPMOJB	1	Y/N	MONITOR = JOBNAMES - Jobnames are monitored	@MB
AAOPMOJS	1	Y/N	MONITOR = JOBNAMEST - Jobnames are monitored with timestamps displayed	@MO
AAOPMOSE	1	Y/N	MONITOR = SESS - Userids are displayed with each TSO initiation and termination	@ME
AAOPMOST	1	Y/N	MONITOR = SESST - Userids and timestamps are displayed with each TSO initiation and termination	@MP
AAOPMOSS	1	Y/N	MONITOR = STATUS -Dataset names and dispositions are displayed with each dataset that is freed	@SS
AAOPRTCA	1	Y/N	ROUTCODE = ALL - Console is enabled for all route codes	@CA

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPRTC�	1	Y/N	ROUTCODE=NONE -Console is not enabled for any route codes	@CN
AAOPR001	1	Y/N	ROUTE CODE 001 Enabled	@001
AAOPR002	1	Y/N	ROUTE CODE 002 Enabled	@002
AAOPR003	1	Y/N	ROUTE CODE 003 Enabled	@003
AAOPR004	1	Y/N	ROUTE CODE 004 Enabled	@004
AAOPR005	1	Y/N	ROUTE CODE 005 Enabled	@005
AAOPR006	1	Y/N	ROUTE CODE 006 Enabled	@006
AAOPR007	1	Y/N	ROUTE CODE 007 Enabled	@007
AAOPR008	1	Y/N	ROUTE CODE 008 Enabled	@008
AAOPR009	1	Y/N	ROUTE CODE 009 Enabled	@009
AAOPR010	1	Y/N	ROUTE CODE 010 Enabled	@010
AAOPR001	1	Y/N	ROUTE CODE 011 Enabled	@011
AAOPR012	1	Y/N	ROUTE CODE 012 Enabled	@012
AAOPR013	1	Y/N	ROUTE CODE 013 Enabled	@013
AAOPR014	1	Y/N	ROUTE CODE 014 Enabled	@014
AAOPR015	1	Y/N	ROUTE CODE 015 Enabled	@015
AAOPR016	1	Y/N	ROUTE CODE 016 Enabled	@016
AAOPR017	1	Y/N	ROUTE CODE 017 Enabled	@017

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR018	1	Y/N	ROUTE CODE 018 Enabled	@018
AAOPR019	1	Y/N	ROUTE CODE 019 Enabled	@019
AAOPR020	1	Y/N	ROUTE CODE 020 Enabled	@020
AAOPR021	1	Y/N	ROUTE CODE 021 Enabled	@021
AAOPR022	1	Y/N	ROUTE CODE 022 Enabled	@022
AAOPR023	1	Y/N	ROUTE CODE 023 Enabled	@023
AAOPR024	1	Y/N	ROUTE CODE 024 Enabled	@024
AAOPR025	1	Y/N	ROUTE CODE 025 Enabled	@025
AAOPR026	1	Y/N	ROUTE CODE 026 Enabled	@026
AAOPR027	1	Y/N	ROUTE CODE 027 Enabled	@027
AAOPR028	1	Y/N	ROUTE CODE 028 Enabled	@028
AAOPR029	1	Y/N	ROUTE CODE 029 Enabled	@029
AAOPR030	1	Y/N	ROUTE CODE 030 Enabled	@030
AAOPR031	1	Y/N	ROUTE CODE 031 Enabled	@031
AAOPR032	1	Y/N	ROUTE CODE 032 Enabled	@032
AAOPR033	1	Y/N	ROUTE CODE 033 Enabled	@033
AAOPR034	1	Y/N	ROUTE CODE 034 Enabled	@034
AAOPR035	1	Y/N	ROUTE CODE 035 Enabled	@035
AAOPR036	1	Y/N	ROUTE CODE 036 Enabled	@036

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR037	1	Y/N	ROUTE CODE 037 Enabled	@037
AAOPR038	1	Y/N	ROUTE CODE 038 Enabled	@038
AAOPR039	1	Y/N	ROUTE CODE 039 Enabled	@039
AAOPR040	1	Y/N	ROUTE CODE 040 Enabled	@040
AAOPR041	1	Y/N	ROUTE CODE 041 Enabled	@041
AAOPR042	1	Y/N	ROUTE CODE 042 Enabled	@042
AAOPR043	1	Y/N	ROUTE CODE 043 Enabled	@043
AAOPR044	1	Y/N	ROUTE CODE 044 Enabled	@044
AAOPR045	1	Y/N	ROUTE CODE 045 Enabled	@045
AAOPR046	1	Y/N	ROUTE CODE 046 Enabled	@046
AAOPR047	1	Y/N	ROUTE CODE 047 Enabled	@047
AAOPR048	1	Y/N	ROUTE CODE 048 Enabled	@048
AAOPR049	1	Y/N	ROUTE CODE 049 Enabled	@049
AAOPR050	1	Y/N	ROUTE CODE 050 Enabled	@050
AAOPR051	1	Y/N	ROUTE CODE 051 Enabled	@051
AAOPR052	1	Y/N	ROUTE CODE 052 Enabled	@052
AAOPR053	1	Y/N	ROUTE CODE 053 Enabled	@053
AAOPR054	1	Y/N	ROUTE CODE 054 Enabled	@054
AAOPR055	1	Y/N	ROUTE CODE 055 Enabled	@055

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR056	1	Y/N	ROUTE CODE 056 Enabled	@056
AAOPR057	1	Y/N	ROUTE CODE 057 Enabled	@057
AAOPR058	1	Y/N	ROUTE CODE 058 Enabled	@058
AAOPR059	1	Y/N	ROUTE CODE 059 Enabled	@059
AAOPR060	1	Y/N	ROUTE CODE 060 Enabled	@060
AAOPR061	1	Y/N	ROUTE CODE 061 Enabled	@061
AAOPR062	1	Y/N	ROUTE CODE 062 Enabled	@062
AAOPR063	1	Y/N	ROUTE CODE 063 Enabled	@063
AAOPR064	1	Y/N	ROUTE CODE 064 Enabled	@064
AAOPR065	1	Y/N	ROUTE CODE 065 Enabled	@065
AAOPR066	1	Y/N	ROUTE CODE 066 Enabled	@066
AAOPR067	1	Y/N	ROUTE CODE 067 Enabled	@067
AAOPR068	1	Y/N	ROUTE CODE 068 Enabled	@068
AAOPR069	1	Y/N	ROUTE CODE 069 Enabled	@069
AAOPR070	1	Y/N	ROUTE CODE 070 Enabled	@070
AAOPR071	1	Y/N	ROUTE CODE 071 Enabled	@071
AAOPR072	1	Y/N	ROUTE CODE 072 Enabled	@072
AAOPR073	1	Y/N	ROUTE CODE 073 Enabled	@073
AAOPR074	1	Y/N	ROUTE CODE 074 Enabled	@074

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR075	1	Y/N	ROUTE CODE 075 Enabled	@075
AAOPR076	1	Y/N	ROUTE CODE 076 Enabled	@076
AAOPR077	1	Y/N	ROUTE CODE 077 Enabled	@077
AAOPR078	1	Y/N	ROUTE CODE 078 Enabled	@078
AAOPR079	1	Y/N	ROUTE CODE 079 Enabled	@079
AAOPR080	1	Y/N	ROUTE CODE 080 Enabled	@080
AAOPR081	1	Y/N	ROUTE CODE 081 Enabled	@081
AAOPR082	1	Y/N	ROUTE CODE 082 Enabled	@082
AAOPR083	1	Y/N	ROUTE CODE 083 Enabled	@083
AAOPR084	1	Y/N	ROUTE CODE 084 Enabled	@084
AAOPR085	1	Y/N	ROUTE CODE 085 Enabled	@085
AAOPR086	1	Y/N	ROUTE CODE 086 Enabled	@086
AAOPR087	1	Y/N	ROUTE CODE 087 Enabled	@087
AAOPR088	1	Y/N	ROUTE CODE 088 Enabled	N/A**
AAOPR089	1	Y/N	ROUTE CODE 089 Enabled	N/A**
AAOPR090	1	Y/N	ROUTE CODE 090 Enabled	N/A**
AAOPR091	1	Y/N	ROUTE CODE 091 Enabled	N/A**
AAOPR092	1	Y/N	ROUTE CODE 092 Enabled	N/A**
AAOPR093	1	Y/N	ROUTE CODE 093 Enabled	N/A**

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR094	1	Y/N	ROUTE CODE 094 Enabled	N/A**
AAOPR095	1	Y/N	ROUTE CODE 095 Enabled	N/A**
AAOPR096	1	Y/N	ROUTE CODE 096 Enabled	N/A**
AAOPR097	1	Y/N	ROUTE CODE 097 Enabled	N/A**
AAOPR098	1	Y/N	ROUTE CODE 098 Enabled	N/A**
AAOPR099	1	Y/N	ROUTE CODE 099 Enabled	N/A**
AAOPR100	1	Y/N	ROUTE CODE 100 Enabled	N/A**
AAOPR101	1	Y/N	ROUTE CODE 101 Enabled	N/A**
AAOPR102	1	Y/N	ROUTE CODE 102 Enabled	N/A**
AAOPR103	1	Y/N	ROUTE CODE 103 Enabled	N/A**
AAOPR104	1	Y/N	ROUTE CODE 104 Enabled	N/A**
AAOPR105	1	Y/N	ROUTE CODE 105 Enabled	N/A**
AAOPR106	1	Y/N	ROUTE CODE 106 Enabled	N/A**
AAOPR107	1	Y/N	ROUTE CODE 107 Enabled	N/A**
AAOPR108	1	Y/N	ROUTE CODE 108 Enabled	N/A**
AAOPR109	1	Y/N	ROUTE CODE 109 Enabled	N/A**
AAOPR110	1	Y/N	ROUTE CODE 110 Enabled	N/A**
AAOPR111	1	Y/N	ROUTE CODE 111 Enabled	N/A**
AAOPR112	1	Y/N	ROUTE CODE 112 Enabled	N/A**

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPR113	1	Y/N	ROUTE CODE 113 Enabled	N/A**
AAOPR114	1	Y/N	ROUTE CODE 114 Enabled	N/A**
AAOPR115	1	Y/N	ROUTE CODE 115 Enabled	N/A**
AAOPR116	1	Y/N	ROUTE CODE 116 Enabled	N/A**
AAOPR117	1	Y/N	ROUTE CODE 117 Enabled	N/A**
AAOPR118	1	Y/N	ROUTE CODE 118 Enabled	N/A**
AAOPR119	1	Y/N	ROUTE CODE 119 Enabled	N/A**
AAOPR120	1	Y/N	ROUTE CODE 120 Enabled	N/A**
AAOPR121	1	Y/N	ROUTE CODE 121 Enabled	N/A**
AAOPR122	1	Y/N	ROUTE CODE 122 Enabled	N/A**
AAOPR123	1	Y/N	ROUTE CODE 123 Enabled	N/A**
AAOPR124	1	Y/N	ROUTE CODE 124 Enabled	N/A**
AAOPR125	1	Y/N	ROUTE CODE 125 Enabled	N/A**
AAOPR126	1	Y/N	ROUTE CODE 126 Enabled	N/A**
AAOPR127	1	Y/N	ROUTE CODE 127 Enabled	N/A**
AAOPR128	1	Y/N	ROUTE CODE 128 Enabled	N/A**
AAOPSTOR	5	Numeric	STORAGE - Number of megabytes of storage that can be used for message queuing	@STOR
AAOPUD	1	Y/N	UD - Operator is to receive undeliverable messages	@UD

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOPALTG	8	Char	Default group associated with this operator	
AAOPAUTO	1	Y/N	Operator is to receive messages automated within the sysplex	@AU
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

** Due to ISPF limitations, these fields are not supported.

AATBLE06 Table

Information:Userid - OPERPARM Mscopes

Main Feed:0251

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AAOPMSCU	8	Char	Userid
AAOPMSCN	20	Char	Userid name
AAOPMSCS	8	Char	Mscope entry (system name)
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE29 Table

Information:Userid - WORKATTR Segment

Main Feed:0260

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAWKUSER	8	Char	Userid	
AAWKUNME	20	Char	Userid name	
AAWKROOM	60	Char	Room for delivery	
AAWKDEPT	60	Char	Department for delivery	
AAWKBLDG	60	Char	Building for delivery	
AAWKNAME	60	Char	Area for delivery	
AAWKADR1	60	Char	Address line 1	
AAWKADR2	60	Char	Address line 2	
AAWKADR3	60	Char	Address line 3	
AAWKADR4	60	Char	Address line 4	
AAWKACNT	255	Char	Account number	AAWKACNT1 (51 chars) AAWKACNT2 (51 chars) AAWKACNT3 (51 chars) AAWKACNT4 (51 chars) AAWKACNT5 (51 chars)
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE11 Table

Information:Userid - OMVS Segment

Main Feed:0270

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOMUUSR	8	Char	Userid	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOMUNME	20	Char	Userid name	
AAOMUUID	10	Char	OMVS UID	
AAOMUHML	1023	Char**	OMVS Home Path associated with the UID	AAOMUHML01 through AAOMUHML31 (33 chars)
AAOMUDFL	1023	Char**	OMVS Default Program associated with the UID	AAOMUDFL01 through AAOMUDFL31 (33 chars)
AAOMUHMS	40	Char**	First 40 characters of the Home Path (for display)	
AAOMUDFS	40	Char**	First 40 characters of the Default Program (for display)	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

** Characters are in upper and lower case

** Characters can contain alphanumeric, national and blank characters

AATBLE30 Table

Information:Userid - NETVIEW Segment

Main Feed:0280

Field Name	Length	Content	Description	Adhoc Substitution Mask
AANVUSER	8	Char	Userid	
AANVNAME	20	Char	Userid name	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AANVCTL	8	Char	CTL Value - GENERAL GLOBAL SPECIFIC	
AANVMSGR	1	Y/N	Eligible to receive unsolicited messages	@MS
AANVCNNM	8	Char	Default Console Name	
AANVNGMF	1	Y/N	Authorized to Netview graphic Monitoring Facility	@MF
AANVIC	255	Char	Command list executed at logon	AANVIC1 (51 chars) AANVIC2 (51 chars) AANVIC3 (51 chars) AANVIC4 (51 chars) AANVIC5 (51 chars)
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE31 Table

Information:Userid - NETVIEW (opclasses) Segment

Main Feed:0281

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AANVOUSR	8	Char	Userid
AANVONME	20	Char	Userid name
AANVOOPC	4	Numeric	OPCLASS value from 1 to 2040

Field Name	Length	Content	Description
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE32 Table

Information:Userid - NETVIEW (Domains) Segment

Main Feed:0282

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AANVDUSR	8	Char	Userid
AANVDNME	20	Char	Userid name
AANVDOMN	5	Char	Domain
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE33 Table

Information:Userid - DCE Segment

Main Feed:0290

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADCUSER	8	Char	Userid	
AADCNAME	20	Char	Userid name	
AADCUUID	36	Char	User Principal Universal Unique Identifier (UUID)	
AADCPRNM	1023	Char**	DCE User Principal Name associated with the z/OS id	AADCPRNM01 through AADCPRNM31 (33 chars)

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADCPRNS	40	Char**	First 40 characters of the principal name (for display)	
AADCHCNM	1023	Char**	DCE Cell Name (Home)	AADCHCNM01 through AADCHCNM31 (33 chars)
AADCHCNS	40	Char**	First 40 characters of the DCE Cell Name (for display)	
AADCHCUD	36	Char	DCE Cell UUID (Home)	
AADCAUTL	1	Y/N	DCE Automatic Login	@AU
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

** Characters are in upper and lower case

** Characters can contain alphanumeric, national and blank characters

AATBLE03 TableA

Information:Userid - Security Categories

Main Feed:0201

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAUSSCUS	8	Char	Userid	
AAUSSCNA	20	Char	Userid name	
AAUSSCSC	5	Numeric	Security category (numeric value)	@SCSC
AAUSSCSN	39	Char	Security category	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE04 Table

Information:Userid - Clauth Authority

Main Feed:0202

Field Name	Length	Content	Description	Adhoc Substitution Mask
AACLUSER	8	Char	Userid	
AACLNAME	20	Char	Userid name	
AACLCLAS	8	Char	Class	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE34 Table

Information:Userid - RRSF Information

Main Feed:0206

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARRUSER	8	Char	Userid	
AARRUNME	20	Char	Userid name	
AARRNODE	8	Char	Target node name	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARRTUSR	8	Char	Target userid	
AARRVERS	3	Numeric	Version of this record	@VE
AARRPEER	1	Y/N	Is this a peer userid?	@PE
AARRMNGR	1	Y/N	Is the userid the manager?	@MN
AARRBMGR	1	Y/N	Is the remote userid the manager?	@BM
AARRRPND	1	Y/N	Is this remote RACF association pending?	@RP
AARRLPND	1	Y/N	Is this local RACF association pending?	@LP
AARRPSYN	1	Y/N	Is there password synchronization with this userid?	@PS
AARRRERR	1	Y/N	Was a system error encountered on the remote system?	@RE
AARRGTD1	10	1900-01-01	GMT date stamp for when this record was defined	
AARRGTT1	15	HH:MM:SS.TTHHTT	GMT time stamp for when this record was defined (i.e,11:34.880989).	
AARRGTD2	10	1900-01-01	GMT date stamp when this association was approved or refused. Based on the REMOTE_REFUSAL bit setting.	
AARRGTT2	15	HH:MM:SS.TTHHTT	GMT time stamp when this association was approved or refused (i.e,11:34.880989). Based on the REMOTE_REFUSAL bit setting.	
AARRCRID	8	Char	Userid who created this entry.	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE12 Table

Information:Connect Profiles

Main Feed:0205, 0102(auth)

Field Name	Length	Content	Description	Adhoc Substitution Mask
AACTUSER	8	Char	Userid	
AACTNAME	20	Char	Name	
AACTGRP	8	Char	Connect group	
AACTOWNR	8	Char	Connect owner	
AACTUACC	7	Char	Connect UACC NONE READ UPDATE CONTROL ALTER	@CTUACC
AACTUCCN	1	Numeric	Connect UACC (numeric value) 0=NONE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A
AACTAUTH	7	Char	Connect authority	@CTAUTH

Field Name	Length	Content	Description	Adhoc Substitution Mask
AACTATHN	1	Numeric	Connect authority (numeric value) 0=NONE 1= USE 2=CREATE 3=CONNECT 4=JOIN	N/A
AACTSPEC	1	Y/N	Group Special?	@SP
AACTOPER	1	Y/N	Group Operations?	@OP
AACTAUDI	1	Y/N	Group Auditor?	@AU
AACTGRPA	1	Y/N	Group GRPACC?	@GR
AACTADSP	1	Y/N	Group ADSP?	@AD
AACTREVO	1	Y/N	Group Revoke?	@RV
AACTRVDT	10	1900-01-01	Group Revoke date	
AACTRSDT	10	1900-01-01	Group Resume date	
AACTLCTM	8	HH:MM:SS	Last connect time	
AACTLCDT	10	1900-01-01	Last connect date	
AACTRACI	5	Numeric	Number of RACINITs issued for this user/group combination	@RACI
AACTNOTR	1	Y/N	Does this user have the NOTERMUACC attribute in this group?	@NT
AACTCTDT	10	1900-01-01	Connection date	
AACTDFLT	1	Y/N	Default Group Connect	@DF
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

Group Profile Related Tables

This section describes SSA ISPF tables that provide RACF group profile information.

AATBLE13 Table

Information:General Group Information

Main Feed:0100

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAGROUP	8	Char	Group	
AAGPSUPR	8	Char	Superior Group	
AAGPOWNR	8	Char	Profile Owner	
AAGPMDDS	44	Char	Model Dataset	
AAGPTERM	1	Y/N	TERMUACC?	@TU
AAGPUSER	1	Y/N	Does the group have users connected?	@US
AAGPSUBG	1	Y/N	Does the group have subgroups?	@SG
AAGPCRDT	10	1900-01-01	Creation Date	
AAGPUACC	7	Char	Default universal access NONE EXECUTE READ UPDATE CONTROL ALTER	@GPUACC
AAGPUCCN	1	Numeric	Default universal access (Numeric value) 0=NONE 1=EXECUTE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAGPINDT	255	Char	Installation Data	AAGPINDT1 (51 chars) AAGPINDT2 (51 chars) AAGPINDT3 (51 chars) AAGPINDT4 (51 chars) AAGPINDT5 (51 chars)
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE15 Table

Information:Group - DFP Segment

Main Feed:0110

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADFGROP	8	Char	Group	
AADFGMCL	8	Char	Management Class	
AADFGSCL	8	Char	Storage Class	
AADFGDCL	8	Char	Data Class	
AADFGDAP	8	Char	Data Application	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE02 Table

Information:Group - OMVS Data
Main Feed:0120

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAOMGGRP	8	Char	Group	
AAOMGGID	10	Char	Group OMVS GID	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

Dataset Profile Related Tables

This section describes SSA ISPF tables that provide dataset profile information.

AATBLE17 Table

Information:General Dataset Profile Information

Main Feed:0400

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADSPROF	44	Char	Dataset Profile	
AADSTYPE	1	G/D/M/T	Profile Type G = Generic D = Discrete M = Model T = Tape	AADSTYPE (types are spelled out in substitution)
AADSVOLM	6	Char	Volume	@VOLM
AADSOWNR	8	Char	Profile Owner	
AADSHLQ	8	Char	High Level Qualifier	
AADSUACC	7	Char	UACC (universal access) NONE EXECUTE READ UPDATE CONTROL ALTER	@DSUACC
AADSUCCN	1	Numeric	UACC (numeric value) 0=NONE 1=EXECUTE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A
AADSWARN	1	Y/N	Is warning active?	@WN
AADSNTFY	8	Char	Notify id	
AADSRESO	8	Char	DFP Resowner	
AADSLEVL	2	Numeric	Profile Level	N/A
AADSERSE	1	Y/N	For DASD data set, is this dataset to be scratched when delete?	@ER

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADSCRDT	10	1900-01-01	Creation Date	
AADSLRFD	10	1900-01-01	Last Referenced Date	
AADSLCHD	10	1900-01-01	Last Changed Date	
AADSALCN	5	Numeric	Alter Count	@ALCN
AADSCOCN	5	Numeric	Control Count	@COCN
AADSUPCN	5	Numeric	Update Count	@UPCN
AADSRECN	5	Numeric	Read Count	@RECN
AADSGPDS	1	Y/N	Is this a group data set?	@GD
AADSDVCE	8	Char	EBCDIC name of the device type on which the dataset resides	
AADSINDT	255	Char	Installation Data	AADSINDT1 (51 chars) AADSINDT2 (51 chars) AADSINDT3 (51 chars) AADSINDT4 (51 chars) AADSINDT5 (51 chars)
AADSGPID	8	Char	Connect group of creator of dataset profile	
AADSADLV	7	Char	Local audit level of auditor-specified auditing that is performed ALL SUCCESS FAIL NONE	@DSADLV
AADSGALV	7	Char	Global audit level of auditor-specified auditing that is performed ALL SUCCESS FAIL NONE	@DSGALV

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADSAOKL	7	Char	Audit OK Level NONE READ UPDATE CONTROL ALTER	@DSAOKL
AADSAFAL	7	Char	Audit Failure Level NONE READ UPDATE CONTROL ALTER	@DSAFAL
AADSGOKL	7	Char	Global Audit OK Level NONE READ UPDATE CONTROL ALTER	@DSGOKL
AADSGFAL	7	Char	Global Audit Failure Level NONE READ UPDATE CONTROL ALTER	@DSGFAL
AADSSECL	3	Numeric	Security Level	@SL
AADSSCLN	39	Char	Name of Security Level	
AADSRETN	5	Numeric	Retention period of the dataset	@RETN
AADSSCLB	8	Char	Security Label	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE20 Table

Information:Dataset Profile Permissions

Main Feed:0402 (cnd), 0404 (std)

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADPRSCE	44	Char	Dataset Profile	
AADPRTYP	1	G/D/M/T	Profile Type G = Generic D = Discrete M = Model T = Tape	AADPRTYP (types are spelled out in substitution)
AADPRVOL	6	Char	Volume	@VOLM
AADPACID	8	Char	Access Entry	
AADPACET	8	Char	Access Entry Type USER GROUP GENERAL OBSOLETE	
AADPACNA	20	Char	If access entry type is USER, this field will contain the user name	
AADPACLV	7	Char	Access Level NONE EXECUTE READ UPDATE CONTROL ALTER	@DPACLV
AADPACLN	1	Numeric	Access Level (numeric value) 0=NONE 1=EXECUTE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A
AADPACCN	5	Numeric	Access Count	@ACCN
AADPACTY	3	Char	Permit Type STD=Standard CND=Conditional	@TY
AADPACCE	8	Char	Conditional Entry	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AADPACCC	8	Char	Conditional Class (that is, PROGRAM)	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE27 Table

Information:Dataset Profile Security Categories

Main Feed:0401

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAD1PROF	44	Char	Dataset Profile	
AAD1TYPE	1	G/D/M	Profile Type G = Generic D = Discrete M = Model	AAD1TYPE (types are spelled out in substitution)
AAD1VOLM	6	Char	Volume	@VOLM
AAD1SCTN	5	Numeric	Security Category (numeric value)	@SCTN
AAD1SCAT	39	Char	Security Category (name)	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

General Resource Profile Related Tables

This section describes SSA ISPF tables that provide general resource profile information.

AATBLE22 Table

Information:General Resource Profile Information

Main Feed:0500

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARSPROF	44	Char	Resource Profile (Short/Display name)	
AARSTYPE	1	G/D	Profile Type G = Generic D = Discrete	AARSTYPE (types are spelled out in substitution)
AARSPRFL	246	Char	Resource Profile (Long name)	AARSPRFL1 (51 chars) AARSPRFL2 (51 chars) AARSPRFL3 (51 chars) AARSPRFL4 (51 chars) AARSPRFL5 (42 chars)
AARSPFLN	3	Numeric	Length of resource profile	@LN
AARSCLAS	8	Char	Resource Class	
AARSOWNR	8	Char	Profile Owner	
AARSUACC	7	Char	UACC (universal access) NONE EXECUTE READ UPDATE CONTROL ALTER	@RSUACC

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARSUCCN	1	Numeric	UACC (numeric value) 0=NONE 1=EXECUTE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A
AARSWARN	1	Y/N	Warning?	@WN
AARSSNGL	1	Y/N	If this is a TAPEVOL profile, is there only one data set on this tape?	@SN
AARSTPAU	1	Y/N	If this is a TAPEVOL profile, is the TAPEVOL protection automatic?	@TP
AARSTVTC	1	Y/N	If this is a TAPEVOL profile, is there a tape volume table of contents on this tape?	@TV
AARSNTFY	8	Char	Notify Userid	
AARSTSUN	1	Y/N	Can the terminal be used on Sunday?	@SU
AARSTMON	1	Y/N	Can the terminal be used on Monday?	@MO
AARSTTUE	1	Y/N	Can the terminal be used on Tuesday?	@TU
AARSTWED	1	Y/N	Can the terminal be used on Wednesday?	@WE
AARSTTHU	1	Y/N	Can the terminal be used on Thursday?	@TH
AARSTFRI	1	Y/N	Can the terminal be used on Friday?	@FR
AARSTSAT	1	Y/N	Can the terminal be used on Saturday?	@SA
AARSTSTT	8	HH:MM:SS	After what time may a user logon from this terminal? (Start Time)	
AARSTENT	8	HH:MM:SS	After what time may a user not logon from this terminal? (End Time)	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARSZOFF	5	HH:MM	Time zone in which the terminal is located.	@ZOFF
AARSZDIR	1	Char	The direction of the time zone shift E=East W=West	@ZD
AARSLEVL	3	Numeric	Resource Level	@LV
AARSCRDT	10	1900-01-01	Create Date	
AARSLRFD	10	1900-01-01	Last Referenced Date	
AARSLCHD	10	1900-01-01	Last Changed Date	
AARSALCN	5	Numeric	Alter Count	@ALCN
AARSCOCN	5	Numeric	Control Count	@COCN
AARSUPCN	5	Numeric	Update Count	@UPCN
AARSRECN	5	Numeric	Read Count	@RECN
AARSINDT	255	Char	Installation Data	AARSINDT1 (51 chars) AARSINDT2 (51 chars) AARSINDT3 (51 chars) AARSINDT4 (51 chars) AARSINDT5 (51 chars)
AARSADLV	7	Char	Local audit level of auditor-specified auditing that is performed ALL SUCCESS FAIL NONE	@RSADLV

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARSGALV	7	Char	Global audit level of auditor-specified auditing that is performed ALL SUCCESS FAIL NONE	@RSGALV
AARSAOKL	7	Char	Audit OK Level NONE READ UPDATE CONTROL ALTER	@RSAOKL
AARSAFAL	7	Char	Audit Failure Level NONE READ UPDATE CONTROL ALTER	@RSAFAL
AARSGOKL	7	Char	Global Audit OK Level NONE READ UPDATE CONTROL ALTER	@RSGOKL
AARSGFAL	7	Char	Global Audit Failure Level NONE READ UPDATE CONTROL ALTER	@RSGFAL
AARSSECL	3	Numeric	Security Level	@SL
AARSSCLN	39	Chars	Name of Security Level	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARSAPDT	255	Char	Application data	AARSAPDT1 (51 chars) AARSAPDT2 (51 chars) AARSAPDT3 (51 chars) AARSAPDT4 (51 chars) AARSAPDT5 (51 chars)
AARSSCLB	8	Char	Security Label	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE26 Table

Information:General Resource Profile Permissions

Main Feed:0507 (cnd), 0505 (std)

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARPRSCE	44	Char	Resource Profile (short/display length)	
AARPRSCL	246	Char	Resource Profile (full length)	AARPRSCL1 (51 chars) AARPRSCL2 (51 chars) AARPRSCL3 (51 chars) AARPRSCL4 (51 chars) AARPRSCL5 (42 chars)
AARPRSLN	3	Numeric	Length of resource profile	@LN
AARPRCLS	8	Char	Resource Class	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AARPACID	8	Char	Access Entry	
AARPACET	8	Char	Access Entry Type USER GROUP GENERAL OBSOLETE	
AARPACNA	20	Char	If access entry type is USER, this field will contain the user name	
AARPACLV	7	Char	Access Level NONE EXECUTE READ UPDATE CONTROL ALTER	@RPACLV
AARPACLN	1	Numeric	Access Level (numeric value) 0=NONE 1=EXECUTE 2=READ 3=UPDATE 4=CONTROL 5=ALTER	N/A
AARPACCN	5	Numeric	Access Count	@ACCN
AARPACTY	3	Char	Permit Type STD=Standard CND=Conditional	@TY
AARPACCE	8	Char	Conditional Entry	
AARPACCC	8	Char	Conditional Class (that is, PROGRAM)	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE25 Table

Information:General Resource Profile Members

Main Feed:0503

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR1MPRF	40	Char	Resource Profile (Short/Display)	
AAR1MCLS	8	Char	Resource class	
AAR1MPFL	246	Char	Resource Profile (Long)	AAR1MPFL1 (51 chars) AAR1MPFL2 (51 chars) AAR1MPFL3 (51 chars) AAR1MPFL4 (51 chars) AAR1MPFL5 (42 chars)
AAR1MPLN	3	Numeric	Length of resource profile	@LN
AAR1MMEM	40	Char	Member (Short/Display)	
AAR1MMML	246	Char	Member (Long)	AAR1MMML1 (51 chars) AAR1MMML2 (51 chars) AAR1MMML3 (51 chars) AAR1MMML4 (51 chars) AAR1MMML5 (42 chars)
AAR1MMLN	3	Numeric	Length of resource profile member	@LM
AAR1GLBA	7	Char	For GLOBAL profiles - access that is allowed NONE READ UPDATE CONTROL ALTER	@R1GLBA
AAR1PADD	8	PADCHK NOPADC HK	For PROGRAM profiles -Program access to data set (PADS)	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR1PADV	6	Char	For PROGRAM profiles -volume upon which the program resides	R1PADV
AAR1SECL	5	Numeric	For SECLEVEL profile in the SECDATA class - numeric value for security level	@SECL
AAR1CATG	5	Numeric	For CATEGORY profile in the SECDATA class - numeric value for security category	@CATG
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE14 Table

Information:General Resource Tape Volume Data

Main Feed:501

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AAR2TPRF	40	Char	Resource Profile (Short/Display)
AAR2TCLS	8	Char	Resource class
AAR2TPFL	246	Char	Resource Profile (Long)
AAR2TPLN	3	Numeric	Length of resource profile
AAR2TSEQ	5	Numeric	File sequence number of the tape dataset
AAR2TCRD	10	1900-01-01	Creation date of the tape data set
AAR2TDIS	1	Y/N	Discrete profile exists
AAR2TINN	44	Char	RACF internal data set name
AAR2TINV	255	Char	Volumes upon which the dataset resides
AAR2TCRN	44	Char	Dataset name used when creating the dataset

Field Name	Length	Content	Description
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE16 Table

Information:General Resource Profile Security Categories

Main Feed:0502

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR3PROF	40	Char	Resource Profile (Short/Display)	
AAR3CLAS	8	Char	Resource class	
AAR3PRFL	246	Char	Resource Profile (Long)	AAR3PRFL1 (51 chars) AAR3PRFL2 (51 chars) AAR3PRFL3 (51 chars) AAR3PRFL4 (51 chars) AAR3PRFL5 (42 chars)
AAR3PRLN	3	Numeric	Length of resource profile	@LN
AAR3CATN	5	Numeric	Security Category (numeric value)	@CATN
AAR3CATG	39	Char	Security Category	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE18 Table

Information:General Resource Session Segment

Main Feed:0510

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR4PROF	40	Char	Resource Profile (Short/Display)	
AAR4CLAS	8	Char	Resource class	
AAR4PRFL	246	Char	Resource Profile (Long)	AAR4PRFL1 (51 chars) AAR4PRFL2 (51 chars) AAR4PRFL3 (51 chars) AAR4PRFL4 (51 chars) AAR4PRFL5 (42 chars)
AAR4PRLN	3	Numeric	Length of resource profile	@LN
AAR4SKEY	8	Char	Key associated with the APPC session	
AAR4LOCK	1	Y/N	Profile is locked	@LK
AAR4KDTE	10	1900-01-01	Last date that the session key was changed	
AAR4KINT	5	Numeric	Number of days that the key is valid	@KINT
AAR4SLSF	5	Numeric	Current number of failed attempts	@SLSF
AAR4MAXF	5	Numeric	Number of failed attempts before lockout	@MAXF
AAR4CNVS	8	Char	Security checking performed when sessions are established NONE CONVSEC PERSISTV ALREADYV AVPV	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE19 Table

Information:General Resource Session Entities

Main Feed:0511

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AAR5PROF	40	Char	Resource Profile (Short/Display)
AAR5CLAS	8	Char	Resource class
AAR5PRFL	246	Char	Resource Profile (Long)
AAR5PRLN	3	Numeric	Length of resource profile
AAR5ENTN	35	Char	Entity name
AAR5FLCN	5	Numeric	Number of failed session attempts
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE21 Table

Information:General Resource DLFDATA Segment

Main Feed:0520

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR6PROF	40	Char	Resource Profile (Short/Display)	
AAR6CLAS	8	Char	Resource class	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR6PRFL	246	Char	Resource Profile (Long)	AAR6PRFL1 (51 chars) AAR6PRFL2 (51 chars) AAR6PRFL3 (51 chars) AAR6PRFL4 (51 chars) AAR6PRFL5 (42 chars)
AAR6PRLN	3	Numeric	Length of resource profile	@LN
AAR6RETN	1	Y/N	Resource is retained	@RE
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE23 Table

Information:General Resource DLFDATA Job Names

Main Feed:0521

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AAR7PROF	40	Char	Resource Profile (Short/Display)
AAR7CLAS	8	Char	Resource class
AAR7PRFL	246	Char	Resource Profile (Long)
AAR7PRLN	3	Numeric	Length of resource profile
AAR7JOBN	8	Char	Job name
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

AATBLE24 Table

Information:General Resource STDATA (Started Task) Segment

Main Feed:0540

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR8PROF	40	Char	Resource Profile (Short/Display)	
AAR8CLAS	8	Char	Resource class	
AAR8PRFL	246	Char	Resource Profile (Long)	AAR8PRFL1 (51 chars) AAR8PRFL2 (51 chars) AAR8PRFL3 (51 chars) AAR8PRFL4 (51 chars) AAR8PRFL5 (42 chars)
AAR8PRLN	3	Numeric	Length of resource profile	@LN
AAR8USER	8	Char	Userid assigned	
AAR8GROP	8	Char	Group assigned	
AAR8PRIV	1	Y/N	Process runs privileged	@PV
AAR8TRST	1	Y/N	Process runs trusted	@TR
AAR8TRCE	1	Y/N	Entry is to be traced	@TC
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE35 Table

Information:General Resource SFVMR (SystemView) Segment

Main Feed:0550

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR9PROF	40	Char	Resource Profile (Short/Display)	

Field Name	Length	Content	Description	Adhoc Substitution Mask
AAR9CLAS	8	Char	Resource class	
AAR9PRFL	246	Char	Resource Profile (Long)	AAR9PRFL1 (51 chars) AAR9PRFL2 (51 chars) AAR9PRFL3 (51 chars) AAR9PRFL4 (51 chars) AAR9PRFL5 (42 chars)
AAR9PRLN	3	Numeric	Length of resource profile	@LN
AAR9SCRIP	8	Char	Script Name	
AAR9PARM	8	Char	Parm Name	
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).	N/A

AATBLE36 Table

Information:General Resource Tape Volumes

Main Feed:0504

** Not Available for Adhoc Reporting

Field Name	Length	Content	Description
AAR0PROF	40	Char	Resource Profile (Short/Display)
AAR0CLAS	8	Char	Resource class
AAR0PRFL	246	Char	Resource Profile (Long)
AAR0PRLN	3	Numeric	Length of resource profile
AAR0VOLM	6	Char	Tape Volume
AQSEL	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).

Field Name	Length	Content	Description
AAMARK	1	Blank	Reserved - Field is not to be updated by users except on temporary basis (that is, TBOPEN NOWRITE).



APPENDIX C

Miscellaneous SSA Features

This appendix describe miscellaneous features that do not belong to a specific SSA function.

Revise or Delete Stored Jobs

The SSA Revise/Delete Stored Jobs option allows users to access their stored JCL with the SSA ISPF based storage facility. Below is the Review Generated JCL screen that the Reports, Command Generation and The SCHEDULER use after file tailoring has created the JCL based on your input. This screen is the most common interface to store generated JCL.

```

----- SSA -----
Review Generated JCL

Command ==>

Dataset In Use ==> 'USER01.SSA.TEMP.JCL(BATCH)'

OPTION ==> E

Enter E to Edit the Generated JCL

V to View the Generated JCL
S to Submit the Generated JCL
ST to Store the Generated JCL
SC to Schedule the Generated JCL

Hit Enter to Continue      PF03=EXIT/PF01=HELP

```

When the user enters “ST” and hits enter they are presented with a popup screen in which they can enter a title for the job up to 60 characters in length. Below is a sample of the title entry screen.

```

----- SSA -----
Review Generated JCL

Command ==>

Da |----- SSA -----|
   |Job Storage          |
   |Command ==>         |
   |Enter the Title of the Job you want to Store: |
   |==> _____|
   |Hit Enter to Continue      PF03/EXIT/PF01=HELP|
   |-----|
   |SC to Schedule the Generated JCL|
   |Hit Enter to Continue      PF03=EXIT/PF01=HELP|

```

The title entered is the title shown when you choose the Revise/Delete Stored Jobs option.

Below is a sample of the Revise/Delete Stored Jobs display.

```

----- SSA -----
Revise/Delete Stored Jobs

Command ==>

Scroll ==> CSR

R = Revise or D = Delete

SELECT      Stored Job Title
-----
____ TEST STORE
____ REPORT ON APF AUTHORIZED LIBRARIES WITH PERMITS EXPANDED
____ REPLICATE USERID JOB FOR PAYROLL USERIDS
____ ACCESS REPORT ON DEMONSTRATION USERIDS
____ THIS IS THE REPORT FOR WALK04 USERID
***** Bottom of data *****

```


Select as many stored jobs as you wish; enter “R” to revise the stored job or “D” to delete the stored jobs. If you chose to delete a stored job, a prompt appears to confirm the deletion request.

The JCL Revision screen has a few differences from the Review JCL screen displayed before as shown below.

```
----- SSA -----
                        JCL Revision
Command ==>

Dataset In Use ==> 'USER01.TSCSSA.TEMP.JCL(BATCH)'

OPTION ==> E

Enter E    to Edit the JCL
      V    to View the JCL
      SC   to Schedule the JCL
      S    to Submit the JCL
      REST to Re-Store the JCL with the same title
      STN  to Store the JCL with a new title

Hit Enter to Continue      PF03=EXIT/PF01=HELP
```

The JCL Revision screen allows you to restore the JCL with the same title it had when retrieved, or store the JCL with a new title that leaves the original job intact.

Retrieve or Store Commands

After using either the Adhoc command generation facility in Online Generic Searches, or any of the Command Generation functions in online mode, you are presented with the Process Generated Commands Edit Session. Below is a sample of the screen.

```
Process Generated Commands ----- SSA ----- Process Generated Commands
Command ==>                               Scroll ==> CSR

      Action Command                      Action Taken
      -----
      AAEXEC                          Execute Commands Immediately
      AABATCH                         Place Commands in Batch JCL
      AASCHED                         Schedule Commands
      AASTORE                         Store or Retrieve Commands

EDIT ---- USER01.TSCSSA.COMMAND.OUTPUT----- COLUMNS 00001 00072
***** ***** Top of Data *****
=NOTE= COMMANDS ARE READY FOR EXECUTION
000001 ADDUSER USER001 NAME('TEST USERID      ') -
000002   DFLTGRP(MEGA      ) OWNER(MEGA      )
000003 ALTUSER  USER001 SPECIAL OPERATIONS AUDITOR
000004 PASSWORD USER(USER001 ) INTERVAL(180)
000005 ALTUSER  USER001 CLAUTH(USER      )
000006 CONNECT  USER001 GROUP(ADMIN  ) OWNER(ADMINAID) -
000007   AUTH(USE      ) -
000008   UACC(NONE      )
000009 CONNECT  USER001 GROUP(ADMINAID) OWNER(GOODPAO ) -
000010   AUTH(USE      ) -
000011   UACC(NONE      )
000012 CONNECT  USER001 GROUP(MEGA    ) OWNER(MEGA    ) -
```

One of the features available from this screen is the AASTORE macro. The AASTORE macro stores currently displayed commands, or retrieves previously stored commands into the edit session. Enter AASTORE from the command line to begin storing or retrieving commands. You will then be presented with the Generated Command(s) Storage or Retrieval screen as shown below.

```
Process Generated Commands ----- SSA ----- Process Generated Commands
Command ==> aastore                               Scroll ==> CSR

      Action Command                      Action Taken
      -----
      ----- SSA -----
      Generated Command(s) Storage or Retrieval
      Command ==>

      Do you want to Store the commands or Retrieve prior stored
      commands (S/R): S
      *****
      =NOT Enter the dataset below where you want the commands stored or
      0000 retrieved from.
      0000
      0000 Destination ==> USER01.TSCSSA.STORE.COMMANDS
      0000
      0000 Enter the disposition of the allocation for the destination
      0000 dataset (SHR=SHARE - commands will replace contents, or
      0000 MOD=APPEND - commands will be appended to dataset contents).
      0000
      0000 Disposition (SHR/MOD) ==> SHR
      0000
      0000 Hit Enter to Continue      PF03=EXIT/PF01=HELP
      0000
```

Complete the following fields of the Generated Command(s) Storage or Retrieval screen:

Store or Retrieve	Indicate if you want to store the currently displayed commands, or retrieve previously stored commands into the edit session.
Destination	Enter the name of the dataset to store or retrieve commands. The default for this dataset is the allocation prefix set in your SSA configuration and SSA.STORE.COMMANDS. If the dataset does not exist and you specified Store, SSA prompts you to confirm the allocation request. The dataset must have the following allocation attributes: RECFM=F or FB LRECL=80 DSORG=PS
Disposition	You can indicate SHR (share) which will cause either option to copy over the commands that exist in the destination dataset, or you can indicate MOD (append) which will append the commands to whatever is in the destination dataset.

MAIN SSA Screen

The SSA Main Menu shown below has a scrolling information area that provides details concerning your system and the off-loaded SSA database you are currently pointing at. The Main Menu gets refreshed upon activation of the screens through startup program AASTART.

```

Main Menu ----- SSA ----- Main Menu
Smart Security Administrator

Option ==>

PF03=EXIT
PF01=HELP

Legend
-----
| RACF Userid ==> USER1 |
| Date ==> 12/01/1999 |
| Time ==> 14:37 |
| Version ==> 1 |
| Mod-Level ==> 3.0b |
| RACF Version ==> 2.06 |
| MVS Version ==> SP6.0.6 |
| ISPF Version ==> 4.5 |
| CPU ID ==> 123456 |
| CPU Type ==> 9672 |
| CPU Model ==> Z27 |
| SMF ID ==> SYSD |
| Date of Extract ==> 99/12/01 |
| Extract Creator ==> USER1 |
| Total Users ==> 292 |
| TSO Segment ==> 113 |
| CICS Segment ==> 97 |
| DFP Segment ==> 3 |
| Language Seg ==> 0 |
| OPERPARM Seg ==> 2 |
| WORKATTR Seg ==> 0 |
| OMVS Segment ==> 48 |
| Netview Seg ==> 0 |
| DCE Segment ==> 0 |
| RRSF ==> 0 |
| Total Connects ==> 407 |
| Total Groups ==> 114 |
| DFP Segment ==> 1 |
| OMVS Segment ==> 27 |
| Total DSN Profs ==> 65 |
| Total DSN Perms ==> 150 |
| Total RSC Profs ==> 135 |
| Total RSC Perms ==> 370 |

Unicom Systems, Inc
15535 San Fernando Mission Blvd
Mission Hills, CA Phone (818) 838-0606 - FAX (818) 838-0776
Web Site - http://www.unicomsi.com
```

AAERASE CLIST

SSA stores vital user information in an ISPF profile variable pool. If users need to clear stored values either, they can execute CLIST AAERASE. AAERASE must be executed in an ISPF environment when you are logged on to the logon procedure containing SSA libraries. Upon execution, AAERASE displays which variable group it is currently purging. Below is a sample of the display:

```
Menu  Utilities  Compilers  Options  Status  Help
-----
                                ISPF Primary Option Menu
Option ==> TSO AAERASE
                                More:      +
0  Settings      Terminal and user parameters      User ID . : USER01
1  View          Display source data or listings    Time. . . : 12:07
2  Edit          Create or change source data       Terminal. : 3278
3  Utilities     Perform utility functions          Screen. . : 1
4  Foreground    Interactive language processing    Language. : ENGLISH
-----
      ----- SSA Progress Indicator -----
      The following functions are being performed.
      Please be Patient.

      General ==> Purging ISPF Profile Stored Variables
      Sub     ==> Purging Group 11
-----
M More      Additional IBM Products
Enter X to Terminate using log/list defaults
```




www.unicomsi.com

We welcome feedback on our documentation. Please email us at:
tech.authors@unicomsi.com

www.unicomglobal.com