SC28-0733-5
File No. S370-89

Program Product

MVS Resource Access Control Facility (RACF) Command Language Reference

Program Number 5740-XXH
Version 1, Release 6

Sixth Edition (December, 1983)

This is a major revision of, and obsoletes, SC28-0733-4. See the Summary of Amendments following the Contents for a summary of the changes that have been made to this manual. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

This edition applies to Version 1, Release 6 of the program product RACF (Resource Access Control Facility) Program Number 5740-XXH and to all subsequent versions until otherwise indicated in new editions or Technical Newsletters. Changes are made periodically to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 Bibliography),* GC20-0001, for the editions that are applicable and current.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this publication is not intended to imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for reader's comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Information Development, Department D58, Building 920-2, PO Box 390, Poughkeepsie, N. Y. 12602. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Preface

This publication describes the syntax and the functions of the RACF (Resource Access Control Facility) commands for RACF Version 1, Release 6. It is intended for use by RACF-defined users who are responsible for creating, updating or maintaining the profiles for users, groups, DASD data sets, and general resources on the RACF data set.

Readers must be familiar with the RACF concepts and terminology described in the *RACF General Information Manual.*

The major divisions in this book are:

Chapter 1: Introduction - gives a general description of the functions of the RACF commands.

Chapter 2: Basic Information for Using RACF Commands - gives general information required to use the RACF commands.

Chapter 3: The RACF Commands - gives the syntax and function of each RACF command. The commands are presented in alphabetical sequence.

Appendix A: RACF/ISPF Panels.

Related RACF Publications

MVS Resource Access Control Facility (RACF) - General Information, GC28-0722.

MVS Resource Access Control Facility (RACF) Security Administrator's Guide, SC28-1340.

MVS Resource Access Control Facility (RACF) Auditor's Guide, SC28-1342.

MVS System Programming Library: Resource Access Control Facility (RACF), SC38-1343.

MVS Resource Access Control Facility (RACF) Messages and Codes, SC38-1014.

MVS Resource Access Control Facility (RACF) - Program Logic Manual, LY28-0730.

Related System Publications

TSO Command Language Reference, GC28-0646

OS/VS2 TSO Terminal User's Guide, GC28-0645 or *MVS/Extended Architecture TSO Terminal User's Guide*, GC28-1274

TSO Extensions User's Guide, SC28-1333

OS/VS2 JCL GC28-0692 or *MVS/Extended Architecture JCL*, GC22-1148.

Contents

Figures

Summary of Amendments

Summary of Amendments
for SC28-0733-5
for RACF Version 1, Release 6

Additions and changes have been made to the commands in this publication to reflect the new RACF Version 1 Release 6 functions.

The following commands are updated to support AUDITOR authority enhancements:

LISTDSD, RLIST, LISTUSER, LISTGRP, SEARCH, and SETROPTS.

All the RACF commands (except RVARY) have been updated to support group-SPECIAL, group-OPERATIONS, and group-AUDITOR attributes.

The following commands are updated to support the eight-character userid:

ADDUSER, ALTUSER, CONNECT, DELUSER, LISTUSER

The CONNECT command is updated to include the new operands AUDITOR/NOAUDITOR and OWNER.

The ADDSD, ALTDSD, DELDSD, and PERMIT commands are updated to include the GENERIC operand.

The PERMIT command is updated to include the FGENERIC operand.

The LISTDSD command is updated to include the VOLUME operand.

The PERMIT command is updated to include the RESET operand.

The ADDSD, ALTDSD, RDEFINE, and RALTER commands are updated to include the new operands WARNING/NOWARNING.

The SEARCH command is updated to include the WARNING operand.

The SETROPTS command is updated to include the new JES options and the new REFRESH and REALDSN/NOREALDSN operands.

Introduction

The profiles in the RACF data set contain the information necessary for the RACF functions. The RACF commands allow you to list and to make additions, modifications, and deletions to the profiles for users, groups, data sets, and resources belonging to classes defined in the class descriptor table (CDT), as well as to connect profiles. (A connect profile is a record in the RACF data set. Each user has one connect profile for each group to which the user is connected.)

Figure 1 shows, in alphabetic order, each of the commands and its functions.

RACF Command	Command Functions
ADDGROUP	– Define one or more new groups as a subgroup of an existing group. – Specify a model data set profile for a group.
ADDSD*	– Create one or more generic data set profiles. – Create one or more discrete data set profiles and optionally RACF-indicate the DASD data set(s) that the profiles apply to. (Default is to RACF-indicate.) – Create a new data set model profile.
ADDUSER	– Define one or more new users and connect the users to their default connect group. – Specify a model data set profile for a user.
ALTDSD*	– Change one or more discrete or generic data set profiles. – Protect a single volume of a multivolume, non-VSAM DASD data set. – Remove protection from a single volume of a multivolume, non-VSAM DASD data set.
ALTGROUP	– Change the superior group of one or more groups. – Change the owner of one or more groups. – Change the terminal indicator for one or more groups.
ALTUSER	– Change one or more users' attributes. – Change one or more users' default universal access authority or level of group authority within a specific group. – Revoke or reestablish one or more users' privileges to access the system. – Change the installation-defined data associated with one or more users. – Alter a model profile name for a user.
CONNECT	– Connect one or more users to a group. – Modify one or more users' connection to a group. – Establish user's authority to modify profiles.
DELDSD*	– Delete a generic data set profile. – Delete a discrete data set profile and optionally remove RACF-indication from the data set the profile applies to. (The default is to remove RACF-indication.)
DELGROUP*	– Delete one or more groups and their relationship to the superior group.
DELUSER*	– Delete one or more users and remove all their connections to RACF groups.
LISTDSD*	– List the details of one or more discrete or generic data set profiles including the users and groups authorized to access the data set(s) that the profiles apply to.
LISTGRP	– List the details of one or more group profiles including the users connected to the group.
LISTUSER	– List the details of one or more user profiles including all groups each user is connected to.
PASSWORD	– Change a user's password. – Change a user's password change interval. – Reset another user's password to a known default value.
PERMIT*	– Give authority to access a resource to specific users or groups. – Remove the authority of specific users or groups to access a RACF-protected resource. – Change the level of access authority to a resource for specific users or groups. – Copy the list of authorized users from one resource profile to another.
RALTER	– Change the discrete and/or generic profiles for one or more resources whose class is defined in the class descriptor table. – Maintain global tables.
RDEFINE	– Create a discrete or generic general resource profile for one or more resources whose classes are defined in the class descriptor table. – Maintain global tables.
RDELETE	– Delete discrete or generic profiles for one or more resources whose classes are defined in the class descriptor table. – Maintain global tables.
REMOVE*	– Remove a user from a group and assign a new owner for any group data sets owned by the user.
RLIST	– List the details of discrete or generic profiles for one or more resources whose class is defined in the class descriptor table. – Maintain global tables.
RVARY	– Dynamically deactivate and reactivate the RACF function. – Deactivate tape volume protection while RACF is deactivated. – Switch the primary and back-up RACF data sets.

Figure 1 (Part 1 of 2). Functions of RACF Commands

RACF Command	Command Functions
SEARCH*	– List the resource names that meet a search criterion for a class of resources. – Create a CLIST using resource names for a class that meets the search criteria.
SETROPTS	– Dynamically set system-wide options relating to resource protection, generic profile checking, terminal universal access authority, statistics gathering, logging of RACF events, and user password expiration interval. – Control global access checking for selected individual resources and/or generic names with selected generalized access rules. – Enable or disable single-level data set name support. – Establish password syntax rules. – Activate password processing for rejecting reused passwords, limiting invalid password attempts, and warning of password expiration. – Activate profile modeling for GDG, group, and user data sets. – Enable or disable list-of-groups processing. – Control the use of automatic data set protection (ADSP). – Display current options in effect. – Initiate refreshing of in-storage generic profiles and global access checking tables.
*Installation exit provided.	

Figure 1 (Part 2 of 2). Functions of RACF Commands

Basic Information for Using RACF Commands

You use the RACF commands to add, modify, or delete RACF profiles and to define system-wide options. You must be defined to RACF with a sufficient level of authority to issue the command. To issue the RACF commands from the foreground, you must be defined to TSO.

How to Enter RACF Commands

RACF commands can be entered in the foreground during a TSO terminal session, or in the background using a batch job. Alternatively, you can use the RACF ISPF panels rather than entering commands.

Entering RACF Commands in the Foreground

To enter the RACF commands in the foreground, you must be familiar with the following TSO information:

- How to conduct a TSO terminal session
- How to use the TSO commands
- How to use system-provided aids (HELP command, attention interrupt, conversational messages).

See *TSO Terminal User's Guide* and *TSO Command Language Reference* for full descriptions of these items.

The TSO LOGON command is used to identify you to the system as a RACF user via the *user-identity* (userid), *password*, GROUP, and OIDCARD operands. To change your RACF password, you can use the *newpassword* operand on the LOGON command. If you have more than one account number defined in your TSO profile, you must supply an account number on the LOGON command.

The default data set name prefix in your TSO profile is used as the first-level qualifier of a DASD data set name if you do not enter the fully qualified name in a command. This is done for both TSO and RACF commands. RACF also uses the TSO default prefix as the first-level qualifier for the name of a command procedure (CLIST) created as a result of the RACF SEARCH command.

If you frequently use RACF commands on RACF-protected DASD data sets, you can set your TSO default prefix as follows:

- Set the default prefix to your userid if you do a good deal of work with your own data sets.
- Set the default prefix to a specific RACF group name if you are working mostly with data sets from that group. (This can be done only if the group name is from 1 to 7 positions in length. If the group name is 8 positions long, you must always enter fully qualified group data set names on the commands.)

The examples of the commands in this book are presented in uppercase letters. When entering commands from a terminal, you can use either uppercase or lowercase letters.

Entering Commands Via ISPF Panels

You can use the RACF ISPF (Interactive System Productivity Facility) panels to define and modify group, user, and resource profiles and to define system wide options. To use the RACF ISPF panels, select RACF on the appropriate ISPF panel. Then select the desired RACF function from the RACF ISPF panel menu. You then fill in the necessary information in the panel. Appendix A shows the ISPF menu and data entry panels.

Note: To use the RACF ISPF panels, ISPF (program number 5668-960) must be installed.

Entering RACF Commands in the Background

You can enter RACF commands in the background by submitting a batch job as follows:

- Using the batch internal or remote reader facility of the Job Entry Subsystem (JES)
- From a terminal by using the TSO SUBMIT command.

The level of support provided by the job entry subsystem (JES) at your installation determines what RACF data you need to enter on your JCL. If your level of JES includes the RACF user identification propagation feature, then any jobs you submit to the background while logged onto TSO will automatically be identified to RACF with the same user and group identifiers as your TSO session. (User, password, and group information is not required on the JOB statement, but if you do specify this information, it overrides the propagated specifications.)

If your level of JES does not include the RACF user identification propagation feature, then you must include the USER, PASSWORD, and optionally, GROUP parameters on the JCL JOB statement.

The USER, PASSWORD, and GROUP parameters on the JCL JOB statement identify you to the system as a RACF user. To change your RACF password, you can use the "newpassword" subparameter of the PASSWORD parameter. For information on how to code these parameters, see *JCL*.

As an alternative to coding PASSWORD on JCL statements, the TSO SUBMIT command can be used (for systems that do not have the JES RACF user identification propagation feature) to automatically include this information during job submission. To use this feature, you should code the USER (userid) and PASSWORD operands on the SUBMIT command. These operands are then put on the JCL JOB statement generated by the command. When the job is processed, RACF uses the name of the user's default group as the current connect group.

Note: The TSO Extensions program product (program number 5665-285) must be installed if the installation wishes to use SUBMIT command parameters to facilitate the submission of batch jobs that access RACF-protected resources.

Example of RACF Commands in the Background

The following example illustrates how RACF commands can be used in the background.

```
//jobname     JOB    ...,USER=MYNAME,PASSWORD=ABC,...
//STEP1       EXEC   PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT    DD     SYSOUT=A
//SYSTSIN     DD     *
 ADDGROUP     PROJECTA
 ADDUSER      (PAJ5 ESH25)
 ADDSD  'PROJECTA.XYZ.DATA'
 PERMIT 'PROJECTA.XYZ.DATA' ID(PAJ5) ACCESS(UPDATE)
/*
```

In the background, as in the foreground, the user's TSO default data set name prefix is used as the first-level qualifier of a DASD data set name if the fully qualified DASD data set name is not given in the command. It is also used as the first-level qualifier for the name of a command procedure (CLIST) created as a result of the RACF SEARCH command. The default prefix is in the TSO profile for the user specified in the USER parameter on the JCL JOB statement or the USER operand in the TSO SUBMIT command.

For a full description of how to use commands in the background, see *TSO Terminal User's Guide.*

Syntax of RACF Commands and Operands

The syntax of RACF commands is the same as the syntax of TSO commands. For example, one or more blanks or a comma are valid delimiters for use between operands.

The syntax for all occurrences of the *userid, group-name, password, profile-name, volume-serial,* ǎnd *terminal-name* operands in this book are described below:

userid one to eight alphameric characters beginning with an alphabetic, #, $, or @ character. Note that for TSO users who are defined to RACF, the userid cannot exceed seven characters.

group-name one to eight alphameric characters beginning with an alphabetic, #, $, or @ character

password one to eight alphameric characters

profile-name either a discrete name or a generic name, as follows:

For the DATASET class:

discrete name same as TSO data-set-name (see *TSO Command Language Reference*) except that the first-level qualifier (or the qualifier supplied by a command installation exit) must be a valid RACF-defined userid or group name

generic name same as discrete name except that at least one level (other than the first) may be an *, or any but the first-level qualifier may contain a % character (or characters) in any position of the name. The last qualifier may contain up to eight characters, including the % generic character, optionally followed by the generic character *, for a total of nine characters. You can also use the GENERIC operand to define as a generic profile a profile name that does not use either of the generic characters.

For the general resource classes:

discrete name as defined in the class descriptor table

generic name same as a discrete name for the general resource classes, except that a single * can appear last in the name or a % can appear in any position. You can also use the GENERIC operand to define as a generic profile a profile name that does not use either of the generic characters. An * alone is a valid generic name.

volume-serial one to six alphameric, #, $, or @ characters

terminal-name one to eight alphameric characters beginning with an alphabetic, #, $, or @ character.

Return Codes from RACF Commands

All of the RACF commands (except RVARY) issue the following return codes. RVARY issues return codes of 0, 8, and 12.

Decimal Code	Meaning
0	Normal completion.
4	The command encountered an error and attempted to continue processing.
8	The command encountered a user error or an authorization failure and terminated processing.
12	The command encountered a system error and terminated processing.

Note: The return codes can be interrogated via CLIST processing.

Installation Exit Routines from RACF Commands

RACF provides exits that can be used by installation-written routines when certain RACF commands are issued:

- ICHCNX00 - from ADDSD, ALTDSD, DELDSD, LISTDSD, PERMIT, and SEARCH commands
- ICHDEX01 - from ALTUSER and PASSWORD commands.
- ICHRDX01 and ICHRDX02 - from ADDSD and DELDSD command.
- ICHRCX01 and ICHRCX02 - from ALTDSD, DELDSD, LISTDSD, PERMIT, RALTER, RDELETE, RLIST and SEARCH commands
- ICHCCX00 - from DELGROUP, DELUSER, and REMOVE commands
- ICHPWX01 - from ALTUSER and PASSWORD commands

Users can install installation-written routines to provide additional security processing during the processing of the RACF commands. For example, the ICHPWX01 pre-processing exit can be written to install an installation-written routine to examine a new password and new password interval.

For a complete description of these exits, see *MVS System Programming Library: Resource Access Control Facility (RACF)*

RACF Attributes and Authorities Required to Issue Commands

Because RACF provides system security, only certain users are authorized to issue some of the commands. In some instances, you can only issue certain operands of the commands. RACF checks your **user attribute** and **group authority**, and in some cases, the **resource access authority** of the resource affected by the command, before allowing the command to complete.

The following topics briefly describe the attributes and authorities as they pertain to issuing RACF commands and using RACF ISPF panels. For a complete description about assigning user authorization, see the *RACF Security Administrator's Guide*. For a complete description of attributes, group authorities, and resource access authorities, see *RACF Security Administrator's Guide* and *RACF General Information*

Users with the SPECIAL, AUDITOR, or OPERATIONS Attributes

Users who have been assigned the SPECIAL, AUDITOR, or OPERATIONS attributes have specially defined authorities and limits for all the profiles on the RACF data set. In contrast, users who have the group-SPECIAL, group-AUDITOR, and group-OPERATIONS attributes can affect group, user, resource, and data set profiles only within the scope of their groups.

Users With the Group-SPECIAL, Group-AUDITOR, or Group-OPERATIONS Attributes

Users who have been connected to groups with group-SPECIAL, group-AUDITOR, or group-OPERATIONS attributes can issue commands for profiles that are "within the scope of the group." Within the scope of the group means the subgroups owned by the group.

Scope of a Group

The scope of the group is the range of profiles over which a user connected to the group (or superior group) with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute has authority. The authority within the scope of the group varies depending on the type of profile, as follows:

Data Set Profiles: A data set profile is within the scope of a group for a user with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute if:

- The data set profiles are owned by the group, or

- The data set profiles have a high-level qualifier that is the group name

- The data set profiles are owned by a user who in turn is owned by the group

- The data set profiles have a high-level qualifier that is a userid owned by the group

General Resource Profiles: A resource profile is within the scope of a group for a user with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute if:

- The resource profiles are owned by the group, or

- The resource profiles are owned by users whose profile is owned by the group

User Profiles: A user is within the scope of a group for a user with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute if the user profiles are owned by the group.

Group Profiles: A group profile is within the scope of a group for a user with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute if:

- The profiles are owned by the group itself, or

- The profiles are owned by subgroups of the group, even if the profiles themselves are not owned by the superior group.

Connect Profiles: A connect profile is within the scope of a group for a user with the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attribute if the profile is connected to the group or its subgroups.

Profiles NOT Within the Scope of a Group

The following profiles are not within the scope of a group:

- User and group profiles that are not in the group or any of its subgroups but are owned by users owned by the group

- Connect profiles for users owned by the group but connected to other groups

- User profiles for users that are connected to the group but are not owned by the group

Group Authorities

Group authorities, which define user responsibilities within the group, are:

- **USE**, which allows the user to access resources to which the group is authorized
- **CREATE**, which allows the user to create RACF data set profiles for the group
- **CONNECT**, which allows the user to "connect" other users to the group
- **JOIN**, which allows the user to add new subgroups or users to the group, as well as assign group authorities to the new members

Resource Access Authorities

Both users and groups can be granted or denied access to a resource explicitly, by assigning to each a specific access authority to the resource, or implicitly, with a **universal access authority** (UACC).

UACC is the default **resource access authority**. All users or groups in the system who are not specifically named in the list of authorized users -- the access list -- of that resource profile can still access the resource with the authority specified by UACC. UACC also applies to users not defined to RACF. The resource access authorities are:

- **ALTER**, which specifies that the user or group has full control over the resource
- **CONTROL**, used only for VSAM data sets, which specifies that the user or group has access authority that is equivalent to the VSAM control password
- **UPDATE**, which specifies that the user or group is authorized to access the resource for the purpose of reading or writing.
- **READ**, which specifies that the user or group is authorized to access the resource for the purpose of reading only
- **NONE**, which specifies that the user or group is not permitted to access the resource

Attribute and Authority Summary

The following chart summarizes the attributes and authorities that can be assigned, and the RACF commands and operands that can be issued for each authority. The chart is divided into four types of authorities: user attributes, group authorities, access authorities, and miscellaneous authorities (ownership requirements and userid requirements).

The authorities required to issue each command are listed in the section "RACF Requirements" that appears with each command in this publication.

User Attributes	Commands and Operands you can Issue	
SPECIAL or group-SPECIAL	ADDGROUP	with all operands
	ADDSD	with all operands
	ADDUSER	with all operands
	ALTDSD	with all operands except GLOBALAUDIT
	ALTGROUP	with all operands
	ALTUSER	with all operands except UAUDIT/NOUAUDIT
	CONNECT	with all operands
	DELDSD	with all operands
	DELGROUP	with all operands
	DELUSER	with all operands
	LISTDSD	with all operands
	LISTGRP	with all operands
	LISTUSER	with all operands
	PASSWORD	with all operands
	PERMIT	with all operands
	RALTER	with all operands except GLOBALAUDIT
	RDEFINE	with all operands
	RDELETE	with all operands
	REMOVE	with all operands
	RLIST	with all operands
	SEARCH	with all operands
	SETROPTS	with all operands except AUDIT/NOAUDIT/SAUDIT/NOSAUDIT/ CMDVIOL/NOCMDVIOL which require the AUDITOR attribute. User with group-SPECIAL attribute can issue only REFRESH and LIST.
AUDITOR or group-AUDITOR	ALTDSD	only with GLOBALAUDIT
	ALTUSER	only with UAUDIT/NOUAUDIT
	LISTDSD	with all operands, lists GLOBALAUDIT option
	LISTUSER	with all operands, lists UAUDIT/NOUAUDIT operand
	RALTER	only with GLOBALAUDIT
	RLIST	with all operands, lists GLOBALAUDIT option
	SETROPTS	only with AUDIT/NOUAUDIT/SAUDIT/NOSAUDIT/ CMDVIOL/NOCMDVIOL/LIST which require the AUDITOR attribute

Figure 2 (Part 1 of 5). Summary of Authorities and Commands

<table>
<tr><th>User Attributes</th><th colspan="2">Commands and Operands you can Issue</th></tr>
<tr><td>OPERATIONS or
group-OPERATIONS</td><td>SEARCH
SETROPTS</td><td>with all operands
only with REFRESH</td></tr>
<tr><td>CLAUTH</td><td>ADDUSER[1]
ALTUSER[2]
RALTER[3]
RDEFINE[4]
SETROPTS</td><td>with all operands except OPERATIONS/NOOPERATIONS/SPECIAL/ NOSPECIAL/AUDITOR/NOAUDITOR
only with CLAUTH/NOCLAUTH
only with ADDVOL
with all operands
only with REFRESH</td></tr>
<tr><td colspan="3">[1]applies when you have the CLAUTH attribute of USER and you either are the owner of, have JOIN authority in the default group specified in the command, or the profile is within the scope of a group in which you have the group-SPECIAL attribute.
[2]applies when you have the CLAUTH attribute for the class to be added/deleted, you are the owner of the user's profile, or the profile is within the scope of a group in which you have the group-SPECIAL attribute.
[3]applies when you have the CLAUTH attribute of TAPEVOL and you also have sufficient authority to issue the command.
[4]applies when you have the CLAUTH attribute of DASDVOL, TAPEVOL, or TERMINAL, and applies to the specific class.</td></tr>
<tr><td>GRPACC none
ADSP
REVOKE</td><td colspan="2"></td></tr>
</table>

Figure 2 (Part 2 of 5). Summary of Authorities and Commands

Group Authorities	Commands and Operands you can Issue	
USE	none	
CREATE	ADDSD[1]	with all operands except NOSET
CONNECT	ADDSD[1]	with all operands except NOSET
	ALTUSER	only with GROUP/AUTHORITY/UACC
	CONNECT	with all operands except SPECIAL/NOSPECIAL/OPERATIONS/ NOOPERATIONS/AUDITOR/NOAUDITOR
	LISTGRP	with all operands
	REMOVE	with all operands
JOIN	ADDGROUP[2]	with all operands
	ADDSD[1]	with all operands except NOSET
	ADDUSER[3]	with all operands except OPERATIONS/SPECIAL/AUDITOR
	ALTGROUP[4]	with all operands except OWNER
	ALTUSER	only with GROUP/AUTHORITY/UACC
	CONNECT	with all operands except SPECIAL/NOSPECIAL/OPERATIONS/ NOOPERATIONS
	DELGROUP[2]	with all operands
	LISTGRP	only with (group-name ...)
	REMOVE	with all operands

[1] applies to group data sets.

[2] applies to superior group.

[3] applies to default group specified in command and only if you have the CLAUTH attribute of USER.

[4] applies to current and new superior groups. You may have JOIN authority in one group and be owner of or be connected with the groups-SPECIAL attribute to another group.

Figure 2 (Part 3 of 5). Summary of Authorities and Commands

Access Authorities	Commands and Operands you can Issue	
NONE	none	
READ	LISTDSD	with all operands except AUTHUSER
	RLIST	with all operands except AUTHUSER
	SEARCH	with all operands
UPDATE	LISTDSD	with all operands except AUTHUSER
	RLIST	with all operands except AUTHUSER
	SEARCH	with all operands
CONTROL	LISTDSD	with all operands except AUTHUSER
	RLIST	with all operands except AUTHUSER
	SEARCH	with all operands
ALTER	ALTDSD[1]	with all operands except OWNER/NOSET/GLOBALAUDIT
	DELDSD[1]	with all operands except NOSET
	LISTDSD	with all operands
	PERMIT[1]	with all operands
	RALTER[2]	with all operands except OWNER/ADDVOL/GLOBALAUDIT
	RDELETE[1]	with all operands
	RLIST[1]	with all operands
	SEARCH	with all operands

[1] applies to discrete profiles only.
[2] applies to ADDVOL operand only if you also have CLAUTH attribute for TAPEVOL.

Figure 2 (Part 4 of 5). Summary of Authorities and Commands

Miscellaneous Authorities	Commands and Operands you can Issue	
Owner of user profile	ALTUSER[1]	only with userid/NAME/OWNER/DFLTGRP/DATA/GRPACC/NOGRPACC/ADSP/NOADSP/REVOKE/RESUME/PASSWORD/NOPASSWORD/OICARD/NOOIDCARD/CLAUTH/NOCLAUTH
	DELUSER	with all operands
	LISTUSER	with all operands
	PASSWORD	only with USER
Owner of group profile	ADDGROUP[2]	with all operands
	ADDUSER[3]	with all operands except OPERATIONS/SPECIAL/AUDITOR
	ALTGROUP[4]	with all operands
	ALTUSER	only with GROUP/AUTHORITY/UACC
	CONNECT	with all operands except SPECIAL/NOSPECIAL/OPERATIONS/NOOPERATIONS
	DELGROUP[5]	with all operands
	LISTGRP	with all operands
	REMOVE	with all operands
Owner of resource profile	ALTDSD	with all operands except NOSET/GLOBALAUDIT
	DELDSD	with all operands except NOSET
	LISTDSD	with all operands
	PERMIT	with all operands
	RALTER[6]	with all operands except GLOBALAUDIT
	RDELETE	with all operands
	RLIST	with all operands
	SEARCH	with all operands
Userid is current user	ALTUSER	only with NAME/DFLTGRP
	LISTUSER	only with userid
	PASSWORD	only with PASSWORD/INTERVAL
Userid is first-level qualifier of data set name (or qualifier supplied by a command installation exit)	ADDSD	with all operands
	ALTDSD	with all operands except OWNER/GLOBALAUDIT
	DELDSD	with all operands
	LISTDSD	with all operands
	PERMIT	with all operands
	SEARCH	with all operands
None	RVARY[7]	with all operands

[1] applies to CLAUTH/NOCLAUTH only if you have the CLAUTH attribute for the class to be added/deleted.
[2] applies to superior group.
[3] applies to default group specified in the command and only if you have the CLAUTH attribute of USER.
[4] applies to current and new superior groups. You may have JOIN authority in one group and be owner of another group.
[5] applies to superior group or group to be deleted.
[6] applies to ADDVOL operand only when you also have CLAUTH attribute of TAPEVOL.
[7] although no special authority is needed to issue the command, the security operator must approve the change of RACF status to active or inactive before the command is allowed to complete.

Figure 2 (Part 5 of 5). Summary of Authorities and Commands

The RACF Commands

This chapter gives the syntax and function for each RACF command. The commands are presented in alphabetical order.

Note that the description for each command starts on a right-hand page, therefore enabling you to separate the descriptions to provide a tailored package for the users of your system based on their needs and authority to issue the commands.

Key to Symbols in Command Definitions

1. UPPERCASE - must appear as shown.
2. lowercase - information supplied by the user.
3. Item . . . - the item can be listed more than once.
4. Stacked items - alternatives; only one item from the stack can be specified.
5. { } groups alternative items.
6. [ ] - optional item; the item may be specified.
7. <u>KEYWORD</u> - default when no item is specified.
8. **BOLDFACE** or **boldface** - information that must be given for a command.

ADDGROUP Command

Use the ADDGROUP command to define a new group to RACF.

The command adds a profile for the new group to the RACF data set. It also establishes the relationship of the new group to the superior group you specify.

RACF Requirements

To use the ADDGROUP command, you must:

- have the SPECIAL attribute, or
- have the group-SPECIAL attribute within a superior group, or
- be the owner of the superior group, or
- have JOIN authority to the superior group.

Note: You need not have the SPECIAL attribute to specify the OWNER keyword.

```
{ADDGROUP}      (group-name ... )
{AG      }
                [SUPGROUP(group-name)]

                [OWNER(userid or group-name)]

                 [TERMUACC  ]
                 [NOTERMUACC]

                [ MODEL(dsname) ]

                [ DATA('installation-defined-data')]
```

group-name
specifies the name of the group whose profile is to be added to the RACF data set. If you are defining more than one group, the list of group names must be enclosed in parentheses.

This operand is required and must be the first operand following ADDGROUP. Each name must be unique and must not currently exist in the RACF data set as a group name or a userid.

SUPGROUP(group-name)
specifies the name of an existing RACF-defined group. This group will be the superior group of the group being defined.

If this operand is not specified, your current connect group is used as the default value.

If the owner is a group, then OWNER and SUPGROUP must specify the same group name.

A group-SPECIAL user can specify only a SUPGROUP group to which he has authority.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the owner of the new group. If you do not specify an owner, you are defined as the owner of the group. If you specify a group name, then OWNER and SUPGROUP must specify the same group name.

TERMUACC

specifies that the universal access authority specified for a terminal (on the SETROPTS, RDEFINE, or RALTER command) will be used by the group or users connected to the group during authorization checking to access the terminal. This is the default value if both TERMUACC and NOTERMUACC are omitted.

NOTERMUACC

specifies that the group or a user connected to the group must be authorized via the PERMIT command with at least READ authority to access a terminal.

MODEL(dsname)

specifies the name of a discrete data set profile to be used as a model for new group-name data sets. For this parameter to be effective, the MODEL(GROUP) option (specified on the SETROPTS command) must be active.

Note that dsname will always be prefixed by the group name when the model is accessed.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the group profile. The data must be enclosed in apostrophes. Use the LISTGRP command to list this information.

ADDGROUP Examples

Example 1

Operation: User IA0 wants to add the group PROJECTA as a subgroup of RESEARCH. User IA0 will be the owner of group PROJECTA. Group PROJECTA will use the universal access authority specified for a terminal to access the terminal.

Known: User IA0 has JOIN authority to group RESEARCH.

User IA0 is logged on to group RESEARCH.

Command: ADDGROUP PROJECTA

Defaults: SUPGROUP(RESEARCH), OWNER(IA0), TERMUACC

Example 2

Operation: User ADM1 wants to add the group PROJECTB as a subgroup of RESEARCH. Group RESEARCH will be the owner of group PROJECTB. Group PROJECTB must be authorized to use terminals via the PERMIT command.

Known: User ADM1 has JOIN authority to group RESEARCH.

User ADM1 is logged on to group SYS1.

Command: ADDGROUP PROJECTB SUPGROUP(RESEARCH) OWNER(RESEARCH) NOTERMUACC

Defaults: None

Example 3

Operation: User ADM1 wants to add the group SYSINV as a subgroup of RESEARCH. This group will be used as the administrative group for RACF and will use a model name of 'SYSINV.RACF.MODEL.PROFILE'.

Known: User ADM1 has JOIN authority to group RESEARCH.

Command: ADDGROUP SYSINV SUPGROUP(RESEARCH) MODEL(RACF.MODEL.PROFILE) DATA('RACF ADMINISTRATION GROUP')

Defaults: OWNER(ADM1), TERMUACC

ADDSD Command

Use the ADDSD command to RACF-protect DASD data sets with either discrete or generic profiles.

Discrete Profile: When you use the ADDSD command to RACF-protect a data set with a discrete DASD data set profile, RACF:

- Defines the data set with a discrete profile that contains the volume and unit information for the data set
- Sets the RACF indicator (in the DSCB for a non-VSAM data set, or in the catalog entry for a VSAM data set) to indicate that the data set is protected by a discrete profile.

When you RACF-protect a non-VSAM data set with a discrete profile, the data set must be online and not currently in use. For a VSAM data set, the catalog for the data set must be online. The VSAM data set itself must also be online if the VSAM catalog recovery option is being used. If the required data set or catalog is not online, the ADDSD command processor will request that the volume be mounted.

To protect an ISAM data set with a discrete profile, the prime, index, and overflow data components of the data set must all reside on the same device type. If the components reside on different volumes, protect the data set as if it were a multi-volume data set. Use the ADDSD command and specify all the volumes in the VOLUME operand.

Generic Profile: You can use the ADDSD command to protect one or more similarly named DASD data sets with a generic profile. You can define a generic profile by using the GENERIC operand with the ADDSD command. The generic profile name can contain one or more generic characters (% or *). However, if you use the GENERIC operand, the profile name need not contain any generic characters.

Note: The protection offered by a generic profile is different depending on the level of data management support installed on your system. When your data management support includes the RACF "always-call" feature, generic profiles protect all data sets that they apply to, including existing data sets and data sets to be allocated in the future. In addition, a generic profile on a system with always-call controls the **allocation** of data sets. To allocate a new DASD data set that will be protected by an existing generic profile, that profile must give the user ALTER authority to the data set. If the new data set is a group data set, the data set requires either ALTER authority in the profile or CREATE authority in the group.

Note that if the new data set is a PDS (partitioned data set), the user will require at least UPDATE authority in the profile because the data set will be opened to create a PDS directory.

When your data management support does not include data management RACF always-call, generic profiles apply only to data sets that are RACF-indicated and do not have an associated discrete profile.

Data sets that are not RACF-indicated but are protected by a generic profile and always call are NOT PROTECTED if they are transferred (in any way) to another system that does not have RACF, always-call, and appropriate predefined generic profiles.

Regardless of whether a discrete or generic profile is defined, the profile automatically authorizes certain users to access the data set or data sets as follows:

- For a user data set, the user whose userid matches the first-level qualifier of the profile name (or the qualifier supplied by the RACF naming conventions table or by a command installation exit) has full authority.

- For a group data set, your userid is placed on the access authority list and you are given ALTER authority. If you have the GRPACC attribute, the group name is placed on the access list with UPDATE authority.

- If modeling is active for the user or group profile, the access list will be supplemented by the model profile information.

- For both user and group data set profiles, the universal access authority is set to the value in the UACC operand if it is entered, or to the default value associated with your current connect group.

RACF Requirements

The level of authority you need to use the ADDSD command and the types of profiles you can define are as follows:

- To protect one or more user data sets with RACF:

  - The first-level qualifier of the data set name (or the qualifier supplied by the RACF naming conventions table or by a command installation exit) must match your userid, or

  - You must have the SPECIAL attribute, or

  - The userid for the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute.

  You may not protect a user data set for someone else (first-level qualifier or installation-supplied qualifier is not your userid) unless you have the SPECIAL attribute or the data set profile is within the scope of a group in which you have the group-SPECIAL attribute.

- To protect a group data set with RACF, you must have at least CREATE authority in the group, or the SPECIAL attribute, or the OPERATIONS attribute, or the data set profile must be within the scope of a group in which you have either the group-SPECIAL attribute or group-OPERATIONS attribute.

  Note: To protect a group data set where the first-level qualifier of the data set name is VSAMDSET, you do not need either CREATE authority in the VSAMDSET group or the SPECIAL attribute. (A universal group authority of CREATE applies to the RACF-defined VSAMDSET group.)

- To define to RACF a data set that was brought from another system where it was RACF-indicated and RACF-protected with a discrete profile, either 1) you must have the SPECIAL attribute, or the data set profile is within the scope of a group in which you have the group-SPECIAL attribute, or 2) the first-level qualifier of the data set name (or the qualifier supplied by the naming conventions routine or a command installation exit) must be your userid.

- When either a user or group uses modeling to protect a data set with a discrete profile, RACF copies the following fields from the model profile: level number, audit flags, global audit flags, UACC, owner, warning, access list, and installation data.

Note: You need not have the SPECIAL attribute to specify the OWNER keyword.

```
{ ADDSD }      profile-name[/password]
{ AD    }
               [UNIT(type)]

               [VOLUME(volume-serial...)]

               [OWNER(userid or group-name)]

               [UACC(access-authority)]

               [        {  NONE                                          }  ]
               [        {{ ALL      }                                    }  ]
               [ AUDIT( {{ SUCCESS  }  [(audit-access-level)]  } ... } ) ]
               [        {{ FAILURES }                          }     }   ]

               [LEVEL(nn)]

               [ SET     ]
               [ NOSET   ]
               [ MODEL   ]
               [ GENERIC ]

               [ DATA('installation-defined-data')]

                 [WARNING]
```

profile-name

specifies the name of the discrete or generic profile to be added to the RACF data set. If you specify more than one name, the list of names must be enclosed in parentheses.

The first-level qualifier of the profile name (or the qualifier determined by the naming conventions table or by a command installation exit) must be either a userid or group name. To specify a userid other than your own, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute. To define a group data set where the first-level qualifier of the data set name is not VSAMDSET, you must have at least CREATE authority in the specified group, or the SPECIAL attribute, or the data set must be within the scope of a group in which you have the group-SPECIAL attribute.

This operand is required and must be the first operand following ADDSD.

Note: If you are protecting an OS CVOL, use the naming convention SYSCTLG.Vxxxxxx where the x's represent the volume serial number for the volume containing the CVOL.

Note: Alias data set names are not supported.

Note: If your data managements support does not include always-call, a VSAM data set must be cataloged in a catalog that is also RACF-protected in order for the data set to be RACF protected.

password

specifies the data set password if you are protecting an existing password-protected data set. If you specify a generic or model profile, this operand is ignored.

For a non-VSAM password-protected data set, the WRITE level password must be available.

For a VSAM password-protected data set, one of the following conditions must exist: (1) the MASTER level password for the data set must be available, or, (2) if the catalog containing the entry for the data set is RACF-protected, then you must have ALTER access to the catalog, or (3) if the catalog containing the entry for the data set is not RACF-protected, but is password-protected, then the MASTER level password for the catalog must be available. (For a VSAM data set that is not password-protected, you do not need the password or RACF access authority for the catalog.)

A password is not required if you are using the NOSET operand.

If the command is executing in the foreground and you omit the password for a password-protected data set, the logon password is used. You will be prompted if the password you enter or the logon password is incorrect. (If it is a non-VSAM multi-volume data set, you will be prompted once for each volume on which the data set resides.)

If the command is executing in a batch job and you either omit the password for a password-protected data set or supply an incorrect password, the operator will be prompted. (If it is a non-VSAM multi-volume data set, the operator will be prompted once for each volume on which the data set resides.)

UNIT(type)

specifies the unit type on which a non-VSAM data set resides. You may specify an installation-defined group name, a generic device type or a specific device address. If the data set is not cataloged, the UNIT and VOLUME operands are required. Do not use the UNIT and VOLUME operands for a VSAM data set. You must specify UNIT and VOLUME for data sets cataloged with an esoteric name (such as an installation-defined group name). If you specify a generic or model profile name, this operand is ignored.

VOLUME(volume-serial ...)

specifies the volume(s) on which a non-VSAM data set resides. If the data set is not cataloged, the VOLUME and UNIT operands are required. Do not use the VOLUME and UNIT operands for a VSAM data set. You must specify VOLUME and UNIT for data sets cataloged with an esoteric name (such as an installation-defined group name). If you specify a generic or model profile name, this operand is ignored.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the owner of the data set. When you define a group data set, the user you designate as owner must have at least USE authority in the group specified by the first-level qualifier of the data set name (or the qualifier determined by the naming conventions routine or by a command installation exit). If this operand is omitted, you are defined as the owner, and, for group data sets, the userid is added to the access list for the data set with ALTER access authority.

Note: The user specified as the owner does not automatically have access to the data set. Use the PERMIT command to add the owner to the access list as desired.

UACC(access-authority)

specifies the universal access authority to be associated with the data set or sets. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. If UACC is not specified or if the UACC keyword is entered with no access authority, your default value in your current connect group is used. (For non-VSAM data sets, CONTROL authority implies UPDATE authority.)

AUDIT

specifies which access attempts you want to log on the SMF data set. The following options are available:

ALL

indicates that you want to log both authorized accesses and detected unauthorized access attempts.

SUCCESS

indicates that you want to log authorized accesses.

<u>FAILURES</u>

indicates that you want to log detected unauthorized attempts.

NONE

indicates that you do not want any logging to be done.

audit−access−level

specifies which access level(s) you want logged on the SMF data set. The levels are:

<u>READ</u>

logs access attempts at any level. This is the default value if no access level is specified.

UPDATE

logs access attempts at the UPDATE, CONTROL, and ALTER levels.

CONTROL

logs access attempts at the CONTROL and ALTER levels.

ALTER

logs ALTER access-level attempts only.

FAILURES (READ) is the default value if the AUDIT operand is omitted from the command.

LEVEL(nn)

specifies a level indicator, where nn is an integer between 0 and 99. The default is 0.

The meaning of the value is assigned by your installation. It is not used by the authorization function in RACHECK but is available to the RACF post-processing installation exit routine for the RACHECK SVC.

It is included on all records that log data set accesses and is listed by the LISTDSD command.

SET

specifies that the data set will be RACF-indicated. It is the default value and is used when you are protecting a data set with RACF. If the indicator is already on, the command will fail. If you specify a generic profile, this operand is ignored.

NOSET

specifies that the data set will not be RACF-indicated.

The NOSET operand is used when you are defining a data set to RACF that is brought from another system where it was RACF-protected. (The data set is already RACF-indicated.)

Note: If NOSET is specified and the data set is not already RACF-indicated, RACF access control to that data set is not enforced.

If NOSET is specified, the volume(s) on which the data set or catalog resides need not be on-line and the password in the first operand of this command is not required.

To use the NOSET operand, either you must have the SPECIAL attribute or the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) must be your userid. If you specify a generic profile, this operand is ignored.

MODEL

creates a model profile to be used when new data sets are created. The SETROPTS command MODEL keyword with GROUP or USER subkeywords controls whether this profile is used for group-named or userid-named data sets.

When you specify MODEL, you may omit UNIT and VOLUME, but you must omit SET, NOSET, and GENERIC.

GENERIC

specifies that RACF is to treat the profile name as a generic name, even if it does not contain any generic characters.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the data set profile. Use the LISTDSD command to list this information. It is available to the RACF post-processing installation exit routine for RACHECK. If the profile is a model profile, the information is copied to the installation-defined data area for new profiles.

WARNING

specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

ADDSD Examples

Example 1

Operation: User ADM1 wants to create a generic profile to protect all data sets having the first-level qualifier SALES.

Known: User ADM1 has the SPECIAL attribute and the operating system has data management RACF always-call.

Command: ADDSD 'SALES.*' UACC(NONE) AUDIT(ALL(READ))

Defaults: OWNER(ADM1) LEVEL(0)

Example 2

Operation: User AEH0 wants to protect the data set AEH0.DEPT1.DATA with a discrete RACF profile.

Known: User AEH0 is RACF-defined.

AEH0.DEPT1.DATA is not cataloged. It resides on volume USER03 which is a 3330 volume.

Command: ADDSD 'AEH0.DEPT1.DATA' UNIT(3330) VOLUME(USER03)

Defaults: OWNER(AEH0) UACC(UACC of user AEH0 in current connect group) AUDIT(FAILURES(READ)) LEVEL(0) SET

Example 3

Operation: User ADM1 wants to RACF-define the DASD data set SYS1.ICH02.DATA which was brought from another system where it was protected by a discrete RACF profile and was RACF-indicated.

Known: User ADM1 has the SPECIAL attribute.

SYS1.ICH02.DATA is cataloged.

User ADM1 has create authority in group SYS1 and is connected to groups SYS1 with the group-SPECIAL attribute.

Command: ADDSD 'SYS1.ICH02.DATA' OWNER(SYS1) UACC(NONE) AUDIT(ALL NOSET

Defaults: LEVEL(0)

Example 4

Operation: User AEHO wants to create a model profile for group RSC and place an installation-defined description in the profile.

Known: User AEHO has at least CREATE authority in group RSC.

Command: ADDSD 'RSC.ACCESS.PROFILE' MODEL DATA('PROFILE THAT CONTAINS MODELING INFORMATION')

Defaults: OWNER(AEHO), UACC(UACC of user AEHO in current group) AUDIT(FAILURES(READ)) LEVEL(0)

ADDUSER Command

Use the ADDUSER command to define a new user to RACF and establish the user's relationship to an existing RACF-defined group.

The command adds a profile for the new user to the RACF data set and creates a connect profile that connects the user to whichever default group you specify. the user's default universal access authority.

RACF Requirements

To use the ADDUSER command, you must:

- have the SPECIAL attribute, or
- have the CLAUTH attribute for the USER class and:
  - the default group is within the scope of a group in which you have the group-SPECIAL attribute, or
  - be the owner of the default group specified in this command, or
  - have JOIN authority in the default group specified in this command.

You must have the SPECIAL attribute to give the new user the OPERATIONS, SPECIAL, or AUDITOR attribute.

You cannot assign a user an attribute or authority higher than your own.

You need not have the SPECIAL attribute to specify the OWNER keyword.

```
{ADDUSER}        (userid...)
{AU     }
                 [NAME('user-name')]

                 [ PASSWORD(password) ]
                 [ NOPASSWORD         ]

                 [OWNER(userid or group-name)]

                 [DFLTGRP(group-name)]

                 [AUTHORITY(group-authority)]

                 [UACC(access-authority)]

                 [ CLAUTH(class-name...) ]
                 [ NOCLAUTH              ]

                 [ GRPACC   ]
                 [ NOGRPACC ]

                 [ ADSP   ]
                 [ NOADSP ]

                 [ SPECIAL   ]
                 [ NOSPECIAL ]

                 [ OPERATIONS   ]
                 [ NOOPERATIONS ]

                 [ AUDITOR   ]
                 [ NOAUDITOR ]

                 [ OIDCARD   ]
                 [ NOOIDCARD ]

                 [DATA('installation-defined-data')]

                 [MODEL(dsname)]
```

userid

specifies the user to be defined to RACF. If you are defining more than one user, the list of userids must be enclosed in parentheses.

This operand is required and must be the first operand following ADDUSER.

Each userid must be unique and must not currently exist on the RACF data set as a userid or a group name.

NAME('user-name')

specifies the user name to be associated with the new userid. You may use a maximum of 20 alphameric characters, optionally enclosed in apostrophes. If you omit the NAME operand, a default of 20 #'s ('###...') is used.

PASSWORD(password)

specifies the password to be associated with the user. If both PASSWORD and NOPASSWORD are omitted, or if the keyword PASSWORD is entered with no value, the group name given in the DFLTGRP operand is used as the default password.

The password is always set expired. The password change interval is set to the value specified on the INTERVAL operand of the SETROPTS command, and the date of the last password update is set to 0. The initial system default for the password change interval is 30 days.

NOPASSWORD

specifies that the new user does not need to supply a password when entering the system. NOPASSWORD is only valid if OIDCARD is also specified. If NOPASSWORD is specified and NOOIDCARD is specified (or defaulted to), then PASSWORD is assumed.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the owner of the RACF profile for the user being added. If this operand is omitted, you are defined as the owner.

DFLTGRP(group-name)

specifies the name of a RACF-defined group to be used as the default group for the user. If no group is specified, your current connect group is used as the default.

Note: You do not have to issue the CONNECT command to connect a new user to his or her default group.

AUTHORITY(group-authority)

specifies the level of group authority for the new user in the default group. The valid group authority values are USE, CREATE, CONNECT and JOIN. If this operand is omitted or if the keyword AUTHORITY is entered with no value, the default value is USE.

This option is group-related. If a user is connected to other groups (with the CONNECT command), the user can have a different group authority in each group.

UACC(access-authority)

specifies the default value for the universal access authority for all new resources the user defines while connected to the specified default group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. If this operand is omitted or if the keyword UACC is entered with no value, the default is NONE.

This option is group-related. If a user is connected to other groups (with the CONNECT command), the user can have a different default universal access authority in each group.

Note: When a user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using his or her default group as the current connect group, any RACF data set or tape volume profiles the user defines will be assigned this default universal access authority value.

CLAUTH(class-name ...)

specifies the classes in which the new user is allowed to define profiles to RACF for protection. Classes you can specify are USER, and any resource class defined in the class descriptor table. In order to enter the CLAUTH operand, you must have the SPECIAL attribute or have the CLAUTH attribute for the classes specified. If you do not have sufficient authority for a specified class, the CLAUTH specification for that class is ignored, and processing continues with the next class name specified.

NOCLAUTH

specifies that the new user is not to have the CLAUTH attribute. This is the default if both CLAUTH and NOCLAUTH are omitted.

GRPACC

specifies that any group data sets defined by the new user will be automatically accessible to other users in the group. The group whose name is used as the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority to the data set. The GRPACC keyword overrides NOGRPACC specified on the CONNECT command.

NOGRPACC

specifies that the new user will not have the GRPACC attribute. This is the default value if both GRPACC and NOGRPACC are omitted.

ADSP

specifies that all permanent DASD data sets created by the new user will automatically be RACF-protected by discrete profiles. The ADSP keyword overrides NOADSP specified on the CONNECT command. The ADSP operand attribute is ignored at LOGON/job initiation if SETROPTS NOADSP is in effect.

NOADSP

specifies that the new user is not to have the ADSP attribute. This is the default value if both ADSP and NOADSP are omitted.

SPECIAL

specifies that the new user will be allowed to issue all RACF commands with all operands except the operands that require the AUDITOR attribute. The SPECIAL keyword overrides NOSPECIAL specified on the CONNECT command.

You must have the SPECIAL attribute in order to enter the SPECIAL keyword.

NOSPECIAL

specifies that the new user is not to have the SPECIAL attribute. This is the default if both SPECIAL and NOSPECIAL are omitted.

OPERATIONS

specifies that the new user will have authorization to do maintenance operations on all RACF-protected DASD data sets, tape volumes, and DASD volumes except those where the access list specifically limits the OPERATIONS user to an access authority that is less than the operation requires. This limitation is accomplished via the PERMIT command. The

OPERATIONS keyword overrides NOOPERATIONS specified on the CONNECT command.

You must have the SPECIAL attribute in order to enter the OPERATIONS keyword.

NOOPERATIONS

specifies that the new user is not to have the OPERATIONS attribute. This is the default if both OPERATIONS and NOOPERATIONS are omitted.

AUDITOR

specifies that the new user will have full responsibility for auditing the use of system resources, and will be able to control the logging of detected accesses to any RACF-protected resources during RACF authorization checking and accesses to the RACF data set.

You must have the SPECIAL attribute in order to enter the AUDITOR keyword.

NOAUDITOR

specifies that the new user will not have the AUDITOR attribute. This is the default value if both AUDITOR and NOAUDITOR are omitted.

OIDCARD

specifies that the new user must supply an operator identification card when logging onto the system. If you specify the OIDCARD operand, the system will prompt you to enter the new user's operator identification card as part of the processing of the ADDUSER command. If the OIDCARD operand is specified in a job executing in the background or when you cannot be prompted in the foreground, the ADDUSER command will fail.

NOOIDCARD

specifies that the new user will not be required to supply an operator identification card. This is the default value if both OIDCARD and NOOIDCARD are omitted.

NOOIDCARD is only valid if PASSWORD is also specified (or defaulted to). If NOOIDCARD and NOPASSWORD are both specified (or defaulted to), the PASSWORD default is assumed.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the user's profile (enclosed in apostrophes if special characters are included). Note that only 254 characters will be chained off of the ACEE. Use the LISTUSER command to list this information. When the user executes a job in the background or during a TSO session, the data is available (in the ACEE) to the RACDEF and the RACHECK pre-processing and post-processing installation exit routines, and the RACINIT post-processing installation exit routines.

MODEL(dsname)

specifies the name of a discrete data set profile that will be used as a model when new data profiles are created that have 'userid' as the first-level qualifier. For this parameter to be effective, the MODEL(USER) option (specified on the SETROPTS command) must be active. The data set name will always be prefixed by "userid" when the model is accessed.

ADDUSER Examples

Example 1

Operation: User IA0 wants to define user PAJ5 and ESH25 to RACF and assign RESEARCH as their default group.

Known: User IA0 has JOIN authority to group RESEARCH and the CLAUTH attribute for the USER class.

User PAJ5 and ESH25 are not defined to RACF.

User IA0 is logged on to group RESEARCH.

Command: ADDUSER (PAJ5 ESH25)

Defaults: NAME(###...) PASSWORD(RESEARCH) OWNER(IA0) DFLTGRP(RESEARCH) AUTHORITY(USE) UACC(NONE) NOGRPACC NOADSP NOSPECIAL NOOPERATIONS NOCLAUTH NOAUDITOR NOOIDCARD

Example 2

Operation: User WJE10 wants to define user RGH01 to RACF and assign PAYROLL as the default and owning group. The password will be PASS, group authority will be CREATE, and universal access authority will be READ.

Known: User WJE10 has JOIN authority to group PAYROLL and the CLAUTH attribute for the USER class.

User WJE10 is not logged on to group PAYROLL.

User RGH01 is not defined to RACF.

The name of user RGH01 is RG Harris.

Command: ADDUSER RGH01 DFLTGRP(PAYROLL) OWNER(PAYROLL) PASSWORD(PASS) NAME(RGHARRIS) AUTHORITY(CREATE) UACC(READ)

Defaults: NOSPECIAL NOOPERATIONS NOCLAUTH NOOIDCARD NOAUDITOR

Example 3

Operation: User TTU01 wants to define user PIZ33 to RACF. User PIZ33 is to be the AUDITOR for the installation, and is to have class authority to terminals and tape volumes. User PIZ33 will not be required to enter a password, but will be identified via an OIDCARD.

Known: User TTU01 has the SPECIAL attribute.

User TTU01 is connected to group RESEARCH.

User PIZ33 is not defined to RACF.

Command: (entered in TSO foreground) ADDUSER PIZ33 NOPASSWORD OIDCARD CLAUTH(TAPEVOL TERMINAL) AUDITOR

User TTU01 will be prompted to enter the OIDCARD for PIZ33.

Defaults: NAME(###...) OWNER(TTU01) DFLTGRP(RESEARCH) AUTHORITY(USE) UACC(NONE) NOGRPACC NOADSP NOSPECIAL NOOPERATIONS

Example 4

Operation: User TTU5 wants to define user RADMIN to RACF. User RADMIN is to be a member of and be owned by the SYSINV group and have a model name of 'RADMIN.RACF.ACCESS'.

Known: User TTU5 has at least JOIN authority to group SYSINV and the CLAUTH attribute for the USER class.

Command: ADDUSER RADMIN DFLTGRP(SYSINV) MODEL(RACF.ACCESS) NAME('RACF ADMINISTRATOR') AUTHORITY(JOIN) ADSP UACC(NONE) OWNER(SYSINV)

Defaults: NOGRPACC, NOSPECIAL, NOOPERATIONS, NOAUDITOR

ALTDSD Command

Use the ALTDSD command to:

- Modify an existing profile discrete or generic data set profile.
- Protect a single volume of a multi-volume, non-VSAM DASD data set. (At least one volume must already be RACF-protected.)
- Remove RACF-protection from a single volume of a multi-volume, non-VSAM DASD data set. (The last volume cannot be deleted from the profile.)

RACF Requirements

To use the ALTDSD command you must have sufficient authority over the profile. The following checks (1 through 7) are made until one of the conditions is met.

1. You have the SPECIAL attribute.
2. The data set profile is within the scope of a group in which you have the group-SPECIAL attribute.
3. You are the owner of the profile.
4. The first-level qualifier of the profile name (or the qualifier supplied by the RACF naming conventions table or by a command installation exit) is your userid.

For discrete profiles only:

5. You are on the access list for the discrete profile and you have ALTER authority. (If you have any other level of authority, you may not alter this profile.)
6. Your current connect group is on the access list and has ALTER authority. (If your group has any other level of authority, you may not alter this profile.)
7. The universal access authority is ALTER.

To use the GLOBALAUDIT keyword, you must have the AUDITOR attribute or the data set profile must be within the scope of a group in which you have the group-AUDITOR attribute.

If you have the AUDITOR attribute or the data set profile is within the scope of a group in which you have the group-AUDITOR attribute, but do not satisfy one of the above checks (1-7), you may specify only the GLOBALAUDIT operand.

```
{ALTDSD}      profile-name[/password]
{ALD   }
              [OWNER(userid or group-name)]

              [UACC(access-authority)]

              [         {   NONE                                            }   ]
              [  AUDIT( { {{ALL     }                                        } ) ]
              [         { {{SUCCESS }  [(audit-access-level)] } ...          }   ]
              [         { {{FAILURES}                                        }   ]

              [               {   NONE                                            }    ]
              [  GLOBALAUDIT( { {{ALL     }                                        }  ) ]
              [               { {{SUCCESS }  [(audit-access-level)] } ...          }    ]
              [               { {{FAILURES}                                        }    ]

              [LEVEL(nn)]

              [ ADDVOL  (volume-serial) ]
              [ DELVOL  (volume-serial) ]

              [VOLUME(volume-serial)]

              [ALTVOL(old-volume-serial new-volume-serial)]

              [UNIT(type)]

              [GENERIC]
              [SET    ]
              [NOSET  ]

              [ DATA('installation-defined-data') ]
              [ NODATA                            ]

              [WARNING  ]
              [NOWARNING]
```

Note: If you specify a generic profile, the following operands are ignored: ADDVOL, DELVOL, VOLUME, ALTVOL, UNIT, SET, and NOSET.

profile-name

specifies the name of a discrete or generic data set profile. If you specify more than one profile, the list of names must be enclosed in parentheses.

This operand is required and must be the first operand following ALTDSD.

Note: Alias data set names are not supported.

password

specifies the data set password if you are altering the profile for a password-protected data set. This operand applies only if the ADDVOL and SET operands are used for a volume of a multi-volume password-protected data set. The WRITE level password must then be available.

If the command is executing in the foreground and you omit the password for a password-protected data set, the logon password is used. You will be prompted if the password you enter or the logon password is incorrect.

If the command is executing in a batch job and you either omit the password for a password-protected data set or supply an incorrect password, the operator will be prompted.

This operand can only be used for non-VSAM data sets. If you specify a generic profile, this operand is ignored.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be made the new owner of the profile. The owner of a group data set profile must have at least USE authority in the group to which the data sets belong.

To change the owner of a profile, you must be the current owner of the data set, have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Note: The user specified as the owner does not automatically have access to the data set. Use the PERMIT command to add the owner to the access list as desired.

UACC(access-authority)

specifies the new universal access authority to be associated with the data set or sets. The universal access authorities are ALTER, CONTROL, READ, UPDATE, and NONE. If the UACC keyword is entered without a value, it is ignored. (For non-VSAM data sets, CONTROL authority implies UPDATE authority.)

AUDIT

specifies which new access attempts you want to log on the SMF data set. The following options are available:

ALL

indicates that you want to log both authorized accesses and detected unauthorized access attempts.

SUCCESS

indicates that you want to log authorized accesses.

FAILURES

indicates that you want to log detected unauthorized access attempts.

NONE

indicates that you do not want any logging to be done.

If the AUDIT keyword is specified without a value, it is ignored.

audit-access-level

specifies which access level(s) you want to log on the SMF data set. The levels are:

READ

logs access attempts at any level. This is the default value if no access level is specified.

UPDATE

logs access attempts at the UPDATE, CONTROL, and ALTER levels.

CONTROL

logs access attempts at the CONTROL and ALTER levels.

ALTER

logs ALTER access-level attempts only.

GLOBALAUDIT

specifies which access attempts the user who has the AUDITOR attribute wants to log on the SMF data set. The options ALL, SUCCESS, FAILURES, and NONE and the audit-access levels, are the same as those described under the AUDIT keyword.

To use the GLOBALAUDIT keyword, you must have the AUDITOR attribute or the profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Note: Regardless of the value specified in the GLOBALAUDIT keyword, all access attempts specified on the AUDIT keyword will always be logged.

LEVEL(nn)

specifies a new level indicator, where nn is an integer between 0 and 99.

The meaning of the value is assigned by your installation. It is not used by the authorization function in RACHECK but is available to the RACF post-processing installation exit routine for the RACHECK SVC. It is included on all records that log data set accesses and is listed by the LISTDSD command.

ADDVOL(volume-serial)

specifies that you want to RACF-protect the portion of the data set residing on this volume. At least one other portion of the data set on a different volume must already have been RACF-protected. This operand can only be used for non-VSAM data sets.

The volume must be on-line unless the NOSET operand is specified. If it is not on-line and the NOSET operand is omitted, the ALTDSD command processor will request that the volume be mounted. This operand is ignored if you specify a generic name.

DELVOL(volume-serial)

specifies that you want to remove RACF-protection from the portion of the data set residing on this volume. If no other portions of this data set on another volume are RACF-protected, the command will terminate. (Use the DELDSD command to delete the profile from RACF.) This operand can only be used for non-VSAM data sets.

The volume must be on-line unless the NOSET operand is specified. If it is not on-line and the NOSET operand is omitted, the ALTDSD command processor will request that the volume be mounted. This operand is ignored if you specify a generic name.

VOLUME(volume-serial)

specifies the volume on which the non-VSAM data set or the catalog for the VSAM data set resides.

If this operand is specified and the volume-serial does not appear in the profile for the data set, the command is failed.

If the data set name appears more than once in the RACF data set and this operand is not specified, the command is failed. If the data set name appears only once and this operand is not specified, no volume serial checking is performed and processing continues. This operand is ignored if you specify a generic name.

ALTVOL(old-volume-serial new-volume-serial)

specifies that you want to change the volume serial number in the data set profile. This operand can be specified for both VSAM and non-VSAM data sets. If ALTVOL is specified, the SET and NOSET operands are ignored. When ALTVOL is specified, the data set profile is modified but RACF indicator processing is not performed. This operand is ignored if you specify a generic name.

To use the ALTVOL operand, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) must be your userid.

UNIT(type)

specifies the unit type to be added to the data set profile on which a non-VSAM data set resides. You may specify an installation-defined group name, a generic device type, or a specific device address. This operand is ignored if you specify a generic name.

GENERIC

specifies that RACF is to treat the profile name as a generic name, even if it does not contain any generic characters.

SET or NOSET

specifies whether the data set should be RACF-indicated or not. These keywords are ignored if you do not use the ADDVOL or DELVOL operand. This operand is ignored if you specify a generic name.

SET

specifies that:

- The data set on this volume will be RACF-indicated if the ADDVOL operand is specified. If the indicator is already on, the command will fail.

- The RACF-indicator for the data set on this volume will be set off if the DELVOL operand is specified. If the indicator is already off, the command will fail.

The volume indicated in the ADDVOL or DELVOL operand must be on-line.

NOSET

specifies that the RACF indicator for the data set will not be changed.

The volume indicated in the ADDVOL or DELVOL operand does not have to be online.

To use the NOSET operand, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) must be your userid. If you are not authorized, the NOSET and ADDVOL or DELVOL operands are ignored.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the data set profile. The data must be enclosed in apostrophes. Use the LISTDSD command to list this information. The data is also available to the RACHECK pre-processing and post-processing installation exit routines and is copied if this is a model profile, to the installation-defined data area for new data set profiles.

NODATA

specifies that the ALTDSD command is to delete any installation-defined data in the data set profile.

WARNING

specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

NOWARNING

specifies that if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

ALTDSD Examples

Example 1

Operation: User AEH0 owns data set profile PAYROLL.DEPT2.DATA and wants to assign ownership of the data set to group PAYROLL.

Known: Data set PAYROLL.DEPT2.DATA is RACF-defined with a discrete profile.

Command: ALTDSD 'PAYROLL.DEPT2.DATA' OWNER(PAYROLL)

Defaults: None

Example 2

Operation: User WRH0 wants to change the universal access authority to READ for data set RESEARCH.PROJ02.DATA and wants to have all accesses to the data set logged on SMF.

Known: User WRH0 has ALTER access to data set profile RESEARCH.PROJ02.DATA.

User WRH0 is logged onto group RESEARCH.

Data set RESEARCH.PROJ02.DATA is RACF-defined with a generic profile.

Command: ALTDSD 'RESEARCH.PROJ02.DATA' UACC(READ) AUDIT(ALL(READ)) GENERIC

Defaults: None

Example 3

Operation: User CD0 wants to remove RACF-protection from volume 222222 of the multi-volume data set CD0.PROJ2.DATA.

Known: CD0.PROJ2.DATA is a non-VSAM data set that resides on volumes 111111 and 222222 and is defined to RACF with a discrete profile. Volume 222222 is on-line. User CDO's TSO profile specifies PREFIX (CDO).

Command: ALTDSD PROJ2.DATA DELVOL(222222)

Default: SET

Example 4

Operation: User RVD02 wants to have all successful accesses to data set PAYROLL.ACCOUNT on volume SYS003 to be logged to the SMF data set.

Known: User RVD02 has the AUDITOR attribute.

Command: ALTDSD 'PAYROLL.ACCOUNT' GLOBALAUDIT(SUCCESS(READ)) VOLUME(SYS003)

Defaults: None

Example 5

Operation: User SJR1 wants to modify the installation-defined information associated with data set 'SYSINV.ADMIN.DATA'.

Known: User SJR1 has ALTER authority to the data set profile.

Command: ALTDSD 'SYSINV.ADMIN.DATA' DATA('LIST OF REVOKED RACF USERIDS')

Defaults: None

Example 6

Operation: User ADM1 wants to log all unauthorized access attempts and all successful updates to data sets protected by the generic profile SALES.ABC.*.

Known: User ADM1 has the SPECIAL attribute.

Command: ALTDSD ‘SALES.ABC.*’ AUDIT (FAILURES(READ) SUCCESS (UPDATE)).

Defaults: None

ALTGROUP Command

Use the ALTGROUP command to:

- Change the superior group of a group.
- Change the owner of a group.
- Change the terminal indicator for a group.
- Change a model profile name for a group.
- Change the installation-defined data associated with a group.

RACF Requirements

To change the superior group of a group:

- you must have the SPECIAL attribute, or
- the group profile must be within the scope of a group in which you have the group-SPECIAL attribute, or
- you must be the owner or have JOIN authority in both the current and the new superior groups.

Note: You can have JOIN authority in one group and be the owner of or have the group-SPECIAL attribute in the other group.

If you have the SPECIAL attribute, or if the group profile is within the scope of a group in which you have the group-SPECIAL attribute, or you are the current owner of the group, you can specify any keyword.

```
{ALTGROUP}      (group-name...)
{ALG     }
                [SUPGROUP(group-name)]

                [OWNER(userid or group-name)]

                [ TERMUACC   ]
                [ NOTERMUACC ]

                [ MODEL(dsname) ]
                [ NOMODEL       ]

                [ DATA('installation-defined-data') ]
                [ NODATA                            ]
```

group-name

specifies the name of the group whose attributes you want to modify. If you specify more than one group name, the list of names must be enclosed in parentheses.

This operand is required and must be the first operand following ALTGROUP.

SUPGROUP(group-name)

specifies the name of the RACF-defined group you want to make the new superior group for the group to be altered.

The new superior group must not be the same as the current one and it must not have any level of subgroup relationship to the group to be altered.

To change a superior group, you must have the SPECIAL attribute, the group profile must be within the scope of a group in which you have the group-SPECIAL attribute, or you must have JOIN authority in or be the owner of both the current and new superior groups. Note that you can have JOIN authority in one group and be the owner of or have the group-SPECIAL attribute in the other group.

If owner is a group name, then OWNER and SUPGROUP must specify the same group name.

OWNER(userid or group-name)

specifies a RACF-defined user or group you want to be the new owner of the group.

To change the owner of a group, you must be the current owner of the group, have the SPECIAL attribute, or have the group-SPECIAL attribute in the group owning the profile.

If you specify a group name, then OWNER and SUPGROUP must specify the same group name.

TERMUACC

specifies that the universal access authority specified for a terminal will be used by the group or users connected to the group during authorization checking to access the terminal.

NOTERMUACC

specifies that the group or a user connected to the group must be authorized via the PERMIT command with at least READ authority to access a terminal.

MODEL(dsname)

specifies the name of a data set profile that RACF is to use as a model when new data set profiles are created that have ‘group name’ as the first-level qualifier. For this parameter to be effective, the MODEL(GROUP) option on the SETROPTS command must be active. If the ALTGROUP command cannot find the ‘dsname’ profile, it issues a warning message and places the profile name in the group entry.

Note that dsname is always prefixed by the group name.

NOMODEL

specifies that the ALTGROUP command is to delete the model name in the group profile.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the group profile. The data must be enclosed in apostrophes. Use the LISTGRP command to list this information.

NODATA

specifies that the ALTGROUP command is to delete any installation-defined data in the group profile.

ALTGROUP Examples

Example 1

Operation: User WJB10 wants to change the superior group and owning group for PROJECTA from RESEARCH to PAYROLL. Users connected to group PROJECTA will be authorized access to terminals according to the universal access authority of the terminal.

Known: User WJB10 has JOIN authority in RESEARCH and is the owner of PAYROLL.

PROJECTA is a subgroup of RESEARCH.

Command: ALTGROUP PROJECTA SUPGROUP(PAYROLL) OWNER(PAYROLL) TERMUACC

Defaults: None

Example 2

Operation: User ADM1 wants to change the superior group for PROJECTB from SYS1 to RESEARCH and assign RESEARCH as the new owner.

Known: User ADM1 has the SPECIAL attribute.

PROJECTB is a subgroup of SYS1.

Command: ALTGROUP PROJECTB SUPGROUP(RESEARCH) OWNER(RESEARCH)

Defaults: None

Example 3

Operation: User SJR2 wants to change the installation-defined information associated with the RSC1 group and delete the model name.

Known: User SJR2 is the owner of group RSC1.

Command: ALTGROUP RSC1 DATA('RESOURCE USAGE ADMINISTRATION') NOMODEL

Defaults: None

ALTUSER Command

Use the ALTUSER command to:

- Change a user's system wide user attributes.
- Change a user's default universal access authority or level of group authority within a specified group.
- Revoke or reestablish a user's privilege to access the system.
- Change the installation-defined data associated with a user.
- Change the user's password or OIDCARD requirements.
- Alter a model profile name for a user.

A change to the user's level of authority in a group (via the AUTHORITY operand) is reflected in the appropriate group profile. A change to the user's default universal access authority for a group (via the UACC operand) is reflected in the appropriate connect profile. The user's profile is updated for all other changes.

Note: If the user is currently in the system, changes to the attributes (except for OWNER and AUTHORITY) do not take effect until the next time the user enters the system, although the LISTUSER command shows the new values.

RACF Requirements

The level of authority required depends on which of the user's attributes you want to change.

- If you have the SPECIAL attribute, you may use all of the operands except UAUDIT/NOUAUDIT.
- If the user profile is within the scope of a group in which you have the group-SPECIAL attribute, you may use all of the operands except SPECIAL, AUDITOR, OPERATIONS, and UAUDIT/NOUAUDIT.
- If you are the owner of the user's profile, you may use any of the following operands for user-related attributes:

  NAME
  OWNER
  DFLTGRP
  GRPACC or NOGRPACC
  ADSP or NOADSP
  REVOKE or RESUME
  PASSWORD or NOPASSWORD
  OIDCARD or NOOIDCARD
  DATA or NODATA
  MODEL or NOMODEL

- Each user may change his or her name field or default group (NAME and DFLTGRP operands).

- If you have JOIN authority or CONNECT authority, or if the group profile is within the scope of a group in which you have the group-SPECIAL attribute, or if you are the owner of the specified group, you may use the following operands for group-related user attributes:

  GROUP
  AUTHORITY
  UACC

- You must have the SPECIAL attribute to specify the AUDITOR/NOAUDITOR, SPECIAL/NOSPECIAL, and OPERATIONS/NOOPERATIONS operands as system-wide user attributes.

- You must have either the AUDITOR attribute or the user profile must be within the scope of a group in which you have the group-AUDITOR attribute for you to specify the UAUDIT/NOUAUDIT operand.

- If you are the owner of the user's profile and have the CLAUTH attribute for the class to be added or deleted, you may specify the CLAUTH and NOCLAUTH operands.

```
{ALTUSER}          (userid...)
{ALU    }
                   [NAME(user-name)]

                   [ PASSWORD[(password)] ]
                   [ NOPASSWORD           ]

                   [OWNER(userid or group-name)]

                   [GROUP(group-name)]

                   [DFLTGRP(group-name)]

                   [AUTHORITY(group-authority)]

                   [UACC(access-authority)]

                   [ CLAUTH(class-name ...)   ]
                   [ NOCLAUTH(class-name ...) ]

                   [ GRPACC   ]
                   [ NOGRPACC ]

                   [ ADSP   ]
                   [ NOADSP ]

                   [ SPECIAL   ]
                   [ NOSPECIAL ]

                   [ OPERATIONS   ]
                   [ NOOPERATIONS ]

                   [ UAUDIT  ]
                   [ NOAUDIT ]

                   [ AUDITOR   ]
                   [ NOAUDITOR ]

                   [ OIDCARD   ]
                   [ NOOIDCARD ]

                   [ REVOKE ]
                   [ RESUME ]

                   [ DATA('installation-defined-data') ]
                   [ NODATA                            ]

                   [ MODEL(dsname) ]
                   [ NOMODEL       ]
```

userid

specifies the RACF-defined user or users whose attributes you want to change. If you specify more than one userid, the list must be enclosed in parentheses.

This operand is required and must be the first operand following ALTUSER.

NAME(user-name)

specifies the new user name to be associated with the userid. You may use a maximum of 20 alphanumeric characters, enclosed in apostrophes if special characters are included.

PASSWORD[(password)]

specifies the password to be associated with the user. If PASSWORD is specified without a value, the default password is the user's default group name. If the password value is omitted and DFLTGRP is specified, the default password is the user's old default group name.

The date of the last password update is set to 0, thus forcing a password change at the next LOGON or job start.

NOPASSWORD

specifies that the user does not need to supply a password when entering the system.

NOPASSWORD is only valid if the user has the OIDCARD attribute or if OIDCARD is specified on this command.

If both NOPASSWORD and NOOIDCARD are specified, both are ignored.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the new owner of the user's profile.

GROUP(group-name)

specifies the name of a group to which the user is connected.

Changes to the group-related user attributes UACC and AUTHORITY are applied to the specified group. If you omit the GROUP operand, the changes are made to the user's default group. If you omit the GROUP operand and DFLTGRP is specified, the changes are made to the user's old default group.

DFLTGRP(group-name)

specifies the name of a RACF-defined group to be used as the new default group for the user. The user must already be connected to the group with at least USE authority.

The user remains connected to the old default group.

AUTHORITY(group-authority)

specifies the new level of authority the user will have in the group specified in the GROUP operand. The valid group authority values are USE, CREATE, CONNECT, and JOIN. If the keyword AUTHORITY is entered without a value, the operand is ignored.

UACC(access-authority)

specifies the new default value for the universal access authority for all new resources the user defines while connected to the specified default group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. If the keyword UACC is entered without a value, the operand is ignored.

This option is group-related. If the user is connected to other groups, the user can have a different default universal access authority in each group.

Note: When a user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using the group specified in the GROUP operand as the current connect group, any data set or tape volume RACF profiles the user defines will be assigned this default universal access value.

CLAUTH(class-name ...)
specifies the classes in which the user is allowed to define profiles to RACF for protection in addition to the classes previously allowed for the user. Classes you can specify are USER, and any resource class defined in the class descriptor table. Any class names specified are added to the class names previously specified for this user.

In order to enter the CLAUTH operand, you must have the SPECIAL attribute, or the user's profile must be within the scope of a group in which you have the group-SPCIAL attribute and have the CLAUTH attribute, or you must be the owner of the user's profile and have the CLAUTH attribute for the class to be added. If you do not have sufficient authority for a specified class, the CLAUTH specification for that class is ignored, and processing continues with the next class name specified.

NOCLAUTH(class-name ...)
specifies that the user is not allowed to define profiles to RACF for class names specified. The valid values are USER, and any resource class name defined in the class descriptor table. Any class names specified are deleted from the class names previously specified for this user.

In order to enter the NOCLAUTH operand, you must have the SPECIAL attribute, or the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute and have the CLAUTH attribute, or you must be the owner of the user's profile and have the CLAUTH attribute for the class to be deleted. If you do not have sufficient authority for a specified class, the NOCLAUTH specification for that class is ignored, and processing continues with the next class name specified.

GRPACC
specifies that group data sets defined by this user will automatically be accessible to other users in the group. The group whose name is used as the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority to the data set. The GRPACC keyword overrides NOGRPACC specified on the CONNECT command.

NOGRPACC
specifies that the user will no longer have the GRPACC attribute.

ADSP
specifies that all permanent DASD data sets created by the user will automatically be RACF-protected by discrete profiles. The ADSP keyword overrides NOADSP specified on the CONNECT command.

The ADSP attribute is ignored at LOGON/job initiation if SETROPTS NOADSP is in effect.

NOADSP

specifies that the user will no longer have the ADSP attribute.

SPECIAL

specifies that the user will be allowed to issue all RACF commands with all operands except the operands that require the AUDITOR attribute. The SPECIAL keyword overrides NOSPECIAL specified on the CONNECT command.

You must have the SPECIAL attribute in order to use the SPECIAL keyword.

NOSPECIAL

specifies that the user will no longer have the SPECIAL attribute.

You must have the SPECIAL attribute in order to use the NOSPECIAL keyword.

OPERATIONS

specifies that the user will have authorization to do maintenance operations on all RACF-protected DASD data sets, tape volumes, and DASD volumes except those where the access list specifically limits the OPERATIONS user to an access authority that is less than the operation requires. This limitation is accomplished via the PERMIT command. The OPERATIONS keyword overrides NOOPERATIONS specified on the CONNECT command.

You must have the SPECIAL attribute to use the OPERATIONS keyword.

NOOPERATIONS

specifies that the user will no longer have the OPERATIONS attribute.

You must have the SPECIAL attribute in order to use the NOOPERATIONS keyword.

UAUDIT

specifies that all RACHECK and RACDEF SVCs issued for the user and all RACF commands (except SEARCH, LISTDSD, LISTGRP, LISTUSER, and RLIST) issued by the user will be logged. (When the user is initially defined to RACF by the ADDUSER command, the system assumes NOUAUDIT.)

You must have the AUDITOR attribute or the user profile must be within the scope of a group in which you have the group-AUDITOR attribute in order tc enter the UAUDIT operand.

NOUAUDIT

specifies that no UAUDIT logging is to be performed. This keyword does not override any other auditing options (for example, CMDVIOL specified on SETROPTS) that may be in effect.

You must have the AUDITOR attribute or have the user profile within the scope of a group in which you have the group-AUDITOR attribute in order to enter the NOUAUDIT keyword.

AUDITOR

specifies that the user will have full responsibility for auditing the use of system resources, and will be able to control the logging of detected accesses to any RACF-protected resources during RACF authorization checking and accesses to the RACF data set.

You must have the SPECIAL attribute in order to enter the AUDITOR keyword.

NOAUDITOR

specifies that the AUDITOR attribute will be removed from the user.

You must have the SPECIAL attribute in order to enter the NOAUDITOR keyword.

OIDCARD

specifies that the user must supply an operator identification card when logging onto the system. If you specify the OIDCARD operand, the system will prompt you to enter the user's new operator identification card as part of the processing of the ALTUSER command. If the OIDCARD operand is specified in a job executing in the background or when you cannot be prompted in the foreground, the ALTUSER command will fail.

NOOIDCARD

specifies that the user will not be required to supply an operator identification card. NOOIDCARD is only valid if the user has the PASSWORD attribute or if PASSWORD is specified for the user on this command.

If both NOOIDCARD and NOPASSWORD are specified, both are ignored.

REVOKE

specifies that the user is prohibited from accessing the system. The user's profile and data sets are not deleted from the RACF data set. The REVOKE keyword overrides RESUME specified on the CONNECT command.

RESUME

specifies that a user is allowed to use the system again.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data that is kept in the user's profile. The data must be enclosed in apostrophes. Use the LISTUSER command to list this information.

When the user executes a job in the background or during a TSO session, the data is available (in the ACEE) to the RACDEF pre-processing, the RACHECK pre-processing and post-processing installation exit routines, and the RACINIT post-processing installation exit routines.

NODATA

specifies that the ALTUSER command is to delete the installation-defined data in the user's profile.

MODEL(dsname)

specifies the name of a data set that RACF is to use as a model when new data set profiles are created that have 'userid' as the first-level qualifier. For this parameter to be effective, the MODEL(USER) option (specified on the SETROPTS command) must be active. If the ALTUSER command cannot find the 'dsname' profile, it issues a warning message but places the model name in the userid entry.

Note that dsname will always be prefixed by the userid.

NOMODEL

specifies that the ALTUSER command is to delete the model name data in the user's profile.

ALTUSER Examples

Example 1

Operation: User IA0 wants to alter the level of group authority from USE to CREATE for user DAF0 in the user's default group so that user DAF0 can define generic profiles for data sets in group RESEARCH.

Known: User IA0 is the owner of user DAF0 and has JOIN authority in the group RESEARCH.

The default group for user DAF0 is RESEARCH.

Command: ALTUSER DAF0 AUTHORITY(CREATE)

Defaults: GROUP(RESEARCH)

Example 2

Operation: User CD0 wants to correct his name and change his default group to PAYROLL.

Known: The default group for user CD0 is RESEARCH.

User CD0 has USE authority in the group PAYROLL.

Command: ALTUSER CD0 NAME(CDAVIS) DFLTGRP(PAYROLL)

Defaults: None

Example 3

Operation: User IA0 wants to revoke user ESH25's privilege to enter the system.

Known: User IA0 is connected to group PAYROLL with the group-SPECIAL attribute. Group PAYROLL is user ESH25's default group.

Command: ALTUSER ESH25 REVOKE

Defaults: None

Example 4

Operation: User RGB01 wants to remove from USER1 all class authorities and the AUDITOR attribute, and wants to audit all activity by user USER1.

Known: User RGB01 has the SPECIAL and AUDITOR attributes.

User USER1 is an existing user.

Command: ALTUSER USER1 NOCLAUTH(TAPEVOL DASDVOL USER TERMINAL) NOAUDITOR UAUDIT

Defaults: None

Example 5

Operation: User RADMIN wants to change the installation-defined information contained in the SJR1 userid entry, and delete the model name information.

Known: User RADMIN is the owner of userid SJR1.

Command: ALTUSER SJR1 DATA('RESOURCE USAGE ADMINISTRATOR') NAME('TOM P.') NOMODEL

Defaults: None

CONNECT Command

Use the CONNECT command to connect a user to a group, modify a user's connection to a group, or assign the group-related user attributes. If a connection is being created, defaults are available as stated for each operand. If an existing connection is being modified, no defaults apply.

RACF Requirements

The specified users and group must already be defined to RACF.

To use the CONNECT command, you must:

- have the SPECIAL attribute, or
- have the group-SPECIAL attribute in the group, or
- be the owner of the group, or
- have JOIN or CONNECT authority in the group.

You may not give a user a higher level of authority in the group than you have.

```
{CONNECT}     (userid ... )
{CO     }
              [GROUP(group-name)]

              [OWNER(userid or group-name)]

              [AUTHORITY(group-authority)]

              [UACC[(access-authority)]

               [GRPACC  ]
               [NOGRPACC]

               [ADSP  ]
               [NOADSP]

               [SPECIAL  ]
               [NOSPECIAL]

               [AUDITOR  ]
               [NOAUDITOR]

               [OPERATIONS  ]
               [NOOPERATIONS]

               [REVOKE]
               [RESUME]
```

userid

specifies the RACF-defined user to be connected to or modified in the group specified in the GROUP operand. If you are specifying more than one user, the userids must be enclosed in parentheses.

The approximate number of groups you can specify is 2950. Refer to *SPL: RACF* for information about how to determine the exact maximum number of groups.

This operand is required and must be the first operand following CONNECT.

GROUP(group-name)

specifies a RACF-defined group. If you omit this operand, the user will be connected to or modified in your current connect group.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the owner of the connect profile. If a connection is being created and you do not specify an owner, you are defined as the owner of the connect profile.

AUTHORITY(group-authority)

specifies the level of authority the user is to have in the group. The valid group authority values are USE, CREATE, CONNECT, and JOIN. If a connection is being created and this keyword is omitted or entered without a value, the default value is USE.

You may not give a user a higher level of authority in the group than you have.

UACC[(access-authority)]

specifies the default value for the universal access authority for all new resources the user defines while connected to the specified group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. If a connection is being created and this operand is omitted or entered without a value, the default is NONE.

This option is group-related. The user can have a different default universal access authority in each of the groups to which the user is connected.

Note: When a user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using the group specified in the GROUP operand as the current connect group, any data set or tape volume RACF profiles the user defines will be assigned this default universal access authority value.

GRPACC

specifies that any group data sets defined by the user, when connected to this group, will be automatically accessible to other users in the group. The group whose name is used as the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority to the data set.

NOGRPACC

specifies that the user will not have the GRPACC attribute. If a connection is being created, this is the default value if both GRPACC and NOGRPACC are omitted. A user attribute of GRPACC specified on the ADDUSER or ALTUSER command will override NOGRPACC as a connect attribute.

ADSP

specifies that all permanent DASD data sets created by the user, when connected to this group, will automatically be RACF-protected by discrete profiles.

The ADSP attribute is ignored at LOGON/job initiation if SETROPTS NOADSP is in effect.

NOADSP

specifies that the user is not to have the ADSP attribute. If a connection is being created, this is the default value if both ADSP and NOADSP are omitted. A user attribute of ADSP specified on the ADDUSER or ALTUSER command will override NOADSP as a connect attribute.

SPECIAL

specifies that the user will have the group-SPECIAL attribute when connected to this group. To enter the SPECIAL operand, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOSPECIAL

specifies that the user is not to have the group-SPECIAL attribute. If a connection is being created, this is the default value if both SPECIAL and NOSPECIAL are omitted. If an existing connection is being modified, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are modifying the user's profile.

A user attribute of SPECIAL specified on the ADDUSER or ALTUSER command will override NOSPECIAL as a connect attribute.

AUDITOR

specifies that the user will have the group-AUDITOR attribute when connected to this group.

To enter the AUDITOR operand, you must have either the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOAUDITOR

specifies that the user is not to have the group-AUDITOR attribute when connected to this group. When a connection is being created, this is the default value if both AUDITOR and NOAUDITOR are omitted. If an existing connection is being modified, you must have either the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are modifying the user's profile.

A user attribute of AUDITOR specified on the ADDUSER or ALTUSER command will override NOAUDITOR as a connect attribute.

OPERATIONS

specifies that the user will have the group-OPERATIONS attribute when connected to this group. The user will have authorization to do maintenance operations on all RACF-protected DASD data sets, tape volumes, and DASD volumes within the scope of the group except those where the access list specifically limits the OPERATIONS user to an access authority that is less than the operation requires. (This limitation is accomplished via the PERMIT command.)

To enter the OPERATIONS keyword, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOOPERATIONS

specifies that the user is not to have the group-OPERATIONS attribute in this group. If a connection is being created, this is the default value if both OPERATIONS and NOOPERATIONS are omitted. If an existing connection is being modified, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are modifying the user's profile.

A user attribute of OPERATIONS specified on the ADDUSER or ALTUSER command will override NOOPERATIONS as a connect attribute.

REVOKE

specifies that the user is prohibited from accessing the system by attempting to connect to this group. The user's profile and data sets are not deleted from the RACF data set, thus prohibiting access to data by this user on behalf of this group.

RESUME

specifies that the user, when connected to this group, is allowed to use the system again. If a connection is being created, this is the default value if both REVOKE and RESUME are omitted. A user attribute of REVOKE specified on the ALTUSER command will override RESUME as a connect attribute.

CONNECT Examples

Example 1

Operation: User WJE10 wants to connect users AFG5 and GMD2 to group PAYROLL and to make PAYROLL the owner of the connect profiles.

Known: User WJE10 has JOIN authority to group PAYROLL.

User WJE10 is logged on to group PAYROLL.

Users AFG5 and GMD2 are defined to RACF but not connected to group PAYROLL.

Command: CONNECT (AFG5 GMD2) OWNER(PAYROLL)

Defaults: GROUP(PAYROLL) AUTHORITY(USE) UACC(NONE) NOADSP NOGRPACC RESUME NOOPERATIONS NOSPECIAL NOAUDITOR

Example 2

Operation: User WRH0 wants to CONNECT user PDJ6 to group RESEARCH with CREATE authority and universal access of UPDATE.

Known: User WRH0 has CONNECT authority to group RESEARCH.

User WRH0 is not logged on to group RESEARCH.

User PDJ6 is defined to RACF but is not connected to group RESEARCH.

Command: CONNECT PDJ6 GROUP(RESEARCH) AUTHORITY(CREATE) UACC(UPDATE)

Defaults: NOGRPACC RESUME NOOPERATIONS NOSPECIAL NOAUDITOR NOADSP OWNER(WRH0)

DELDSD Command

Use the DELDSD command to remove RACF protection for DASD data sets that are protected by either discrete or generic profile.

When RACF-protection is removed for a DASD data set protected by a discrete profile:

- The RACF indicator for the data set is turned off. The indicator is in the DSCB for a non-VSAM data set or in the catalog entry for a VSAM data set.

- The data set profile is deleted from the RACF data set. (**Note:** The data set itself is not physically deleted or scratched.)

To remove RACF protection from a non-VSAM data set that is protected by a discrete profile, the data set must be online and not currently in use. For a VSAM data set that is protected by a discrete profile, the catalog for the data set must be online. The VSAM data set itself must also be online if the VSAM catalog recovery option is being used. If the required data set or catalog is not online, the DELDSD command processor will request that the volume be mounted.

RACF Requirements

To remove RACF protection from a DASD data set or to delete a generic data set profile, you must have sufficient authority over the data set. The following checks are made until one of the conditions is met:

1. You have the SPECIAL attribute.

2. The data set profile is within the scope of a group in which you have the group-SPECIAL attribute.

3. The first-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your userid.

4. You are the owner of the profile.

For discrete profiles only:

5. The data set is protected by a discrete profile and you are on the access list with ALTER authority.

6. The data set is protected by a discrete profile and your group or one of your groups (if list of groups checking is active) is on the access list and has ALTER authority.

7. The data set is protected by a discrete profile and the universal access authority is ALTER.

```
{DELDSD}          (profile-name...)
{DD    }
                  [VOLUME(volume-serial)]

                  [ SET     ]
                  [ NOSET   ]
                  [ GENERIC ]
```

Note: If you specify a generic name, RACF ignores the VOLUME, SET, and NOSET operands.

profile-name

specifies the name of the discrete or generic profile. If you specify more than one profile, the list must be enclosed in parentheses.

This operand is required and must be the first operand following DELDSD.

Note: Alias data set names are not supported.

VOLUME(volume-serial)

specifies the volume on which the non-VSAM data set or the catalog for the VSAM data set resides.

If this operand is specified and the volume-serial does not appear in the profile for the data set, the command fails.

If the data set name appears more than once in the RACF data set and this operand is not specified, the command fails. If the data set name appears only once and this operand is not specified, no volume-serial checking is performed and processing continues.

If the profile name contains a generic character or if you specify the GENERIC operand, RACF ignores this operand.

SET or NOSET

specifies whether the RACF indicator should be set off or not.

If the profile name contains a generic character or if you specify the GENERIC operand, RACF ignores this operand.

SET

specifies that the RACF indicator for the data set will be turned off. It is the default value and is used when you are removing RACF protection for a data set. If the indicator is already off, the command will fail.

NOSET

specifies that the RACF indicator will not be turned off.

The NOSET operand is used when you are exporting a RACF-defined data set to another system using RACF. Leaving the indicator on prevents unauthorized access to the data set until it can be redefined on the new system. (To delete multiple data set profiles, see Example 2 for the SEARCH command.)

If NOSET is specified, the volume(s) on which the data set or catalog reside(s) need not be online.

To use the NOSET operand, you must have the SPECIAL attribute, the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the first-level qualifier of the data set name (or the qualifier supplied by the naming conventions table or by a command installation exit) must be your userid.

GENERIC

specifies that RACF is to treat the profile name as a generic name, even if it does not contain any generic characters.

DELDSD Examples

Example 1

Operation: User EH0 wants to remove discrete profile RACF protection from data set CD0.DEPT1.DATA.

Known: User EH0 owns data set CD0.DEPT1.DATA.

Command: DELDSD 'CD0.DEPT1.DATA'

Defaults: SET

Example 2

Operation: User KLE05 wants to remove discrete profile protection from data set KLE05.DUPDS1.DATA. The data set is a duplicate data set, and the user wants to remove the profile for the data set on volume DU2 without turning off the RACF indicator.

Command: DELDSD DUPDS1.DATA VOLUME(DU2) NOSET

Defaults: None

Example 3

Operation: User KLE05 wants to delete the generic profile and remove RACF protection from the data set or sets protected by the profile SALES.*.DATA

Known: User KLE05 has the group-SPECIAL attribute in group "SALES."

Command: DELDSD 'SALES.*.DATA'

Defaults: None

DELGROUP Command

Use the DELGROUP command to delete a group and its relationship to its superior group from RACF.

There are however, other places in the RACF data set where the group name may appear and is not deleted. For example, the group name could be in the access list for any resource. The RACF cross reference utility program can be used to find any occurrences of the group name in the RACF data set. (See *SPL: RACF* for a description of this utility.) Use the PERMIT command to remove access authorities.

RACF Requirements

To use the DELGROUP command:

- you must have the SPECIAL attribute, or
- the group to be deleted must be within the scope of a group in which you have the group-SPECIAL attribute, or
- you must be the owner of the superior group, or
- you must have JOIN authority in the superior group, or
- you must be the owner of the group to be deleted.

```
{DELGROUP}          (group-name...)
{DG      }
```

group-name
specifies the name of the group whose profile is to be removed from the RACF data set. If you are deleting more than one group, the list of group names must be enclosed in parentheses.

You must enter at least one group name and the following conditions must exist:

- The group must be defined to RACF.
- The group must not have any subgroups.
- The group must not have any group data sets (data sets whose names are qualified by the group name or begin with the value supplied by an installation exit).
- The group must not have any users connected to it.

DELGROUP Example

Example 1

Operation: User WJE10 wants to delete subgroups DEPT1 and DEPT2 from group PAYROLL.

Known: User WJE10 has JOIN authority to group PAYROLL.

DEPT1 and DEPT2 are subgroups of group PAYROLL.

Neither DEPT1 nor DEPT2 have any subgroups or users connected to them. In addition neither group has any group data sets.

Command: DELGROUP (DEPT1 DEPT2)

Defaults: None

DELUSER Command

Use the DELUSER command to delete a user from RACF.

This command removes the user's profile and all connections the user has to RACF groups (all connect profiles for the user).

There are however, other places in the RACF data set where the user's userid may appear that are not deleted. Specifically, the user could be the owner of a group, the owner of a user's profile, the owner of a group data set, or could be in the access list for any resource. Using the REMOVE command, assign new owners for any group data sets the user owns in groups other than his default group. Then use the DELUSER command. The RACF cross reference utility program can then be used to find any other occurrences of the userid. (See *SPL: RACF* for a description of this utility.) Use the ALTGROUP, ALTUSER, ALTDSD, RALTER, and PERMIT commands to change ownerships and remove access authorities.

RACF Requirements

To use the DELUSER command:

- you must have the SPECIAL attribute, or
- the user profile to be deleted must be within the scope of a group in which you have the group-SPECIAL attribute, or
- you must be the owner of the user's profile.

Note: JOIN authority in the user's default group is not sufficient authority to delete the user from RACF.

```
{DELUSER}       (userid ... )
{DU     }
```

userid

specifies the userid of the user whose profile is to be deleted from the RACF data set. If you are deleting more than one user, the list of userids must be enclosed in parentheses. You must enter at least one userid and the following conditions must exist:

- The user must be defined to RACF.
- The user must not have any user data sets defined to RACF. (User data sets are data sets whose names are qualified by the userid of the user being deleted or begin with the value supplied by an installation exit.)

DELUSER Example

Example 1

Operation: User WJE10 wants to delete user AEH0 from RACF.

Known: User AEH0 is defined to RACF.

User AEH0 is not the owner of any RACF profiles.

User WJE10 is connected to group PAYROLL (and is the owner of user AEH0) with the group-SPECIAL attribute.

Command: DELUSER AEH0

Defaults: None

LISTDSD Command

Use the LISTDSD command to list details of DASD data set profiles.

You may request the details for any number of profiles by giving the full name of each profile. You may also request the details for all profiles whose names are qualified by specific userids, group names, and/or character strings.

The details that are given for each DASD data set profile are:

- The level.
- The owner.
- The type of access attempts (as specified by the AUDIT operand on the ADDSD or ALTDSD command) that are being logged on the SMF data set.
- The universal access authority.
- Your level of access authority.
- The group under which the profile was created.
- Whether it is a VSAM or a non-VSAM data set profile.
- The type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set (for auditors only).
- The volume serial number (volser) of the volume on which the data set resides. For both a single volume and multi-volume VSAM data set, the volser represents the volume containing the catalog entry for the data set. For a non-VSAM data set, the volser represents the volume containing the data set itself. If it is a multi-volume non-VSAM data set, a list of volsers is given. The list represents the volumes on which the protected data set resides. They are not listed in any particular order.
- Unit information for the data set (if unit information had been specified in the UNIT operand on the ADDSD or ALTDSD command).

You may request additional details as follows:

- Historical data:
  - date the data set was defined to RACF
  - date the data set was last referenced (See Note)
  - date the data set was last updated. (See Note)
- The number of times the data set was accessed by all users for each of the following access authorities:

  ALTER, CONTROL, UPDATE, READ (See Note)
- Installation-defined data as specified on the DATA operand of the ADDSD or ALTDSD command.

- The type of data set, if profile is MODEL.
- A list of:
  - all users and groups authorized to access the data set,
  - the level of authority for each user and group, and
  - the number of times each user has accessed the data set. (See Note)

Note: These details are not meaningful if resource statistics gathering is bypassed at your installation.

RACF Requirements

You must have a sufficient level of authority for each profile listed as the result of your request. The following checks are made for each profile until one of the conditions is met:

1. You have the SPECIAL attribute.
2. The profile is within the scope of a group in which you have the group-SPECIAL attribute
3. The first-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your userid.
4. You are the owner of the profile.
5. You are on the profile's access list with least READ authority. (If your level of authority is NONE, the data set is not listed.)
6. Your current connect group is on the access list and has at least READ authority. (If the group's level of authority is NONE, the data set is not listed.)
7. The universal access authority is at least READ.
8. You have the AUDITOR attribute.
9. The data set profile is within the scope of a group in which you have the group-AUDITOR attribute.

If you satisfy one of the first seven conditions and, in addition, have the AUDITOR attribute or the profile is within the scope of a group in which you have the group-AUDITOR attribute, the type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set are *also* displayed.

When requesting to see the access list for a profile with the AUTHUSER operand, your level of authority is checked for each profile until one of the conditions is met:

1. You have the SPECIAL attribute.
2. The profile is within the scope of a group in which you have the group-SPECIAL attribute.
3. The first-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your userid.

4. You are the owner of the profile.

5. You are on the profile's access list with ALTER authority. (If you have any other level of authority, you may not use the operand.)

6. Your current connect group is on the access list and has ALTER authority. (If your group has any other level of authority, you may not use the operand.)

7. The universal access authority is ALTER.

8. You have the AUDITOR attribute.

9. The data set profile is within the scope of a group in which you have the group-AUDITOR attribute.

```
{LISTDSD}       [DATASET(profile-name ...)]
{LD     }       [ID(name ...)             ]
                [PREFIX(char ...)         ]

                [GENERIC  ]
                [NOGENERIC]

               [VOLUME(volume-serial...)]

               [STATISTICS]

               [HISTORY]

               [AUTHUSER]

               [ALL]
```

DATASET(profile-name ...)
specifies the names of one or more discrete or generic profiles. If a specified name appears more than once in the RACF data set, LISTDSD will display information about all the data sets with that name to which you have proper authority.

Note that alias data set names are not supported.

ID(name ...)
specifies one or more userids and/or group names. All users and groups must be defined to RACF. Details are listed for all discrete and generic profiles that have the specified userids or group names as the first-level qualifier name (or as the qualifier supplied by a command installation exit).

Note that if neither the DATASET, PREFIX, nor ID operand is present, your userid is used as the default value for the ID operand.

PREFIX(char ...)

specifies one or more character strings. Details are listed for all profiles whose names begin with the specified character strings. The character string may contain one or more levels specified as *.

Note that comparison between the character strings and the profile names is not limited to the first-level qualifier. For example, if PREFIX(A.B.C) is specified, profiles A.B.C, A.B.CAD, and A.B.C.X are selected if found.

GENERIC or NOGENERIC

specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be selected. If neither operand is specified, both profile types are selected.

These operands are ignored unless generic profile command processing is enabled.

VOLUME(volume-serial...)

limits the profiles listed to those found on the specific volume or list of volumes identified by volume serial number. RACF does not list profiles with the same name found on other volumes. RACF ignores this operand for generic profiles.

STATISTICS

specifies that you want to list the statistics for each profile. The list will contain the number of times the profile was accessed by users with READ, UPDATE, CONTROL and ALTER authorities. A separate total is given for each authority level. (See Note)

HISTORY

specifies that you want to list the following data:

- date each profile was defined to RACF
- date each discrete or generic profile was last referenced (See Note)
- date each data set was last updated. (See Note)

AUTHUSER

specifies that you want to see the access list for each profile. The output will show:

- all users and groups authorized to access the data set,
- the level of authority for each user and group, and
- the number of times each user has accessed the data set. (See Note)

You must have sufficient authorization to use the AUTHUSER operand (see RACF Requirements above).

ALL

specifies that you want all information for each data set displayed at your terminal. The access list is not included unless you have sufficient authority to use the AUTHUSER operand (see RACF Requirements above). The type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set is not included unless you have the AUDITOR attribute.

Note: These details are not meaningful if resource statistics gathering is being bypassed at your installation. For generic profiles, the statistics and history information only reflect updates made to the generic profiles themselves.

LISTDSD Examples

Example 1

Operation: User DAF0 wants to list all information for his own data set profiles.

Known: User DAF0 is RACF-defined, and does not have the AUDITOR attribute.

Command: LISTDSD ALL

Defaults: ID(DAF0)

Output: See Figure 3.

Example 2

Operation: User IA0 wants to list the users authorized to data set SYS1.PLIBASE.

Known: User IA0 has ALTER authority to SYS1.PLIBASE, and does not have the AUDITOR attribute.

Command: LISTDSD DATASET('SYS1.PLIBASE') AUTHUSER

Defaults: None

Output: See Figure 4.

Example 3

Operation: User ADM1 wants to list a generic profile SALES.*.ABC.

Known: User ADM1 is the owner of the generic profile, and generic profile command processing is enabled. User ADM1 has the group-AUDITOR attribute in group SALES.

Command: LISTDSD DATASET('SALES.*.ABC')

Defaults: None

Output: See Figure 5.

```
LISTDSD ALL
 INFORMATION FOR DATASET DAF0.DS2.DATA
 LEVEL  OWNER     UNIVERSAL ACCESS   WARNING
 -----  --------  ----------------   -------
  00    DAF0             READ          NO
AUDITING
--------
SUCCESS(READ),FAILURES(ALTER)
YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
NONE GIVEN        RESEARCH     NON-VSAM
VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------  ----
231406                            SYSDA
NO INSTALLATION DATA
CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY)  (YEAR)        (DAY)  (YEAR)      (DAY)  (YEAR)
-------------  -------------------  ----------------
 145     82          145     82         145     82
ALTER COUNT  CONTROL COUNT   UPDATE COUNT  READ COUNT
-----------  -------------   ------------  ----------
  00005          00010          00008         00010
  USER    ACCESS   ACCESS COUNT
-------   -------   ------------
IA0         READ       00010
ADM1        READ       00000
PROJECTA  UPDATE       00008
INFORMATION FOR DATASET DAF0.DS3.DATA
 LEVEL  OWNER     UNIVERSAL ACCESS   WARNING
 -----  --------  ----------------   -------
  00    DAF0             READ          NO
AUDITING
--------
ALL(UPDATE)
YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
NONE GIVEN      RESEARCH       NON-VSAM
VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------  ----
231406                            SYSDA
NO INSTALLATION DATA
CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY)  (YEAR)        (DAY)  (YEAR)      (DAY)  (YEAR)
-------------  -------------------  ----------------
 145     82          145     82         145     82
ALTER COUNT  CONTROL COUNT   UPDATE COUNT  READ COUNT
-----------  -------------   ------------  ----------
 00005           00000          00008         00010
 USER     ACCESS   ACCESS COUNT
-------   -------  ------------
NO USERS IN ACCESS LIST
```

Figure 3. Example 1 Output for LISTDSD Command

```
LISTDSD  DATASET('SYS1.PL1BASE')  AUTHUSER
 INFORMATION FOR DATASET SYS1.PLIBASE

 LEVEL  OWNER    UNIVERSAL ACCESS  WARNING
 -----  -------- ----------------  -------
  00    IAO             READ          NO

AUDITING
--------
SUCCESS(UPDATE)

YOUR ACCESS  CREATION GROUP   DATASET TYPE
-----------  --------------   ------------
   ALTER          SYS1           NON-VSAM

VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------- ----
231407                             SYSDA

INSTALLATION DATA
--------------------------------------------------
PL/1 LINK LIBRARY

  USER     ACCESS   ACCESS COUNT
-------   -------   ------------
ESH25     UPDATE       00009
PROJECTB   READ        00015
IAO        ALTER       00020
```

Figure 4. Example 2 Output for LISTDSD Command

```
LISTDSD DATASET('SALES.*.ABC')
 INFORMATION FOR DATASET SALES.*.ABC (G)

 LEVEL  OWNER    UNIVERSAL ACCESS  WARNING
 -----  -------- ----------------  -------
  00    ADM1            READ          NO

 AUDITING
 --------
 ALL(READ)

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN      RESEARCH        NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 NO INSTALLATION DATA
```

Figure 5. Example 3 Output for LISTDSD Command

LISTGRP Command

Use the LISTGRP command to list details of specific RACF group profiles.

The following information is given for each group:

- the superior group of the group
- the owner of the group
- the terminal option of the group
- any subgroups under the group,
- installation defined data as specified by the DATA operand of the ADDGROUP and ALTGROUP command,
- the name of the data set model profile.

The following information is given for each user connected to the group:

- userid,
- user's level of authority in the group,
- number of times the user has entered the system using this group as the current connect group,
- user's default universal access authority,
- connect attributes (group-related user attributes).

RACF Requirements

You must have a sufficient level of authority in each group listed as the result of your request. You must:

- Have the SPECIAL attribute, or
- Have the group-SPECIAL attribute in each group to be listed or within the scope of the group to be listed, or
- Have the AUDITOR attribute, or
- Have the group-AUDITOR attribute in each group to be listed or within the scope of each group to be listed, or
- Be the owner of the group, or
- Have JOIN or CONNECT authority in the group.

To list details of all RACF group profiles, you must have the SPECIAL or AUDITOR attribute.

```
{LISTGRP}        [(group-name ... )]
{LG     }        [*                ]
```

group-name

specifies the name of one or more RACF-defined groups. If you specify more than one group name, the names must be enclosed in parentheses.

*

specifies that you are requesting details for all RACF-defined groups to which you have the required authority.

Note: If no information is entered after LISTGRP, your current connect group is used as the default value.

LISTGRP Examples

Example 1

Operation: User IA0 wants to list the group entries for group RESEARCH.

Known: User IA0 has CONNECT authority to group RESEARCH.

Command: LISTGRP RESEARCH

Defaults: None

Output: See Figure 6.

Example 2

Operation: User ADM1 wants to list the group entries for all groups.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Command: LISTGRP *

Defaults: None

Output: See Figure 7.

```
LISTGRP RESEARCH
INFORMATION FOR GROUP RESEARCH
    SUPERIOR GROUP=SYS1         OWNER=IBMUSER
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= PAYROLLB
    USER(S)=      ACCESS=      ACCESS COUNT=     UNIVERSAL ACCESS=
    IBMUSER         JOIN          000000              ALTER
       CONNECT   ATTRIBUTES=NONE
    DAF0            JOIN          000002              READ
      CONNECT    ATTRIBUTES=NONE
    IA0             CONNECT       000004              READ
      CONNECT    ATTRIBUTES=ADSP SPECIAL OPERATIONS
    ESH25           USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
    PROJCTB         USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
    RV2             CREATE        000000              READ
      CONNECT    ATTRIBUTES=NONE
    RV3             CREATE        000000              READ
      CONNECT    ATTRIBUTES=NONE
    ADM1            JOIN          000000              READ
      CONNECT    ATTRIBUTES=OPERATIONS
    AEH0            USE           000000              READ
      CONNECT    ATTRIBUTES=REVOKED
```

Figure 6. Example 1 Output for LISTGRP Command

```
LISTGRP *
INFORMATION FOR GROUP PAYROLLB
    SUPERIOR GROUP=RESEARCH     OWNER=IBMUSER
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    NO SUBGROUPS
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      IBMUSER       JOIN          000000               ALTER
         CONNECT ATTRIBUTES=NONE
      DAFO          CREATE        000000               READ
         CONNECT ATTRIBUTES=NONE
      IA0           CREATE        000000               READ
         CONNECT ATTRIBUTES=ADSP SPECIAL OPERATIONS
      AEHO          CREATE        000000               READ
         CONNECT ATTRIBUTES=REVOKED
INFORMATION FOR GROUP RESEARCH
    SUPERIOR GROUP=SYS1         OWNER=IBMUSER
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= PAYROLLB
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      IBMUSER       JOIN          000000               ALTER
         CONNECT ATTRIBUTES=NONE
      DAFO          JOIN          000002               READ
         CONNECT ATTRIBUTES=NONE
      IA0           CONNECT       000004               READ
         CONNECT ATTRIBUTES=ADSP SPECIAL OPERATIONS
      ESH25         USE           000000               READ
         CONNECT ATTRIBUTES=NONE
      PROJECTB      USE           000000               READ
         CONNECT ATTRIBUTES=NONE
      RV2           CREATE        000002               READ
         CONNECT ATTRIBUTES=NONE
      RV3           CREATE        000000               READ
         CONNECT ATTRIBUTES=NONE
      ADM1          JOIN          000001               READ
         CONNECT ATTRIBUTES=OPERATIONS
      AEHO          USE           000000               READ
         CONNECT ATTRIBUTES=REVOKED
```

Figure 7. Example 2 Output for LISTGRP Command

LISTUSER Command

Use the LISTUSER command to list the details of specific RACF user profiles.

The following information is given for the user:

- Userid
- User's name. (If the user's name was not specified on the ADDUSER command, then UNKNOWN is listed as the user's name.)
- Owner of the user's profile
- Date the user was defined to RACF
- Default group
- Date the user's password was last updated
- Password change interval (in number of days)
- User's attributes
- Date and time the user last entered the system
- Classes in which the user is authorized to define profiles
- Installation-defined data
- Name of data set model profile

In addition, the following information is given for each group the user is connected to:

- Group name
- User's authority in the group
- Userid of the person who connected the user to this group
- Date the user was connected to this group
- Number of times the user has entered the system with this group as the current connect group
- Default universal access authority
- Date and time the user last entered the system using this group as the current connect group
- Connect attributes (group-related user attributes)
- Name of group data set model profile

RACF Requirements

To list details of a user's profile:

- you must be the owner of the user's profile, or
- you must have the SPECIAL attribute, or
- the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute
- you must have the AUDITOR attribute, or
- the user's profile must be within the scope of a group in which you have the group-AUDITOR attribute

You can list the details of your own user profile.

To list details of all RACF-defined user profiles:

- you must have the SPECIAL attribute, or
- the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute
- you must have the AUDITOR attribute, or
- the user's profile must be within the scope of a group in which you have the group-AUDITOR attribute

If you have the AUDITOR attribute or the profile is within the scope of a group in which you the group-AUDITOR attribute, the UAUDIT/NOUAUDIT attribute is also displayed.

```
{LISTUSER}        [(userid...)]
{LU      }        [ *         ]
```

userid

specifies a RACF-defined user. If you specify more than one user, the list of userids must be enclosed in parentheses.

*

specifies that you are requesting details for all RACF-defined users to which you have the required authority.

Note: If no information is entered after LISTUSER, your userid is used as the default value.

LISTUSER Examples

Example 1

Operation: User DAF0 wants to list her user attributes.

Known: User DAF0 is RACF-defined.

Command: LISTUSER

Defaults: DAF0 (userid)

Output: See Figure 8.

Example 2

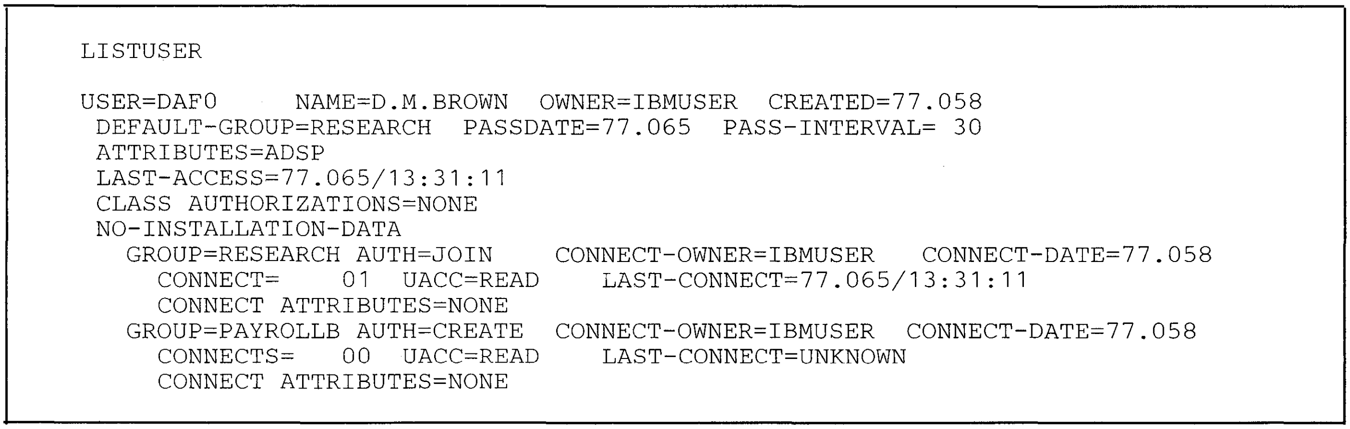
Operation: User ADM1 wants to list the user attributes of the RACF users IBMUSER, ADM1, and DAF0.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Command: LISTUSER (IBMUSER ADM1 DAF0)

Defaults: None

Output: See Figure 9.



```
LISTUSER

USER=DAF0     NAME=D.M.BROWN  OWNER=IBMUSER  CREATED=77.058
 DEFAULT-GROUP=RESEARCH  PASSDATE=77.065  PASS-INTERVAL= 30
 ATTRIBUTES=ADSP
 LAST-ACCESS=77.065/13:31:11
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
   GROUP=RESEARCH AUTH=JOIN    CONNECT-OWNER=IBMUSER   CONNECT-DATE=77.058
     CONNECT=     01  UACC=READ    LAST-CONNECT=77.065/13:31:11
     CONNECT ATTRIBUTES=NONE
   GROUP=PAYROLLB AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=77.058
     CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
     CONNECT ATTRIBUTES=NONE
```

Figure 8. Example 1 Output for LISTUSER Command

```
LISTUSER (IBMUSER ADM1 DAF0)
USER=IBMUSER  NAME=G. SMITH  OWNER=IBMUSER  CREATED=81.263
 DEFAULT-GROUP=SYS1     PASSDATE=82.104  PASS-INTERVAL=N/A
 ATTRIBUTES=SPECIAL OPERATIONS
 ATTRIBUTES=AUDITOR
 LAST-ACCESS=82.146/15:45:23
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
  GROUP=SYS1      AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=81.263
    CONNECTS=   456  UACC=READ    LAST-CONNECT=82.146/15:45:23
    CONNECT ATTRIBUTES=NONE
  GROUP=VSAMDSET  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=81.263
    CONNECTS=    00  UACC=NONE    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
  GROUP=SYSCTLG   AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=81.263
    CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
  GROUP=RESEARCH  AUTH=JOIN     CONNECT-OWNER=IBMUSER CONNECT-DATE=82.144
    CONNECTS=    00  UACC=ALTER    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
  GROUP=PAYROLLB  AUTH=JOIN     CONNECT-OWNER=IBMUSER  CONNECT-DATE=82.144
    CONNECTS=    00  UACC=ALTER    LAST-CONNECT=UNKNOWN
    CONNECT   ATTRIBUTES=NONE
USER=ADM1 NAME=S.A.SMITH           OWNER=IBMUSER   CREATED=82.144
 DEFAULT-GROUP=RESEARCH  PASSDATE=00.000PASS-INTERVAL=254
 ATTRIBUTES=SPECIAL
 ATTRIBUTES=AUDITOR
 LAST-ACCESS=82.146/16:16:14
 CLASS AUTHORIZATIONS=USER
 NO-INSTALLATION-DATA
 MODEL-NAME=ALLENA
  GROUP=RESEARCH  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=82.144
    CONNECTS=    01  UACC=READ    LAST-CONNECT=82.146/16:16:14
    CONNECT ATTRIBUTES=OPERATIONS
  GROUP=VSAMDSET  AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=82.144
    CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=OPERATIONS
USER=DAF0     NAME=D.M.BROWN   OWNER=IBMUSER  CREATED=82.144
 DEFAULT-GROUP=RESEARCH  PASSDATE=00.000  PASS-INTERVAL= 254
 ATTRIBUTES=ADSP
 LAST-ACCESS=82.146/15:11:31
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
  GROUP=RESEARCH  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=82.144
    CONNECTS=    02  UACC=READ    LAST-CONNECT=82.146/15:11:31
    CONNECT ATTRIBUTES=NONE
  GROUP=PAYROLLB AUTH=CREATE   CONNECT-OWNER=IBMUSER  CONNECT-DATE=82.144
    CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
```

Figure 9. Example 2 Output for LISTUSER Command

PASSWORD Command

Use the PASSWORD command to:

- Change your current password to a specified value.
- Change the password interval (the number of days that a password remains valid).
- Specify a password that never expires.
- Reset a user's password to a known default value.

The PASSWORD command allows you to change your password at any time. It also allows you to change the number of days that a password is valid or specify that a current password will be valid indefinitely.

The reset function of the command means that no one in the system need know another user's password. If a user's password is lost, this command allows you, if you have sufficient authority, to reset the password to a known, expired value without having to know the current value. The user can then LOGON to the system or submit a batch job and change the reset value to a new password known only to the user.

RACF Requirements

You may change your password or your password change interval if you are a RACF-defined user and if you are required to enter a RACF user password.

In order to reset another user's password to the user's default value or set a password that never expires:

- you must have the SPECIAL attribute, or
- the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute, or
- you must be the owner of the user's profile.

To change another user's password interval, or set a password that never expires, you must have the SPECIAL attribute or have the profile within the scope of a group in which you have the group-SPECIAL attribute.

```
{PASSWORD}       [PASSWORD(current-password new-password)]
{PW      }
                  [INTERVAL(change-interval)]
                  [NOINTERVAL               ]

                 [USER(userid...)]
```

PASSWORD(current-password new-password)

specifies your current password and the new one you want. If you enter only the PASSWORD operand, you will be prompted so that you can enter the current and new passwords in print inhibit mode.

The current and new passwords must have different values. If you specify your current password incorrectly, you are notified and the PASSWORD operand is ignored.

This operand is ignored if the USER operand is present.

You may change your own password at any time.

INTERVAL(change-interval)

indicates the number of days during which a password remains valid; the range is from 1 through 254 days.

The value specified here cannot exceed the value specified in the INTERVAL operand of the SETROPTS command, if specified. The initial system default after RACF initialization is 30 days.

If INTERVAL is specified (on the PASSWORD command) without a change-interval value, the installation-specified maximum is used.

To specify the INTERVAL operand with the USER keyword, you must have the SPECIAL attribute or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

This operand is ignored if the interval is specified incorrectly.

NOINTERVAL

sets a password that never expires. To specify NOINTERVAL, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute. Specifying the NOINTERVAL keyword without the USER keyword defines your own password as a password that never expires. Specifying the NOINTERVAL keyword with the USER keyword sets the password to the user's default group and sets the password expired.

You can use the INTERVAL keyword at any time to reinstate an expiration interval for a password previously defined with the NOINTERVAL keyword.

USER(userid ...)

specifies one or more users whose passwords are to be reset. You may reset your own password by including your userid in the list.

Each user's current password is set to the user's respective default group name and the password is set expired. To change your own password, use the PASSWORD operand, not the USER operand. Specifying USER with your own userid resets your password to the name of your default group, and sets the password as expired.

PASSWORD Examples

Example 1

Operation: User AEH0 wants to change his password from XY262 to YZ344 and increase his change interval to 60 days.

Known: User AEH0 is RACF-defined.

The maximum installation change-interval is at least 60 days.

Command: PASSWORD PASSWORD(XY262 YZ344) INTERVAL(60)

Defaults: None

Example 2

Operation: User ADM1 wants to reset the passwords for users CD0 and DAF0 to the names of their default group.

Known: User ADM1 has the group-SPECIAL attribute in group PAYROLL. Group PAYROLL is the owning group of users CD0 and DAF0.

Users CD0 and DAF0 are RACF-defined.

Command: PASSWORD USER(CD0 DAF0)

Defaults: None

Example 3

Operation: User ADM1 wants to set a password that never expires for user CD2.

Known: User ADM1 has the SPECIAL attribute. User CD2 is RACF-defined.

Command: PASSWORD USER(CD2) NOINTERVAL

Defaults: None

PERMIT Command

Use the PERMIT command to:

- Give authority to access a discrete or generic resource profile to specific RACF-defined users or groups.

- Remove authority to access a discrete or generic resource profile from specific users or groups.

- Change the level of access authority to a discrete or generic resource profile for specific users or groups.

- Copy the list of authorized users from one discrete or generic resource profile to another profile of either type and modify the new list as you require.

- Delete an existing access list.

RACF Requirements

To perform any of the PERMIT functions, you must have sufficient authority over the resource. The following checks are made until one of the conditions is met:

1. You have the SPECIAL attribute.

2. The profile is within the scope of a group in which you have the group-SPECIAL attribute.

3. You are the owner of the resource.

4. If the resource belongs to the DATASET class, the first-level qualifier of the profile name (or the qualifier supplied by the naming conventions routine or a command installation exit) is your userid.

For discrete profiles only:

5. You are on the access list for the resource and you have ALTER authority. (If you have any other level of authority, you may not use the command for this resource.)

6. Your current connect group is on the access list and has ALTER authority. (If your group has any other level of authority, you may not use the command for this resource.)

7. The universal access authority is ALTER.

When copying the list of authorized users from one resource profile to another, you must have sufficient authority, as described in the preceding list, for both of the resources.

```
{PERMIT}        profile-name-1
{PE    }
                [CLASS(profile-name-1-class)]

                [VOLUME(volume-serial)]

                [GENERIC]

                [ID(name ...)]

                [ACCESS(access-authority)]
                [DELETE                  ]

                [RESET]

                [FROM(profile-name-2)]

                [FCLASS(profile-name-2-class)]

                [FVOLUME(volume-serial)]

                [FGENERIC]
```

profile-name-1

specifies the name of an existing discrete or generic profile whose access list you want to modify. If the name specified is a tape volume serial number that is a member of a tape volume set, the authorization assigned by this command will apply to all the volumes in the volume set.

Only one profile may be specified.

If the profile does not belong to the DATASET class, the CLASS operand must also be specified.

This operand is required and must be the first operand following PERMIT.

CLASS(profile-name-1-class)

specifies the name of the class to which resource-1 belongs. The valid class names are DATASET and those classes defined in the class descriptor table. If this operand is omitted, the default value is DATASET.

VOLUME(volume-serial)

specifies the volume on which the non-VSAM DASD data set or the catalog for the VSAM data set resides.

If this operand is specified and the volume-serial does not appear in the profile for the data set, the command is failed.

If the data set name appears more than once in the RACF data set and this operand is not specified, the command is failed.

This operand is valid only for CLASS(DATASET), and is ignored for all other CLASS values.

If a generic profile is specified, this operand is ignored.

GENERIC

specifies that RACF is to treat profile-name-1 as a generic name, even if it does not contain any generic characters.

ID(name ...)

specifies userid(s) and/or group name(s) for RACF-defined users or groups whose authorization to access the resource is to be given, removed, or changed. If this operand is omitted, the ACCESS and DELETE keywords are ignored.

ACCESS(access-authority)

specifies the access authority you want to associate with the names given in the ID operand. The valid access authorities are: NONE, READ, UPDATE, CONTROL, and ALTER. If you specify the ACCESS keyword and omit the access authority, the default value of READ is used.

Note: For non-VSAM DASD data sets, DASD volumes, and tape volumes, CONTROL authority implies UPDATE authority. For terminals, IMS/VS transactions (TIMS), IMS/VS transaction groups (GIMS), and applications (APPL), IMS/VS applications (AIMS), CICS/VS transactions (TCICSTRN), CICS/VS transaction groups (GCICSTRN), CICS/VS program specification blocks (PCICSPSB), and CICS/VS PSB groups (QCICSPSB) listed in the class descriptor table, CONTROL and UPDATE authority imply READ authority.

If you use the ID operand and omit the ACCESS and DELETE operand, the default value is ACCESS(READ).

DELETE

specifies that you are removing the names mentioned in the ID operand from the access list for the resource.

If you use the ID operand and omit the ACCESS and DELETE operand, the default value is ACCESS(READ).

RESET

specifies that RACF is to delete the entire current access authority list from the profile. If you specify RESET with ID and ACCESS, RACF deletes the current access authority list from the profile before it adds the new names to the list. If you specify RESET with ID and DELETE, RACF ignores the RESET operand and deletes the specific IDs.

Note: If you specify RESET without an ID, the resulting access list will be empty. This means that, for a general resource or a group data set profile, you must be the owner, have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute in order to update the access list again.

FROM(profile-name-2)

specifies the name of the existing discrete or generic profile whose access list you want to copy to the access list for profile-1. If the FCLASS operand is not specified, the name is assumed to be the name of a resource in the same class as profile-1.

The access list for profile-1 is modified as follows:

- Authorizations for profile-2 are added to the access list for profile-1.
- If a group or user is authorized to both resources, the authority for profile-1 is kept.
- If a group or user is authorized via the ID operand and is also authorized to profile-2, the authority in the ID operand is used.

Profile-name-2 may be the name of either a discrete or a generic profile.

To use this operand you must have sufficient authority for both of the resources (see RACF Requirements).

FCLASS(profile-name-2-class)

specifies the name of the class to which profile-2 belongs. The valid class names are DATASET and those classes defined in the class descriptor table. If this operand is omitted, the class specified (or defaulted to) on the CLASS operand is assumed. This operand is valid only if the FROM operand is also specified.

FVOLUME(volume-serial)

specifies the volume for the FROM data set on which the non-VSAM DASD data set or the catalog for the VSAM data set resides.

If this operand is specified and a data set is not defined to RACF on that volume-serial, the command is failed.

If the data set name appears more than once in the RACF data set and this operand is not specified, the command is failed. This operand is valid only for FCLASS(DATASET), when a discrete profile has been specified in profile-2 and is ignored for all other FCLASS values.

FGENERIC

specifies that profile-name-2 is to be treated as a generic name, even if it does not contain any generic characters.

PERMIT Examples

Example 1

Operation: User WJE10 wants to give UPDATE access authority to data set WJE10.DEPT2.DATA to all the users in the group RESEARCH. Data set WJE10.DEPT2.DATA is protected by a discrete profile.

Known: User WJE10 and group RESEARCH are RACF-defined.

Data set WJE10.DEPT2.DATA is RACF-defined.

Command: PERMIT 'WJE10.DEPT2.DATA' ID(RESEARCH) ACCESS(UPDATE)

Defaults: CLASS(DATASET) DISCRETE

Example 2

Operation: User WRH0 wants to give all users authorized to access the data set RESEARCH.PROJ01.DATA on volume DASD22 the authority to access RESEARCH.PROJ01.DATA on volume DASD11. User WRH0 also wants to give user AEH10 READ authority to RESEARCH.PROJ01.DATA.

Known: User WRH0 has ALTER access to both RESEARCH.PROJ01.DATA data sets. Both data sets are protected by discrete profiles.

Command: PERMIT 'RESEARCH.PROJ01.DATA' ID(AEH10) FROM('RESEARCH.PROJ01.DATA') VOLUME(DASD11) FVOLUME(DASD22)

Defaults: ACCESS(READ) CLASS(DATASET) FCLASS(DATASET)

Example 3

Operation: User RVD2 wants to delete user HAE34's access to tape volume TAP2X.

Known: User RVD2 is the owner of the profile for tape volume TAP2X.

Command: PERMIT TAP2X CLASS(TAPEVOL) ID(HAE34) DELETE

Defaults: None

Example 4

Operation: User ADM1 wants to copy the access list from the generic profile SALES.*.ABC to the discrete profile protecting the data set SALES.EUROPE.ABC

Known: User ADM1 has the SPECIAL attribute. SALES.EUROPE.ABC is in the DATASET class.

Command: PERMIT 'SALES.EUROPE.ABC' FROM ('SALES.*.ABC')

Defaults: CLASS (DATASET),FCLASS(DATASET)

RALTER Command

Use the RALTER command to:

- Alter the profile for one or more resources belonging to classes defined in the class descriptor table
- Maintain the global access checking table

RACF Requirements

To alter the profile for a resource belonging to a class defined in the class descriptor table, you must have sufficient authority over the resource. The following checks (1 through 7) are made until one of the conditions is met. Check 7 is made for the GLOBALAUDIT operand.

1. You have the SPECIAL attribute.
2. The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.
3. You are the owner of the profile.

For discrete profiles only:

4. You are on the access list for the resource and you have ALTER authority. If you have any other level of authority, you may not use the command for this resource.
5. Your current connect group is on the access list and has ALTER authority. If your group has any other level of authority, you may not use the command for this resource.
6. The universal access authority for the resource is ALTER.

For both discrete and generic profiles:

7. You have the AUDITOR attribute or the profile is within the scope of a group in which you have group-AUDITOR attribute.

The following operands have restrictions noted with the description of each operand:

ADDVOL
ADDMEM
DELMEM
GLOBALAUDIT

```
{RALTER}        class-name
{RALT  }
                (profile-name ... )

                [OWNER(userid or group-name)]

                [UACC(access authority)]

                [        ( ( NONE                                   )     ) ]
                [        ( ( ALL      )                             )     ) ]
                [ AUDIT( ( ( SUCCESS  )  [(audit-access-level)]     ) ... ) ) ]
                [        ( ( FAILURES )                             )     ) ]

                [              ( ( NONE                                    )     ) ]
                [              ( ( ALL                                     )     ) ]
                [ GLOBALAUDIT( ( ( SUCCESS     [(audit-access-level)]      ) ... ) ) ]
                [              ( ( FAILURES                                )     ) ]

                [LEVEL(nn)]

                [ADDVOL(volume-serial ... )]
                [DELVOL(volume-serial ... )]

                [ADDMEM(member ... )]
                [DELMEM(member ... )]

                [DATA('installation-defined-data')]
                [NODATA                           ]

                [APPLDATA('application-data')]
                [NOAPPLDATA                  ]

                [WARNING  ]
                [NOWARNING]
```

class-name

specifies the name of the class to which the resource belongs. The valid class names are those specified in the class descriptor table.

This operand is required and must be the first operand following RALTER.

(profile-name ...)

specifies the name of an existing discrete or generic profile to be changed in the specified class. The class descriptor table (CDT) is used to determine the syntax of resource names within the class and whether the resource is a group.

If you specify more than one resource-name, the list of names must be enclosed in parentheses.

If the resource specified is a tape volume serial number that is a member of a tape volume set, the definitions of all the volumes in the set will be changed.

Only a single volume serial number can be specified in this operand if you also specify the ADDVOL or DELVOL operand in this command.

If class-name is specified as GLOBAL, profile-names must either be DATASET or a valid class name (other than a group name) as specified in the CDT. If the class-name is specified as GLOBAL and the ADDMEM or DELMEM operand is specified, only one profile-name can be specified.

This operand is required and must be the second operand following RALTER.

If the class-name specified is a resource group class, the profile-name specified cannot be generic.

Note: Each resource specified in this operand will be processed independently, and all options specified in this command will apply to each named resource. If an error occurs while processing a resource, a message will be issued and processing will continue with the next resource.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the new owner of the resource being altered.

To change the owner of a resource, you must be the current owner of the resource, or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Note: The user specified as the owner does not automatically have access to the resource. Use the PERMIT command to add the owner to the access list as desired.

UACC(access-authority)

specifies the universal access authority to be associated with this resource. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE.

Note: For tape volumes and DASD volumes, CONTROL authority implies UPDATE authority. For terminals, IMS/VS transactions (TIMS), IMS/VS transaction groups (GIMS) and applications (APPL), CONTROL and UPDATE authority imply READ authority.

AUDIT

specifies which access attempts you want to log on the SMF data set. The following options are available:

ALL

specifies that you want to log both authorized accesses and detected unauthorized attempts to access the resource.

SUCCESS

specifies that you want to log authorized accesses to the resource.

FAILURES

specifies that you want to log detected unauthorized attempts to access the resource.

NONE

specifies that you do not want any logging to be done for accesses to the resource.

audit-access-level

specifies which access level(s) you want to log on the SMF data set. The levels are:

READ

logs access attempts at any level. This is the default value if no access level is specified.

UPDATE

logs access attempts at the UPDATE, CONTROL, and ALTER levels.

CONTROL

logs access attempts at the CONTROL and ALTER levels.

ALTER

logs ALTER access-level attempts only.

GLOBALAUDIT

specifies which access attempts the user who has the AUDITOR attribute wants to log on the SMF data set. The options ALL, SUCCESS, FAILURES, and NONE, and the audit-access-level values are the same as described under the AUDIT keyword.

To use the GLOBALAUDIT keyword, you must have the AUDITOR attribute or the resource profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Note: Regardless of the value specified in the GLOBALAUDIT keyword, all access attempts specified on the AUDIT keyword will always be logged.

LEVEL(nn)

specifies a level indicator, where nn is an integer between 00 and 99. The meaning of the value is assigned by your installation. It is available to RACF post-processing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs. It is included on all records that log resource accesses and is listed by the RLIST command.

ADDVOL(volume-serial ...)

specifies the tape volume serial numbers to be added to the tape volume set represented by the resource-name identified in the second required operand of this command. Only a single volume serial number can be specified as the resource-name when the ADDVOL operand is also specified in the command. The resource-name may by any of the volumes currently defined to the volume set.

To use the ADDVOL operand, you must have the SPECIAL attribute, or you must have the CLAUTH attribute for the TAPEVOL resource class, in addition to the other RACF requirements for using the RALTER command.

If a generic profile is specified, this operand is ignored.

Note: The ADDVOL operand is only valid for the TAPEVOL resource class.

DELVOL(volume-serial ...)

specifies the tape volume serial numbers to be deleted from the tape volume set represented by the resource-name identified in the second required operand of this command. Only a single volume can be specified as the resource-name when the DELVOL operand is also specified in the command. The resource-name may be any of the volumes currently defined to the volume set except one of the volumes to be deleted; if the resource-name is included on the DELVOL operand, it will be ignored.

If a generic profile is specified, this operand is ignored.

Note: The DELVOL operand is only valid for the TAPEVOL resource class.

ADDMEM(member...)

specifies the resource names that are to be added to the members of the resource group indicated by the profile-name operand.

To use the ADDMEM operand, you must have ALTER authority, be the owner of the member resource, or the member resource must be within the scope of a group in which you have the group-SPECIAL attribute. To add a resource that is not defined to RACF, you must be authorized to define resources in the member class (via the CLAUTH operand of the ADDUSER or ALTUSER command).

To use the ADDMEM operand if class-name is specified as GLOBAL and profile-name is specified as DATASET, you must either have the SPECIAL attribute, the member must be within the scope of a group in which you the group-SPECIAL attribute, or the high-level qualifier of the member name must be your user ID.

If class-name is specified as GLOBAL, "member" specifies the name of an entry in the global access checking table followed by the access level to be permitted, in the following format:

```
entry-name [ /  ( READ    )      ]
                ) UPDATE  (
               <  CONTROL  >
                ) ALTER   (
                ( NONE    )
```

If profile-name is specified as DATASET, entry-name can include an asterisk (*) as any qualifier (including the first level). The asterisk stands for any qualifier in the corresponding position. In the last position, an asterisk stands for any number of qualifiers. Entry-name can also include the percent sign (%) in any position and the percent sign can substitute for any character in the corresponding position. In addition, one or more qualifiers in the entry-name can consist of the keyword "&RACUID," which represents the current user id or "&RACGPID" which represents your current connect group.

If profile-name is not specified as DATASET, entry-name can include an asterisk as the last character, standing for any number of trailing characters.

DELMEM(member...)

specifies the resource names that are to be deleted from the resource group indicated by the profile-name operand. This operand is ignored if the class name specified is not a resource group class.

If class-name is specified as GLOBAL, the rules for "member" are the same as given for ADDMEM.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the profile for the resource. The data must be enclosed in apostrophes.

This information is listed by the RLIST command. It is also available to RACF post-processing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs.

NODATA

specifies that the RALTER command is to delete the installation-defined data in the resource profile.

APPLDATA('application-data')

specifies a text string that will be associated with each of the named resources. The text string is entered between apostrophes and a maximum of 255 characters is allowed.

For the TIMS and GIMS class, to force the user to reenter his password whenever the transaction or transactions listed in the profile-name or ADDMEM operands are used, specify application-data as REVERIFY.

This information, if present, can be displayed with the RLIST command and will be included in the resident profile generated by RACLIST.

NOAPPLDATA

specifies that the RALTER command is to delete the text string that was present in the profile associated with the resource.

WARNING

specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

NOWARNING

specifies that, if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

RALTER Examples

Example 1

Operation: User TRA02 wants to change the owner and universal access for terminal TERMID01.

Known: User TRA02 has the SPECIAL attribute.

Terminal TERMID01 is defined to RACF.

Command: RALTER TERMINAL TERMID01 OWNER(TRA02) UACC(ALTER)

Defaults: None

Example 2

Operation: User RFF22 wants to add volume TAP02 to the tape volume set, change the level of the tape volume set, and change the AUDIT and GLOBALAUDIT logging options.

Known: User RFF22 is the owner of the tape volume set.

User RFF22 has the AUDITOR attribute.

TAP01 is a volume of the tape volume set.

Command: RALTER TAPEVOL TAP01 AUDIT(SUCCESS(READ)) LEVEL(22) GLOBALAUDIT(SUCCESS(UPDATE)FAILURES(READ)) ADDVOL(TAP02)

Defaults: None

Example 3

Operation: User RFF23 wants to delete the two data fields associated with the terminal T3E8.

Known: User RFF23 is the owner of the T3E8 terminal entry.

Command: RALTER TERMINAL T3E8 NODATA NOAPPLDATA

Defaults: None

Example 4

Operation: User ADM1 wants to delete the data fields associated with the generic profile * in the TERMINAL class.

Known: User ADM1 has the SPECIAL attribute.

Command: RALTER TERMINAL * NODATA NOAPPLDATA

Defaults: None

RDEFINE Command

Use the RDEFINE command to define to RACF all resources belonging to classes specified in the class descriptor table.

Also, use the RDEFINE command to create entries in the global access checking table.

The command adds a profile for the resource to the RACF data set in order to authorize access to the resource.

Your userid is placed on the access list and you are given ALTER authority for the resource.

RACF Requirements

To use the RDEFINE command, you must have the SPECIAL attribute or be authorized as follows:

- If the resource to be defined is not already defined to RACF as a member of a resource group, you must be authorized to define resources for the specified class. This can be accomplished with the ADDUSER or ALTUSER command by specifying the CLAUTH operand.

- If the resource to be defined is a discrete name already defined to RACF as a member of a resource group, you can define it as a resource to RACF if you have ALTER authority, or if the resource group profile is within the scope of a group in which you have the group-SPECIAL attribute, or if you are the owner of the resource group profile. If authority conflicts arise because the resource is a member of more than one group and the user's authority in those groups differs, RACF resolves the conflict by using the least restrictive authority (unless modified by the installation).

- To use the ADDMEM operand, you must have ALTER authority, or be the owner of the member resource, or the member resource must be within the scope of a group in which you have the group-SPECIAL attribute. To add a resource that is not defined to RACF, you must be authorized to define resources in the member class (via the CLAUTH operand of the ADDUSER or ALTUSER command).

- To use the ADDMEM operand if class-name is specified as GLOBAL and profile-name is specified as DATASET, you must either have the SPECIAL attribute, or the member must be within the scope of a group in which you the group-SPECIAL attribute, or the high-level qualifier of the member name must be your user ID.

- If you have CLAUTH authority to the GLOBAL resource group within the scope of the same group in which you also have the group-SPECIAL attribute, you may add global resources where the high-level qualifier is the group name or a userid owned by the group.

```
{RDEFINE}      class-name
{RDEF   }
               (profile-name ... )

               [OWNER (userid or group-name)]

               [UACC(access-authority)]

               [          {  NONE                                          }   ]
               [          {{ ALL     }                                     }   ]
               [  AUDIT(  {{ SUCCESS }  [(audit-access-level)] } ... {  )  ]
               [          {{ FAILURES}                                     }   ]

               [LEVEL(nn)]

               [ADDMEM(member ... )]

               [DATA('installation-defined-data')]

               [APPLDATA('application-data')]

               [WARNING]
```

class-name

specifies the name of the class to which the resource belongs. The valid class names are those specified in the class descriptor table.

This operand is required and must be the first operand following RDEFINE.

profile-name

specifies the name of the discrete or generic profile to be associated with the class being defined. The class descriptor table (CDT) is used to determine if a class is defined to RACF, the syntax of resource names within the class, and whether the resource is a group.

If class-name is specified as global, profile-names must either be DATASET or a valid class name (other than a group name) as specified in the CDT. If the class-name is specified as GLOBAL and the ADDMEM or DELMEM operand is specified, only one profile name can be specified.

If you specify more than one profile name, the list of names must be enclosed in parentheses.

If class-name is a resource group name, a generic profile-name cannot be specified.

This operand is required and must be the second operand following RDEFINE.

Note: Each resource specified in this operand will be processed independently, and all options specified in this command will apply to each named resource. If an error occurs while processing a resource, a message will be issued and processing will continue with the next resource.

OWNER(userid or group-name)

specifies a RACF-defined user or group to be assigned as the owner of the resource being defined. If this operand is omitted, you are defined as the owner.

Note: The user specified as the owner does not automatically have access to the resource. Use the PERMIT command to add the owner to the access list as desired.

UACC(access-authority)

specifies the universal access authority to be associated with this resource. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. If UACC is not specified or if the UACC keyword is entered with no access authority, your default value in your current connect group is used.

Note: For tape volumes and DASD volumes, CONTROL authority implies UPDATE authority. For terminals, IMS/VS transactions (TIMS), IMS/VS transaction groups (GIMS), IMS/VS applications (AIMS), CICS/VS transactions (TCICSTRN), CICS/VS transaction groups (GCICSTRN), CICS/VS program specification blocks (PCICSPSB), and CICS/VS PSB groups (QCICSPSB) listed in the class descriptor table, and applications (APPL), CONTROL and UPDATE authority imply READ authority.

AUDIT

specifies which access attempts you want to log on the SMF data set. The following options are available:

ALL

indicates that you want to log both authorized accesses and detected unauthorized access attempts.

SUCCESS

indicates that you want to log authorized accesses to the resource.

FAILURES

indicates that you want to log detected unauthorized access attempts.

NONE

indicates that you do not want any logging to be done.

Note: If you specify TERMINAL as the class-name, the AUDIT operand does not apply because successful accesses to terminals are not logged on the SMF data set.

audit-access-level

specifies which access level(s) you want to log on the SMF data set. The levels are:

READ

logs access attempts at any level. This is the default value if no access level is specified.

UPDATE

logs access attempts at the UPDATE, CONTROL, and ALTER levels.

CONTROL

logs access attempts at the CONTROL and ALTER levels.

ALTER

logs ALTER access-level attempts only.

FAILURES(READ) is the default value if the AUDIT operand is omitted from the command.

LEVEL(nn)

specifies a level indicator, where nn is an integer between 0 and 99. The default is 0.

The meaning of the value is assigned by your installation. It is available to RACF post-processing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs. It is included on all records that log resource accesses and is listed by the RLIST command.

ADDMEM(member...)

specifies the resource names which are to be added to the members of the resource group indicated by "(resource-name...)."

The member resources may be RACF-protected, but need not be. If the member resource is RACF-protected, the command issuer must have ALTER authority to the member; if the member resource is not RACF-protected, the command issuer must have authority to define resources in the member resource class. This operand is ignored if the class name specified is not a resource group class.

If class-name is specified as GLOBAL, "member" specifies the name of an entry in the global access checking table followed by the access level to be permitted, in the following format:

```
entry-name   [/  ( READ     )  ]
                 ( UPDATE   )
                 { CONTROL  }
                 ( ALTER    )
                 ( NONE     )
```

If profile-name is specified as DATASET, entry-name can include an asterisk as any qualifier (including the first level). The asterisk stands for any qualifier in the corresponding position. In the last position, an asterisk stands for any number of qualifiers. Entry-name can also include the percent sign (%) in any position and the percent sign can substitute for any character in the corresponding position. In addition, one or more qualifiers in the entry-name can consist of the keyword "&RACUID," which represents the accessing user's user id, or "&RACGPID" which represents the accessing user's current connect group.

If profile-name is not specified as DATASET, entry-name can include an asterisk as the last character, standing for any number of trailing characters.

DATA('installation-defined-data')

specifies up to 255 characters of installation-defined data to be kept in the profile for the resource. The data must be enclosed in apostrophes.

This information is listed by the RLIST command. It is also available to RACF post-processing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs.

APPLDATA('application-data')

This parameter specifies a text string that will be associated with each of the named resources. The text string is entered between apostrophes and cannot exceed 255 characters.

For the TIMS and GIMS class, to force the user to reenter his password whenever the transaction or transactions listed in the profile-name or ADDMEM operands are used, specify application-data as REVERIFY.

This information, if present, can be displayed with the RLIST command and will be included in the resident profile generated by RACLIST.

WARNING

specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

RDEFINE Examples

Example 1

Operation: User TBK20 wants to define resource GIMS600 in class GIMS which is a resource group class. He also wants to define TIMS200, TIMS111, TIMS300, and TIMS333 as members of the resource group (GIMS600).

Known: User has the CLAUTH attribute for the GIMS and TIMS classes. GIMS is a resource group class and TIMS is its associated resource member class. TIMS200 and TIMS111 are members of another resource group. The user has ALTER authority to the other resource group.

Command: RDEFINE GIMS GIMS600 ADDMEM(TIMS200 TIMS111 TIMS300 TIMS333)

Defaults: OWNER (TBK20) LEVEL(0) AUDIT(FAILURES(READ)) UACC(NONE)

Example 2

Operation: User ADM1 wants to define a generic profile for all resources starting with a 'T' belonging to the TIMS class, and to require that users must reenter their passwords whenever they enter any IMS transaction starting with a T.

Known: User ADM1 has the SPECIAL attribute.

Command: RDEFINE TIMS T* APPL('REVERIFY')

Defaults: UACC(NONE) OWNER(ADM1) LEVEL(0) AUDIT(FAILURES(READ))

RDELETE Command

Use the RDELETE command to delete RACF resources belonging to classes specified in the class descriptor table.

This command removes the profile for the resource from the RACF data set.

RACF Requirements

To remove RACF protection from a resource class specified in the class descriptor table, you must have sufficient authority over the resource. The following checks are made until one of the conditions is met:

1. You have the SPECIAL attribute.

2. The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.

3. You are the owner of the resource.

For discrete profiles only:

4. You are on the access list for the resource and you have ALTER authority. (If you have any other level of authority, you may not use the command for this resource.)

5. Your current connect group is on the access list and has ALTER authority. (If your group has any other level of authority, you may not use the command for this resource.)

6. The universal access authority for the resource is ALTER.

```
{RDELETE}         class-name
{RDEL   }
                  (profile-name ... )
```

class-name

specifies the name of the class to which the resource belongs. Valid class names are those specified in the class descriptor table.

This operand is required and must be the first operand following RDELETE.

(profile-name...)

specifies the name of the existing discrete or generic profile to be deleted from the specified class. The profiles for these resources will be deleted from the RACF data set. The class descriptor table (CDT) is used to determine if a class is defined to RACF, the syntax of resource names within the class, and whether the resource is a group.

If you specify more than one profile-name, the list of names must be enclosed in parentheses.

If you specify class-name as a resource group class, you cannot specify a generic profile.

If the resource specified is a tape volume serial number that is a member of a tape volume set, the definitions of all the volumes in the set will be deleted.

This operand is required and must be the second operand following RDELETE.

Note: Each resource specified in this operand will be processed independently. If an error occurs while processing a resource, a message will be issued and processing will continue with the next resource.

RDELETE Examples

Example 1

Operation: User JHT01 wants to remove RACF protection from the tape volume set VOL001.

Known: User JHT01 has the SPECIAL attribute.

Command: RDELETE TAPEVOL VOL001

Defaults: None

Example 2

Operation: User ADM1 wants to remove the generic profile T* from the TIMS class.

Known: User ADM1 has the SPECIAL attribute.

Command: RDELETE TIMS T*

Defaults: None

REMOVE Command

Use the REMOVE command to remove a user from a group and to assign a new owner to any group data set profiles the user owns on behalf of that group.

RACF Requirements

To use the REMOVE command:

- you must have the SPECIAL attribute, or
- the group profile must be within the scope of a group in which you have the group-SPECIAL attribute, or
- you must be the owner of the group, or
- you must have JOIN or CONNECT authority in the group.

Note: Ownership of the user's profile is not sufficient authority to remove the user from a group.

```
{REMOVE}        (userid ... )
{RE    }
                [GROUP(group-name)]

                [OWNER (userid or group-name)]
```

userid

specifies the user you want to remove from the group. If you are removing more than one user from the group, the userids must be enclosed in parentheses.

This operand is required and must be the first operand following REMOVE.

GROUP(group-name)

specifies the group from which the user is to be removed. If this operand is omitted, the default is your current connect group. The group cannot be the user's default group.

OWNER(userid or group-name)

specifies a RACF-defined user or group who will own the group data set profiles now owned by the user to be removed.

If this operand is omitted and group data set profiles exist that require a new owner, the user will not be removed from the group. (Group data set profiles are data set profiles whose names are qualified by the group name or begin with the value supplied by an installation exit.)

The new owner of the group data set profiles must have at least USE authority in the specified group. Do not specify a user who is being removed from the group as the new data set profile owner.

REMOVE Examples

Example 1

Operation: User WJE10 wants to remove users AFG5 and GMD2 from group PAYROLL.

Known: User WJE10 has JOIN authority to group PAYROLL.

User WJE10 is logged on to group PAYROLL.

Users AFG5 and GMD2 are connected to group PAYROLL but do not own any group data set profiles and group PAYROLL is not their default group.

Command: REMOVE (AFG5 GMD2)

Defaults: GROUP(PAYROLL)

Example 2

Operation: User WRH0 wants to remove user PDJ6 from group RESEARCH, assigning user DAF0 as the new owner of PDJ6's group data set profiles

Known: User WRH0 has CONNECT authority to group RESEARCH.

User WRH0 is not logged on to group RESEARCH.

User PDJ6 is connected to group RESEARCH and owns group data set profiles (PDJ6's default connect group is not RESEARCH).

User DAF0 is connected to group RESEARCH with USE authority.

Command: REMOVE PDJ6 GROUP(RESEARCH) OWNER(DAF0)

Defaults: None

RLIST Command

Use the RLIST command to display information on resources belonging to classes specified in the class descriptor table.

The class descriptor table is used to determine if a class is defined to RACF, the syntax of resource names within the class, and whether the resource is a group.

Profiles are listed in alphabetical order. Generic profiles are listed in the same order as they are searched for a resource match. (This also applies to the names in the global access table.)

This command lists the information in an existing profile for the resource or resource group.

The details that are given for each profile are:

- The resource class.

- The name of the resource.

- The cross-reference class name (that is, the member class name for resource groups or the group name for non-group resources).

- If the resource named in the command (in the resource-name operand) is a resource group, member resources are listed.

- For non-group resources, the names of all resource groups of which the entity is a member are listed.

- The volumes in a tape volume set (for TAPEVOL class only).

- The level of the resource.

- The owner of the resource.

- The type of access attempts (as specified by the AUDIT operand on the RDEFINE or RALTER command) that are being logged on the SMF data set (for auditors only).

- The universal access authority for the resource.

- Your level of access authority for the resource.

- The installation-defined data.

- The APPLDATA value, if any, is also listed in the output.

- The type of access attempts (as specified by the GLOBALAUDIT operand on the RALTER command) that are being logged on the SMF data set.

- The information specified in the DATA keyword of the RALTER and/or RDEFINE commands.

- The status of the WARNING/NOWARNING indicator.

You may request additional details as follows:

- The number of times the resource was accessed by all users for each of the following access authorities:

  ALTER, CONTROL, UPDATE, READ (See Note)

- Historical data:

  - date the resource was defined to RACF

  - date the resource was last referenced (See Note)

  - date the resource was last accessed at the update level (for DASDVOL and TAPEVOL classes only). (See Note)

- A list of:

  - all users and groups authorized to access the resource,
  - the level of authority for each user and group, and
  - the number of times each user has accessed the resource. (See Note)

Note: These details are not meaningful if resource statistics gathering is being bypassed at your installation.

RACF Requirements

You must have a sufficient level of authority for each resource or resource group listed as the result of your request. The following checks are made for each resource until one of the conditions is met:

1. You have the SPECIAL attribute.

2. The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.

3. You are the owner of the resource.

For discrete profiles only:

4. You are on the access list for the resource and you have at least READ authority. (If your level of authority is NONE, the resource is not listed.)

5. Your current connect group is on the access list and has at least READ authority. (If the group's level of authority is NONE, the resource is not listed.)

6. The universal access authority of the resource is at least READ.

For both generic and discrete profiles:

7. You have the AUDITOR attribute.

8. The resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

You will see the type of access attempts, as specified by the GLOBALAUDIT operand, only if you have the AUDITOR attribute or the resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

When requesting to see the access list for a resource with the AUTHUSER operand, your level of authority is checked for each resource until one of the conditions is met:

1. You have the SPECIAL attribute.

2. The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.

3. You are the owner of the resource.

4. You have the AUDITOR attribute.

5. The resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

For discrete profiles only:

6. You are on the access list for the resource and you have ALTER authority. (If you have any other level of authority, you may not use the operand.)

7. Your current connect group is on the access list and has ALTER authority. (If your group has any other level of authority, you may not use the operand.)

8. The universal access authority of the resource is ALTER.

```
{RLIST}         class-name
{RL   }
                [ (profile-name ... ) ]
                [ *                   ]

                [GENERIC  ]
                [NOGENERIC]

                [STATISTICS]

                [HISTORY]

                [AUTHUSER]

                [RESGROUP]

                [ALL]
```

class-name

specifies the name of the class to which the resource belongs. Valid class names are those specified in the class descriptor table.

This operand is required and must be the first operand following RLIST.

Note that if you specify a class that allows resource names to contain any character (ICHERCDE with OTHER=ANY), then resources in the DATASET class that begin with the same first 4 characters as this class name will also be listed.

(profile-name...)

specifies the name of an existing discrete or generic profile about which information is to be displayed.

If you specify more than one profile-name, the list of names must be enclosed in parentheses.

If the resource specified is a tape volume serial number that is a member of a tape volume set, information on all the volumes in the set will be displayed.

This operand or * is required and must be the second operand following RLIST.

Note that each resource specified in this operand will be processed independently. If an error occurs while processing a resource, a message will be issued and processing will continue with the next resource.

*****

specifies that you want to display information for all resources defined to the specified class for which you have the proper authority.

This operand or the profile-name operand is required and must be the second operand following RLIST.

Note that each resource will be processed independently, and information will be displayed only for those resources for which you have sufficient authority.

If you have the AUDITOR attribute or if the resource profile is within the scope of a group in which you have the group-AUDITOR attribute, GLOBALAUDIT information will be displayed for all resources in the class.

GENERIC or NOGENERIC

specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be listed. If neither operand is specified, both profile types are listed.

These operands are ignored unless generic profile command processing is enabled.

STATISTICS

specifies that you want to list the statistics for each resource. The list will contain the number of times the resource was accessed by users with READ, UPDATE, CONTROL, and ALTER authorities. A separate total is given for each authority level. (See Note)

HISTORY

specifies that you want to list the following data:

- date each profile was defined to RACF
- date each profile was last referenced (see Note)
- date each profile was last updated (see Note)

AUTHUSER

specifies that you want to see the access list for each resource. The output will show:

- all users and groups authorized to access the resource,
- the level of authority for each user and group, and
- the number of times each user has accessed the resource. (see Note)

  You must have sufficient authorization to use the AUTHUSER operand (see RACF Requirements).

RESGROUP

requests a list of all resource groups of which the resource specified by the profile-name operand is a member.

If a profile does *not* exist for the specified resource, RACF lists the names of all resource groups of which the resource is a member and to which the command user is authorized. If a profile *does* exist for the specified resource and the command user has ALTER authority to the resource, RACF lists the names of all groups of which the resource is a member.

If a profile *does* exist for the specified resource but the command user has less than ALTER authority to the resource, RACF lists the names of all groups of which the resource is a member and to which the command user is authorized (SPECIAL attribute, profile owner, or at least READ authority).

ALL

specifies that you want all information for each resource displayed at your terminal. The access list is not included unless you have sufficient authority to use the AUTHUSER operand (see RACF Requirements). The type of access attempts (as specified by the GLOBALAUDIT operand) that are being logged on the SMF data set is not included unless you have the AUDITOR attribute or the resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

Note: These details are not meaningful if resource statistics gathering is being bypassed at your installation.

RLIST Examples

Example 1

Operation: User RV2 wants to list all information about the DASD volume VOL001.

Known: User RV2 is the owner of DASD volume VOL001.

User RV2 has the AUDITOR attribute.

Command: RLIST DASDVOL VOL001 ALL

Defaults: None

Output: See Figure 10.

Example 2

Operation: User ADM1 wants to list all information about the generic profile T* in the TIMS class.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Command: RLIST TIMS T* ALL

Defaults: None

Output: See Figure 11.

```
RLIST DASDVOL VOL001 ALL
CLASS      NAME
-----      ----
DASDVOL    VOL001

LEVEL  OWNER     UNIVERSAL ACCESS  YOUR ACCESS    WARNING
-----  -----     ----------------  ---- ------    -------
 00    RV2            READ            ALTER         NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

AUDITING
--------
SUCCESS(READ),FAILURES(UPDATE)

GLOBALAUDIT
-----------
ALL(CONTROL)

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)     (DAY) (YEAR)
-------------  -------------------  ----------------
  146    82          146    82        146    82

ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
-----------   -------------   ------------   ----------
  000000         000000          000000         000000

USER      ACCESS   ACCESS COUNT
----      ------   ------------
RV2       ALTER       000000
ESH25     READ        000000
```

Figure 10. Example 1 Output for RLIST Command

```
RLIST TIMS T* ALL
CLASS      NAME
-----      ----
TIMS       T* (G)

GROUP   CLASS   NAME
-----   -----   ----
GIMS

RESOURCE GROUPS
-------- ------
NONE

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS    WARNING
-----  -------    ----------------  ---- ------    -------
 00    ADM1            NONE            ALTER         NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
REVERIFY


GLOBALAUDIT
-----------
SUCCESS(UPDATE),FAILURES(READ)

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
-------------  -------------------  ----------------
  146    82          146    82          146    82

ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
-----------   -------------   ------------   ----------
  000000         000000          000000         000000

USER      ACCESS   ACCESS COUNT
----      ------   ------ -----
ADM1      ALTER       000000
READY
```

Figure 11. Example 2 Output for RLIST Command

RVARY Command

Use the RVARY command to:

- Deactivate and reactivate the RACF function when only one RACF data set is in use.
- Deactivate or reactivate primary or backup RACF data sets. (Deactivating a specific primary data set causes all RACF requests for access to that data set to fail. Deactivating a specific backup data set causes RACF to stop duplicating information on that data set.)
- Switch from using a specific primary data set to using its corresponding backup data set.
- Deactivate protection for any resources belonging to classes defined in the CDT while RACF is inactive.

While RACF is deactivated, utilities may be run to diagnose and repair logical errors in the RACF data set. RACF installation exits can provide special handling for requests to access RACF-protected resources (for example, by prompting the operator to allow or deny access). If the RACF data set is itself RACF-protected, the RACHECK installation exit must specifically allow the utilities to access the data set while the RACF function is inactive.

Note: While RACF is deactivated, users can still log onto TSO but RACF does not perform any functions.

All issuances of the RVARY command are logged in the SMF data set (provided that RACF is not permanently inactive, PARSE processing was completed successfully, and RACF is not already in the requested state).

RACF Requirements

No special authority is needed to issue the RVARY command. However, the operator (at the master console or security console) must approve the change of RACF status to active or inactive (in response to message ICH701A) before the command is allowed to complete.

```
RVARY           ┌ ACTIVE            ┐
                │ INACTIVE(NOTAPE)  │
                └ SWITCH            ┘

                [DATASET(data-set-namelist|*)]

                [NOCLASSACT(class-namelist|*)]

                ┌ LIST   ┐
                └ NOLIST ┘
```

ACTIVE
: specifies that the RACF function for, and access to, the RACF data set(s) specified by the DATASET operand is to be reactivated after having been previously deactivated by the INACTIVE operand. If DATASET(*) is specified or the DATASET operand is not used, the command applies to all primary data sets.

INACTIVE

specifies that the RACF function for, and access to, the RACF data set(s) specified by the DATASET operand is to be deactivated. If DATASET(*) is specified or the DATASET operand is not used, the command applies to all primary data sets.

NOTAPE

specifies that tape volume protection for volumes with IBM standard or ANSI labels is no longer in effect. This option takes effect immediately and is valid for the current IPL or until RVARY ACTIVE is issued.

SWITCH

specifies that processing for primary RACF data sets identified by the DATASET operand is to be switched to the corresponding backup data sets. If DATASET(*) is specified or the DATASET operand is not used, the command applies to all primary data sets. No action takes place for backup data sets specified by the DATASET operand.

DATASET(data-set-namelist)

specifies a list of RACF data sets to be reactivated, deactivated, or switched, depending on the ACTIVE | INACTIVE | SWITCH operands. If DATASET(*) is specified or the operand is not used, the command applies to all primary data sets.

NOCLASSACT(class-namelist)

specifies those classes for which RACF protection is not in effect while RACF is inactive. Classnames that are specified for NOCLASSACT have no protection in effect. An * indicates that the option applies to all classes defined in the CDT. 'Class-namelist' may contain any class defined by an entry in the class descriptor table.

LIST

specifies that RACF data set status information is to be listed for all RACF data sets. If ACTIVE or INACTIVE is specified, the status shown is after the specified reactivation or deactivation has taken place. If only LIST is specified (or defaulted to) the operator is not prompted. LIST is the default.

NOLIST

specifies that status information for RACF data sets is not to be listed.

RVARY Examples

Example 1

Operation: User WJE10 wants to temporarily deactivate RACF in order to make repairs to the RACF data set. WJE10 does not want RACF tape volume protection to be enforced while RACF is inactive.

Known: The security operator has been informed by the security administrator that a change of RACF status will be requested.

Command: RVARY INACTIVE(NOTAPE) or RVARY INACTIVE NOCLASSACT(TAPEVOL)

Defaults: LIST

Example 2

Operation: User WJE10 wants to reactivate RACF.

Known: The security operator has been informed by the security administrator that a change of RACF status will be requested.

Command: RVARY

Defaults: LIST

Example 3

Operation: A primary data set (SYS1.RACF) is to be switched with its backup data set (SYS1.RACF1).

Known: The security operator has been informed by the security administrator that a change of RACF status will be requested.

Command: RVARY SWITCH DATASET(SYS1.RACF)

Defaults: LIST

SEARCH Command

Use the SEARCH command to obtain a list of RACF profiles, users, and groups.

One or more of the following can be requested:

- profile names that contain a specific character string
- profiles for resources that have not been referenced for more than a specific number of days
- profiles for data sets that reside on specific volumes (or VSAM data sets that are cataloged in VSAM catalogs on specific volumes)
- VSAM or non-VSAM data sets
- model data set profile names

The selected profile names can be:

- displayed at your terminal
- formatted with specific character strings into a series of commands or messages and retained in a CLIST data set

RACF Requirements

You must have a sufficient level of authority for each profile selected as the result of your request. The following checks are made until one of the conditions is met:

1. You have the SPECIAL attribute.
2. You have the AUDITOR attribute.
3. The profile is within the scope of a group in which you have either the group-SPECIAL or group-AUDITOR attribute.
4. You are the owner of the profile.
5. If the profile is a DASD data set, the first-level qualifier of the data set name (or the qualifier supplied by a command installation exit) is your userid.
6. You are on the access list for the resource and you have at least READ authority. (If your level of authority is NONE, the resource is not selected.)
7. Your current connect group is on the access list and has at least READ authority. (If the group's level of authority is NONE, the resource is not selected.)
8. You have the OPERATIONS attribute or the profile is within the scope of a group in which you have the group-OPERATIONS attribute, and the class is DATASET or a general resource class that specifies OPER=YES in the class descriptor table (CDT).
9. The universal access authority is at least READ.

```
{SEARCH}        [CLASS(profile-name-class)]
{SR    }
                [ MASK(char-1[char-2]) ]
                [ NOMASK               ]

                [ VOLUME                ]
                [ VOLUME(volume-serial) ]

                [AGE(number-of-days) ]

                [ LIST   ]
                [ NOLIST ]

                [CLIST[('string-1'['string-2'])]]

                [GENERIC   ]
                [NOGENERIC ]
                [VSAM      ]
                [NONVSAM   ]
                [ALL       ]
                [MODEL     ]

                 [WARNING]
```

CLASS(profile-name-class)

specifies the name of the class of profiles to be searched. The valid resource classes are DATASET, USER, GROUP, and those specified in the class descriptor table. If this operand is omitted, the default value is DATASET.

To search for another user's profile you must be the owner of the user's profile, or have the SPECIAL or AUDITOR attribute, or the profile must be within the scope of a group in which you have either the group-SPECIAL or group-AUDITOR attribute.

To list details of all RACF-defined user profiles, you must have either the SPECIAL or AUDITOR attribute.

If CLASS(TAPEVOL) is specified, all volumes that meet the search criteria will be processed independently, even if the volumes belong to a tape volume set.

Note: If you specify a class that allows profile names to contain any character (ICHERCDE with OTHER=ANY), then profiles in the DATASET class that begin with the same first 4 characters as this class name and that satisfy the other criteria you specify on this SEARCH command are also listed.

MASK(char-1[char-2])

specifies the strings of alphameric characters used to search the RACF data set. This data defines the range of profile names selected. The two character strings together must not exceed 44 characters for a DASD data set name, or, for general resource classes, the length specified in the class descriptor table.

char-1

Each profile name selected with this command starts with char-1. The string may be any length up to the maximum allowable length of the resource name. All profile names beginning with char-1 are searched.

If * is specified for char-1:

- For DATASET, your userid is used as the default value for char-1.
- For resource classes specified in the class descriptor table, char-1 is ignored and char-2 will identify the character string appearing anywhere in the resource name.

char-2

If you specify char-2, the selected profile names include only those names containing char-2 somewhere after the occurrence of char-1. This limits the list to some subset of resource names identified with char-1.

If you omit both the MASK and NOMASK operands, your userid is used as the default value for the DATASET class, whereas the entire class is searched for any resource class defined in the class descriptor table. (Note that for any resource class defined in the class descriptor table, omitting both operands is the same as NOMASK.)

NOMASK

specifies that all profiles (to which you are authorized) in the specified class will be selected.

VOLUME

specifies that you want the volume information to be displayed for each DASD data set that meets the search criteria specified by the MASK operand.

This operand is ignored if you specify GENERIC.

For non-VSAM data sets, the volume serial number displayed is the location of the data set. For VSAM data sets, the volume serial number displayed is the location of the catalog entry for the data set.

This operand is valid only for CLASS(DATASET), and is ignored for all other class values.

VOLUME(volume-serial ...)

specifies the volumes to be searched (the volume serial number(s) become part of the search criteria). Non-VSAM DASD data sets are selected if they reside on the specified volumes. VSAM data sets are selected if the catalog entries for the data sets reside on the specified volumes.

This operand is ignored if you specify GENERIC.

If the selected data set names are displayed at your terminal, the volume information is included with each data set name.

This operand is valid only for CLASS(DATASET), and is ignored for all other class values.

AGE(number-of-days)

specifies the aging factor to be used as part of the search criteria. Only resources that have not been referenced within the specified number of days are selected, unless you specify CLASS(GROUP). In this case, the SEARCH command uses the date on which the group was defined to determine the age.

You can specify up to 5 digits.

LIST

specifies that the selected data set names, volume serial numbers, or terminal names are to be displayed at your terminal. This is the default value if both LIST and NOLIST are omitted.

NOLIST

specifies that the selected data set names, volume serial numbers, or terminal names are not to be displayed at your terminal.

This operand can only be used when the CLIST operand is specified. If NOLIST is used without CLIST, the command will fail.

If you omit both the NOLIST and LIST keywords, LIST is the default value.

CLIST[('string-1'['string-2'])]

specifies that the selected profile names are to be retained in a CLIST data set. One record is put into the data set for each selected profile name.

'string-1'['string-2']

specifies strings of alphameric characters that are put into the CLIST records along with the selected profile names. Each string must be enclosed in apostrophes. In this way you can build a set of commands that are similar except for the profile name.

The format of the text portion of the CLIST record is as follows:

```
string-1'data-set name'string-2  or
string-1volume-serial-numberstring-2 or
string-1terminal-namestring-2
```

If the result is longer than 243 characters, it is truncated on the right. An 8-position sequence number is placed on the front of the text.

If both strings are missing, the CLIST record contains only the profile name. If you want a string of data to appear only after the resource name, specify 'string-1' as ''.

Note: The DASD data set name for the CLIST data set is generated in the format:

```
x.EXEC.RACF.CLIST
```

where x is the default data set name prefix in your TSO profile.

If a data set with this name is found through the catalog, the records in it are replaced with the new records. If no data set is found, a new one is created and cataloged.

The CLIST data set is a sequential data set with variable length records and a maximum logical record size of 255. This includes a 4 byte length field at the front of the record. The records are numbered in sequence by 10.

GENERIC or NOGENERIC

specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be selected. If neither operand is specified, both profile types are selected.

These operands are ignored unless generic profile command processing is enabled.

VSAM

specifies that only VSAM data sets are to be selected. This operand is ignored for classes other than the DATASET class.

NONVSAM

specifies that only non-VSAM data sets are to be selected. This operand is ignored for classes other than the DATASET class.

ALL

specifies that both VSAM and non-VSAM data set profiles of both the generic type and the discrete type are to be selected. This operand is ignored for classes other than the DATASET class. ALL is the default if VSAM, NONVSAM, GENERIC, NOGENERIC, MODEL, and ALL are omitted.

MODEL

specifies that only data set profiles having the MODEL attribute are to be selected. RACF ignores this keyword for classes other than DATASET.

WARNING

specifies that only resources with the WARNING indicator are to be selected.

This operand is ignored when CLASS is specified as USER or GROUP.

SEARCH Examples

Example 1

Operation: User CD0 wants to list all of her RACF data set profiles.

Known: User CD0 is RACF-defined.

Command: SEARCH

Defaults: MASK(CD0) CLASS(DATASET) LIST ALL

Example 2

Operation: User IA0 wants to remove the RACF profiles for all DATA-type data sets for the group RESEARCH that have not been referenced for 90 days. The user wants a CLIST data set to be created with DELDSD commands for each profile satisfying the search criteria. A list is not desired.

Known: User IA0 is connected to group RESEARCH (and is the owner of all profiles in group RESEARCH) with the group-SPECIAL attribute.

Command: SEARCH MASK(RESEARCH DATA) AGE(90) CLIST('DELDSD ') NOLIST

Defaults: CLASS(DATASET) ALL

Results: A CLIST data set with the name IA0.EXEC.RACF.CLIST is built, and the records in it are in the format:

```
DELDSD 'data-set-name'
```

Example 3

Operation: User ADMIN wishes to find and revoke all userids of users who have not accessed the system in the last 90 days. For this to work, the INITSTATS option (specified on the SETROPTS command) must be in effect.

Known: User ADMIN has the SPECIAL attribute.

Command: SEARCH CLASS(USER) AGE(90) CLIST('ALTUSER ' ' REVOKE')

Defaults: Process all userid entries.

Results: A CLIST data set with the name ADMIN.EXEC.RACF.CLIST listing the userid for each user that has not accessed the system within 90 days, with records in the following format:

```
ALTUSER  userid  REVOKE
```

Example 4

Operation: User ADM1 wants to get a list of all generic profiles for group SALES.

Known: User ADM1 has the SPECIAL attribute.

Command: SEARCH MASK(SALES.*)

Defaults: CLASS(DATASET) LIST ALL

Results: A list of all profiles in the DATASET class beginning with 'SALES.*'. (Since the string specified contains an asterisk, this list will consist only of generic profiles.)

SETROPTS Command

Use the SETROPTS command to dynamically set system-wide RACF options related to resource protection. Specifically, use SETROPTS to do the following:

- gather and display RACF statistics
- protect terminals
- log RACF events
- permit list-of-groups access checking
- control the automatic data set protection (ADSP) attribute for users
- activate profile modeling for GDG, group, and user data sets
- display options currently in effect
- enable or disable the generic profile checking facility on a class-by-class basis or for all classes system-wide
- control user password-expiration interval
- establish password syntax rules
- activate password processing for checking previous passwords and limiting invalid password attempts
- enable or disable the global access checking facility
- activate protection for data sets with single-level names
- control logging of real data set names
- control the job entry subsystem options
- initiate refreshing in-storage profile lists and global access checking tables

If you specify the AUDIT operand, the system will log all modifications to profiles in the RACF data set by use of RACF commands and the RACDEF SVC. Following are the classes that can be specified in the AUDIT operand and the commands and SVCs that will be logged for each class:

USER	GROUP	DATASET	CDT Entries
ADDUSER	ADDGROUP	ADDSD	PERMIT
ALTUSER	ALTGROUP	ALTDSD	RACDEF SVC
CONNECT	CONNECT	DELDSD	RALTER
DELUSER	DELGROUP	PERMIT	RDEFINE
PASSWORD	REMOVE	RACDEF SVC	RDELETE
REMOVE			

RACF Requirements

Most SETROPTS command functions require you to have the SPECIAL or AUDITOR attributes. If you have the SPECIAL attribute, you can use the following operands:

- TERMINAL, CLASSACT/NOCLASSACT, INACTIVE/NOINACTIVE, GRPLIST/NOGRPLIST, GENERIC/NOGENERIC, GENCMD/NOGENCMD, MODEL/NOMODEL, ADSP/NOADSP, GLOBAL/NOGLOBAL, PREFIX/NOPREFIX, STATISTICS/NOSTATISTICS, INITSTATS/NOINITSTATS REALDSN/NOREALDSN,JES,REFRESH and PASSWORD.

If you have the AUDITOR attribute, you can use the following operands:

- AUDIT/NOAUDIT, SAUDIT/NOSAUDIT, and CMDVIOL/NOCMDVIOL.

If you have either the SPECIAL or AUDITOR attribute, you can use the LIST operand, but LIST will only display the auditor options for auditors.

In some situations, you can use SETROPTS even if you do not have the SPECIAL or AUDITOR attributes. These situations are:

- You can use the LIST operand if you have the group-SPECIAL or group-AUDITOR attribute in the current connect group or if GRPLIST is active, in any group that you are connected to. LIST displays the AUDIT/NOAUDIT, SAUDIT/NOSAUDIT, or CMDVIOL/NOCMDVIOL options only if you have the group-AUDITOR attribute.

- You can use REFRESH together with GENERIC if you have the group-SPECIAL, AUDITOR, group-AUDITOR, OPERATIONS, or group-OPERATIONS attribute, or CLAUTH authority for the classes specified.

- You can use REFRESH together with GLOBAL if you have the OPERATIONS attribute or CLAUTH authority for the classes specified.

```
{SETROPTS}    [{CLASSACT   } ({ class-name... }) ]
{SETR    }    [{            } ({ *             }) ]
              [{NOCLASSACT } ({               }) ]

               [TERMINAL( { READ })]
               [          { NONE }  ]

              [{STATISTICS   } ({ class-name ... })]
              [{             } ({ *               })]
              [{NOSTATISTICS } ({                 })]

               [INITSTATS  ]
               [NOINITSTATS]

              [{AUDIT   } ({ class-name ... }) ]
              [{        } ({ *              }) ]
              [{NOAUDIT } ({                }) ]

              [{GENERIC  }   ({class-name... }) ]
              [{NOGENERIC}   ({*             }) ]

              [{GENCMD  }    ({class-name... }) ]
              [{NOGENCMD}    ({*             }) ]

              [{GLOBAL  }    ( {class-name... }) ]
              [{NOGLOBAL}    ( {*             })  ]

               [ADSP  ]
               [NOADSP]

               [PREFIX(prefix)]
               [NOPREFIX      ]

               [SAUDIT  ]
               [NOSAUDIT]

               [CMDVIOL  ]
               [NOCMDVIOL]

               [INACTIVE(unused-userid-interval)]
               [NOINACTIVE                      ]

               [GRPLIST  ]
               [NOGRPLIST]

               [MODEL     {[GDG  ] [USER  ] [GROUP  ]}]
               [          {[NOGDG] [NOUSER] [NOGROUP]}]
               [NOMODEL                               ]
                          (                                          )
                          ( [HISTORY(number-previous-passwords)]     )
                          ( [NOHISTORY                         ]     )
                          (                                          )
                          ( [REVOKE(number-invalid-passwords)]       )
                          ( [NOREVOKE                        ]       )
               PASSWORD(  {                                          }
                          ( [INTERVAL(password-change-interval)]     )
                          ( [RULEn(LENGTH(m1:m2)                ]    )
                          ( [       content-keyword (position)  ]    )
                          ( [NORULEn                            ]    )
                          ( [NORULES                            ]    )
                          (                                          )
                          ( [WARNING(days-before-password-expires)]  )
                          ( [NOWARNING                            ]  )
              [REFRESH]   (                                          )

              [REALDSN  ]
              [NOREALDSN]

              [JES( [{ BATCHALLRACF  } {XBMALLRACF  }    {EARLYVERIFY  }])]
              [     [{ NOBATCHALLRACF} {NOXBMALLRACF}    {NOEARLYVERIFY}])]

              [LIST]
```

CLASSACT

specifies those classes defined by entries in the class descriptor table for which RACF protection is to be in effect. An * indicates that RACF protection is in effect for all classes defined in the class descriptor table.

NOCLASSACT

specifies those classes defined by entries in the class descriptor table for which RACF protection is not to be in effect. An * indicates that RACF protection is not in effect for any of the classes in the class descriptor table. NOCLASSACT is the initial state at RACF initialization.

TERMINAL

is used to set the universal access authority associated with undefined terminals. If you specify TERMINAL but do not specify READ or NONE, the system will prompt you for a value.

STATISTICS(class-name...)

specifies the names of the classes to be added to those previously defined to have statistical information recorded. The valid class names are DATASET and those specified in the class descriptor table.

If * is specified, all of the classes will have statistical information recorded. STATISTICS(*) is the initial state at RACF initialization.

NOSTATISTICS(class-name...)

specifies the names of the classes to be deleted from those previously defined to have statistical information recorded. The valid class names are DATASET and those specified in the class descriptor table.

If * is specified, none of the classes will have statistical information recorded.

INITSTATS

specifies that statistics available during RACINIT SVC processing are to be recorded. These statistics include the date and time RACINIT is issued for a particular user, the number of RACINITs for a user to a particular group, and the date and time of the last RACINIT for a user to a particular group. If you specify the INACTIVE, REVOKE, HISTORY and WARNING keywords, the INITSTATS option must be in effect.

INITSTATS is the initial state at RACF initialization.

NOINITSTATS

specifies that statistics available during RACINIT SVC processing are not to be recorded.

AUDIT(class-name...)

specifies the names of the classes to be added to those previously defined to have modifications to profiles in the RACF data set logged by RACF commands and the RACDEF SVC. The valid class names are USER, GROUP, DATASET, and those specified in the class descriptor table.

If * is specified, logging will occur for all classes.

You must have the AUDITOR attribute in order to enter the AUDIT operand.

NOAUDIT(class-name...)

specifies the names of the classes to be deleted from those previously defined to have modifications to profiles in the RACF data set logged by RACF commands and the RACDEF SVC. The valid class names are USER, GROUP, DATASET, and those specified in the class descriptor table. NOAUDIT(*) is the initial state at RACF initialization.

If * is specified, logging will not occur for any of the classes.

You must have the AUDITOR attribute in order to enter the NOAUDIT operand.

GENERIC(class-name...)

activates the generic profile checking facility for the classes specified. An * specifies the DATASET class plus all the classes in the class descriptor table except group resource classes. Generic profile command processing is automatically activated for all classes for which the generic profile checking facility is activated.

If you specify GENERIC in conjunction with the REFRESH operand, only those currently active and authorized classes are refreshed.

NOGENERIC(class-name...)

disables the generic profile checking facility for the classes specified. NOGENERIC (*) is the state at RACF initialization.

GENCMD(class-name...)

activate generic profile command processing for the specified classes. An * specifies the DATASET class plus all the classes in the class descriptor table except group resource classes.

When GENCMD has been specified for a class, all the command processors can work on generic profiles, but the RACF SVC routines cannot perform generic profile checking. This operand allows the installation to temporarily disable the generic profile checking facility (during maintenance for example) and still use the RACF commands to maintain the generic profiles.

You must have the SPECIAL attribute to enter the GENCMD operand.

NOGENCMD(class-name...)

disables generic profile command processing for the specified classes. NOGENCMD(*) is the state at RACF initialization.

If generic profile checking is active, this operand is ignored.

You must have the SPECIAL attribute to enter the NOGENCMD operand.

GLOBAL(class-name...)
specifies those classes eligible for global access checking. An * specifies the DATASET class plus all the classes in the class descriptor table except group resource classes.

If you specify GLOBAL in conjunction with the REFRESH operand, only those currently active and authorized classes are refreshed.

NOGLOBAL(class-name...)
disables global access checking for the specified classes. NOGLOBAL(*) is the state at RACF initialization. operand.

ADSP
specifies that data sets created by users who have the automatic data set protection (ADSP) attribute will be automatically RACF-protected. This is the state at RACF initialization.

NOADSP
cancels automatic RACF protection for users who have the ADSP attribute.

ADSP forces the creation of a discrete profile for each data set created by users who have the ADSP attribute. It should normally be disabled (via the NOADSP operand) if you specify GENERIC.

PREFIX(prefix)
activates RACF protection for data sets that have single-level names, and specifies the 1-8 character prefix to be used as the first-level qualifier in the internal form of the names. The prefix should be a predefined groupname, and must not be the first-level qualifier of any actual data sets in the system.

NOPREFIX
deactivates RACF protection for data sets that have single-level names.

SAUDIT
specifies that all RACF commands (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH) issued by users with the SPECIAL attribute are to be logged. SAUDIT is the initial state at RACF initialization.

NOSAUDIT
specifies that the commands issued by users with the SPECIAL attribute are not to be logged.

CMDVIOL
specifies that violations detected by RACF commands (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH) during RACF command processing are to be logged. A violation may occur because a user is not authorized to modify a particular profile or is not authorized to enter a particular operand on a command. CMDVIOL is the initial state at RACF initialization.

You must have the AUDITOR attribute in order to enter the CMDVIOL operand.

NOCMDVIOL

specifies that violations detected by RACF commands during RACF command processing are not to be logged (except RVARY and SETROPTS, which are always logged).

You must have the AUDITOR attribute in order to enter the NOCMDVIOL operand.

INACTIVE(unused-userid-interval)

specifies the number of days (1 to 255) that a userid can remain unused and still be considered valid. RACINIT checks the number of days since the last successful invocation of RACINIT against the INACTIVE value and, if the former is larger, revokes the user's right to use the system. If you specify INACTIVE, the INITSTATS keyword must be in effect.

NOINACTIVE

specifies that the RACINIT is not to check the userids against an unused-userid-interval. NOINACTIVE is the initial state at RACF initialization.

GRPLIST

specifies that RACHECK and RACDEF processing is to perform list-of-groups access checking for all system users. When you specify GRPLIST, a user's authority to access a resource is not based only on the authority of the user's current connect group; access is based on the authority of any group to which the user is connected.

Note: List of groups checking does not apply to terminal and APPL classes.

NOGRPLIST

specifies that the user's authority to access a resource is based on the authority of the user's current connect group.

MODEL

specifies a number of subkeywords to permit or disallow various model profile processing options.

GDG

specifies that each member of a generation data group (GDG) can use a common profile identified by the GDG data set base name. When MODEL(GDG) is in effect and RACHECK processes a GDG data set, it first looks for a base profile name in the RACF data set, and, if one exists, uses this common profile. If the GDG base name is not defined in the RACF data set, RACHECK uses the profile for the individual GDG name.

NOGDG

specifies that RACDEF is not to use a common profile for a new GDG data set.

GROUP

specifies that RACDEF is to use a model data set profile to complete the profile information for all group-named data sets.

NOGROUP

specifies that RACDEF is not to use a model profile for new group-named data sets.

USER

specifies that RACDEF is to use a model data set profile to complete the profile information for all userid-named data set.

NOUSER

specifies that RACDEF is not to use a model data set profile for new userid-named data sets.

NOMODEL

specifies that there is no model profile processing for GDG, GROUP, or USER data sets. NOMODEL is the initial state at RACF initialization.

PASSWORD

specifies a number of subkeywords to monitor and check passwords.

HISTORY(number-previous-passwords)

specifies the number of previous passwords (1 to 32) that the SETROPTS command is to save for each userid and compare with an intended new password. If there is a match, the SETROPTS command rejects the intended new password. If you specify HISTORY, the INITSTATS keyword must be in effect.

NOHISTORY

specifies that RACF is not to save previous passwords. NOHISTORY is the initial state at RACF initialization.

REVOKE(number-invalid-passwords)

specifies the number (1 to 254) of consecutive invalid passwords attempts RACF allows before it revokes the userid. If you specify REVOKE, the INITSTATS option must be in effect.

NOREVOKE

specifies that RACF is to ignore the number of consecutive invalid password attempts.

INTERVAL(password-change-interval)

specifies the number of days (1 to 254) that each user's password is to be valid. The value specified in this operand becomes

- A default value for new users defined to RACF via the ADDUSER command.

- An upper limit for users who specify the INTERVAL operand on the PASSWORD command.

(The initial default after RACF initialization is 30 days.)

RULEn(LENGTH(m1:m2) content-keyword(position))

RULEn
specifies an individual syntax rule for new passwords. Eight syntax rules are allowed; thus, n can range from 1 to 8.

LENGTH(m1:m2)
specifies the minimum and maximum password lengths to which this particular rule applies (m2 must be greater than or equal to m1). Because RACF allows passwords no longer than 8 alphameric characters, the value for m2 must be less than or equal to 8. If you omit the m2 value, the rule applies to a password of one length only.

content-keyword(position)
specifies the syntax rules for the positions indicated by the LENGTH keyword. The possible content keywords are:

ALPHA - alphabetic and national characters.

ALPHANUM - alphabetic, national and numeric characters.

Note: This particular content keyword requires at least one alphabetic or national and one numeric character.

VOWEL - vowel characters, namely 'A','E','I','O', and 'U'

NOVOWEL - nonvowel, national and numeric characters

CONSONANT - nonvowel characters

NUMERIC - numeric characters

Each content-keyword is followed by a position (in the form of k, not greater then 8), list of positions (form of k1,k2,k3...in any order), and/or a range (form of k4:k5, where k5 must be greater than or equal to k4). See the following example:

```
RULE1(LENGTH(8) CONSONANT(1,3,5:8) NUMERIC(2,4))
```

Syntax Rule1 applies to passwords 8 characters in length with consonants in positions 1, 3, 5, 6, 7, and 8 and numbers in positions 2 and 4. Thus the password "B2D2GODA" obeys Rule1, and "C3PIBOLO" does not.

If the values in the content keywords do not define every position specified by the LENGTH value, the undefined positions can consist of any combination of alphameric characters.

NORULEn
specifies that RACF is to delete the particular rule identified by n.

NORULES

specifies that RACF is to cancel all password syntax rules established by the installation.

NORULES is the state at RACF initialization.

WARNING(days-before-password-expires)

specifies the number of days (1 to 255) before a password expires when RACF is to issue a warning message to a user. RACF always issues the warning message when the WARNING value exceeds the INTERVAL value. If you don't want the warning with each logon, specify a value for WARNING that is less than the value you specify for INTERVAL. If you specify WARNING, the INITSTATS option must be in effect.

NOWARNING

specifies that RACF is not to issue the warning message for password expiration. NOWARNING is the initial state at RACF initialization.

REFRESH

specifies refreshing the in-storage generic profiles when GENERIC or GLOBAL is specified.

REALDSN

specifies that RACF is to record, in any SMF log records and operator messages, the real data set name (not the naming-conventions name) used on the data set commands and in the RACHECK and RACDEF macros.

NOREALDSN

specifies that RACF is to record, in any SMF log records and operator messages, the data set names modified according to RACF naming conventions.

NOREALDSN is the initial state at RACF initialization.

JES

specifies the job entry subsystem options:

BATCHALLRACF

specifies that the job entry subsystem is to test for the presence of a userid and a password on the job card, or JES propagated RACF identification information for all batch jobs. If the test fails, the job entry subsystem is to fail the job.

NOBATCHALLRACF

specifies that the job entry subsystem should not test for the presence of a userid and a password on the job card, or JES propagated RACF identification information for all batch jobs.

NOBATCHALLRACF is the initial state at RACF initialization.

XBMALLRACF

specifies that the job entry subsystem is to test for the presence of either a userid and password on the job card, or JES propagated RACF identification information for all jobs to be run with an execution batch monitor. If the test fails, the job entry subsystem is to fail the job.

NOXBMALLRACF

specifies that the job entry subsystem should not test for the presence of either a userid and password on the job card, or JES propagated RACF identification information for all jobs to be run with an execution batch monitor.

NOXBMALLRACF is the initial state at RACF initialization.

EARLYVERIFY

specifies that the job entry subsystem is to invoke the system authorization facility (SAF) for jobs that do not qualify for user identification propagation. SAF can call an installation-written exit (if installed) for further verification of userid, group, and password (if specified) at job submission time. Refer to *SPL: RACF* for further information about the MVS router exit.

NOEARLYVERIFY

specifies that the RACF CVT indicator is not to be set and SAF is not to get control.

NOEARLYVERIFY is the initial state at RACF initialization.

LIST

specifies that the current options are to be displayed. If you specify operands in addition to LIST on the SETROPTS command, the other operands will be processed before the current set of options is displayed.

You must have the SPECIAL, AUDITOR, group-SPECIAL, or group-AUDITOR attribute in order to enter the LIST operand. If you have the SPECIAL or group-SPECIAL attribute, the CLASSACT/NOCLASSACT, TERMINAL, INTERVAL, STATISTICS/NOSTATISTICS, INITSTATS/NOINITSTATS, MODEL/NOMODEL, INACTIVE/NOINACTIVE, GRPLIST/NOGRPLIST, GENERIC/NOGENERIC, GENCMD/NOGENCMD, ADSP/NOADSP, GLOBAL/NOGLOBAL, and PREFIX/NOPREFIX options will be displayed. If you have the AUDITOR or the group-AUDITOR attribute, the AUDIT/NOAUDIT, SAUDIT/NOSAUDIT, and CMDVIOL/NOCMDVIOL options will also be displayed along with the options displayed for users with SPECIAL or group-SPECIAL attribute.

SETROPTS Examples

Example 1

Operation: User RVU02 wants to establish system-wide options for his installation. He wants tape volume protection in effect, and a maximum password interval of 60 days.

Known: User RVU02 has the SPECIAL attribute.

Command: SETROPTS PASSWORD(INTERVAL(60)) CLASSACT(TAPEVOL)

Defaults: None

Example 2

Operation: User FRG34 wants to log all activity in the USER and GROUP classes only.

Known: User FRG34 has the AUDITOR attribute.

No logging (via SETROPTS command) is currently specified.

Command: SETROPTS AUDIT(USER GROUP)

Defaults: None

Example 3

Operation: User RVU03 wants to establish a set of syntax rules that obey the following rules:

- Minimum password length is four characters.
- Four-character passwords must have at least one numeric and one alphabetic character.
- Five-character passwords must contain at least one numeric character or be completely alphabetic
- Passwords of six or more characters consist of any combination of alphabetic and numeric characters.

Known: User RVU03 has the SPECIAL attribute.

Command: SETROPTS PASSWORD(RULE1(LENGTH(4:5) ALPHANUM(1:5)) RULE2(LENGTH(5) ALPHA(1:5)) RULE3(LENGTH(6:8) ALPHANUM(1:8)) RULE4(LENGTH(6:8) NUMERIC(1:8)) RULE5(LENGTH(6:8) ALPHA(1:8)))

Defaults: None

Example 4

Operation: User ADM1 wants to enable the generic profile checking facility for the DATASET class.

Known: User ADM1 has the SPECIAL attribute.

Command: SETROPTS GENERIC(DATASET)

Defaults: None

Example 5

Operation: User ADM1 wants to activate global access checking for the DATASET class.

Known: User ADM1 has the SPECIAL attribute.

Command: SETROPTS GLOBAL(DATASET)

Defaults: None

Example 6

Operation: User ADM1 wants to display the RACF options currently in effect.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Command: SETROPTS LIST

Defaults: None

Output: See Figure 12.

```
SETROPTS LIST
ATTRIBUTES = INITSTATS TERMINAL(READ) SAUDIT CMDVIOL
STATISTICS = DATASET DASDVOL TAPEVOL TERMINAL APPL TIMS GIMS AIMS TCICSTRN
             GCICSTRN PCICSPSB QCICSPSB
AUDIT CLASSES = DATASET USER GROUP DASDVOL TAPEVOL TERMINAL APPL TIMS
                GIMS AIMS TCICSTRN GCICSTRN PCICSPSB QCICSPSB
ACTIVE CLASSES = DATASET USER GROUP DASDVOL TAPEVOL TERMINAL APPL TIMS
                 GIMS AIMS TCICSTRN GCICSTRN PCICSPDSB QCICSPSB GMBR GLOBAL
GENERIC PROFILE CLASSES = DATASET DASDVOL TAPEVOL TERMINAL APPL TIMS
                          AIMS TCICSTRN PCICSPSB GMBR
GENERIC COMMAND CLASSES = DATASET DASDVOL TAPEVOL TERMINAL APPL TIMS
                          AIMS TCICSTRN PCICSPSB GMBR
GLOBAL CHECKING CLASSES = NONE
AUTOMATIC DATASET PROTECTION IS IN EFFECT
SINGLE LEVEL NAMES NOT ALLOWED
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
DATA SET MODELLING NOT BEING DONE FOR GDGS.
USER DATA SET MODELLING IS BEING DONE.
GROUP DATA SET MODELLING IS BEING DONE.
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS 254 DAYS.
  NO PASSWORD HISTORY BEING MAINTAINED.
  USERIDS NOT BEING AUTOMATICALLY REVOKED.
  NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(4:5)   LLLLL
    RULE 2  LENGTH(5)     AAAAA
    RULE 3  LENGTH(6:8)   LLLLLLLL
    RULE 4  LENGTH(6:8)   NNNNNNNN
    RULE 5  LENGTH(6:8)   AAAAAAAA
  LEGEND:
   A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
```

Figure 12. Example 6 Output for SETROPTS Command

Appendix A. RACF/ISPF Panels

This appendix contains the RACF panels. The panel illustrations contain the panel identifiers, which you can display with the ISPF command **panelid** entered on the command line. The panel illustrations show how the various panels are related to one another. In a few instances, additional panels from another sequence may be displayed to process your request; these are not illustrated. An example is panel ICHP11, which will display panel ICHP141 when you specify "yes" for the **ACCESS LIST** ===> field.

The panel illustrations use the convention

<<< field name >>>.

to show variable, protected text fields. The variable fields contain the information previously entered on one panel that RACF displays on a subsequent panel.

In most cases, the operands on each panel correspond closely to those used when you issue the RACF commands. However, some minor differences may exist. For example, the AUDIT operand on the commands has the following syntax:

```
                 NONE
                 ALL
     AUDIT       SUCCESS    [(audit-acc-lvl)] ...
                 FAILURES
```

The corresponding panels have two separate fields, one for "AUDIT SUCCESSES" and one for "AUDIT FAILURES." Possible values for each are READ, UPDATE, CONTROL, and ALTER, or NOAUDIT to suppress logging.

When this panel is invoked, the operands are initialized to:

AUDIT SUCCESSES ===>NOAUDIT
AUDIT FAILURES ===>READ

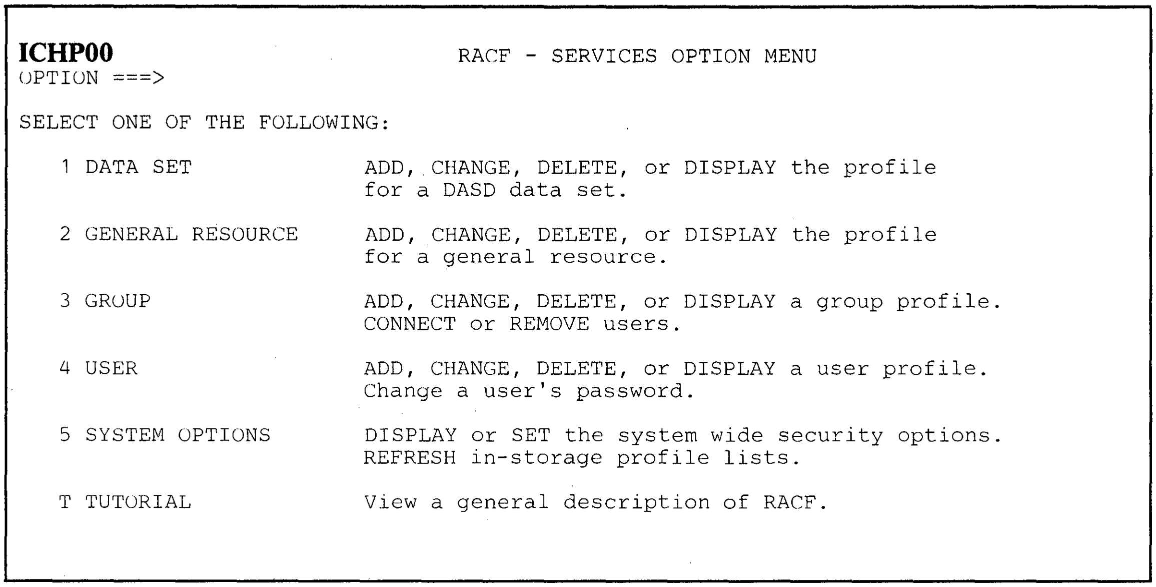
which is equivalent to

AUDIT (FAILURES (READ))

Similarly, the equivalent of AUDIT(ALL(UPDATE)) is achieved by

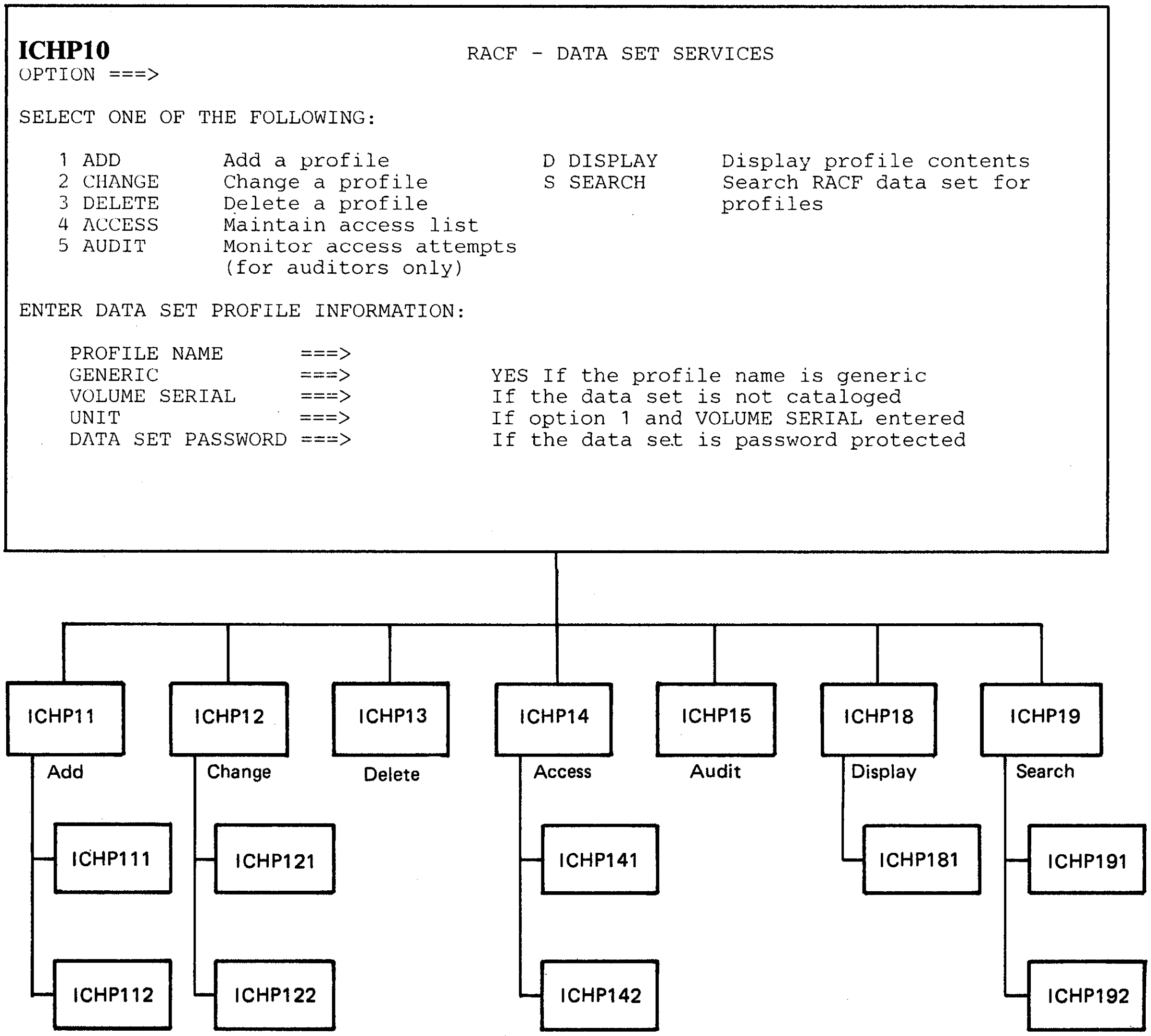
AUDIT SUCCESSES===>UPDATE
AUDIT FAILURES ===>UPDATE

Note that you have to have the same level of authorization to use the panels as you do to issue the commands. If you try to access and write on a panel for which you do not have the proper authorization, RACF will issue a message. You can refer to the topic "RACF Requirements" under each command in Chapter 2 of this book to see the proper authorizations you need to use the panels.



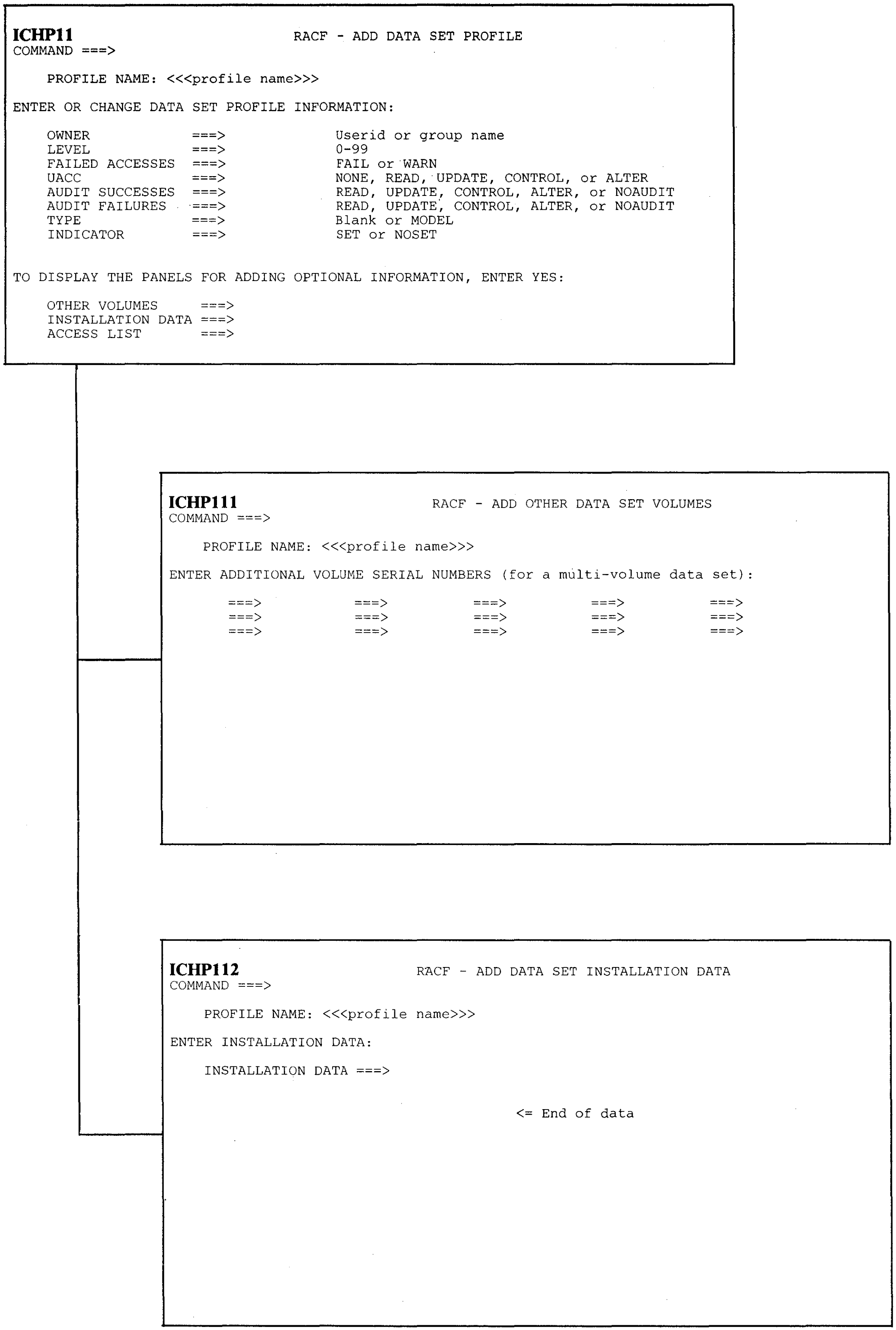
```
ICHP00                            RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 DATA SET               ADD, CHANGE, DELETE, or DISPLAY the profile
                            for a DASD data set.

   2 GENERAL RESOURCE       ADD, CHANGE, DELETE, or DISPLAY the profile
                            for a general resource.

   3 GROUP                  ADD, CHANGE, DELETE, or DISPLAY a group profile.
                            CONNECT or REMOVE users.

   4 USER                   ADD, CHANGE, DELETE, or DISPLAY a user profile.
                            Change a user's password.

   5 SYSTEM OPTIONS         DISPLAY or SET the system wide security options.
                            REFRESH in-storage profile lists.

   T TUTORIAL               View a general description of RACF.
```

Figure 13. Services Option Menu Panel



```
ICHP10                            RACF - DATA SET SERVICES
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 ADD         Add a profile            D DISPLAY     Display profile contents
   2 CHANGE      Change a profile         S SEARCH      Search RACF data set for
   3 DELETE      Delete a profile                       profiles
   4 ACCESS      Maintain access list
   5 AUDIT       Monitor access attempts
                 (for auditors only)

ENTER DATA SET PROFILE INFORMATION:

    PROFILE NAME      ===>
    GENERIC           ===>          YES If the profile name is generic
    VOLUME SERIAL     ===>          If the data set is not cataloged
    UNIT              ===>          If option 1 and VOLUME SERIAL entered
    DATA SET PASSWORD ===>          If the data set is password protected
```

Figure 14. Data Set Services Panel

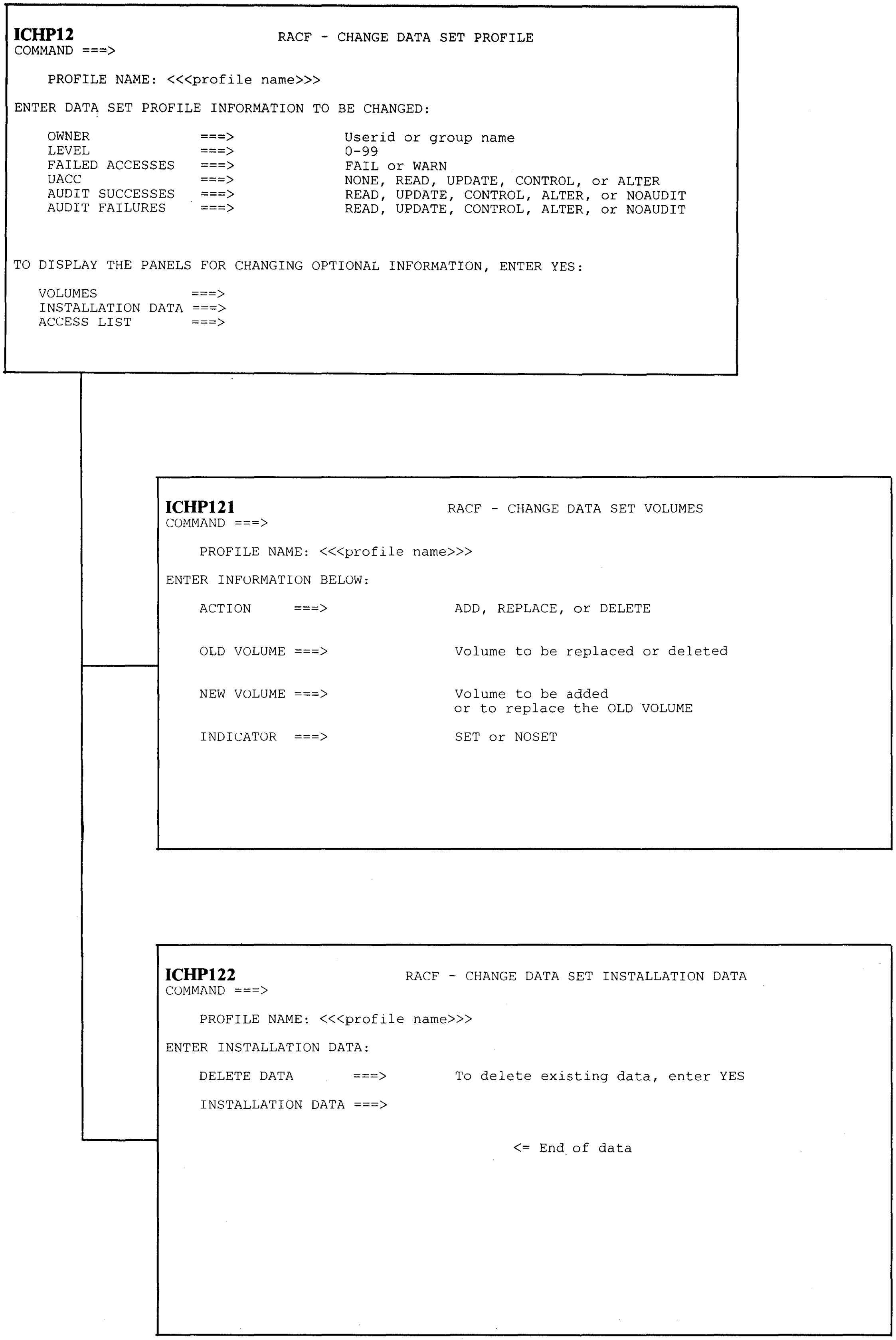


```
ICHP11                        RACF - ADD DATA SET PROFILE
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

    OWNER            ===>              Userid or group name
    LEVEL            ===>              0-99
    FAILED ACCESSES  ===>              FAIL or WARN
    UACC             ===>              NONE, READ, UPDATE, CONTROL, or ALTER
    AUDIT SUCCESSES  ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES   ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    TYPE             ===>              Blank or MODEL
    INDICATOR        ===>              SET or NOSET


TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION, ENTER YES:

    OTHER VOLUMES     ===>
    INSTALLATION DATA ===>
    ACCESS LIST       ===>
```

```
ICHP111                           RACF - ADD OTHER DATA SET VOLUMES
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER ADDITIONAL VOLUME SERIAL NUMBERS (for a multi-volume data set):

       ===>           ===>          ===>          ===>          ===>
       ===>           ===>          ===>          ===>          ===>
       ===>           ===>          ===>          ===>          ===>
```

```
ICHP112                        RACF - ADD DATA SET INSTALLATION DATA
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER INSTALLATION DATA:

    INSTALLATION DATA ===>


                                         <= End of data
```

Figure 15. Add a Profile Panels--Data Sets

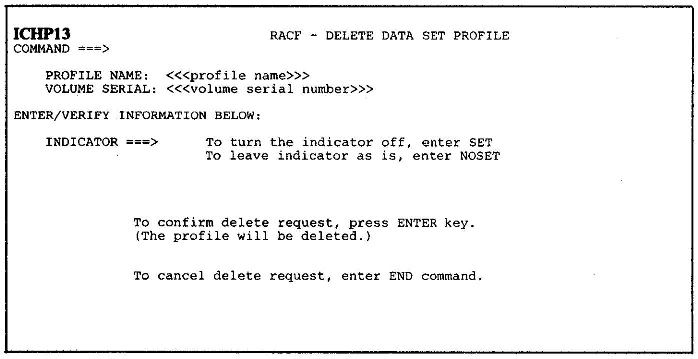


```
ICHP12                       RACF - CHANGE DATA SET PROFILE
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

    OWNER              ===>            Userid or group name
    LEVEL              ===>            0-99
    FAILED ACCESSES    ===>            FAIL or WARN
    UACC               ===>            NONE, READ, UPDATE, CONTROL, or ALTER
    AUDIT SUCCESSES    ===>            READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES     ===>            READ, UPDATE, CONTROL, ALTER, or NOAUDIT


TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION, ENTER YES:

   VOLUMES           ===>
   INSTALLATION DATA ===>
   ACCESS LIST       ===>
```

```
ICHP121                         RACF - CHANGE DATA SET VOLUMES
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER INFORMATION BELOW:

    ACTION     ===>              ADD, REPLACE, or DELETE


    OLD VOLUME ===>              Volume to be replaced or deleted


    NEW VOLUME ===>              Volume to be added
                                 or to replace the OLD VOLUME

    INDICATOR  ===>              SET or NOSET
```

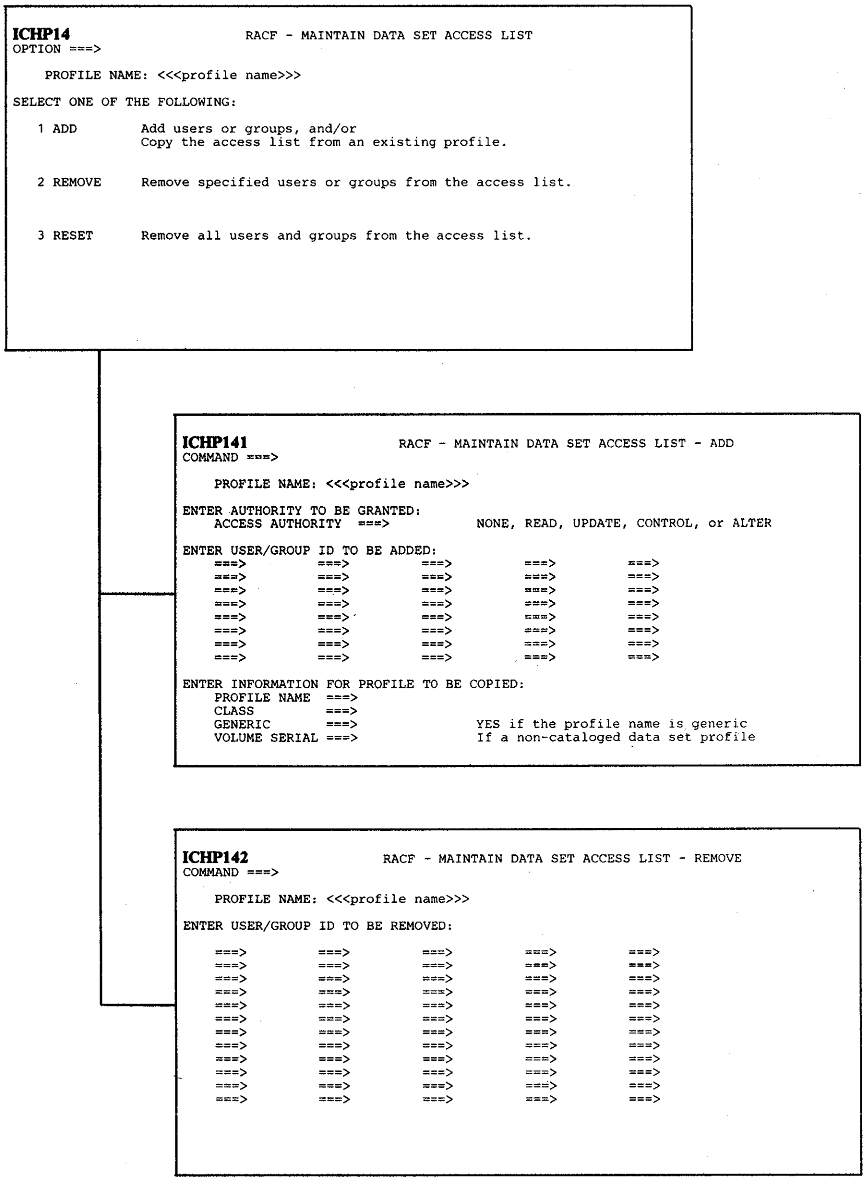
```
ICHP122                    RACF - CHANGE DATA SET INSTALLATION DATA
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER INSTALLATION DATA:

    DELETE DATA       ===>       To delete existing data, enter YES

    INSTALLATION DATA ===>

                                        <= End of data
```

Figure 16. Change a Profile Panels--Data Sets



```
ICHP13                         RACF - DELETE DATA SET PROFILE
COMMAND ===>

    PROFILE NAME:  <<<profile name>>>
    VOLUME SERIAL: <<<volume serial number>>>

ENTER/VERIFY INFORMATION BELOW:

    INDICATOR ===>      To turn the indicator off, enter SET
                        To leave indicator as is, enter NOSET



               To confirm delete request, press ENTER key.
               (The profile will be deleted.)

               To cancel delete request, enter END command.
```

Figure 17. Delete Data Set Profile Panel

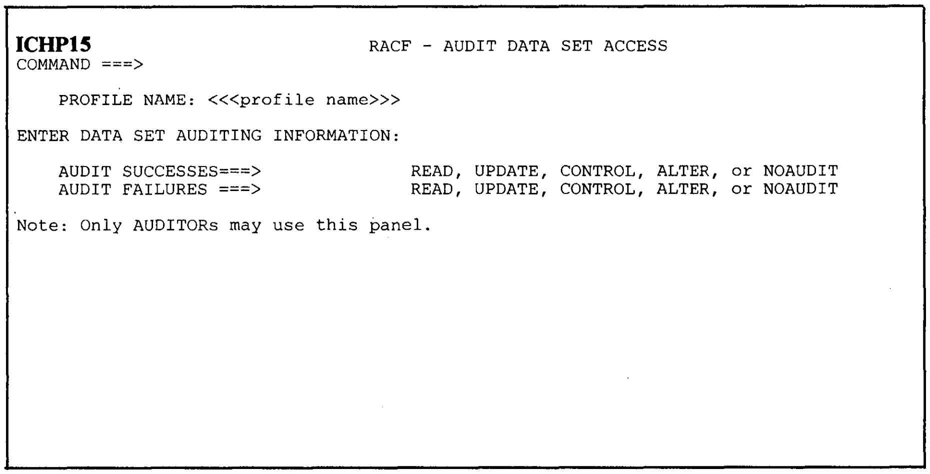


```
ICHP14                      RACF - MAINTAIN DATA SET ACCESS LIST
OPTION ===>

    PROFILE NAME: <<<profile name>>>

SELECT ONE OF THE FOLLOWING:

   1 ADD         Add users or groups, and/or
                 Copy the access list from an existing profile.


   2 REMOVE      Remove specified users or groups from the access list.


   3 RESET       Remove all users and groups from the access list.
```

```
ICHP141                     RACF - MAINTAIN DATA SET ACCESS LIST - ADD
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER AUTHORITY TO BE GRANTED:
    ACCESS AUTHORITY  ===>          NONE, READ, UPDATE, CONTROL, or ALTER

ENTER USER/GROUP ID TO BE ADDED:
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>

ENTER INFORMATION FOR PROFILE TO BE COPIED:
    PROFILE NAME  ===>
    CLASS         ===>
    GENERIC       ===>              YES if the profile name is generic
    VOLUME SERIAL ===>              If a non-cataloged data set profile
```

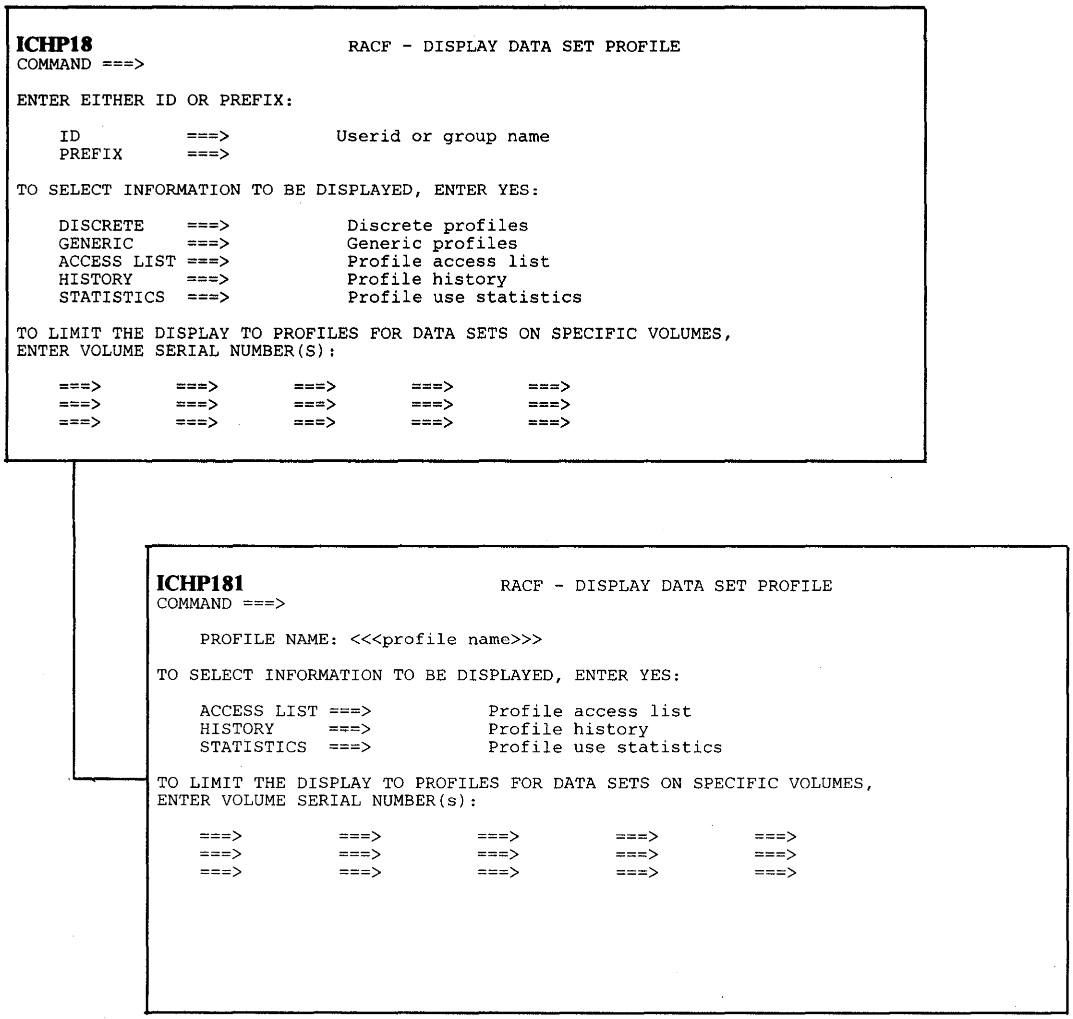
```
ICHP142                     RACF - MAINTAIN DATA SET ACCESS LIST - REMOVE
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER USER/GROUP ID TO BE REMOVED:

    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
```

Figure 18. Maintain Access List Panels--Data Sets



```
ICHP15                              RACF - AUDIT DATA SET ACCESS
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

ENTER DATA SET AUDITING INFORMATION:

    AUDIT SUCCESSES===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT

Note: Only AUDITORs may use this panel.
```

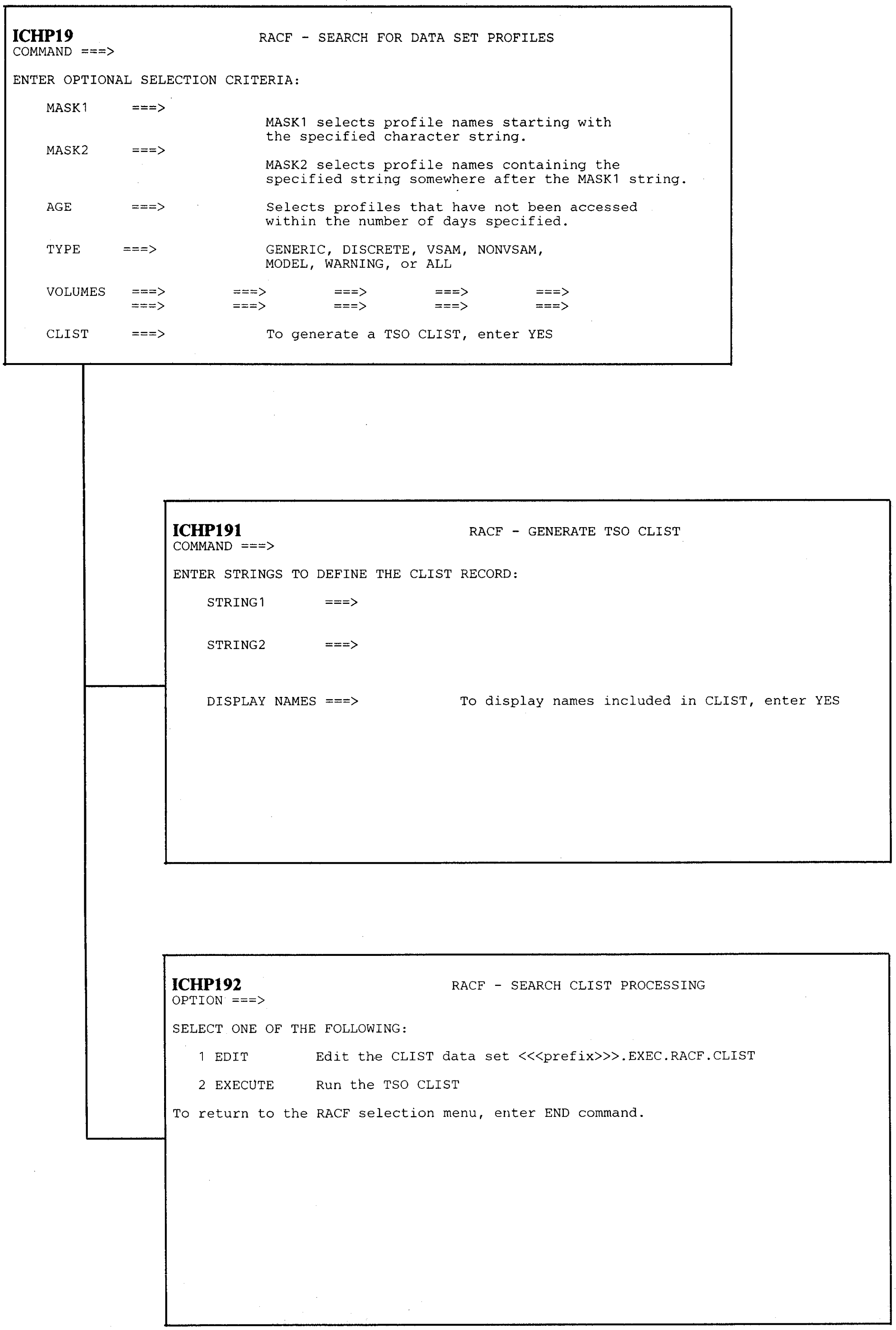
Figure 19. Monitor Access Attempts Panel--Data Sets



```
ICHP18                            RACF - DISPLAY DATA SET PROFILE
COMMAND ===>

ENTER EITHER ID OR PREFIX:

    ID          ===>          Userid or group name
    PREFIX      ===>

TO SELECT INFORMATION TO BE DISPLAYED, ENTER YES:

    DISCRETE    ===>           Discrete profiles
    GENERIC     ===>           Generic profiles
    ACCESS LIST ===>           Profile access list
    HISTORY     ===>           Profile history
    STATISTICS  ===>           Profile use statistics

TO LIMIT THE DISPLAY TO PROFILES FOR DATA SETS ON SPECIFIC VOLUMES,
ENTER VOLUME SERIAL NUMBER(S):

    ===>        ===>        ===>        ===>        ===>
    ===>        ===>        ===>        ===>        ===>
    ===>        ===>        ===>        ===>        ===>
```

```
ICHP181                           RACF - DISPLAY DATA SET PROFILE
COMMAND ===>

    PROFILE NAME: <<<profile name>>>

TO SELECT INFORMATION TO BE DISPLAYED, ENTER YES:

    ACCESS LIST ===>           Profile access list
    HISTORY     ===>           Profile history
    STATISTICS  ===>           Profile use statistics

TO LIMIT THE DISPLAY TO PROFILES FOR DATA SETS ON SPECIFIC VOLUMES,
ENTER VOLUME SERIAL NUMBER(s):

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```

Figure 20. Display Profile Contents Panel--Data Sets

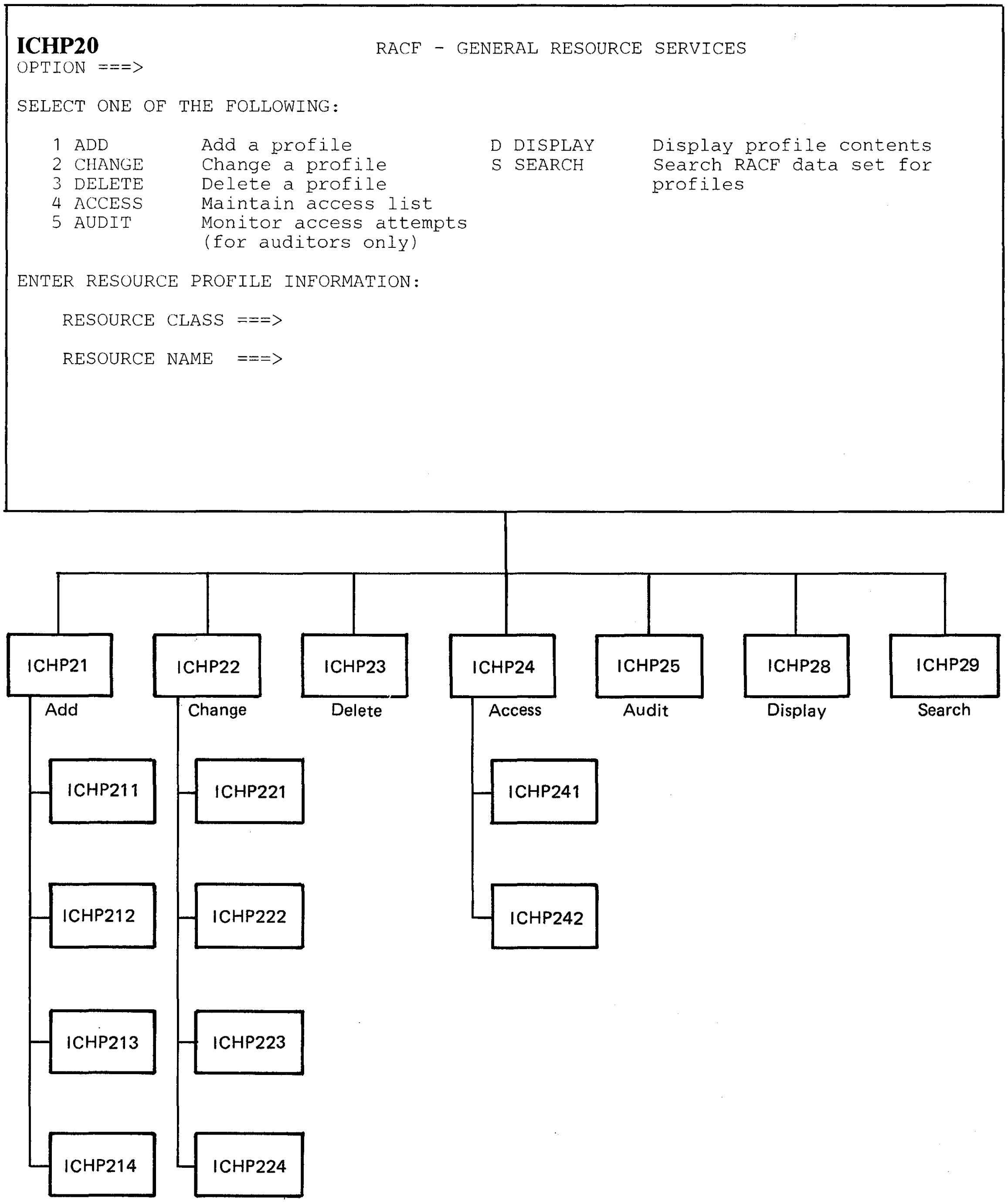


```
ICHP19                        RACF - SEARCH FOR DATA SET PROFILES
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

    MASK1     ===>
                             MASK1 selects profile names starting with
                             the specified character string.
    MASK2     ===>
                             MASK2 selects profile names containing the
                             specified string somewhere after the MASK1 string.

    AGE       ===>           Selects profiles that have not been accessed
                             within the number of days specified.

    TYPE     ===>            GENERIC, DISCRETE, VSAM, NONVSAM,
                             MODEL, WARNING, or ALL

    VOLUMES   ===>        ===>        ===>        ===>        ===>
              ===>        ===>        ===>        ===>        ===>

    CLIST     ===>           To generate a TSO CLIST, enter YES
```

```
ICHP191                       RACF - GENERATE TSO CLIST
COMMAND ===>

ENTER STRINGS TO DEFINE THE CLIST RECORD:

    STRING1       ===>


    STRING2       ===>



    DISPLAY NAMES ===>           To display names included in CLIST, enter YES
```

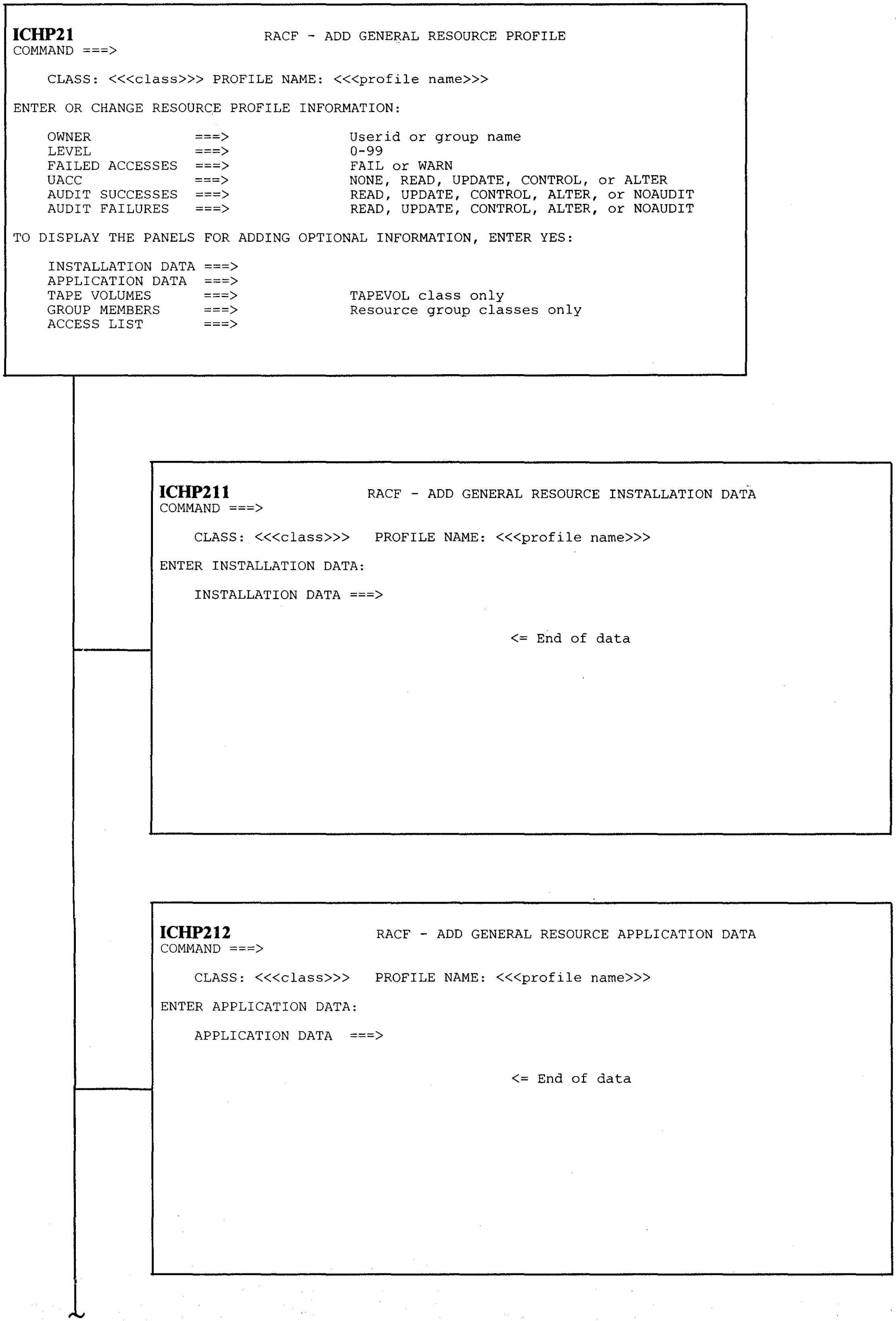
```
ICHP192                       RACF - SEARCH CLIST PROCESSING
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 EDIT        Edit the CLIST data set <<<prefix>>>.EXEC.RACF.CLIST

   2 EXECUTE     Run the TSO CLIST

To return to the RACF selection menu, enter END command.
```

Figure 21. Search RACF Data Set for Profiles Panels--Data Sets



```
ICHP20                              RACF - GENERAL RESOURCE SERVICES
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 ADD       Add a profile            D DISPLAY    Display profile contents
   2 CHANGE    Change a profile         S SEARCH     Search RACF data set for
   3 DELETE    Delete a profile                      profiles
   4 ACCESS    Maintain access list
   5 AUDIT     Monitor access attempts
               (for auditors only)

ENTER RESOURCE PROFILE INFORMATION:

    RESOURCE CLASS ===>

    RESOURCE NAME  ===>
```

Figure 22. General Resource Services Panel



```
ICHP21                        RACF - ADD GENERAL RESOURCE PROFILE
COMMAND ===>

    CLASS: <<<class>>> PROFILE NAME: <<<profile name>>>

ENTER OR CHANGE RESOURCE PROFILE INFORMATION:

    OWNER            ===>              Userid or group name
    LEVEL            ===>              0-99
    FAILED ACCESSES  ===>              FAIL or WARN
    UACC             ===>              NONE, READ, UPDATE, CONTROL, or ALTER
    AUDIT SUCCESSES  ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES   ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION, ENTER YES:

    INSTALLATION DATA ===>
    APPLICATION DATA  ===>
    TAPE VOLUMES      ===>             TAPEVOL class only
    GROUP MEMBERS     ===>             Resource group classes only
    ACCESS LIST       ===>
```

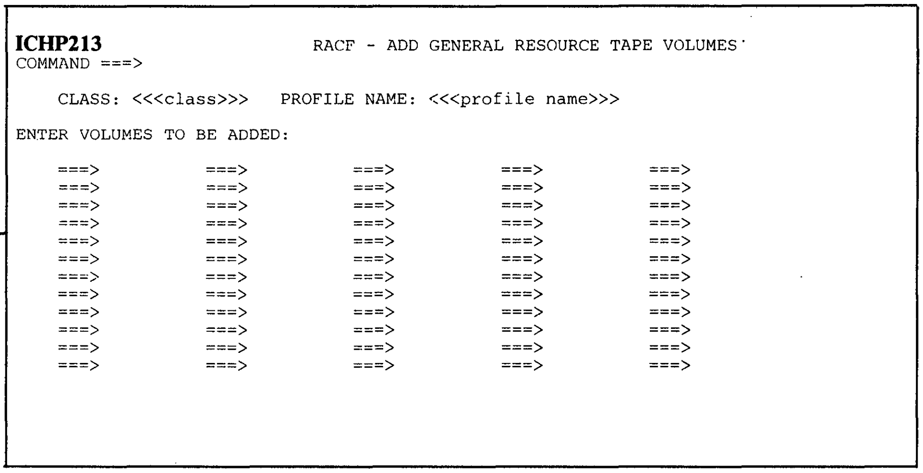
```
ICHP211                 RACF - ADD GENERAL RESOURCE INSTALLATION DATA
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER INSTALLATION DATA:

    INSTALLATION DATA ===>

                                        <= End of data
```

```
ICHP212                  RACF - ADD GENERAL RESOURCE APPLICATION DATA
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER APPLICATION DATA:

    APPLICATION DATA  ===>

                                        <= End of data
```

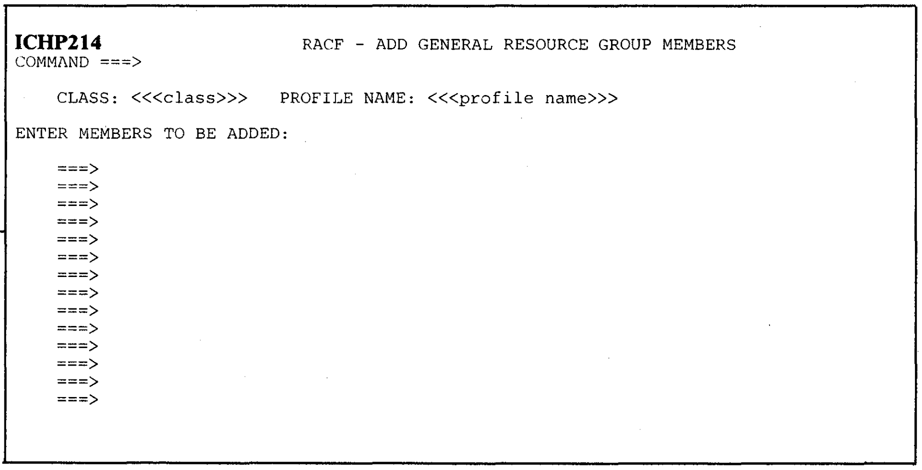
to next page

Figure 23. Add a Profile Panels--General Resources

from previous page

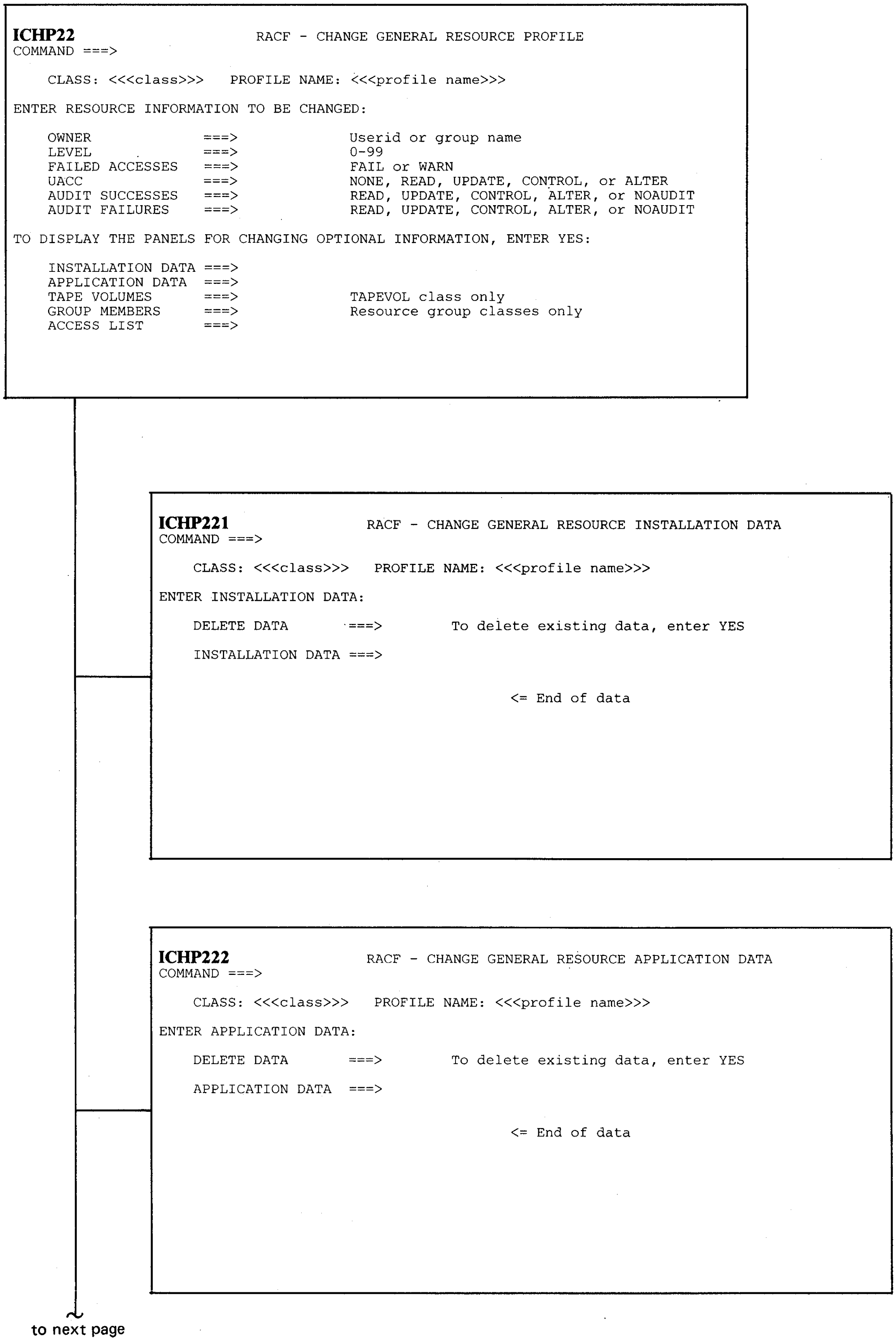


```
ICHP213                   RACF - ADD GENERAL RESOURCE TAPE VOLUMES
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER VOLUMES TO BE ADDED:

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```



```
ICHP214                  RACF - ADD GENERAL RESOURCE GROUP MEMBERS
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER MEMBERS TO BE ADDED:

    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
```

Figure 24. Add a Profile Panels--General Resources (Continued)



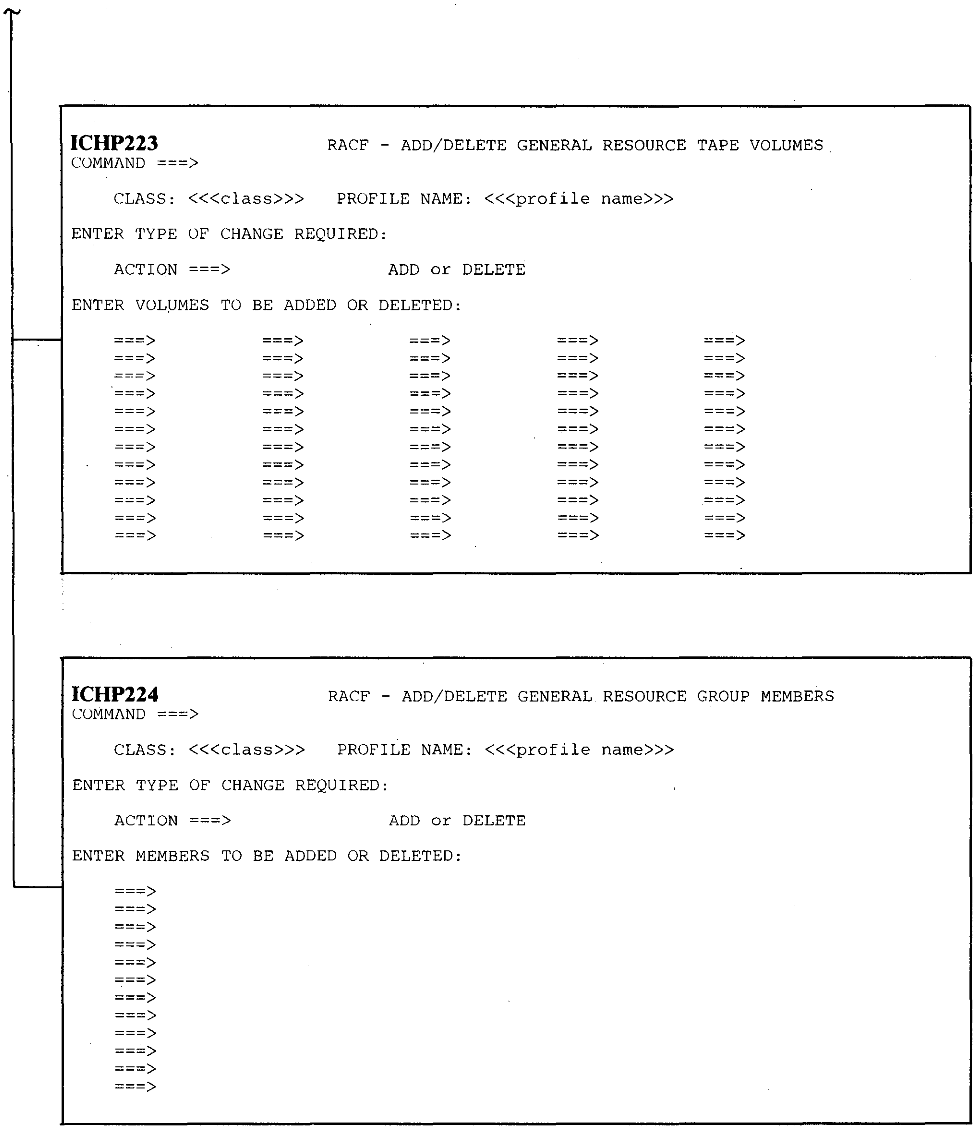
```
ICHP22                    RACF - CHANGE GENERAL RESOURCE PROFILE
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER RESOURCE INFORMATION TO BE CHANGED:

    OWNER              ===>            Userid or group name
    LEVEL              ===>            0-99
    FAILED ACCESSES    ===>            FAIL or WARN
    UACC               ===>            NONE, READ, UPDATE, CONTROL, or ALTER
    AUDIT SUCCESSES    ===>            READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES     ===>            READ, UPDATE, CONTROL, ALTER, or NOAUDIT

TO DISPLAY THE PANELS FOR CHANGING OPTIONAL INFORMATION, ENTER YES:

    INSTALLATION DATA ===>
    APPLICATION DATA  ===>
    TAPE VOLUMES      ===>             TAPEVOL class only
    GROUP MEMBERS     ===>             Resource group classes only
    ACCESS LIST       ===>
```

```
ICHP221                   RACF - CHANGE GENERAL RESOURCE INSTALLATION DATA
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER INSTALLATION DATA:

    DELETE DATA       ===>        To delete existing data, enter YES

    INSTALLATION DATA ===>

                                          <= End of data
```

```
ICHP222                   RACF - CHANGE GENERAL RESOURCE APPLICATION DATA
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER APPLICATION DATA:

    DELETE DATA       ===>        To delete existing data, enter YES

    APPLICATION DATA  ===>

                                          <= End of data
```

Figure 25. Change a Profile Panels--General Resources

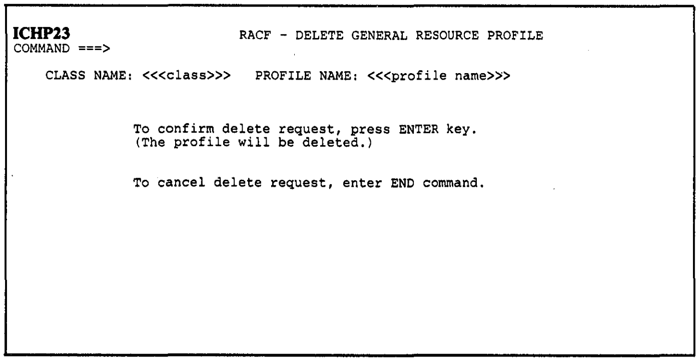
from previous page



```
ICHP223                  RACF - ADD/DELETE GENERAL RESOURCE TAPE VOLUMES
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER TYPE OF CHANGE REQUIRED:

    ACTION ===>                ADD or DELETE

ENTER VOLUMES TO BE ADDED OR DELETED:

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```

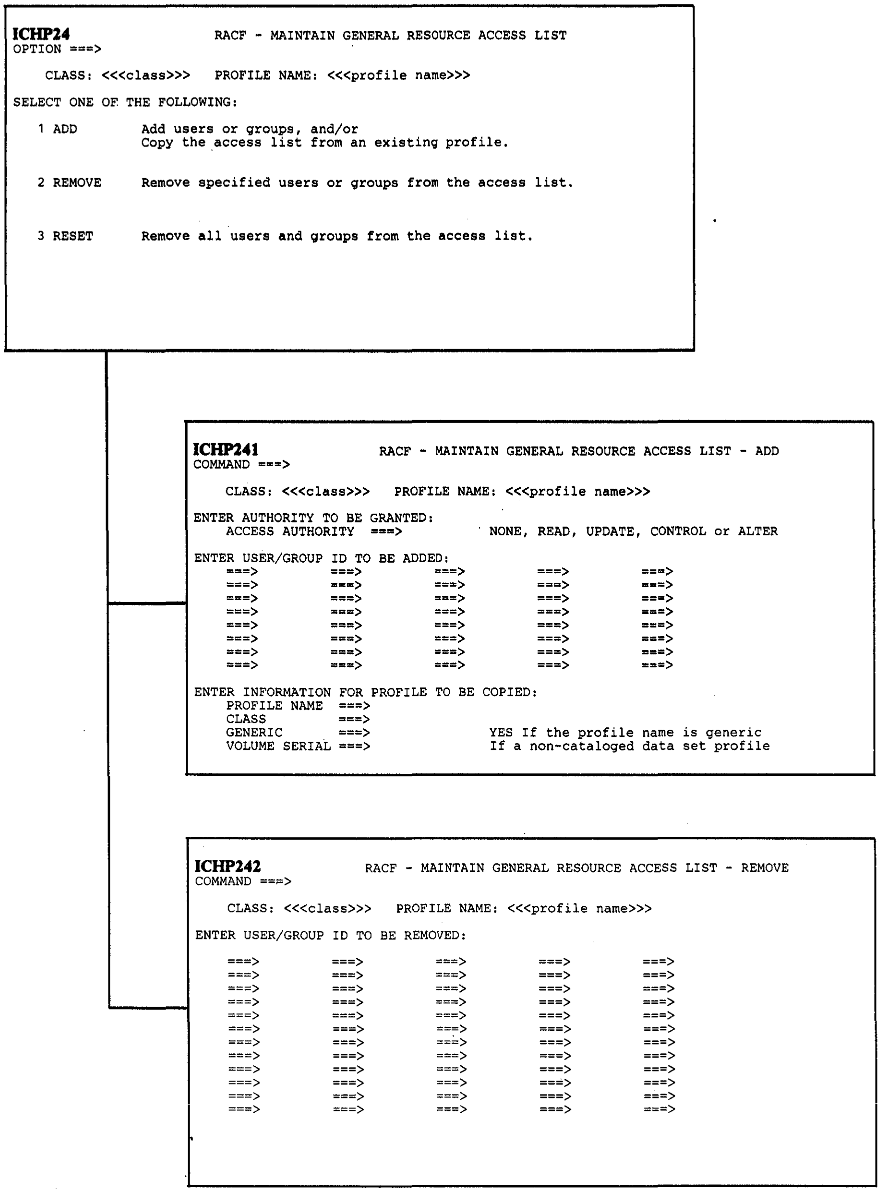
```
ICHP224                  RACF - ADD/DELETE GENERAL RESOURCE GROUP MEMBERS
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER TYPE OF CHANGE REQUIRED:

    ACTION ===>                ADD or DELETE

ENTER MEMBERS TO BE ADDED OR DELETED:

    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
    ===>
```

Figure 26. Change a Profile Panels--General Resources (Continued)



```
ICHP23                      RACF - DELETE GENERAL RESOURCE PROFILE
COMMAND ===>

    CLASS NAME: <<<class>>>   PROFILE NAME: <<<profile name>>>


               To confirm delete request, press ENTER key.
               (The profile will be deleted.)


               To cancel delete request, enter END command.
```

Figure 27. Delete a Profile Panel--General Resources

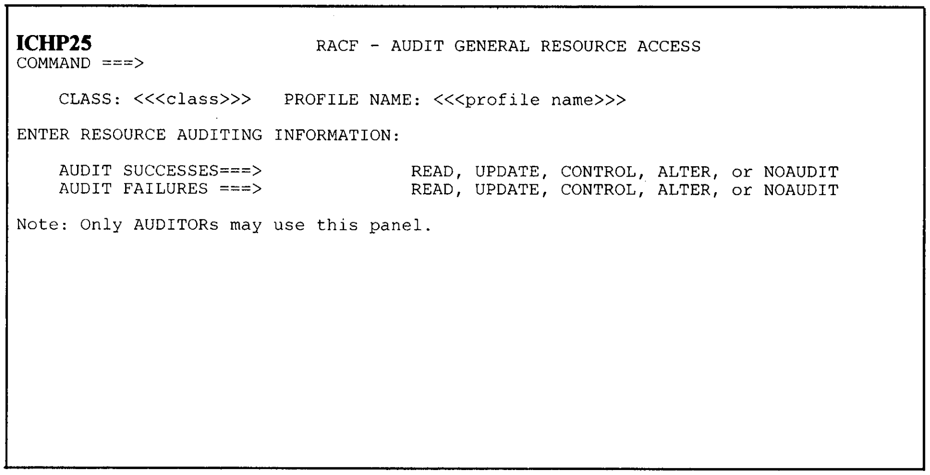


```
ICHP24                   RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST
OPTION ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

SELECT ONE OF THE FOLLOWING:

   1 ADD        Add users or groups, and/or
                Copy the access list from an existing profile.

   2 REMOVE     Remove specified users or groups from the access list.


   3 RESET      Remove all users and groups from the access list.
```

```
ICHP241                RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - ADD
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER AUTHORITY TO BE GRANTED:
    ACCESS AUTHORITY  ===>           NONE, READ, UPDATE, CONTROL or ALTER

ENTER USER/GROUP ID TO BE ADDED:
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>

ENTER INFORMATION FOR PROFILE TO BE COPIED:
    PROFILE NAME  ===>
    CLASS         ===>
    GENERIC       ===>               YES If the profile name is generic
    VOLUME SERIAL ===>               If a non-cataloged data set profile
```

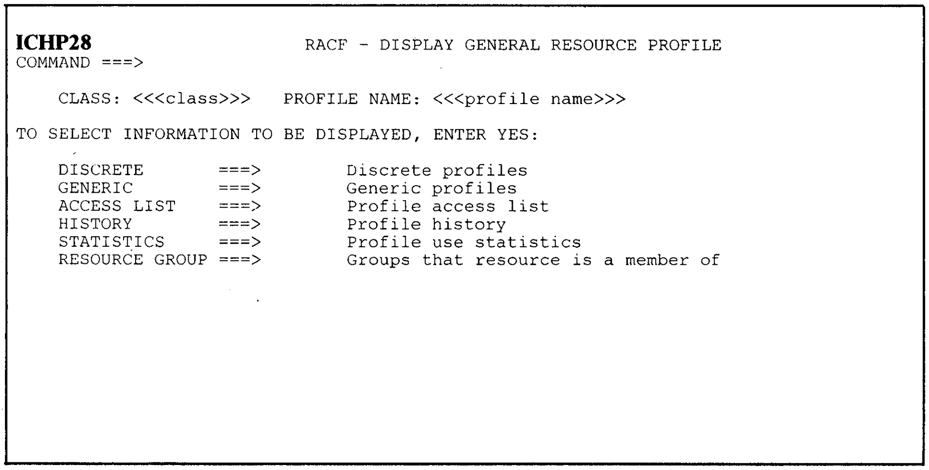
```
ICHP242              RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - REMOVE
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER USER/GROUP ID TO BE REMOVED:

    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
    ===>         ===>         ===>         ===>         ===>
```

Figure 28. Maintain Access List Panels--General Resources



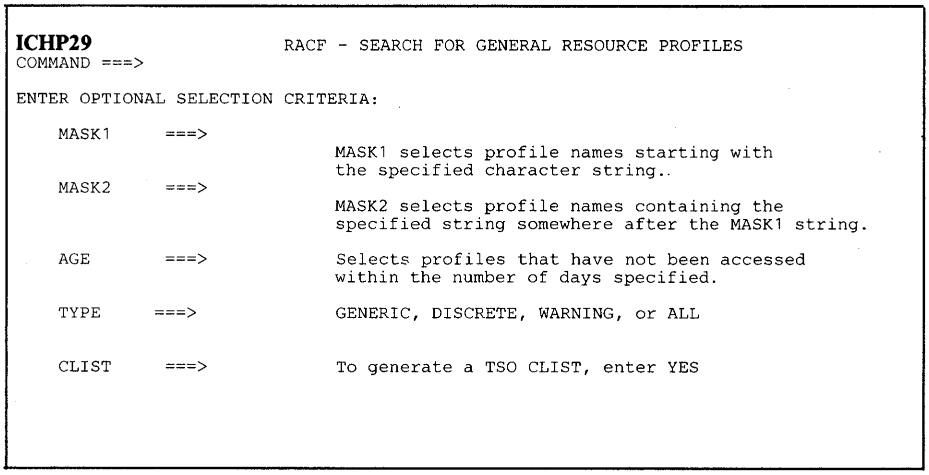
```
ICHP25                       RACF - AUDIT GENERAL RESOURCE ACCESS
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

ENTER RESOURCE AUDITING INFORMATION:

    AUDIT SUCCESSES===>             READ, UPDATE, CONTROL, ALTER, or NOAUDIT
    AUDIT FAILURES ===>             READ, UPDATE, CONTROL, ALTER, or NOAUDIT

Note: Only AUDITORs may use this panel.
```

Figure 29. Monitor Access Attempts Panel--General Resources



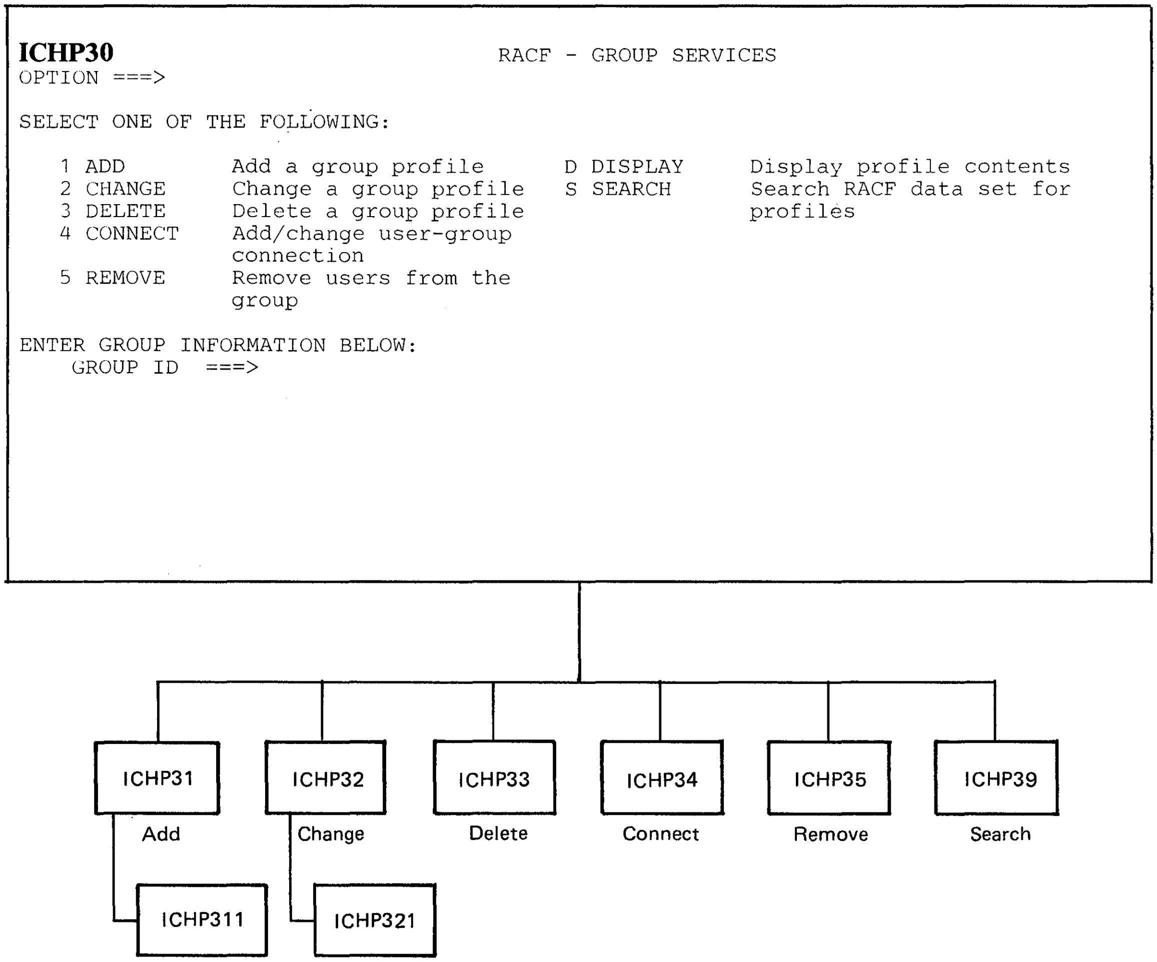
```
ICHP28                      RACF - DISPLAY GENERAL RESOURCE PROFILE
COMMAND ===>

    CLASS: <<<class>>>   PROFILE NAME: <<<profile name>>>

TO SELECT INFORMATION TO BE DISPLAYED, ENTER YES:

    DISCRETE       ===>       Discrete profiles
    GENERIC        ===>       Generic profiles
    ACCESS LIST    ===>       Profile access list
    HISTORY        ===>       Profile history
    STATISTICS     ===>       Profile use statistics
    RESOURCE GROUP ===>       Groups that resource is a member of
```

Figure 30. Display Profile Contents Panel--General Resources



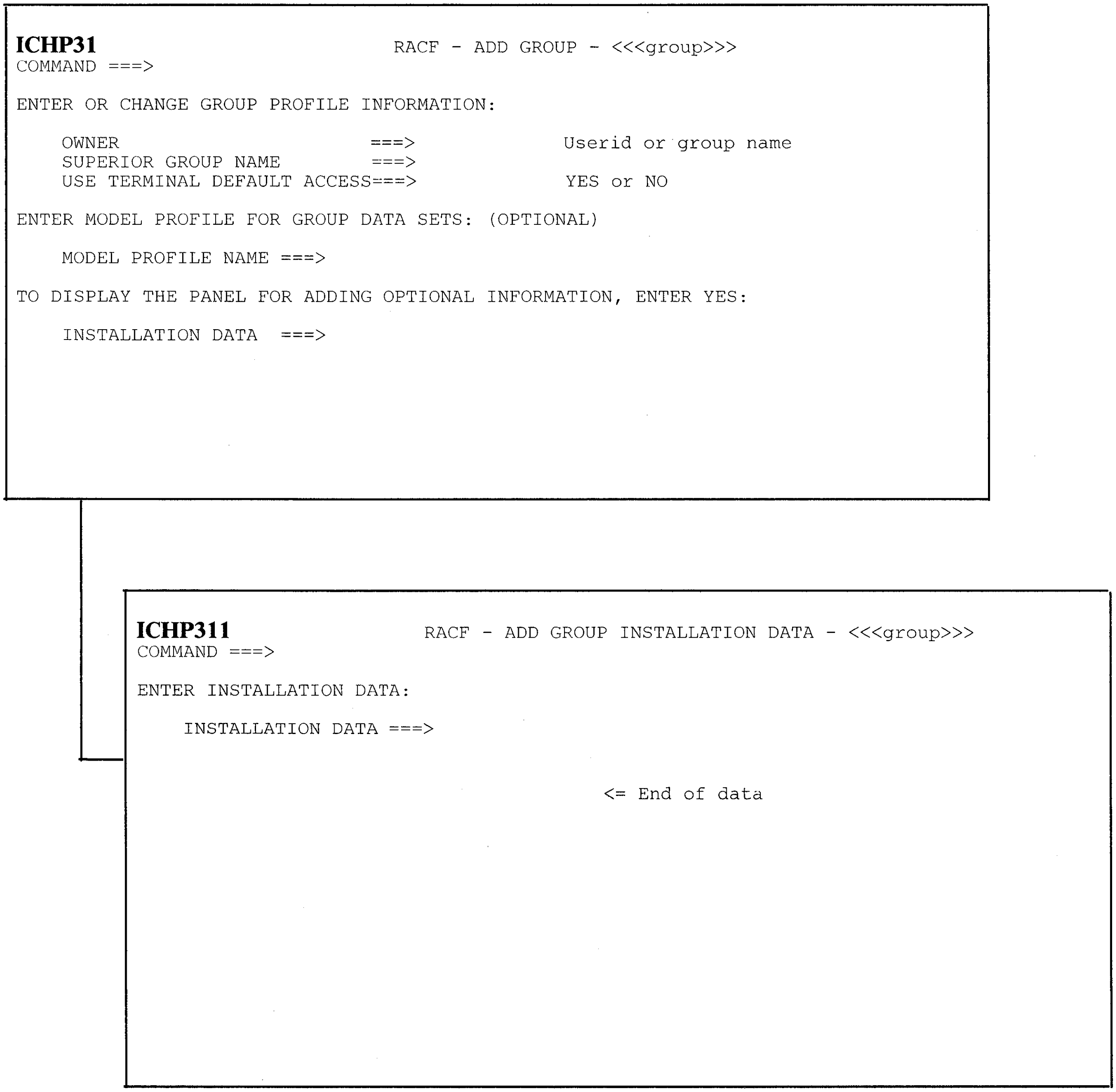
```
ICHP29                    RACF - SEARCH FOR GENERAL RESOURCE PROFILES
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

    MASK1     ===>
                              MASK1 selects profile names starting with
                              the specified character string..
    MASK2     ===>
                              MASK2 selects profile names containing the
                              specified string somewhere after the MASK1 string.

    AGE       ===>            Selects profiles that have not been accessed
                              within the number of days specified.

    TYPE     ===>             GENERIC, DISCRETE, WARNING, or ALL


    CLIST     ===>            To generate a TSO CLIST, enter YES
```

Figure 31. Search RACF Data Set for Profile Panel--General Resources



```
ICHP30                             RACF - GROUP SERVICES
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 ADD         Add a group profile      D DISPLAY     Display profile contents
   2 CHANGE      Change a group profile   S SEARCH      Search RACF data set for
   3 DELETE      Delete a group profile                 profiles
   4 CONNECT     Add/change user-group
                 connection
   5 REMOVE      Remove users from the
                 group

ENTER GROUP INFORMATION BELOW:
    GROUP ID  ===>
```

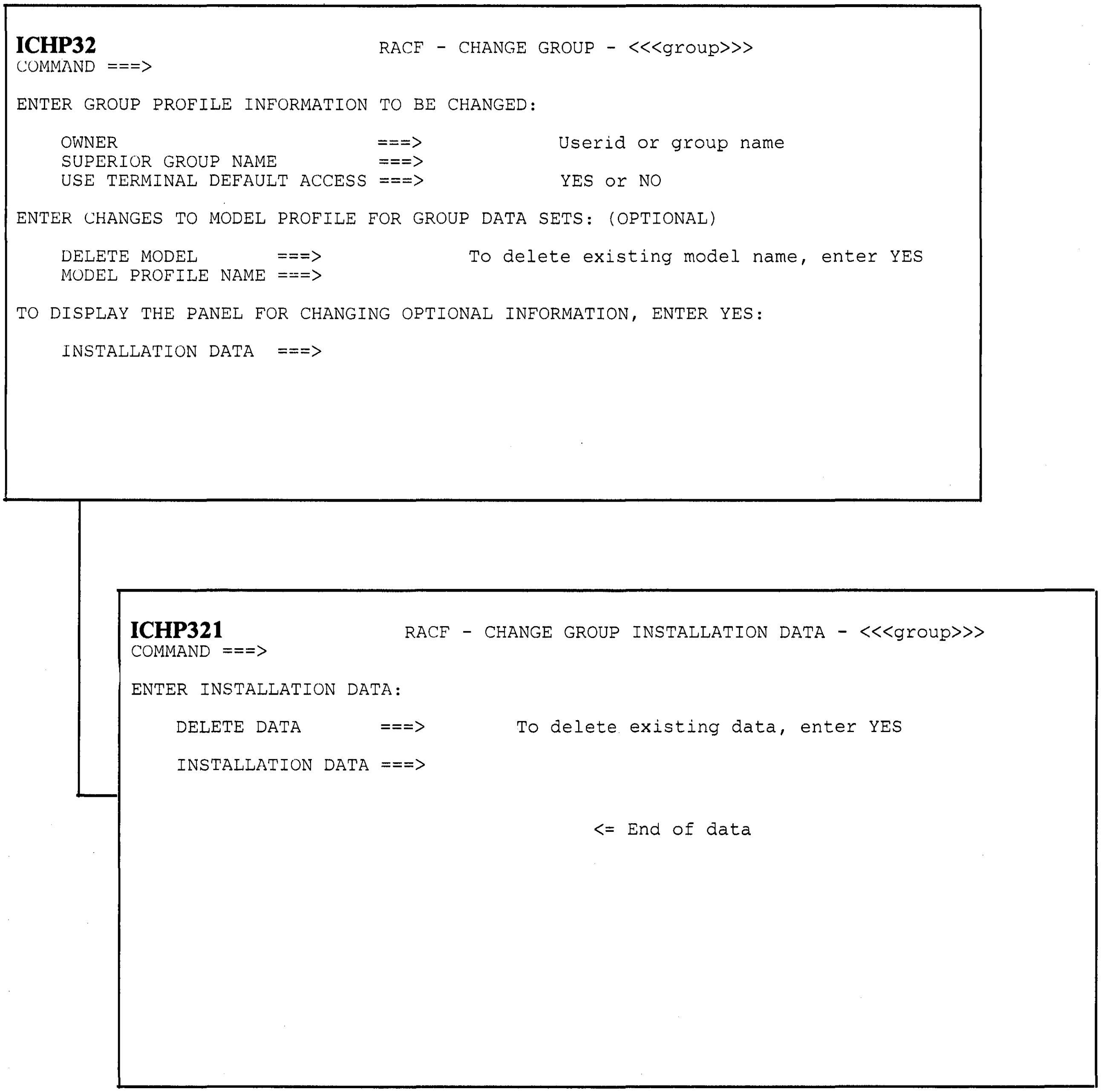
Figure 32. Group Services Panel



```
ICHP31                       RACF - ADD GROUP - <<<group>>>
COMMAND ===>

ENTER OR CHANGE GROUP PROFILE INFORMATION:

    OWNER                        ===>             Userid or group name
    SUPERIOR GROUP NAME          ===>
    USE TERMINAL DEFAULT ACCESS===>               YES or NO

ENTER MODEL PROFILE FOR GROUP DATA SETS: (OPTIONAL)

    MODEL PROFILE NAME ===>

TO DISPLAY THE PANEL FOR ADDING OPTIONAL INFORMATION, ENTER YES:

    INSTALLATION DATA  ===>
```

```
ICHP311                  RACF - ADD GROUP INSTALLATION DATA - <<<group>>>
COMMAND ===>

ENTER INSTALLATION DATA:

    INSTALLATION DATA ===>

                                              <= End of data
```

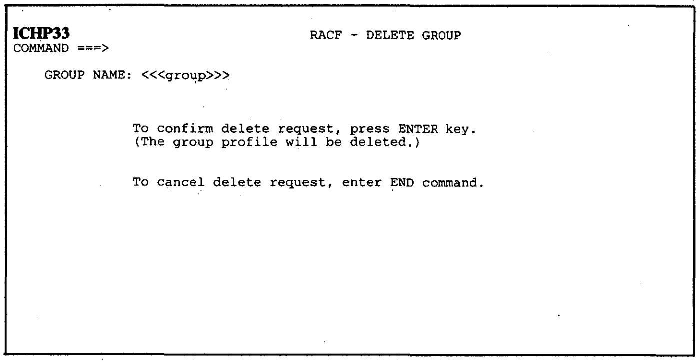
Figure 33. Add a Group Profile Panels



```
ICHP32                         RACF - CHANGE GROUP - <<<group>>>
COMMAND ===>

ENTER GROUP PROFILE INFORMATION TO BE CHANGED:

    OWNER                      ===>          Userid or group name
    SUPERIOR GROUP NAME        ===>
    USE TERMINAL DEFAULT ACCESS ===>         YES or NO

ENTER CHANGES TO MODEL PROFILE FOR GROUP DATA SETS: (OPTIONAL)

    DELETE MODEL       ===>             To delete existing model name, enter YES
    MODEL PROFILE NAME ===>

TO DISPLAY THE PANEL FOR CHANGING OPTIONAL INFORMATION, ENTER YES:

    INSTALLATION DATA  ===>
```

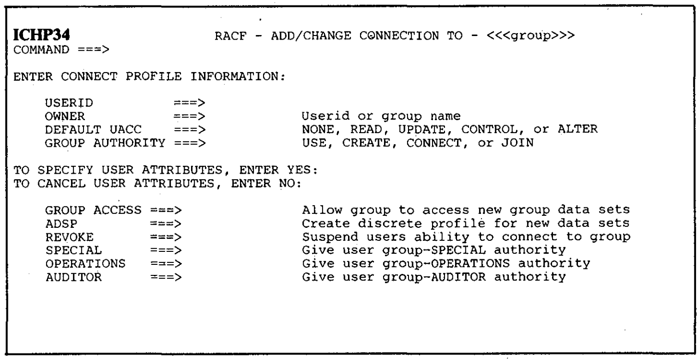
```
ICHP321                  RACF - CHANGE GROUP INSTALLATION DATA - <<<group>>>
COMMAND ===>

ENTER INSTALLATION DATA:

    DELETE DATA       ===>        To delete existing data, enter YES

    INSTALLATION DATA ===>

                                            <= End of data
```

Figure 34. Change a Group Profile Panels



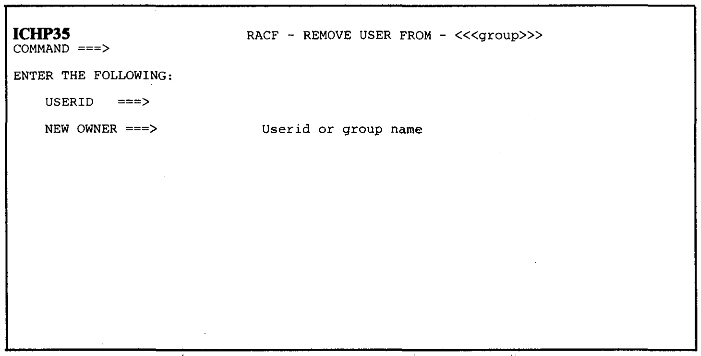
```
ICHP33                               RACF - DELETE GROUP
COMMAND ===>

    GROUP NAME: <<<group>>>


               To confirm delete request, press ENTER key.
               (The group profile will be deleted.)

               To cancel delete request, enter END command.
```

Figure 35. Delete a Group Profile Panel



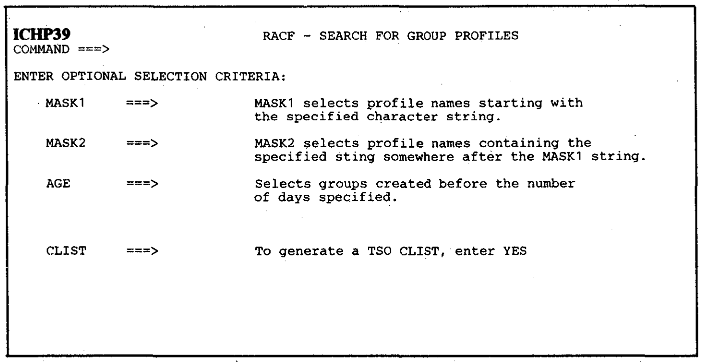
```
ICHP34                  RACF - ADD/CHANGE CONNECTION TO - <<<group>>>
COMMAND ===>

ENTER CONNECT PROFILE INFORMATION:

    USERID          ===>
    OWNER           ===>          Userid or group name
    DEFAULT UACC    ===>          NONE, READ, UPDATE, CONTROL, or ALTER
    GROUP AUTHORITY ===>          USE, CREATE, CONNECT, or JOIN

TO SPECIFY USER ATTRIBUTES, ENTER YES:
TO CANCEL USER ATTRIBUTES, ENTER NO:

    GROUP ACCESS ===>             Allow group to access new group data sets
    ADSP         ===>             Create discrete profile for new data sets
    REVOKE       ===>             Suspend users ability to connect to group
    SPECIAL      ===>             Give user group-SPECIAL authority
    OPERATIONS   ===>             Give user group-OPERATIONS authority
    AUDITOR      ===>             Give user group-AUDITOR authority
```

Figure 36. Add/Change User-Group Connection Panel



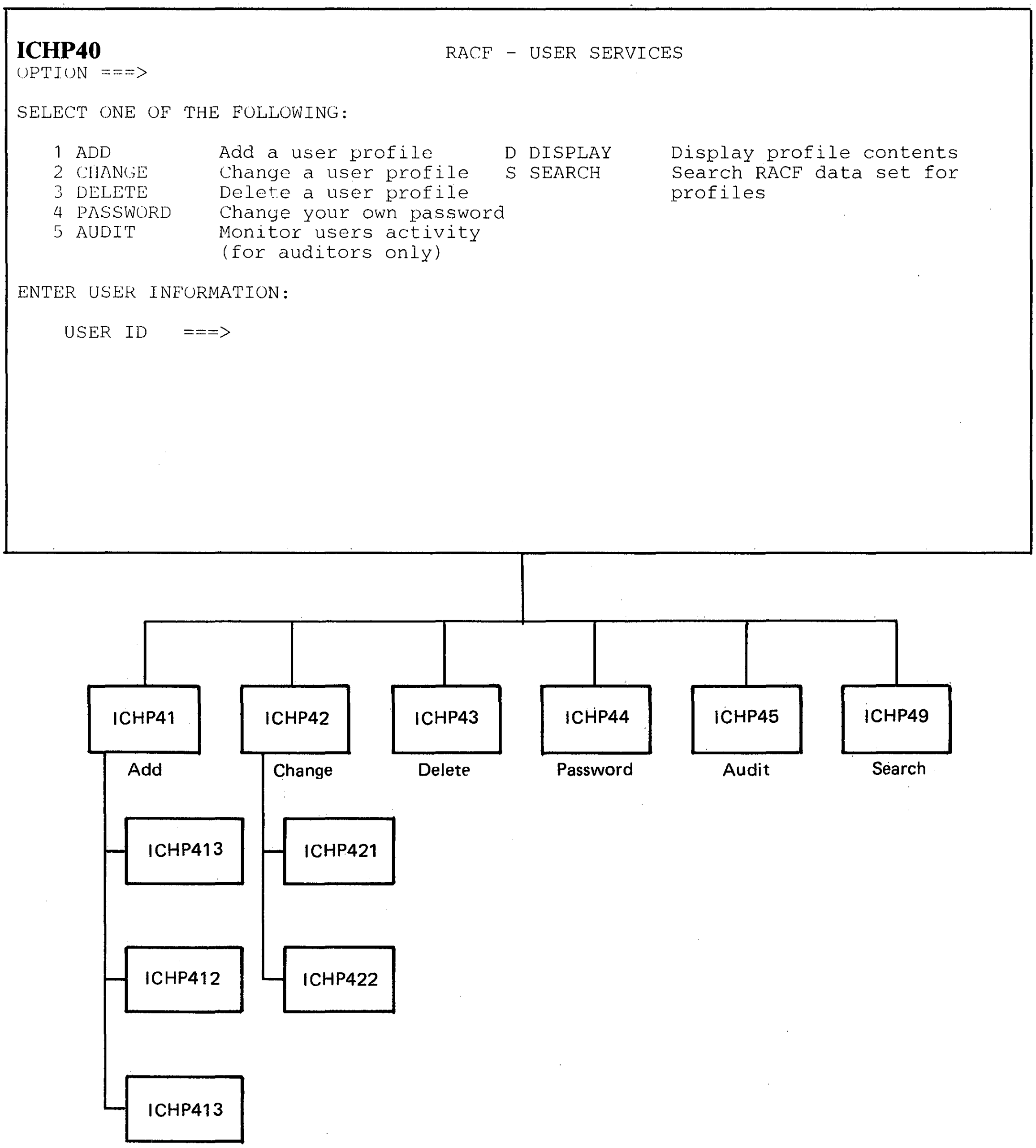
```
ICHP35                       RACF - REMOVE USER FROM - <<<group>>>
COMMAND ===>

ENTER THE FOLLOWING:

    USERID    ===>

    NEW OWNER ===>             Userid or group name
```

Figure 37. Remove Users from the Group Panel



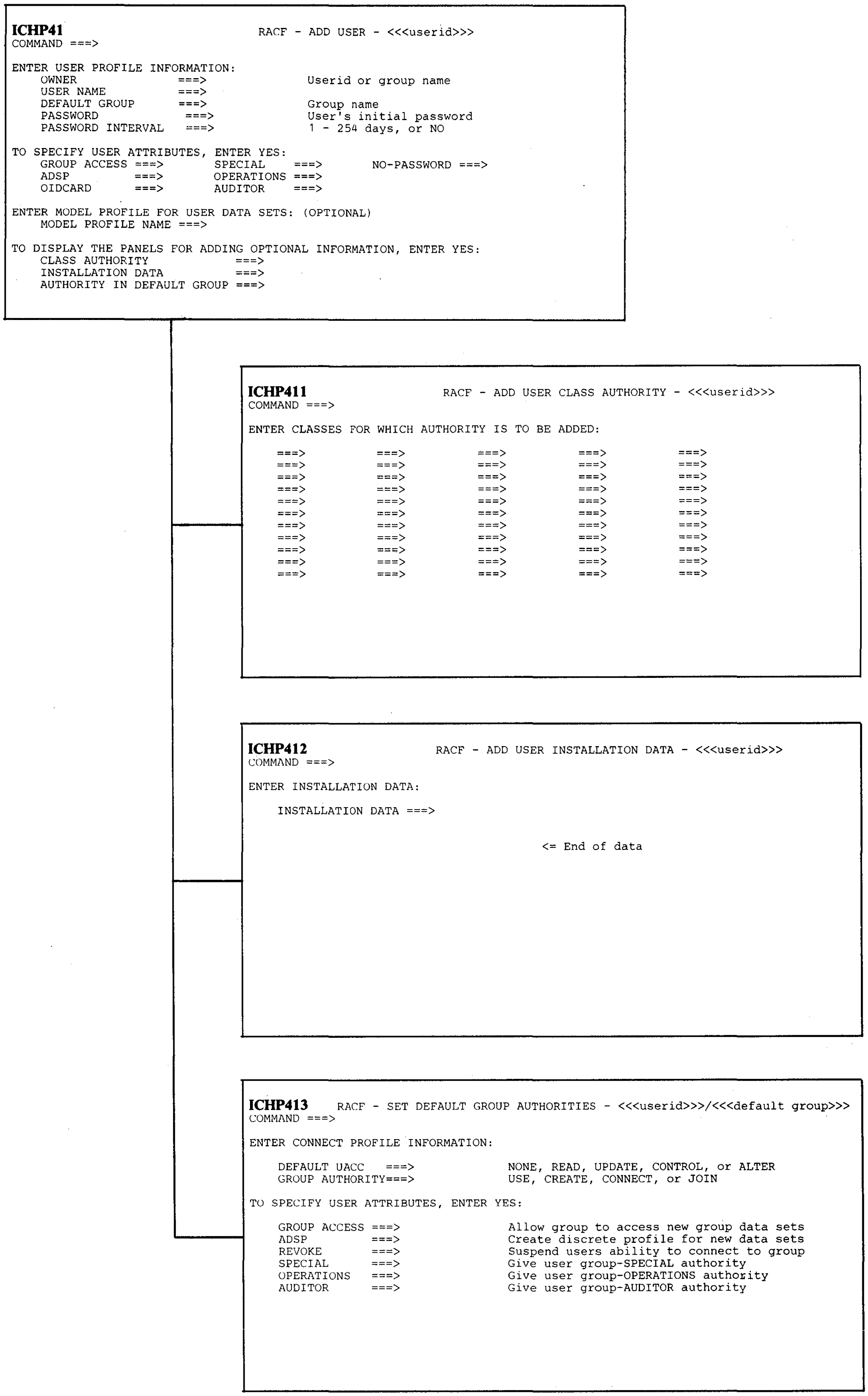
```
ICHP39                         RACF - SEARCH FOR GROUP PROFILES
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

    MASK1      ===>             MASK1 selects profile names starting with
                                the specified character string.

    MASK2      ===>             MASK2 selects profile names containing the
                                specified sting somewhere after the MASK1 string.

    AGE        ===>             Selects groups created before the number
                                of days specified.


    CLIST      ===>             To generate a TSO CLIST, enter YES
```

Figure 38. Search RACF Data Set for Profiles Panel



```
ICHP40                               RACF - USER SERVICES
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 ADD          Add a user profile       D DISPLAY     Display profile contents
   2 CHANGE       Change a user profile    S SEARCH      Search RACF data set for
   3 DELETE       Delete a user profile                  profiles
   4 PASSWORD     Change your own password
   5 AUDIT        Monitor users activity
                  (for auditors only)

ENTER USER INFORMATION:

    USER ID   ===>
```

Figure 39. User Services Panel



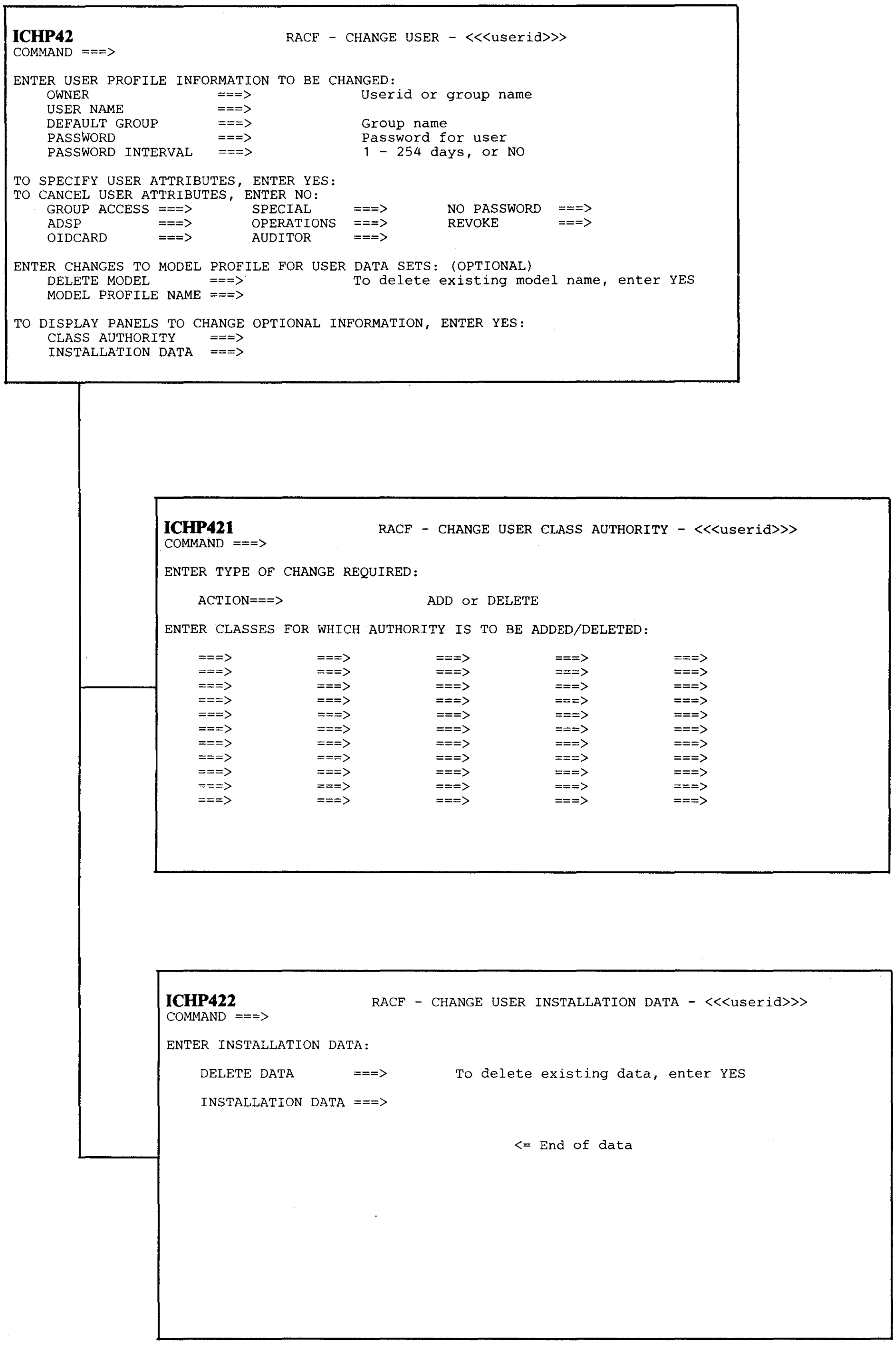
```
ICHP41                          RACF - ADD USER - <<<userid>>>
COMMAND ===>

ENTER USER PROFILE INFORMATION:
    OWNER              ===>              Userid or group name
    USER NAME          ===>
    DEFAULT GROUP      ===>              Group name
    PASSWORD            ===>             User's initial password
    PASSWORD INTERVAL   ===>             1 - 254 days, or NO

TO SPECIFY USER ATTRIBUTES, ENTER YES:
    GROUP ACCESS ===>       SPECIAL    ===>       NO-PASSWORD ===>
    ADSP         ===>       OPERATIONS ===>
    OIDCARD      ===>       AUDITOR    ===>

ENTER MODEL PROFILE FOR USER DATA SETS: (OPTIONAL)
    MODEL PROFILE NAME ===>

TO DISPLAY THE PANELS FOR ADDING OPTIONAL INFORMATION, ENTER YES:
    CLASS AUTHORITY            ===>
    INSTALLATION DATA          ===>
    AUTHORITY IN DEFAULT GROUP ===>
```

```
ICHP411                    RACF - ADD USER CLASS AUTHORITY - <<<userid>>>
COMMAND ===>

ENTER CLASSES FOR WHICH AUTHORITY IS TO BE ADDED:

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```

```
ICHP412                   RACF - ADD USER INSTALLATION DATA - <<<userid>>>
COMMAND ===>

ENTER INSTALLATION DATA:

    INSTALLATION DATA ===>

                                        <= End of data
```

```
ICHP413    RACF - SET DEFAULT GROUP AUTHORITIES - <<<userid>>>/<<<default group>>>
COMMAND ===>

ENTER CONNECT PROFILE INFORMATION:

    DEFAULT UACC    ===>             NONE, READ, UPDATE, CONTROL, or ALTER
    GROUP AUTHORITY===>              USE, CREATE, CONNECT, or JOIN

TO SPECIFY USER ATTRIBUTES, ENTER YES:

    GROUP ACCESS ===>                Allow group to access new group data sets
    ADSP         ===>                Create discrete profile for new data sets
    REVOKE       ===>                Suspend users ability to connect to group
    SPECIAL      ===>                Give user group-SPECIAL authority
    OPERATIONS   ===>                Give user group-OPERATIONS authority
    AUDITOR      ===>                Give user group-AUDITOR authority
```

Figure 40. Add a User Profile Panels



ICHP42

```
                                RACF - CHANGE USER - <<<userid>>>
COMMAND ===>

ENTER USER PROFILE INFORMATION TO BE CHANGED:
    OWNER               ===>            Userid or group name
    USER NAME           ===>
    DEFAULT GROUP       ===>            Group name
    PASSWORD            ===>            Password for user
    PASSWORD INTERVAL   ===>            1 - 254 days, or NO

TO SPECIFY USER ATTRIBUTES, ENTER YES:
TO CANCEL USER ATTRIBUTES, ENTER NO:
    GROUP ACCESS ===>       SPECIAL      ===>       NO PASSWORD  ===>
    ADSP         ===>       OPERATIONS   ===>       REVOKE       ===>
    OIDCARD      ===>       AUDITOR      ===>

ENTER CHANGES TO MODEL PROFILE FOR USER DATA SETS: (OPTIONAL)
    DELETE MODEL       ===>            To delete existing model name, enter YES
    MODEL PROFILE NAME ===>

TO DISPLAY PANELS TO CHANGE OPTIONAL INFORMATION, ENTER YES:
    CLASS AUTHORITY    ===>
    INSTALLATION DATA  ===>
```

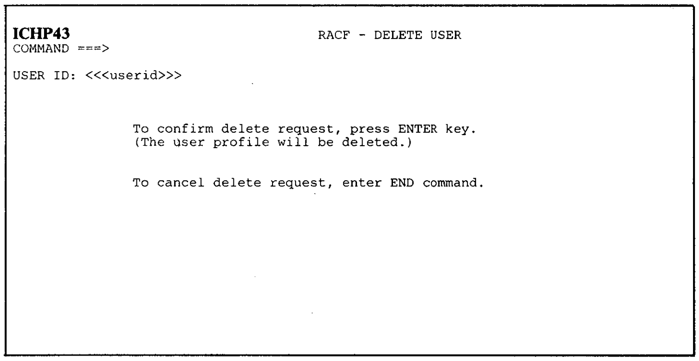
ICHP421

```
                         RACF - CHANGE USER CLASS AUTHORITY - <<<userid>>>
COMMAND ===>

ENTER TYPE OF CHANGE REQUIRED:

    ACTION===>                   ADD or DELETE

ENTER CLASSES FOR WHICH AUTHORITY IS TO BE ADDED/DELETED:

    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
    ===>          ===>          ===>          ===>          ===>
```

ICHP422

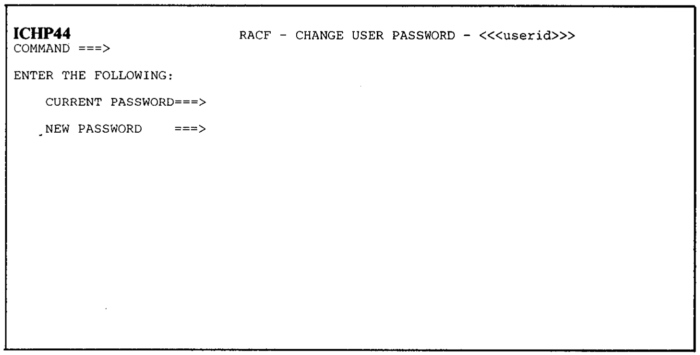
```
                        RACF - CHANGE USER INSTALLATION DATA - <<<userid>>>
COMMAND ===>

ENTER INSTALLATION DATA:

    DELETE DATA       ===>        To delete existing data, enter YES

    INSTALLATION DATA ===>

                                            <= End of data
```

Figure 41. Change a User Profile Panels



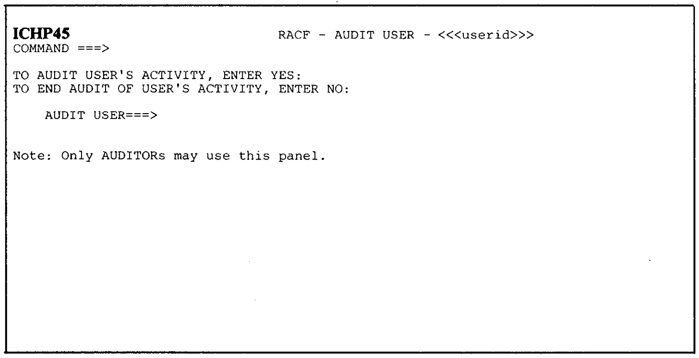
```
ICHP43                               RACF - DELETE USER
COMMAND ===>

USER ID: <<<userid>>>



               To confirm delete request, press ENTER key.
               (The user profile will be deleted.)


               To cancel delete request, enter END command.
```

Figure 42. Delete a User Profile Panel



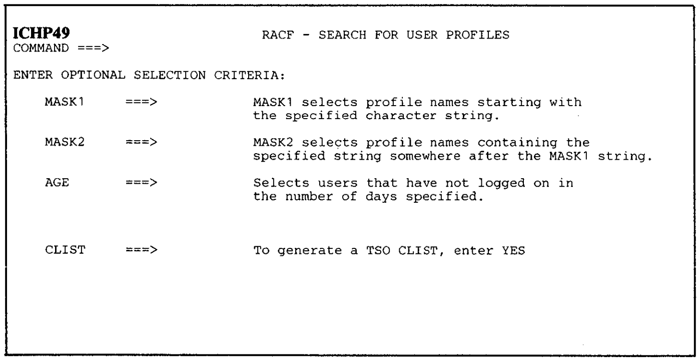
```
ICHP44                      RACF - CHANGE USER PASSWORD - <<<userid>>>
COMMAND ===>

ENTER THE FOLLOWING:

    CURRENT PASSWORD===>

    NEW PASSWORD    ===>
```

Figure 43. Change Your Own Password Panel



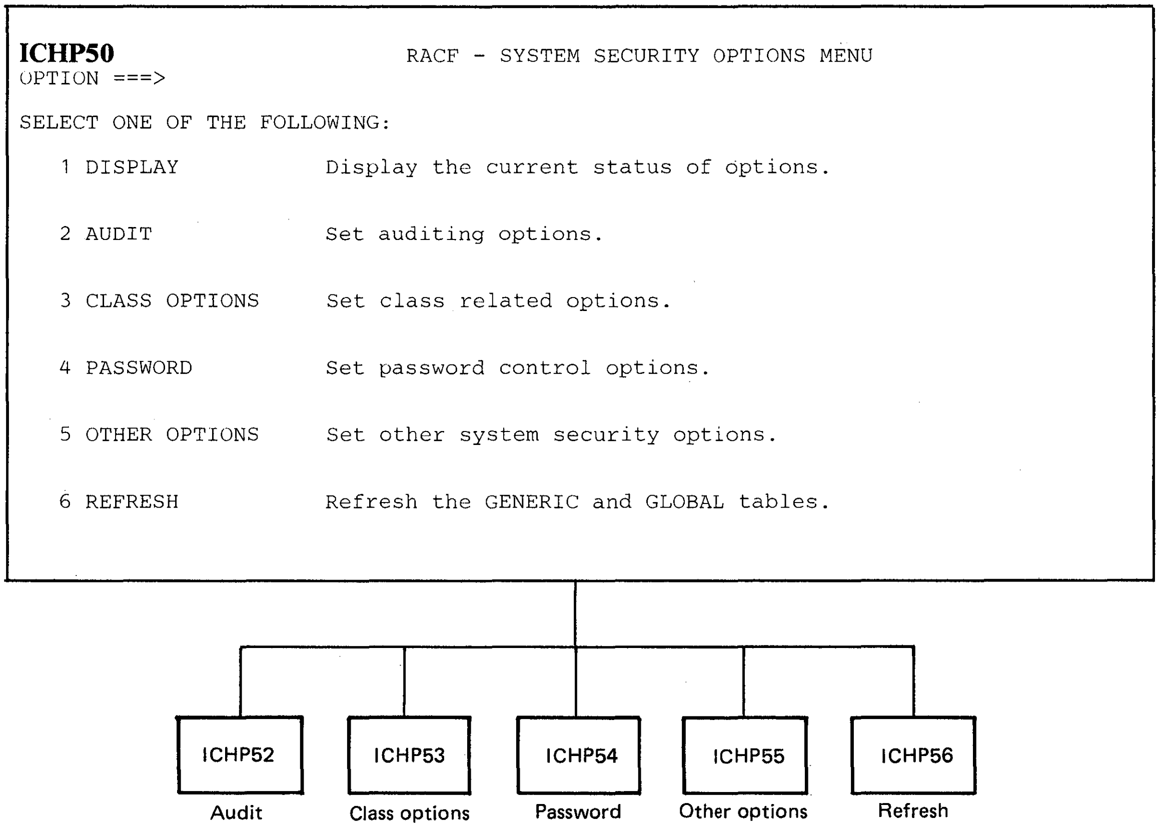
```
ICHP45                           RACF - AUDIT USER - <<<userid>>>
COMMAND ===>

TO AUDIT USER'S ACTIVITY, ENTER YES:
TO END AUDIT OF USER'S ACTIVITY, ENTER NO:

    AUDIT USER===>


Note: Only AUDITORs may use this panel.
```

Figure 44. Monitor Users Activity Panel



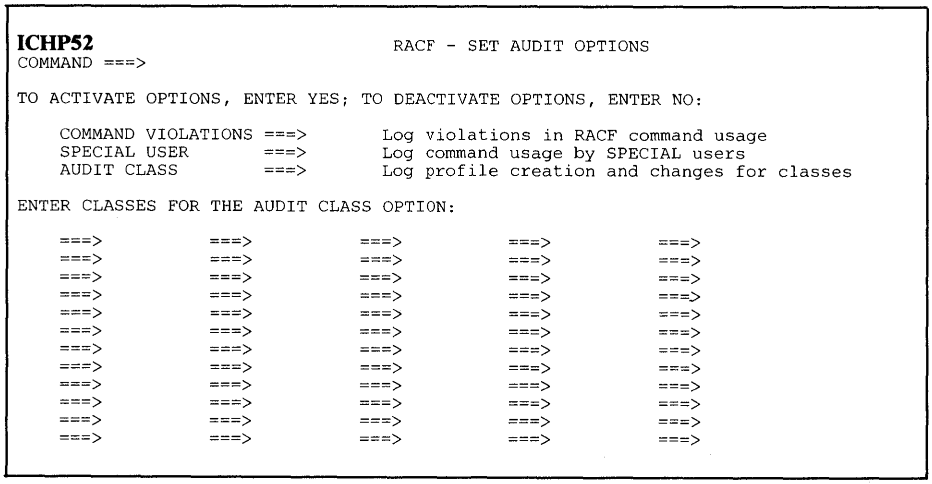
```
ICHP49                         RACF - SEARCH FOR USER PROFILES
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

    MASK1     ===>            MASK1 selects profile names starting with
                              the specified character string.

    MASK2     ===>            MASK2 selects profile names containing the
                              specified string somewhere after the MASK1 string.

    AGE       ===>            Selects users that have not logged on in
                              the number of days specified.


    CLIST     ===>            To generate a TSO CLIST, enter YES
```

Figure 45. Search RACF Data Set for Profile Panel



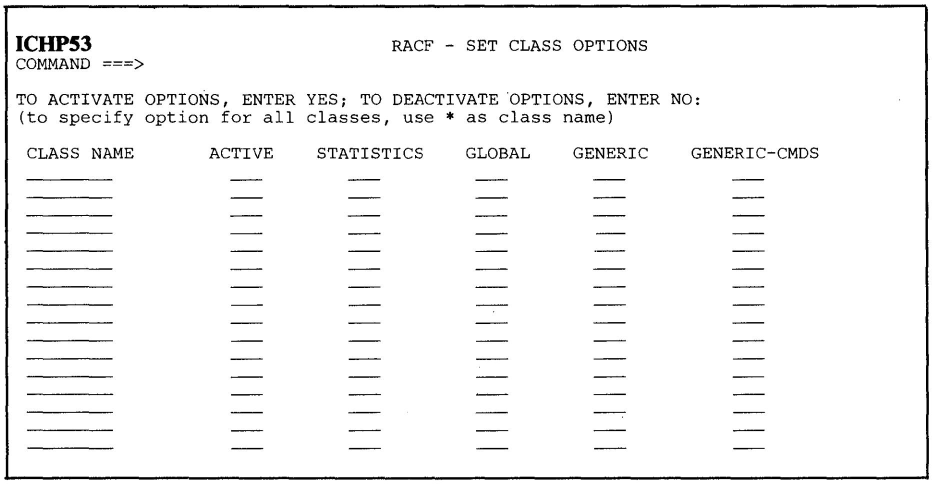
```
ICHP50                        RACF - SYSTEM SECURITY OPTIONS MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 DISPLAY           Display the current status of options.

   2 AUDIT             Set auditing options.

   3 CLASS OPTIONS     Set class related options.

   4 PASSWORD          Set password control options.

   5 OTHER OPTIONS     Set other system security options.

   6 REFRESH           Refresh the GENERIC and GLOBAL tables.
```

Figure 46. System Security Options Menu Panel



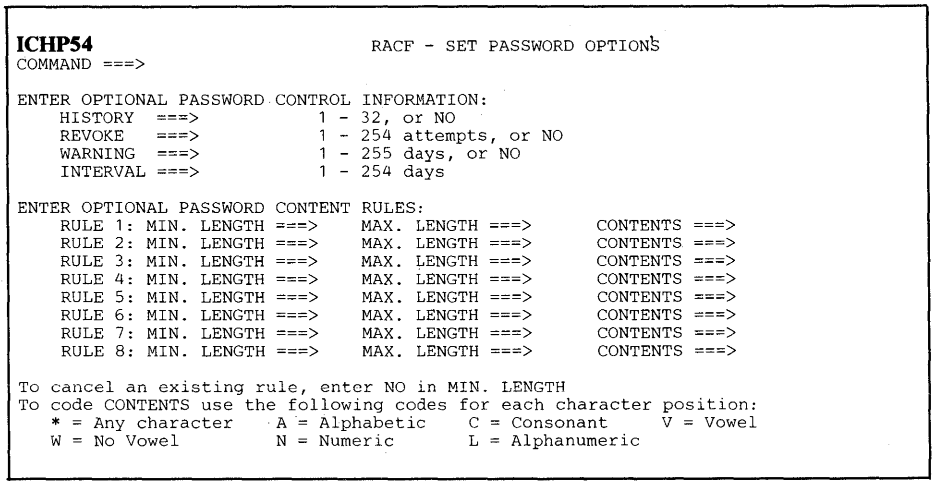
```
ICHP52                        RACF - SET AUDIT OPTIONS
COMMAND ===>

TO ACTIVATE OPTIONS, ENTER YES; TO DEACTIVATE OPTIONS, ENTER NO:

   COMMAND VIOLATIONS ===>      Log violations in RACF command usage
   SPECIAL USER       ===>      Log command usage by SPECIAL users
   AUDIT CLASS        ===>      Log profile creation and changes for classes

ENTER CLASSES FOR THE AUDIT CLASS OPTION:

   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
   ===>          ===>          ===>          ===>          ===>
```

Figure 47. Set Auditing Options Panel



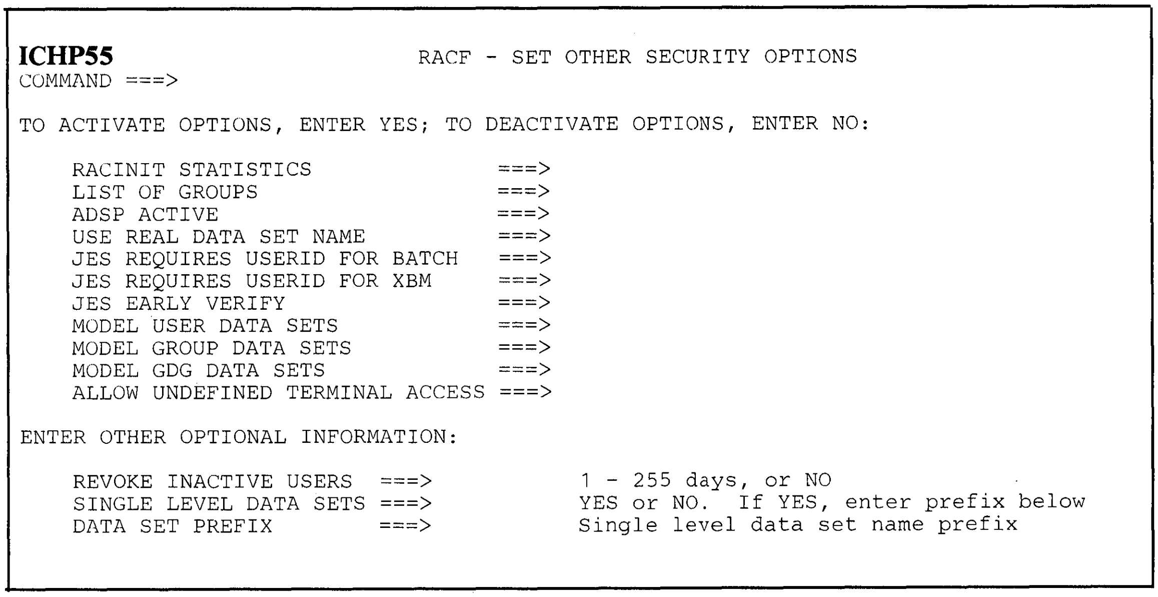
```
ICHP53                        RACF - SET CLASS OPTIONS
COMMAND ===>

TO ACTIVATE OPTIONS, ENTER YES; TO DEACTIVATE OPTIONS, ENTER NO:
(to specify option for all classes, use * as class name)

 CLASS NAME       ACTIVE    STATISTICS    GLOBAL    GENERIC    GENERIC-CMDS
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
 ________         ___         ___          ___        ___          ___
```

Figure 48. Set Class Related Options Panel



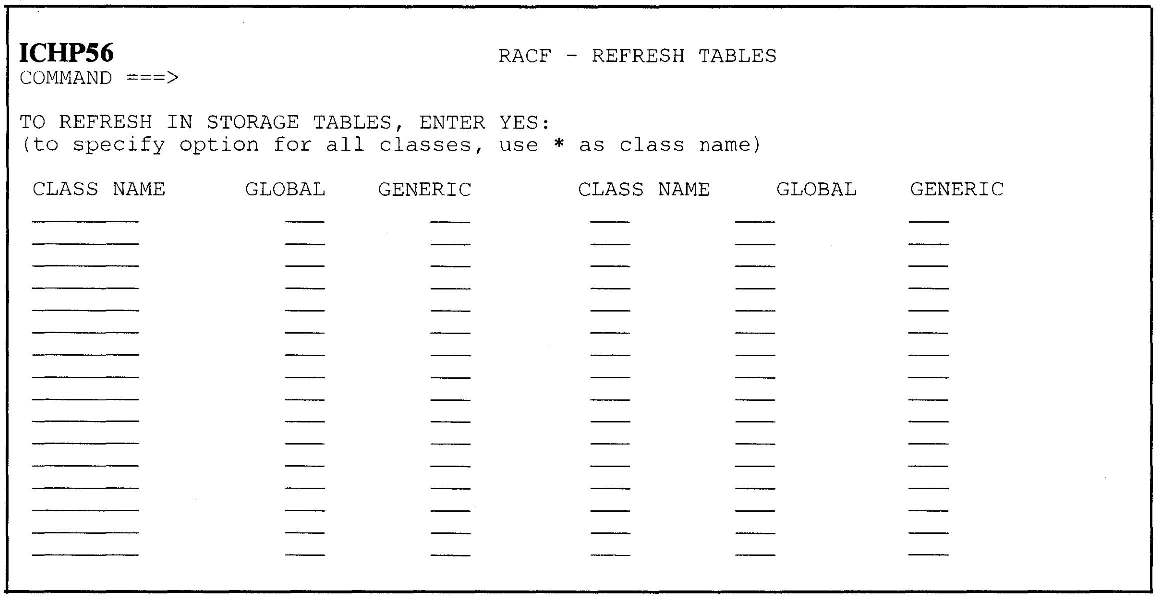
```
ICHP54                      RACF - SET PASSWORD OPTIONS
COMMAND ===>

ENTER OPTIONAL PASSWORD CONTROL INFORMATION:
    HISTORY  ===>          1 - 32, or NO
    REVOKE   ===>          1 - 254 attempts, or NO
    WARNING  ===>          1 - 255 days, or NO
    INTERVAL ===>          1 - 254 days

ENTER OPTIONAL PASSWORD CONTENT RULES:
    RULE 1: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 2: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 3: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 4: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 5: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 6: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 7: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>
    RULE 8: MIN. LENGTH ===>    MAX. LENGTH ===>      CONTENTS ===>

To cancel an existing rule, enter NO in MIN. LENGTH
To code CONTENTS use the following codes for each character position:
   * = Any character    A = Alphabetic    C = Consonant     V = Vowel
   W = No Vowel         N = Numeric       L = Alphanumeric
```

Figure 49. Set Password Control Options Panel



```
ICHP55                         RACF - SET OTHER SECURITY OPTIONS
COMMAND ===>

TO ACTIVATE OPTIONS, ENTER YES; TO DEACTIVATE OPTIONS, ENTER NO:

    RACINIT STATISTICS               ===>
    LIST OF GROUPS                   ===>
    ADSP ACTIVE                      ===>
    USE REAL DATA SET NAME           ===>
    JES REQUIRES USERID FOR BATCH    ===>
    JES REQUIRES USERID FOR XBM      ===>
    JES EARLY VERIFY                 ===>
    MODEL USER DATA SETS             ===>
    MODEL GROUP DATA SETS            ===>
    MODEL GDG DATA SETS              ===>
    ALLOW UNDEFINED TERMINAL ACCESS ===>

ENTER OTHER OPTIONAL INFORMATION:

    REVOKE INACTIVE USERS  ===>        1 - 255 days, or NO
    SINGLE LEVEL DATA SETS ===>        YES or NO.  If YES, enter prefix below
    DATA SET PREFIX        ===>        Single level data set name prefix
```

Figure 50. Set Other System Security Options Panel



```
ICHP56                               RACF - REFRESH TABLES
COMMAND ===>

TO REFRESH IN STORAGE TABLES, ENTER YES:
(to specify option for all classes, use * as class name)

 CLASS NAME       GLOBAL    GENERIC        CLASS NAME     GLOBAL     GENERIC
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
 ________            ___         ___         ___          ___           ___
```

Figure 51. Refresh the GENERIC and GLOBAL Tables

Index

MVS Resource Access Control Facility (RACF)
Command Language Reference
SC28-0733-5

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. This form may be used to communicate your views about this publication. They will be sent to the author's department for whatever review and action, if any, is deemed appropriate.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comments are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If comments apply to a Selectable Unit, please provide the name of the Selectable Unit ________.

If you wish a reply, give your name and mailing address:

____

____

____

What is your occupation? ________________________________

How do you use this publication? ________________________________

Number of latest Newsletter associated with this publication: ________________

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments.)

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

SC28-0733-5

Reader's Comment Form

Fold and tape

Please Do Not Staple

Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape

Please Do Not Staple

Fold and tape

Cut or Fold Along Line

MVS Resource Access Control Facility (RACF) Command Language Reference Printed in U.S.A. SC28-0733-5

MVS Resource Access Control Facility (RACF)
Command Language Reference
SC28-0733-5

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. This form may be used to communicate your views about this publication. They will be sent to the author's department for whatever review and action, if any, is deemed appropriate.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comments are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If comments apply to a Selectable Unit, please provide the name of the Selectable Unit ________.

If you wish a reply, give your name and mailing address:

____

____

____

What is your occupation? ________________________________

How do you use this publication? ________________________________

Number of latest Newsletter associated with this publication: ________________

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments.)

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

SC28-0733-5

Reader's Comment Form

Cut or Fold Along Line

Fold and tape

Please Do Not Staple

Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS PERMIT 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape

Please Do Not Staple

Fold and tape

IBM®

MVS Resource Access Control Facility (RACF)
Command Language Reference
SC28-0733-5

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. This form may be used to communicate your views about this publication. They will be sent to the author's department for whatever review and action, if any, is deemed appropriate.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation whatever. You may, of course, continue to use the information you supply.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comments are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If comments apply to a Selectable Unit, please provide the name of the Selectable Unit ________.

If you wish a reply, give your name and mailing address:

____

____

____

What is your occupation? ____

How do you use this publication? ____

Number of latest Newsletter associated with this publication: ____________________

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments.)

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

SC28-0733-5

Reader's Comment Form

Fold and tape   Please Do Not Staple   Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS   PERMIT 40   ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE:

International Business Machines Corporation
Department D58, Building 920-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape   Please Do Not Staple   Fold and tape

IBM®

Cut or Fold Along Line