Resource Access Control Facility (RACF) General User's Guide

SC28-1341-3

Production of this Book

This book was prepared and formatted using the BookMaster® document markup language.

Fourth Edition (December, 1988)

This is a major revision of, and obsoletes, SC28-1341-3 and Technical Newsletter SN28-1218. See the Summary of Changes following the Edition Notice for a summary of the changes 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 Releases 8.1 and 8.2 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 or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product in this publication is not intended to state or imply that only IBM's product may be used. Any functionally equivalent product may be used instead. This statement does not expressly or implicitly waive any intellectual property right IBM may hold in any product mentioned herein.

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 921-2, PO Box 390, Poughkeepsie, NY 12602. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

About this Book

This book is for users who need to use RACF to protect their own data sets or minidisks. You can also use this book if you are responsible for the security of a group data set or minidisk.

If you need information on working with resources other than data sets or minidisks, users, or groups of users, see the *RACF Security Administrator's Guide*, SC28-1340. If you need information on auditing (such as how to use the RACF report writer), see the *RACF Auditor's Guide*, SC28-1342. If you need more information on RACF concepts, see *RACF General Information*, GC28-0722. For other information about RACF, see the publications described in Figure 1-1 on page ix.

This book assumes that you know how to conduct a terminal session on your system.

To use RACF on MVS, you must:

- Know how to conduct a TSO terminal session
- Know how to enter commands or use ISPF panels
- Be RACF-defined.

To find out more about a TSO terminal session, see the *TSO/E Primer*, GC28-1292.

To use RACF on VM, you must:

- Know how to conduct a CMS terminal session
- Know how to enter commands or use ISPF panels
- Be RACF-defined.

To find out more about a CMS terminal session, see the *VM/SP CMS Primer*, SC24-5236, or the *VM/XA CMS Primer*, SC23-0368.

Trademarks

The following are trademarks of International Business Machines Corporation.

- MVS/ESA™
- MVS/XA™
- MVS/SP™

How to Use This Book

To use this book, first decide what operating system you are working on, then decide whether you prefer RACF commands or ISPF panels.

If you are using MVS (TSO) and prefer commands, use Chapter 1.

If you are using MVS (TSO) and prefer ISPF panels, use Chapter 2.

If you are using VM and prefer commands, use Chapter 3.

If you are using VM and prefer ISPF panels, use Chapter 4.

Each chapter contains step-by-step procedures, which are written so that they require no previous experience with RACF. In general, each task is repeated in each of the chapters.

Do You Have Problems, Comments, or Suggestions?

Your suggestions and ideas can contribute to the quality and the usability of this book. If you have problems using this book, or if you have suggestions for improving it, complete and mail the Reader's Comment Form found at the back of the book.

The RACF Library

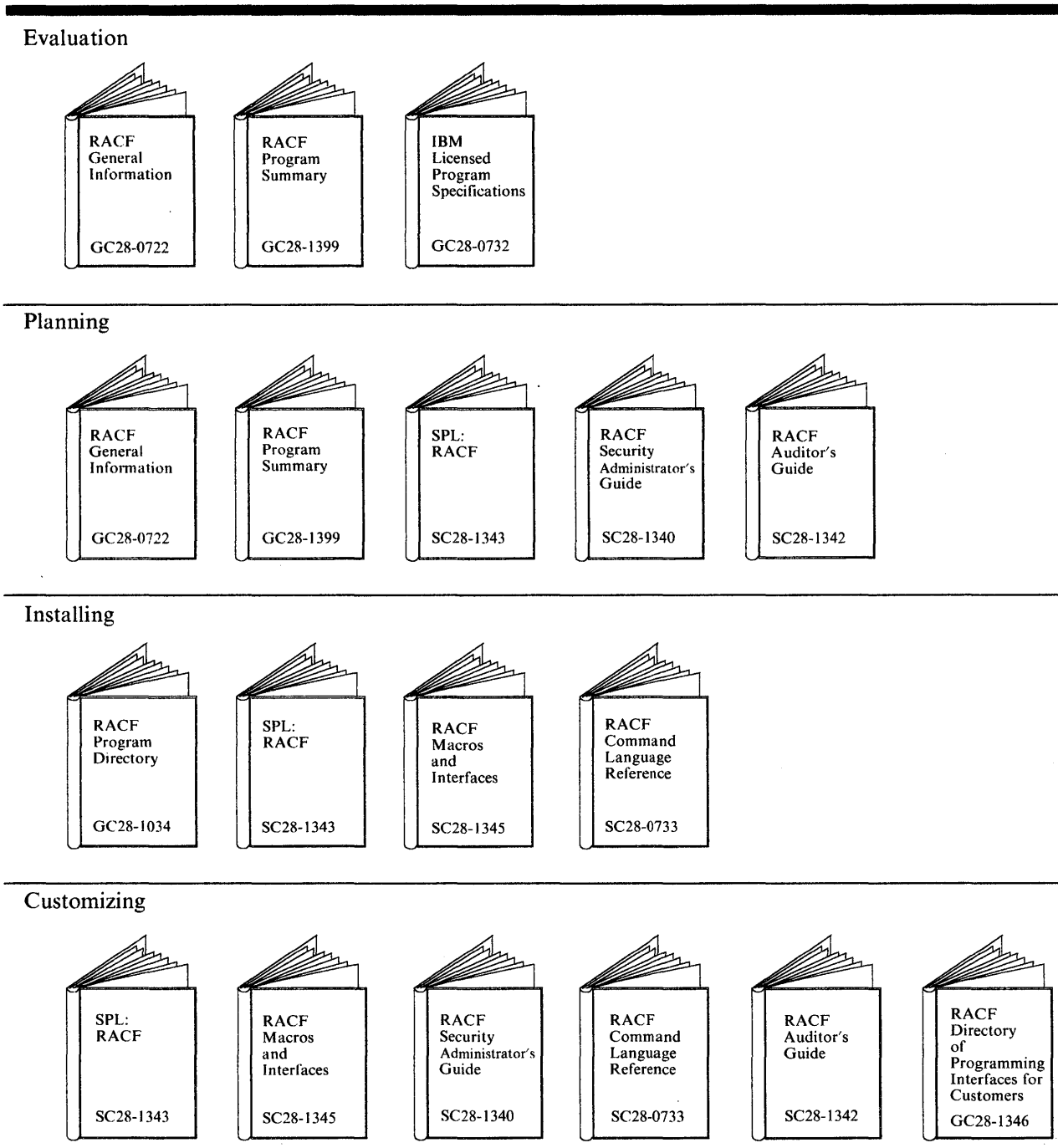
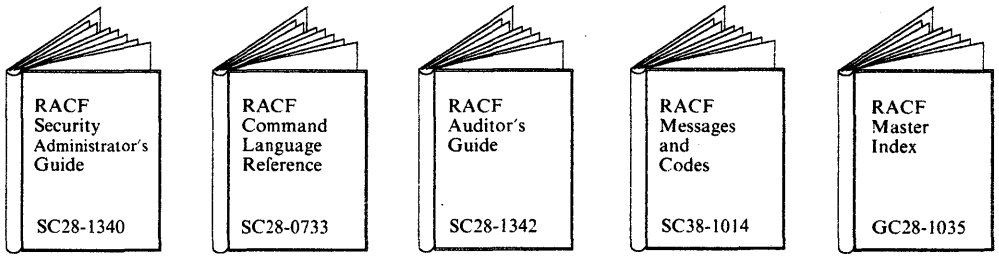
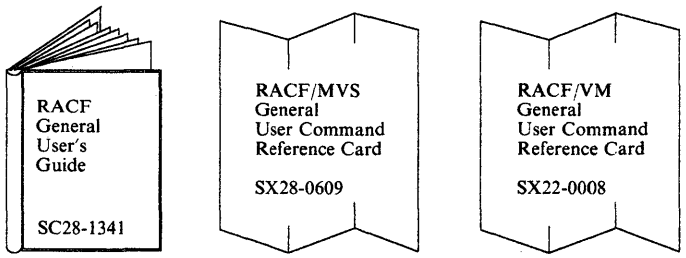


Figure 1-1 (Part 1 of 2). The RACF Library

Administering



End Use



Diagnosis

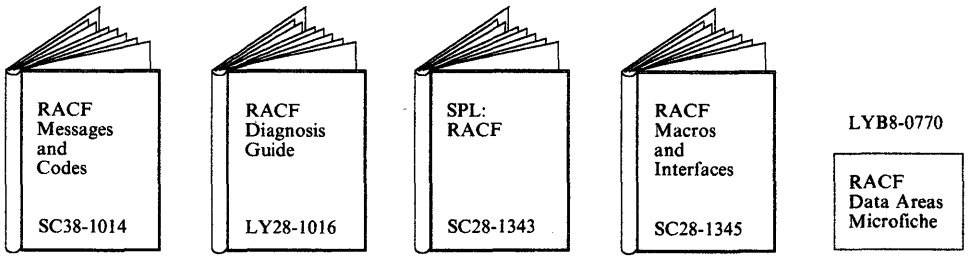


Figure 1-1 (Part 2 of 2). The RACF Library

Summary of Changes

Summary of Changes
for SC28-1341-3
RACF Version 1 Releases 8.1 and 8.2

This revision supports RACF Version 1 Releases 8.1 and 8.2.

The changes for Version 2 Release 8.1 include:

- Description of the DFP information that is now included in user profiles on MVS.
- Description of EXECUTE access authority for data sets.
- Description of enhanced generic naming.

There are no technical changes for RACF Version 1 Release 8.2.

The following changes are for maintenance:

- The title of the book has been changed to better describe the intended audience.
- Chapters 1 and 2 have been omitted. RACF concepts needed by general users are in the appropriate tasks.
- Information on specifying the audit type has been omitted. The audit type provides information for RACF auditors, not for general users. Information on specifying a user ID to be notified in case of failed accesses has been added to the appropriate tasks.
- Tasks MVS-16 through MVS-20 have been omitted; they are not RACF tasks.
- For VM users, the RACFPERM and RACFLIST EXECs have been described.
- A section describing when profile changes take effect has been added.
- A glossary of RACF terms has been added.

Summary of Changes
for SC28-1341-2
as updated August 1, 1988
by Technical Newsletter SN28-1218

This newsletter contains information about RACF tape volume (TAPEVOL) protection in the United States Department of Defense C2 environment.

Summary of Changes
for SC28-1341-2
RACF Version 1 Release 8

This revision supports Version 1 Release 8 of the Resource Access Control Facility (RACF), Program Number 5740-XXH and includes the following information:

- Description of the TSO information now included in user profiles on MVS.
- Enhancement of user tasks for this release of RACF.
- Reduction of redundancy within some tasks.
- Re-writing of some tasks to better explain the context in which steps are taken.

Chapter 1. Using RACF Commands On MVS

This chapter includes the following tasks, which describe how to use RACF commands on MVS:

ICH Messages

If a RACF command fails, you will get a message. If the message ID begins with ICH, you can get an online explanation of the message by typing:

```
HELP command-name MSGID(message-id)
```

For example, to display the explanation for message ICH09004I (an ADDSD message) enter the following:

```
HELP ADDSD MSGID(ICH09004I)
```

Note: If you get a message, but do not get a message ID, enter the following command:

```
PROFILE MSGID
```

Then re-enter the RACF command that failed.

Task MVS-1. Finding Out If And How You Are RACF-Defined

SITUATION: Your first step is to find out if you can use RACF. As a starting point, you must find out if you have been RACF-defined.

There are two procedures to find out if you're defined to RACF. One is for TSO/E users and the other is for non-TSO/E users. If you are not sure whether your installation has installed TSO/E, use the procedure for non-TSO/E users.

> Be aware that, if you are RACF-defined and this is the first time you have ever logged on to the system, you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the format of the assigned password.

For TSO/E Users: Log on to the system. Simply observe the right side of your logon parameter screen. If the NEW PASSWORD and GROUP IDENT fields appear, you are a RACF-defined user.

The following is an example of a screen for a TSO/E user:

```
ENTER LOGON PARAMETERS BELOW:      RACF LOGON PARAMETERS:

USERID       ======> ABCXYZ1

PASSWORD     ======>               NEW PASSWORD  =====>

PROCEDURE    ======> PROC01        GROUP IDENT   =====>

ACCT NMBR    ======> A4446B

SIZE         ======>

PERFORM      ======>

COMMAND      ======>
```

For Non-TSO/E Users: Log on to the system by entering your userid. If you are not aware that you have a userid, see your RACF security administrator or someone in authority at your installation, for example, a supervisor. Without a userid you cannot use the system.

To find out if you are a RACF-defined user, issue the following command:

```
LISTUSER
```

If you are not a RACF-defined user, you will get a command-violation message. A command-violation message indicates you are not authorized to issue this command.

If you discover that you are not RACF-defined, contact your RACF security administrator or someone in authority at your installation, for example, a supervisor. You must be RACF-defined to use RACF.

If you are a RACF-defined user, you will see output similar to that shown in Figure 1-1 on page 1-4. Other examples are shown in Figure 1-2 on page 1-9 and in Figure 1-3 on page 1-10.

```
The following is the first part of the RACF information that describes
you as a user:

USER=your   NAME=your name      OWNER=the owner   CREATED=date you were
     userid                           of this profile     defined to RACF

 DEFAULT-GROUP=your     PASSDATE=date your    PASS-INTERVAL=length of time
              default           password was               your password
              group name        last updated               is valid

 ATTRIBUTES=your operating privileges and restrictions

 REVOKE DATE=date on which      RESUME DATE=date on which RACF allows
            RACF prevents you              you to use the system
            from using the system          again

 LAST-ACCESS=last date you used the system

 CLASS AUTHORIZATIONS=installation-assigned classes in which you
                      can define profiles.

 INSTALLATION-DATA=information your installation maintains about you

 MODEL-NAME=a profile used as a model for new data set profiles

 LOGON ALLOWED=time during which you can access the system


The following portion of the RACF information describes the RACF group(s)
you belong to and what you can do as a member of the group(s):


  GROUP=name  AUTH=your  CONNECT-OWNER=owner   CONNECT-DATE=date you
        of         group             of this              were connected
        group      authority           group              to this group

    CONNECTS=number of times   UACC=universal    LAST-CONNECT=last time
          you were connected        access                  you were
               to this group        authority               connected

    CONNECT ATTRIBUTES=your operating privileges as a member of this group

    REVOKE DATE=date on which      RESUME DATE=date on which RACF
                RACF prevents you             allows you to access
                from accessing the system     the system again
                through this group            through this group

The following is the second part of the RACF information that
describes you as a user:

SECURITY-LEVEL=your installation-assigned security level

CATEGORY-AUTHORIZATION
 your installation-assigned security categories
```

Figure 1-1. Output of LISTUSER Command on MVS

Here are detailed descriptions of the terms appearing in the RACF information:

USER
Your userid is the name the system knows you by. It is frequently a combination of such identifying information as your name, initials, personnel number, or department.

NAME
Your name as recorded in your user profile.

OWNER
The user ID or group name of the owner of your user profile. The owner of your profile can modify your profile.

CREATED
The date you were defined to RACF.

DEFAULT-GROUP
RACF connects each user to at least one group. If you are a member of only one group, that group is your default group and that group name appears in this field.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups you belong to, you can ignore this field. If you have difficulty using group resources of a group that you belong to, logon again and specify the group you want to be connected to at the logon panel. (If you don't specify the group, RACF assumes the group named in this field.)

PASSDATE
The date you last updated your password.

PASS-INTERVAL
The length of time in days your current password is valid. You must change your password before this interval expires.

ATTRIBUTES
The operating privileges and restrictions assigned to you. There are two types of attributes: user and connect. This field describes your system-wide attributes. See the CONNECT ATTRIBUTES field for your group-level attributes.

NONE	Allows no *special* operating privileges or restrictions. Users with NONE can still use RACF. In fact, most attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.
SPECIAL	Allows full authorization to all profiles in the RACF data base and allows you to perform all RACF functions except those requiring the AUDITOR attribute.
AUDITOR	Allows you to audit the use of system resources, to control the logging of detected accesses to resources, and to create security reports.
OPERATIONS	Allows you to have full authorization to all RACF-protected data sets and to general resources that meet certain conditions (described in the *RACF Security Administrator's Guide*). OPERATIONS allows you to perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.

GRPACC — Allows you to have the group data sets you allocate automatically accessible to other users in the specified group.

CLAUTH — Allows you to define profiles for any class specified in the class name.

ADSP — ADSP is the automatic data set protection attribute. If you have the ADSP attribute, RACF creates a discrete profile for every permanent DASD or tape data set you create.

REVOKE — Prohibits a user from entering the system. (You should never be able to see this attribute when you list your own profile.)

REVOKE DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF prevents you from using the system. In the group portion of the output, this is the date on which RACF prevents you from using the system when you try to connect to the group.

RESUME DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF allows you to use the system again. In the group portion of the output, this is the date on which RACF allows you to use the system again when you are connected to the group.

LAST-ACCESS
The date is the last time you were on the on the system. RACF keeps records of all persons who have used the system, and what they have done, as well as recording unauthorized attempts to use of the system.

CLASS-AUTHORIZATIONS
Your installation assigns resources to various classes. The class appearing in this field is the class in which the user is authorized to assign RACF protection.

INSTALLATION-DATA
Additional information your installation maintains about you and your authority. If you need help in understanding anything included here, see your RACF security administrator or the owner of your user profile.

MODEL-NAME
If a profile name appears in this field, the profile is used as a model when you create data set profiles that have your userid as the high-level qualifier.

LOGON-ALLOWED
The days of the week and/or hours in the day that RACF allows you to access the system from a terminal. These restrictions apply only to when you can log on to the system. If you are working on the system and an end-time occurs, RACF will not force you off the system. Also, these logon restrictions do not apply to batch jobs; you can still submit a batch job at any time.

The following portion is repeated once for each RACF group of which you are a member:

GROUP
The name of a group of which you are a member.

AUTH
The group authorities you have because you are a member of this group.

USE — Allows you to enter the system under the control of the specified group. You may use any of the resources the group may use.

CREATE — On MVS systems, allows you to RACF-protect group data sets and control who can access them. It includes the privileges of the USE authority.

CONNECT — Allows you to connect RACF-defined users to the specified group and assign these users the USE, CREATE, or CONNECT authority. It includes the privileges of the CREATE authority.

JOIN — Allows you to define new users or groups to RACF and to assign group authorities. To define new users, you must also have the user attribute, CLAUTH(USER). JOIN authority includes all the privileges of the CONNECT authority.

CONNECT-OWNER
The owner of this group.

CONNECT-DATE
The date you were first connected to this group.

CONNECTS
The number of times you have been connected to this group.

UACC
The universal access authority for resources you create while connected to this group. If a user is not specifically listed in the access list describing a resource owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner specified in the UACC.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-10. Permitting an Individual or a Group to Use a Data Set" on page 1-32 for information on how to permit selected users or groups to access a data set.)

LAST-CONNECT
The last time you were connected to the group.

CONNECT-ATTRIBUTES
The operating privileges and restrictions assigned to you when you are connected to this group. Connect attributes are also called group-level attributes. The connect (group-level) attributes are:

NONE
SPECIAL
AUDITOR
OPERATIONS
GRPACC
ADSP
REVOKE

For descriptions of these attributes, see the ATTRIBUTES field on page 1-5.

REVOKE DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF prevents you from using the system. In the group portion of the output, this is the date on which RACF prevents you from using the system when you try to connect to the group.

RESUME DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF allows you to use the system again. In the group portion of the output, this is the date on which RACF allows you to use the system again when you are connected to the group.

SECURITY-LEVEL
Your installation can define various security levels. The name appearing in this field is the security level assigned to you.

CATEGORY-AUTHORIZATION
Your installation can define various security categories. The names appearing in this field are the security categories assigned to you.

```
USER=AHLEE   NAME=A.H.LEE     OWNER=JONES   CREATED=88.096
DEFAULT-GROUP=PAYROLL   PASSDATE=88.124  PASS-INTERVAL= 30
ATTRIBUTES=NONE
REVOKE DATE=NONE   RESUME DATE=NONE
LAST-ACCESS=88.130/13:47:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED   (DAYS)           (TIME)
-----------------------------------------------------------------
ANYDAY                           ANYTIME
GROUP=PAYROLL  AUTH=USE  CONNECT-OWNER=JONES  CONNECT-DATE=88.096
  CONNECTS= 05   UACC=NONE   LAST-CONNECT=88.130/13:47:18
  CONNECT ATTRIBUTES=NONE
  REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
```

Figure 1-2. Output of LISTUSER Command on MVS: Example 1

Figure 1-2 is for a RACF user connected to only one group, PAYROLL.

In the example, user A.H. Lee has none of the possible user attributes, but can still use RACF. For example, Lee can create, change, and delete RACF profiles to protect his data sets.

```
USER=SMITH   NAME=J.E.SMITH   OWNER=JONES  CREATED=88.096
DEFAULT-GROUP=SEARCH  PASSDATE=88.103   PASS-INTERVAL= 30
ATTRIBUTES=AUDITOR
REVOKE DATE=NONE   RESUME DATE=NONE
LAST-ACCESS=88.114/13:47:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED   (DAYS)          (TIME)
-------------------------------------------------------------
ANYDAY                          ANYTIME
GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=88.096
   CONNECTS= 01   UACC=NONE   LAST-CONNECT=88.114/13:50:18
   CONNECT ATTRIBUTES=NONE
   REVOKE DATE=NONE   RESUME DATE=NONE
GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=88.096
   CONNECTS= 00  UACC=READ  LAST-CONNECT=88.114/13:55:18
   CONNECT ATTRIBUTES=NONE
   REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
```

Figure 1-3. Output of LISTUSER Command on MVS: Example 2

Figure 1-3 is for a RACF user connected to two groups, SEARCH and PAYROLL.

In the example, Smith has the AUDITOR system-wide attribute. Not only can Smith control access to her data sets, but, as system AUDITOR, she can audit security controls and create security reports.

In the SEARCH group, Smith has JOIN group authority and can assign group authorities to members of the group. In the PAYROLL group, Smith has CREATE group authority and can create data set profiles to protect group data sets.

In the PAYROLL group, Smith also has assigned a UACC (universal access authority) of READ. If Smith logs on using PAYROLL as the current connect group, any data set profiles she creates will have a UACC of READ (unless she specifies otherwise). For information on how to log on using a different connect group, see "Task MVS-15. Logging On to a Group Other Than Your Default Group" on page 1-41.

Task MVS-2. Finding Out What Authority You Have

SITUATION: To determine what authority you have with RACF, list your user profile. To list your user profile, issue the LISTUSER command.

Note: To find out your authority to a data set, see the field labeled YOUR ACCESS in the display of the data set profile. See "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

PROCEDURE:

Step 1. To find out what you can do using RACF, issue the following command:

```
LISTUSER
```

You will see output similar to that shown in Figure 1-4 on page 1-13 that displays the contents of your profile.

A RACF security administrator creates and maintains your user profile, which describes you to RACF. Your profile contains:

- RACF information: The userid or group name of the owner of the profile, your userid, information about your operating privileges and restrictions, information about your default group and other groups to which you belong, and other important information.
- TSO information (optional; your profile may not contain TSO information). Your defaults for job class (JOBCLASS), message class (MSGCLASS), hold class (HOLDCLASS), SYSOUT class (SYSOUTCLASS), account number (ACCTNUM), logon procedure (PROC), region size (SIZE), maximum region size (MAXSIZE), unit name (UNIT), destination identifier (DEST), and user data (USERDATA).

  To see the TSO information, issue the LISTUSER command as follows:

  ```
  LISTUSER  your-userid  TSO
  ```

  If there is TSO information in your profile, you will see output similar to that shown in Figure 1-5 on page 1-14.

- DFP information (optional; your profile may not contain DFP information). Your defaults for management class (MGMTCLAS), storage class (STORCLAS), data class (DATACLAS), and the identifier for a data set application (DATAAPPL).

  To see the DFP information, issue the LISTUSER command as follows:

  ```
  LISTUSER  your-userid  DFP
  ```

  If there is DFP information in your profile, you will see output similar to that shown in Figure 1-6 on page 1-15.

Step 2. Determine what your operating privileges and restrictions are. If you need to change your user profile, see your RACF security administrator or the owner of the profile.

```
The following is the first part of the RACF information that describes
you as a user:

USER=your   NAME=your name      OWNER=the owner   CREATED=date you were
     userid                           of this profile     defined to RACF

 DEFAULT-GROUP=your     PASSDATE=date your    PASS-INTERVAL=length of time
              default           password was               your password
              group name        last updated               is valid

 ATTRIBUTES=your operating privileges and restrictions

 REVOKE DATE=date on which      RESUME DATE=date on which RACF allows
            RACF prevents you              you to use the system
            from using the system          again

 LAST-ACCESS=last date you used the system

 CLASS AUTHORIZATIONS=installation-assigned classes in which you
                      can define profiles.

 INSTALLATION-DATA=information your installation maintains about you

 MODEL-NAME=a profile used as a model for new data set profiles

 LOGON ALLOWED=time during which you can access the system


The following portion of the RACF information describes the RACF group(s)
you belong to and what you can do as a member of the group(s):


  GROUP=name  AUTH=your  CONNECT-OWNER=owner   CONNECT-DATE=date you
       of         group             of this              were connected
       group      authority           group              to this group

    CONNECTS=number of times   UACC=universal    LAST-CONNECT=last time
          you were connected        access                    you were
               to this group        authority                 connected

    CONNECT ATTRIBUTES=your operating privileges as a member of this group

    REVOKE DATE=date on which      RESUME DATE=date on which RACF
               RACF prevents you              allows you to access
               from accessing the system      the system again
               through this group             through this group

The following is the second part of the RACF information that
describes you as a user:

SECURITY-LEVEL=your installation-assigned security level

CATEGORY-AUTHORIZATION
 your installation-assigned security categories
```

Figure 1-4. Output of LISTUSER Command on MVS. For a detailed description of the terms in the RACF information and examples of actual RACF information, see Figure 1-1 on page 1-4 in Task MVS-1.

The following describes the TSO information in LISTUSER output:

```
TSO INFORMATION

 JOBCLASS=default  MSGCLASS=default  HOLDCLASS=default  SYSOUTCLASS=default  DEST=default
         job               message           hold                SYSOUT   destination
         class             class             class               class     identifier

 ACCTNUM=default account number

 PROC=default   UNIT=default    USERDATA=user data
      LOGON          unit
      procedure

 SIZE=default   MAXSIZE=default
      region            maximum
      size              region size
```

The following is actual TSO information for a user:

```
TSO INFORMATION
 JOBCLASS=C  MSGCLASS=R  HOLDCLASS=H  SYSOUTCLASS=J  DEST=LIN1215
 ACCTNUM=D5888P
 PROC=PROC01    UNIT=SYSDA      USERDATA=1F09
 SIZE=0001024   MAXSIZE=0004096
```

Figure 1-5. TSO Information in the Output of LISTUSER Command

The following describes the DFP information in LISTUSER output:

```
DFP INFORMATION
   STORCLAS=your default for  MGMTCLAS=your default for
            storage class              management class
   DATACLAS=your default for  APPLICATION-ID=your default for
            data class                        data application
                                              identifier
```

The following is actual DFP information for a user:

```
DFP INFORMATION
   STORCLAS=DFPST01           MGMTCLAS=DFPMG01
   DATACLAS=DFPDT01           APPLICATION-ID=DFPID01
```

Figure 1-6. DFP Information in the Output of LISTUSER Command

Task MVS-3. Finding Out What Data Set Profiles You Have

SITUATION: You have data set profiles, but you are not sure how many you have.

Note: If you want to know which profile protects a particular data set, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

PROCEDURE:

Step 1. To find out what data set profiles you have, issue the SEARCH command as follows:

```
SEARCH
```

RACF will list all of your profiles that are in the DATASET class. If you do not have any DATASET profiles, RACF will display a message telling you that no entries meet the search criteria.

Review the list of profiles, comparing them with the names of the data sets you need to protect.

Any profile name that matches a data set name protects that data set.

Any profile name that includes generic characters (% or *) may or may not protect data sets. See "Enhanced Generic Names" on page A-4 for information on the rules for specifying generic characters.

Task MVS-4. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

Note: You may also change your password while logging on to the system. See "Task MVS-1. Finding Out If And How You Are RACF-Defined" on page 1-2.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may not allow you to re-use a previous password. Ask your RACF security administrator for an explanation of your installation's rules for passwords.

To change your password, issue the PASSWORD command with the PASSWORD keyword as follows:

```
PASSWORD  PASSWORD(current-password   new-password)
```

For example, to change your password from "subject" to "testers," type:

```
PASSWORD  PASSWORD(subject  testers)
```

To change your password interval (that is, the time allowed before you are required to change your password again), issue the PASSWORD command with the INTERVAL keyword as follows:

```
PASSWORD  INTERVAL(interval-you-want)
```

For example, to change your password interval to 15 days, enter the following command:

```
PASSWORD  INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password to a new valid one.

RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you may change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.

To change your password and password interval, issue the PASSWORD command with the PASSWORD and INTERVAL keywords as follows:

```
PASSWORD  PASSWORD(current-password  new-password)  INTERVAL(interval)
```

For example, to change the password from "subject" to "testers" and the interval to 15 days, enter the following command:

```
PASSWORD  PASSWORD(subject testers)  INTERVAL(15)
```

If you don't know what your current password interval is, issue the LISTUSER command and check the PASS-INTERVAL field. If you need more information, see "Task MVS-1. Finding Out If And How You Are RACF-Defined" on page 1-2.

Task MVS-5. Finding Out How a Data Set is Protected

SITUATION: You created a data set that needs protection, but you do not know whether you currently have a profile that protects the data set.

PROCEDURE:

Step 1. Find out if a discrete profile protects the data set by issuing the LISTDSD command as follows:

```
LISTDSD  DATASET('data-set-name')  ALL
```

You will see one of the following on your screen:

- If the data set is protected by a discrete profile, a listing for that profile (like the listing in Figure 1-7 on page 1-19).
- If the data set is not protected by a discrete profile but is protected by a fully-qualified generic profile, and generic profile command processing is active, a listing for the generic profile. (A generic profile is identified by a "G" in parentheses following the profile name.)
- If the data set is not protected by a discrete profile, a message stating that no profile was found (The message says, "NO RACF DESCRIPTION.")

  Note: If generic profile checking is active, and you get the message that no profile was found, you must do Step 2 to check for generic profiles.

Step 2. To determine if the data set is protected by a generic profile, issue the LISTDSD command with the GENERIC operand as follows:

```
LISTDSD  DATASET('data-set-name')  ALL  GENERIC
```

You will see one of the following on your screen:

- If the data set is protected by a fully-qualified generic profile, a listing for that profile
- If the data set is not protected by a fully-qualified generic profile but is protected by a generic profile, a listing for the most specific generic profile that protects the data set
- If the data set is not protected by a generic profile, a message stating that no profile was found

If the command succeeds, you will see a listing of the profile, like the listing in Figure 1-7 on page 1-19.

```
INFORMATION FOR DATASET profile-name

LEVEL    OWNER        UNIVERSAL ACCESS     WARNING     ERASE
-----    -----        ----------------     -------     -----
 00      SMITH            READ               NO         NO

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

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS          CREATION GROUP         DATASET TYPE
-------------        ----------------       -------------
   READ                  DEPTD60                NON-VSAM

VOLUMES ON WHICH DATASET RESIDES              UNIT
---------------------------------             ------
          21345                               SYSDA

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

           SECURITY LEVEL
-----------------------------------------------
NO SECURITY LEVEL

CATEGORIES
-----------
NOCATEGORIES

CREATION DATE     LAST REFERENCE DATE     LAST CHANGE DATE
(DAY)  (YEAR)      (DAY)      (YEAR)       (DAY)   (YEAR)
------------      ------------------     --------------
 070    85          070        85           070     85

ALTER COUNT    CONTROL COUNT    UPDATE COUNT    READ COUNT
-----------    -------------    ------------    ----------
 00000            00000            00002          00000

   ID       ACCESS      ACCESS COUNT
--------   --------    --------------
JONES       UPDATE         00009

PROGRAM       ID       ACCESS    ACCESS COUNT
--------   ---------  --------  --------------
NO ENTRIES IN CONDITIONAL ACCESS LIST

DFP INFORMATION

RESOWNER
--------
SMITH
```

Figure 1-7. Output of LISTDSD Command

Check the following fields for the most important security information about how the data set is protected:

- the LEVEL field (if used at your installation)
- the OWNER field
- the UNIVERSAL ACCESS field
- the WARNING field
- the SECURITY LEVEL field (if used at your installation)
- the CATEGORIES field (if used at your installation)
- the ID field and its related ACCESS and ACCESS COUNT fields
- the PROGRAM field and its related ID, ACCESS, and ACCESS COUNT fields

Here are detailed descriptions of the fields appearing in the output:

INFORMATION FOR DATASET profile-name
This phrase appears for each data set profile listed.

Note: If the profile is a generic profile, the phrase looks like the following:

```
INFORMATION FOR DATASET profile-name (G)
```

LEVEL
A security classification indicator used by each individual installation. If anything other than 00 appears in this field, see your RACF security administrator for an explanation of what the number means.

OWNER
Each RACF-defined data set has an owner. An owner may be a user or a group. When you create a data set and then RACF-protect the data set without specifying an owner, RACF names you the owner of the data set profile. The owner of the profile may modify the data set profile.

UNIVERSAL ACCESS
Each data set protected by RACF has a universal access authority (UACC). The UACC permits users or groups to use the data set in the manner specified in this field. In this example, the UACC is READ. Anyone may read this data set. (The only exception is if the user or group is specifically named in the access list with ACCESS of NONE.)

WARNING
If this field contains YES, RACF permits a user to access this resource *even though his or her access authority is insufficient.* RACF issues a warning message *to the user who is attempting access;* you are notified only if your userid is the NOTIFY userid.

If this field contains NO, RACF denies access to users with insufficient authority to access this resource.

ERASE
If this field contains YES, and erase-on-scratch is in effect on your system, data management will physically erase the DASD data set extents when the data set is deleted. If this field contains NO, data management will not erase DASD data set extents when the data set is deleted.

Exception: Your installation could specify erase-on-scratch for all data sets that have a security level equal to or greater than the security level specified by the installation. If this data set's security level is equal to or greater than the security level specified by the installation, this data set will be erased even if the ERASE field in the profile contains NO.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is SUCCESS(UPDATE). RACF will record all successful attempts to update the data set.

NOTIFY
The userid of a RACF-defined user that RACF notifies when denying access to a data set protected by this profile.

YOUR ACCESS
How you may access this data set.

If you must work with the listed data set but do not have the required authority, ask the owner (OWNER field) to issue a PERMIT command to give you access to the data set.

CREATION GROUP
The group under which the profile was created.

DATASET TYPE
The data set type. It may be either VSAM, NON-VSAM, MODEL, or TAPE.

VOLUME ON WHICH THE DATASET RESIDES
The volume on which a non-VSAM data set resides or the volume on which the catalog for a VSAM data set resides.

UNIT
The unit type for a non-VSAM data set.

INSTALLATION DATA
Any information your installation keeps in this data set profile.

CREATION DATE
The date the profile was created.

SECURITY LEVEL
Your installation can define its own security levels. This security level is a name associated with the numeric value shown in the LEVEL field earlier in this output. The security level displayed is the minimum security level you need to access a data set protected by this profile.

CATEGORIES
Your installation can define its own security categories. The names displayed are the security categories you need to access a data set protected by this profile.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The number of times the profile was altered (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

CONTROL COUNT
The number of times the profile was successfully accessed with CONTROL authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

UPDATE COUNT
The number of times the profile was successfully accessed with UPDATE authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

READ COUNT
The number of times the profile was successfully accessed with READ authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

ID, ACCESS, and ACCESS COUNT
These fields describe the standard access list. ID is the userid or group-id given the access authority listed in the ACCESS field. ACCESS COUNT is the number of times the user listed in the ID field accessed the data set (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

PROGRAM, ID, ACCESS, and ACCESS COUNT
These fields refer to entries in the conditional access list. (A conditional access list is an access list in the data set profile that specifies which program a user must be running to get the specified access authority.) PROGRAM is the program that the user listed in the ID field must run in order to have access to the data set. ACCESS is the level of access to the data set that RACF grants when the user is running the program listed under PROGRAM. ACCESS COUNT is the number of times the user has accessed the data set when running the program listed under PROGRAM (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

DFP INFORMATION
RESOWNER
The RESOWNER field contains the userid or group name of the owner of the resource. In this case, the resource is the data set; the owner of the data set need not be the same as the owner of the profile.

Task MVS-6. Changing a Data Set's Universal Access Authority (UACC)

SITUATION: You have a data set containing research data, which you need to protect so that no one can tamper with the data.

To change a data set's UACC (universal access authority), you must issue the ALTDSD command with the appropriate operands.

PROCEDURE:

Step 1. Find the name of the profile that protects the data set. To do this, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

> Remember that changing the UACC for a generic profile changes the access to all data sets protected by the profile.

Step 2. Decide which level of UACC to specify in the profile.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Warnings

1. Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-10. Permitting an Individual or a Group to Use a Data Set" on page 1-32 for information on how to permit selected users or groups to access a data set.)
2. If you are changing the UACC to restrict access, be certain that any user or group specifically mentioned in the access list has the access to the resource that you intend. For example, if you change the UACC to NONE, and there is a user specifically named in the access list with any authority, that user will still have that authority to the resource.

Step 3. Change the UACC specified in the profile.

To change the UACC, issue the ALTDSD command as follows:

```
ALTDSD     'profile-name'     UACC(access-authority)
```

Examples:

Assume that data set 'SMITH.PROJ.ONE' is protected by a discrete profile. To change the UACC for this data set to NONE, enter the following command:

```
ALTDSD     'SMITH.PROJ.ONE'     UACC(NONE)
```

If you are changing the UACC specified in a generic profile, specify the name of the generic profile. For example, to change the UACC for generic profile SMITH.* to NONE, enter the following command:

```
ALTDSD     'SMITH.*'     UACC(NONE)
```

Task MVS-7. Choosing Between Discrete and Generic Profiles

SITUATION: You need to protect one or more data sets, and no existing profile provides the exact protection needed.

If you need to determine how a particular data set is protected, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

If you need to protect a tape data set, see "Task MVS-12. Protecting a Tape Volume" on page 1-36 or "Task MVS-13. Protecting a Tape Data Set With a Data Set Profile" on page 1-37.

If your installation has always-call support (ask your RACF security administrator), a generic profile might already exist under which the data set is protected. However, that profile might not provide the exact protection you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

- If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set.
- If a data set is protected by more than one generic profile, the *most specific* profile sets the level of protection for the data set.

PROCEDURE:

Step 1. Choose a *generic profile* for one of the following reasons:

- To protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
- If you have a single data set that might be deleted, then re-created, and you want the protection to remain the same, you can create a fully-qualified generic profile. The name of a fully-qualified generic profile matches the name of the data set it protects. Unlike a discrete profile, a fully-qualified generic profile is not deleted when the data set itself is deleted.

To create a generic profile, see "Task MVS-9. Creating a Generic Profile To Protect Data Sets" on page 1-29.

Step 2. Choose a *discrete profile* for the following reason:

- To protect one data set with unique security requirements. The name of a discrete profile matches the name of the data set it protects.

To create a discrete profile, see "Task MVS-8. Creating A Discrete Profile To Protect A Data Set" on page 1-27.

Notes:

1. All the members of a partitioned data set (PDS) are protected by one profile (the profile that protects the data set).
2. If your installation has always-call support, all the components of a VSAM data set are protected by one profile (the profile that protects the cluster name). You do not need to create profiles that protect the index and data components of a cluster. If your installation does *not* have always-call support, you must ensure

that the index and data components of a VSAM cluster are protected the same way the cluster name is protected.

3. For a generic profile, unit and volume information is ignored because the data sets that are protected under the generic profile can be on many different volumes.

Task MVS-8. Creating A Discrete Profile To Protect A Data Set

SITUATION: You have a single data set that needs to be protected with unique security requirements.

If you need to determine how a particular data set is protected, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

If you need to protect a tape data set, see "Task MVS-12. Protecting a Tape Volume" on page 1-36 or "Task MVS-13. Protecting a Tape Data Set With a Data Set Profile" on page 1-37.

PROCEDURE:

Step 1. Decide which RACF protections to use:

- ☐ UACC (universal access authority).

  The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

- ☐ NOTIFY userid.

  The NOTIFY userid is sent a message whenever someone tries to use a data set, and RACF denies the access.

  For example, if your userid is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

  Note: If you do not specify a userid on the NOTIFY keyword, your userid is the default NOTIFY userid.

- ☐ Erase-on-scratch.

  You might want to specify that the data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeroes. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

- ☐ WARNING option.

  Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

  Warning

  WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

- ☐ Your installation may have other security requirements for protecting data, including audit type, level, and security level. See your RACF security administrator for specific information.

Step 2. Create the profile for the data set.

To create a discrete profile for a cataloged data set, issue the ADDSD command as follows:

```
ADDSD  'data-set-name'  UACC(access-authority)
```

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD   'SMITH.PROJ.ONE'    UACC(NONE)
```

To create a discrete profile for a data set that is not cataloged, you must specify the unit type and volume serial number of the data set. Issue the ADDSD command as follows:

```
ADDSD 'data-set-name'   UNIT(type)   VOLUME(volume-serial) +
      UACC(access-authority)
```

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD   'SMITH.PROJ.ONE'   UNIT(3380)   VOLUME(ABC123)   +
        UACC(NONE)
```

To create a discrete profile with a NOTIFY userid, issue the ADDSD command as follows:

```
ADDSD 'data-set-name'   UACC(access-authority)   NOTIFY(userid)
```

For example, if your user ID is SMITH, and you want to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD   'SMITH.PROJ.ONE'   UACC(NONE)   NOTIFY
```

If your user ID is SMITH, and you want JONES to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD   'SMITH.PROJ.ONE'   UACC(NONE)   NOTIFY(JONES)
```

To create a discrete profile for a VSAM data set, you can use the VSAM cluster name on the ADDSD command. The following example illustrates how this is done.

SMITH has created a VSAM cluster using the following command:

```
DEFINE CLUSTER(NAME('SMITH.SAMPLE') VOLUMES(VSAM02) ) +
  INDEX(NAME('SMITH.SAMPLEI') TRACKS(1 1) ) +
  DATA(NAME('SMITH.SAMPLED') CYLINDERS(1 1) KEYS(128 0) +
  CONTROLINTERVALSIZE(X'1000') )
```

If the installation has always-call support, SMITH can protect this cluster with a profile named 'SMITH.SAMPLE', as follows:

```
ADDSD  'SMITH.SAMPLE'   UACC(NONE)  NOTIFY
```

If the installation does *not* have always-call support, SMITH must protect not just the cluster ('SMITH.SAMPLE') but also the index and data components. This can be done with three discrete profiles:

```
ADDSD  'SMITH.SAMPLE'   UACC(NONE)  NOTIFY
ADDSD  'SMITH.SAMPLEI'  UACC(NONE)  NOTIFY
ADDSD  'SMITH.SAMPLED'  UACC(NONE)  NOTIFY
```

Task MVS-9. Creating a Generic Profile To Protect Data Sets

SITUATION: You have several data sets that have the same security requirements and that have some identical characters in their names.

If you need to determine how a particular data set is protected, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

If you need to protect a tape data set, see "Task MVS-12. Protecting a Tape Volume" on page 1-36 or "Task MVS-13. Protecting a Tape Data Set With a Data Set Profile" on page 1-37.

PROCEDURE:

Step 1. Decide how to specify the profile name.

To create a generic profile for your user data set, the high-level qualifier must be your userid. For example, for user ASMITH to protect data set ASMITH.PROJ.ONE, ASMITH must specify a profile name beginning with ASMITH (such as ASMITH.PROJ.* or ASMITH.PROJ.**).

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name or you include the GENERIC keyword on the ADDSD command.

How to specify the generic characters depends on whether your installation uses *enhanced generic naming*, which was introduced in RACF 1.8.1. Ask your RACF security administrator if enhanced generic naming is active.

If enhanced generic naming is active, see Figure A-1 on page A-4 for a description of how to specify generic characters in profile names.

If enhanced generic naming is *not* active, see Figure A-2 on page A-4 for a description of how to specify generic characters in profile names.

Note: Profiles created *before* an installation converts to enhanced generic naming are *not* affected by the conversion. Profiles created *after* the installation converts to enhanced generic naming are governed by the new rules.

Step 2. Decide which RACF protections to use:

☐ UACC (universal access authority)

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Note: If you do not specify UACC, the system uses the value specified in the UACC field in your current connect group. (For more information, see "Task MVS-1. Finding Out If And How You Are RACF-Defined" on page 1-2.)

☐ NOTIFY userid.

The NOTIFY userid is sent a message whenever someone tries to use a data set, and RACF denies the access.

For example, if your userid is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data

set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

Note: If you do not specify a userid on the NOTIFY keyword, your userid is the default NOTIFY userid.

- ☐ Erase-on-scratch.

  If allowed by your installation, you can specify that a data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeroes. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

  Note: Only the data set that is deleted is erased. For example, suppose profile SMITH.SAMPLE*.DATA protects data sets SMITH.SAMPLE1.DATA and SMITH.SAMPLE2.DATA. If SMITH.SAMPLE1.DATA is deleted, only SMITH.SAMPLE1.DATA is erased. SMITH.SAMPLE2.DATA is not affected.

- ☐ WARNING option.

  Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

  Warning

  WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

- ☐ Your installation may have other security requirements for protecting data, including audit type, level, and security level. See your RACF security administrator for specific information.

Step 3. Create the profile.

To create a generic profile, issue the ADDSD command as follows:

```
ADDSD 'profile-name-with-generic-character' UACC(access-authority)
```

To create a fully-qualified generic profile, issue the ADDSD command as follows:

```
ADDSD 'profile-name' UACC(access-authority) GENERIC
```

Example 1. A generic profile for all data sets not otherwise protected

You can create a generic profile to protect all of your data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

- If your system has enhanced generic naming:

  ```
  ADDSD 'prefix.**' UACC(NONE)
  ```

- If your system does not have enhanced generic naming:

  ```
  ADDSD 'prefix.*' UACC(NONE)
  ```

where prefix is your userid. The profile created will allow a universal access authority (UACC) of NONE.

Example 2. A generic profile for data sets whose last qualifier is TESTDATA

You can create a generic profile to protect all of your data sets whose last qualifier is TESTDATA. To do this, enter the following command:

```
ADDSD  'prefix.*.TESTDATA'  UACC(NONE)
```

where prefix is your userid. The profile created will allow a universal access authority (UACC) of NONE. You can permit or deny specific users or groups access to these profiles. For more information, see "Task MVS-10. Permitting an Individual or a Group to Use a Data Set" on page 1-32 or "Task MVS-11. Denying an Individual or a Group Use of a Data Set" on page 1-33.

Note: If you specify the asterisk (*) at the end of the profile name, special rules apply. See "Enhanced Generic Names" on page A-4.

Example 3. A generic profile for group data sets

You can create a generic profile to protect all of a group's data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

- If your system has enhanced generic naming:

  ```
  ADDSD    'groupid.**'    UACC(NONE)
  ```

- If your system does not have enhanced generic naming:

  ```
  ADDSD    'groupid.*'    UACC(NONE)
  ```

where groupid is the group ID. The profile created will allow a universal access authority (UACC) of NONE.

Example 4. A fully-qualified generic profile

You want to allow a universal access of READ to a particular listing file that you will be deleting and re-creating. To do this, enter the following command:

```
ADDSD  'prefix.SAMPLE.LISTING'  UACC(READ)  GENERIC
```

where prefix is your userid. The profile created will allow a universal access authority (UACC) of READ.

Task MVS-10. Permitting an Individual or a Group to Use a Data Set

SITUATION: You would like J.E. Jones, whose userid is JONES, to use a RACF-protected data set.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on MVS" on page A-5.

PROCEDURE:

Step 1. Find the name of the profile that protects the data set. To do this, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

Step 2. Decide whether to use the profile that protects the data set.

- If the profile is a discrete profile, go on to Step 3.
- If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Task MVS-7. Choosing Between Discrete and Generic Profiles" on page 1-25.

Step 3. Decide which access authority to specify for the user.

The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Step 4. Allow access to the data set.

To allow access to your data set, use the PERMIT command with the ACCESS keyword:

```
PERMIT  'profile-name'   ID(userid or groupid)  ACCESS(level)
```

Example 1. Permitting a user to read a data set

Data set SMITH.PROJ.ONE is protected by a discrete profile. To permit user JONES to read data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT    'SMITH.PROJ.ONE'    ID(JONES)    ACCESS(READ)
```

Example 2. Permitting more than one user to read a data set

To permit users JONES and MOORE to read data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT    'SMITH.PROJ.ONE'    ID(JONES, MOORE)   ACCESS(READ)
```

Example 3. Permitting more than one user or group to read a data set

To permit group DEPTD60 and user JONES to read user data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT    'SMITH.PROJ.ONE'    ID(DEPTD60, JONES)   ACCESS(READ)
```

Example 4. Permitting a user to read a group data set

To permit user SMITH to read group data set GROUPID.PROJ.ONE, enter the following command:

```
PERMIT    'GROUPID.PROJ.ONE'  ID(SMITH)   ACCESS(READ)
```

Task MVS-11. Denying an Individual or a Group Use of a Data Set

SITUATION: A colleague who has left the department can still use a data set. For security reasons you wish to exclude the person from using the data set.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on MVS" on page A-5.

PROCEDURE:

Step 1. Find the name of the profile that protects the data set. To do this, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

Step 2. Decide whether to use the profile that protects the data set.

- If the profile is a discrete profile, go on to Step 3.
- If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Task MVS-7. Choosing Between Discrete and Generic Profiles" on page 1-25.

Step 3. Use the PERMIT command to deny access to the data set.

You can use the PERMIT command to do this in two ways:

- One way is to remove the name of the user or group from the access list. However, this will deny access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group will be able to access the data set. See "Removing the User or Group from the Access List" on page 1-34.
- The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. To assign an access of NONE is the best procedure to ensure that the user or group will not be able to access the data set. See "Including the Individual or Group on the Access List with ACCESS(NONE)" on page 1-35.

Removing the User or Group from the Access List: To deny access by removing a user or a group from the access list, issue the PERMIT command with DELETE keyword as follows:

```
PERMIT   'profile-name'   ID(userid or groupid)   DELETE
```

Examples:

To deny user JONES use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(JONES)    DELETE
```

To deny users JONES and MOORE use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(JONES, MOORE)   DELETE
```

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(DEPTD60)   DELETE
```

To deny groups DEPTD60 and DEPTD58 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(DEPTD60, DEPTD58)   DELETE
```

Including the Individual or Group on the Access List with ACCESS(NONE):
Including the user or group on the access list with ACCESS(NONE) is the best way to ensure that the user or group will not be able to access the data set.

To deny access by assigning a user or group an access of NONE, issue the PERMIT command with the ACCESS keyword as follows:

```
PERMIT   'profile-name'    ID(userid or groupid)  ACCESS(NONE)
```

Examples:

To deny user JONES the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(JONES)   ACCESS(NONE)
```

To deny users JONES and MOORE the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(JONES, MOORE)   ACCESS(NONE)
```

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(DEPTD60)   ACCESS(NONE)
```

To deny groups DEPTD60 and DEPTD58 use of user data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT   'SMITH.PROJ.ONE'   ID(DEPTD60, DEPTD58)    ACCESS(NONE)
```

Task MVS-12. Protecting a Tape Volume

SITUATION: You wish to protect a standard-labeled tape volume. (Any data set you then place on that volume is protected under the profile you create for the volume.)

Notes:

1. Each data set on a volume shares a common access list.
2. For non-standard labeled tape volumes, you can issue the RDEFINE command the same way as for standard labeled tapes. However, the only protection you will have is through a mount message that will be issued to the operator when an unauthorized user tries to access the volume.
3. In a United States Department of Defense C2 environment, RACF tape volume (TAPEVOL) protection should be used to protect sensitive tape data sets. More than one data set may be placed on a tape volume *only* if all the data sets have the same access requirements.

PROCEDURE:

Step 1. Determine if you have class authority to the TAPEVOL class.

To protect a volume, you need class authorization to resource class TAPEVOL. If you know that you have authorization to class TAPEVOL, go on to Step 2. To see if you have TAPEVOL class authority, use the LISTUSER command:

```
LISTUSER
```

Check the CLASS-AUTHORIZATIONS field in the profile listing to see if it contains TAPEVOL class authority.

Step 2. Create a general resource profile.

To protect a tape volume, issue the RDEFINE command as follows:

```
RDEFINE    TAPEVOL   profile-name     UACC(access-authority)
```

Example:

To protect tape volume T11011, enter the following command:

```
RDEFINE    TAPEVOL   T11011     UACC(NONE)
```

Task MVS-13. Protecting a Tape Data Set With a Data Set Profile

SITUATION: You have a data set on tape that requires RACF protection.

Note: In a United States Department of Defense C2 environment, RACF tape volume (TAPEVOL) protection should be used to protect sensitive tape data sets. More than one data set may be placed on a tape volume *only* if all the data sets have the same access requirements.

PROCEDURE:

Step 1. Choose between discrete and generic profiles

If your installation has always-call support (ask your RACF security administrator), keep in mind that a generic profile might already exist under which the data set is protected. However, that profile might not provide the exact protection you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

- If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set.
- If a data set is protected by more than one generic profile, the most *specific* profile sets the level of protection for the data set.

The following are some reasons why you would choose a generic or a discrete profile:

- *Generic profile:* Choose a generic profile when you want to protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
- *Discrete profile:* Choose a discrete profile when you want to protect one data set with unique security requirements. The name of a discrete profile matches the name of the data set it protects.

Step 2. Decide which RACF protections to use:

☐ UACC (universal access authority)

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Note: If you do not specify UACC, the system uses the value specified in the UACC field in your current connect group. (For more information, see "Task MVS-1. Finding Out If And How You Are RACF-Defined" on page 1-2.)

☐ NOTIFY userid.

The NOTIFY userid is sent a message whenever someone tries to use a data set, and RACF denies the access.

For example, if your userid is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

- ☐ Your installation may have other security requirements for protecting data, including audit type, level, and security level. See your RACF security administrator for specific information.

Step 3. Create a discrete profile.

If the data set is **cataloged**, issue the ADDSD command with the TAPE operand as follows:

```
ADDSD   'data-set-name'   TAPE   UACC(access-authority)
```

RACF protects the entire data set, even if it is a multivolume data set.

If the data set is **uncataloged**, issue the ADDSD command with the TAPE, UNIT, VOLUME, and FILESEQ operands as follows:

```
ADDSD   'data-set-name'   TAPE   UNIT(type)   +
   VOLUME(volume-serial)   FILESEQ(number)   UACC(access-authority)
```

If an uncataloged data set is a multivolume data set (it resides on more than one volume), you must first use the ADDSD command to create a discrete profile for one volume, then use the ALTDSD command to add the other volumes to the discrete profile (one ALTDSD command for each additional volume).

Example 1. Cataloged Tape Data Set:

You have a cataloged tape data set named SMITH.TEST.DATA1. To protect this data set with a discrete profile, enter the following command:

```
ADDSD   'SMITH.TEST.DATA1'   TAPE   UACC(NONE)
```

Example 2. Uncataloged Tape Data Set:

You have a tape data set named SMITH.TEST.DATA residing on tape volume 111111 with a file sequence of 1. To protect this data set with a discrete profile, enter the following command:

```
ADDSD   'SMITH.TEST.DATA2'   TAPE   UNIT(TAPE)   +
   VOLUME(111111)   FILESEQ(1)   UACC(NONE)
```

Example 3. Uncataloged Multivolume Tape Data Set:

You have a tape data set named SMITH.TEST.DATA residing on tape volumes 111111, 222222, and 333333, with a file sequence of 1. To protect this data set with a discrete profile, enter the following commands:

```
ADDSD   'SMITH.TEST.DATA3'   TAPE   UNIT(TAPE)   +
   VOLUME(111111)   FILESEQ(1)   UACC(NONE)

ALTDSD   'SMITH.TEST.DATA3'  ADDVOL(222222)

ALTDSD   'SMITH.TEST.DATA3'  ADDVOL(333333)
```

Task MVS-14. Removing Protection From Your Data Set

SITUATION: You have a data set containing experimental data which has been published. You no longer feel it is necessary to protect the data.

To remove RACF protection from a data set, you must ensure that no RACF profile protects the data set.

Warning

When you remove RACF protection from a data set, anyone (RACF-defined or not) can access, change, or delete your data set. You can selectively "remove" protection by using the PERMIT command to permit or deny access to your data set by selected users and groups. See "Task MVS-10. Permitting an Individual or a Group to Use a Data Set" on page 1-32 and "Task MVS-11. Denying an Individual or a Group Use of a Data Set" on page 1-33.

PROCEDURE:

Step 1. Find the name of the profile that currently protects the data set. To do this, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

Step 2. Removing RACF protection.

If the data set is protected by a discrete profile, or if you are removing protection from all data sets covered by a generic profile, delete the data set profile by issuing the DELDSD command as follows:

```
DELDSD    'profile-name'
```

This deletes the profile, but leaves the data set intact.

Examples:

To remove RACF protection from data set SMITH.PROJ.ONE, which is protected by a discrete profile, type:

```
DELDSD    'SMITH.PROJ.ONE'
```

To remove RACF protection from data sets SMITH.FIRST.DATA, SMITH.SECOND.DATA, and SMITH.THIRD.DATA, which are protected by profile SMITH.*.DATA, enter the following command:

```
DELDSD  'SMITH.*.DATA'
```

Warning

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected. In the above example RACF protection would be removed from any data set whose name matched the profile name, such as SMITH.OTHER.DATA.

Note also that when you delete a discrete or generic profile, the data set might still be protected by another generic profile. In the examples above, the data sets might be protected by profile SMITH.** (if enhanced generic naming is in effect) or profile SMITH.* (if enhanced generic naming is not in effect).

If the data set is protected by a generic profile, and you want to keep the generic profile to protect other data sets, remove protection by renaming the data set so that its new name is not matched by *any* generic profile.

Example:

If data sets SMITH.FIRST.DATA and SMITH.SECOND.DATA are protected by profile SMITH.*.DATA, and you want to remove protection from SMITH.FIRST.DATA, rename data set SMITH.FIRST.DATA to a name not protected by SMITH.*.DATA, such as SMITH.FIRST.DATA2.

Note: To check if RACF still protects the renamed data set, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18 to find out how the renamed data set is now protected.

To "remove protection" from a data set without deleting a profile or renaming the data set, protect the data set with a profile that has UACC(ALTER) and no names in the access list.

Note: Other security characteristics of the profile, such as LEVEL and SECLEVEL, might still be required by your installation and defined in the profile.

Example:

If data sets SMITH.PROJ.ONE and SMITH.PROJ.TWO are protected by generic profile SMITH.PROJ.*, and you want to remove protection from SMITH.PROJ.ONE, create a new profile SMITH.PROJ.ONE. For specific instructions on creating a discrete profile, see "Task MVS-8. Creating A Discrete Profile To Protect A Data Set" on page 1-27.

Task MVS-15. Logging On to a Group Other Than Your Default Group

Note to the Reader

Use this procedure *only if* your installation does not have list-of-groups processing in effect.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups you belong to, you need not use this procedure.

To find out if list-of-groups processing is in effect, ask your RACF security administrator.

SITUATION: A particular group may use a data set containing a report that is critical to a presentation you are preparing. You need the information.

PROCEDURE:

Step 1. Determine what groups you belong to.

You must first belong to a group before you can log on to it. If you know that you belong to the group you need, proceed with Step 2. If you do not know whether you belong to the group you need, use the LISTUSER command, as described in Task MVS-2, to see a list of the groups you belong to.

Step 2. Log on to a group other than your default group.

For TSO/E Users

This example shows an example of an actual screen. Enter the group name you want to logon to in the GROUP IDENT field of the TSO logon screen. The following screen shows a user logging on to group DEPTD60.

```
ENTER LOGON PARAMETERS BELOW:     RACF LOGON PARAMETERS:

USERID       ======> XYZ1JES

PASSWORD     ======>              NEW PASSWORD ====>

PROCEDURE    ======> PROC01       GROUP IDENT  ====> DEPTD60

ACCT NMBR    ======> A4446B

SIZE         ======>

PERFORM      ======>

COMMAND      ======>
```

For Non-TSO/E Users

Enter:

```
LOGON  userid  GROUP(group-name)
```

The userid is your userid and the group name is the name of the group you wish to log on to.

For example, to log on to group DEPTD60, enter the following command:

```
LOGON  XYZ1JES  GROUP(DEPTD60)
```

Chapter 2. Using RACF ISPF Panels On MVS

This chapter includes the following tasks, which describe how to use RACF ISPF panels on MVS:

Some Notes about RACF ISPF Panels

RACF ISPF panels have a tutorial that gives you a general description of RACF. If you would like to view the tutorial, select the RACF option on the ISPF menu. On the next panel you see, select the tutorial option.

On each RACF ISPF panel, you can get online help by entering the HELP command (this is usually defined as PF1).

The panel illustrations contain the panel identifiers, which you can display by entering the ISPF command PANELID on the command line.

The panel illustrations use the convention

```
<<< field name >>>
```

to show variable, protected text fields. Variable, protected text fields contain the information previously entered on one panel that RACF displays on a subsequent panel.

Task MVS-16. Finding Out If and How You Are RACF-Defined

SITUATION: If you can display your user profile, you are defined to RACF. To find out *how* you are defined to RACF, examine your user profile.

Note: To find out your authority to a data set, see the field labeled YOUR ACCESS in the display of the data set profile. See "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 4. Press ENTER.

Option 4 gives you the following 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
3 DELETE    Delete a user profile             for profiles
4 PASSWORD  Change your own password
5 AUDIT     Monitor users activity
             (for auditors only)

ENTER USER INFORMATION:

USER ID   ===>
```

On the OPTION line, type D. In the USER ID field, type your userid. Press ENTER.

Option D gives you the following panel:

```
ICHP48                RACF - DISPLAY FOR USER PROFILE
COMMAND ===>

ENTER OPTIONAL PARAMETERS:

   RACF      ===>          To list RACF basic information, enter YES
                           (The default will be YES.)

   TSO       ===>          To list TSO information, enter YES
                           (The default will be NO.)

   DFP       ===>          To list DFP information, enter YES
                           (The default will be NO.)
```

Specify YES for the information you want. If you want only RACF information, press ENTER.

The RACF information is similar to that shown in Figure 2-1 on page 2-5. For detailed descriptions of the fields appearing in the output, see Figure 1-1 on page 1-4.

The TSO information is similar to that shown in Figure 2-2 on page 2-6

The DFP information is similar to that shown in Figure 2-3 on page 2-7.

Your RACF security administrator creates and maintains your user profile.

If, after determining what your operating privileges and restrictions are, you need to change your user profile, see your RACF security administrator.

```
The following is the first part of the RACF information that describes
you as a user:

USER=your   NAME=your name      OWNER=the owner   CREATED=date you were
     userid                           of this profile     defined to RACF

 DEFAULT-GROUP=your     PASSDATE=date your    PASS-INTERVAL=length of time
              default           password was               your password
              group name        last updated               is valid

 ATTRIBUTES=your operating privileges and restrictions

 REVOKE DATE=date on which      RESUME DATE=date on which RACF allows
            RACF prevents you             you to use the system
            from using the system         again

 LAST-ACCESS=last date you used the system

 CLASS AUTHORIZATIONS=installation-assigned classes in which you
                      can define profiles.

 INSTALLATION-DATA=information your installation maintains about you

 MODEL-NAME=a profile used as a model for new data set profiles

 LOGON ALLOWED=time during which you can access the system


The following portion of the RACF information describes the RACF group(s)
you belong to and what you can do as a member of the group(s):


  GROUP=name  AUTH=your  CONNECT-OWNER=owner   CONNECT-DATE=date you
        of         group             of this              were connected
        group      authority           group              to this group

    CONNECTS=number of times   UACC=universal    LAST-CONNECT=last time
          you were connected        access                    you were
               to this group        authority                 connected

    CONNECT ATTRIBUTES=your operating privileges as a member of this group

    REVOKE DATE=date on which      RESUME DATE=date on which RACF
                RACF prevents you             allows you to access
                from accessing the system     the system again
                through this group            through this group

The following is the second part of the RACF information that
describes you as a user:

SECURITY-LEVEL=your installation-assigned security level

CATEGORY-AUTHORIZATION
 your installation-assigned security categories
```

Figure 2-1. RACF Information in a User Profile

The following describes the TSO information in a user profile:

```
TSO INFORMATION

 JOBCLASS=default  MSGCLASS=default  HOLDCLASS=default  SYSOUTCLASS=default  DEST=default
         job               message           hold                SYSOUT   destination
         class             class             class               class     identifier

 ACCTNUM=default account number

 PROC=default   UNIT=default    USERDATA=user data
      LOGON          unit
      procedure

 SIZE=default   MAXSIZE=default
      region           maximum
      size             region size
```

The following is actual TSO information for a user:

```
TSO INFORMATION
 JOBCLASS=C  MSGCLASS=R  HOLDCLASS=H  SYSOUTCLASS=J  DEST=LIN1215
 ACCTNUM=P36889
 PROC=PROC01    UNIT=LIN        USERDATA=1F09
 SIZE=0001024   MAXSIZE=0004096
```

Figure 2-2. TSO Information in a User Profile

The following is how DFP information appears in a user profile:

```
DFP INFORMATION
   STORCLAS=your default for  MGMTCLAS=your default for
            storage class              management class
   DATACLAS=your default for  APPLICATION-ID=your default for
            data class                        data application
                                              identifier
```

The following is actual DFP information for a user:

```
DFP INFORMATION
   STORCLAS=DFPST01           MGMTCLAS=DFPMG01
   DATACLAS=DFPDT01           APPLICATION-ID=DFPID01
```

Figure 2-3. DFP Information in a User Profile

Task MVS-17. Finding Out What Data Set Profiles You Have

SITUATION: You have data set profiles, but you are not sure how many you have.

Note: If you want to know which profile protects a particular data set, see "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following 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
TYPE              ===>   Blank, MODEL, or TAPE
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
USE MODEL PROFILE ===>   YES if the profile is to be modeled
```

On the OPTION line, type S. Press ENTER.

Option S gives you the following panel:

```
ICHP19              RACF - SEARCH FOR DATA SET PROFILES              1 of 2
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.
                            Enter * to select undefined SECLEVELs

ENTER INPUT FILTER STRING:
    FILTER    ===>

TO ADD ADDITIONAL INFORMATION ENTER YES:

    Generate TSO CLIST                  ===>
    Specify additional SEARCH criteria  ===>
```

Enter the requested information in the fields on the panel. Press ENTER.

To narrow the list of profiles displayed, you can specify either of the following:

- MASK1, MASK2, or both.
- FILTER

Note: You cannot specify both MASK and FILTER.

MASK1 specifies that RACF select profile names starting with this character string. MASK2 specifies that RACF select only those profile names containing this character string somewhere after the occurrence of MASK1. MASK1 and MASK2 together must not exceed 44 characters.

FILTER allows you to use generic characters (% and *).

For more information on using MASK and FILTER, see the description of the SEARCH command in the *RACF Command Language Reference*.

If you specify YES for the "Specify additional SEARCH criteria" field, RACF displays the following panel:

```
ICHP19A              RACF - SEARCH FOR DATA SET PROFILES              2 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

   AGE       ===>          0-9999 DAYS
   TYPE      ===>          GENERIC, DISCRETE, VSAM, NONVSAM,
                            MODEL, WARNING, TAPE or ALL
   LEVEL     ===>          0-99
   SECLEVEL  ===>
                            Enter * to select undefined SECLEVELs
   CATEGORY  ===>
                            Enter * to select undefined CATEGORYs
   VOLUMES   ===>      ===>      ===>      ===>      ===>
             ===>      ===>      ===>      ===>      ===>
```

Enter the requested information in the fields on the panel. Press ENTER.

For Example:

To find out what profiles you have with your userid as the high-level qualifier, complete the panels as shown:

```
ICHP19              RACF - SEARCH FOR DATA SET PROFILES              1 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

    MASK1 ===> YOUR USERID
                              MASK1 selects profile names starting with
                              the specified character string.
    MASK2 ===>
                              MASK2 selects profile names containing the
                              specified string somewhere after the MASK1 string.
                              Enter * to select undefined SECLEVELs

ENTER INPUT FILTER STRING:
    FILTER    ===>

TO ADD ADDITIONAL INFORMATION ENTER YES:

    Generate TSO CLIST                  ===>
    Specify additional SEARCH criteria  ===>
```

If you specify YES for the "Specify additional SEARCH criteria" field, RACF displays the following panel:

```
ICHP19A              RACF - SEARCH FOR DATA SET PROFILES                2 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

   AGE         ===>            0-9999 DAYS
   TYPE        ===> ALL        GENERIC, DISCRETE, VSAM, NONVSAM,
                                MODEL, WARNING, TAPE or ALL
   LEVEL       ===>            0-99
   SECLEVEL    ===>
                                Enter * to select undefined SECLEVELs
   CATEGORY    ===>
                                Enter * to select undefined CATEGORYs
   VOLUMES     ===>        ===>        ===>        ===>        ===>
               ===>        ===>        ===>        ===>        ===>
```

If you specify ALL for the TYPE field and press ENTER, RACF will list all the profiles with your userid as the high-level qualifier.

Task MVS-18. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

Note: You may also change your password while logging on to the system. See "Task MVS-1. Finding Out If And How You Are RACF-Defined" on page 1-2.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may also not allow you to re-use a previous password. See your RACF security administrator for an explanation of your installation's rules for passwords.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 4. Press ENTER.

Option 4 gives you the following 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   ===>
```

On the OPTION line, type 4 and enter your userid in the USER ID field. Press ENTER.

Option 4 gives you the following panel:

```
ICHP44          RACF - CHANGE USER PASSWORD  - <<<userid>>>
COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>

   NEW PASSWORD      ===>

   INTERVAL          ===>
```

To change your password, enter the requested information. Press ENTER.

If you have chosen an incorrect password, you will get a message stating that the password has not been changed. See your RACF security administrator for an explanation of your installation's rules for passwords.

For Example:

To change your password from "subject" to "tester" complete the panel as follows:

```
ICHP44          RACF - CHANGE USER PASSWORD  - <<<userid>>>
COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>  subject

   NEW PASSWORD      ===>  tester

   INTERVAL          ===>
```

Note: The passwords are shown in this book to illustrate how to enter them. On the system, the passwords are *not* displayed as you type them. This is to prevent others from seeing what they are.

Task MVS-19. Finding Out How a Data Set is Protected

SITUATION: You created a data set that needs protection, but you do not know whether you currently have a profile that protects the data set.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET             ADD, CHANGE, DELETE, or DISPLAY the profile
                           for a 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.

   X  EXIT                 Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following panel:

```
ICHP10                  RACF - DATA SET SERVICES

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
    TYPE              ===>    Blank, MODEL, or TAPE
    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
    USE MODEL PROFILE ===>    YES if the profile is to be modeled
```

On the OPTION line, type D. If you know the profile name that protects the data set, enter the profile name and any other appropriate information.

If you do not know the profile name, leave the PROFILE NAME field blank. Press ENTER.

Note: For a discrete profile, the profile name and data set name are the same.

Option D gives you the following panel:

```
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):

    ===>       ===>       ===>       ===>       ===>
    ===>       ===>       ===>       ===>       ===>
    ===>       ===>       ===>       ===>       ===>
```

Enter information to identify the profile(s) to be displayed, and to describe how much information from each profile is to be displayed.

If you do not know or do not remember the profile name, enter the following:

- PREFIX: Enter as much of the profile name as you remember. You can specify your userid alone, but you will see all profiles for all data sets. Add more qualifiers to make the profile name more specific. However, if you add too many qualifiers, you will get no matches, even though profiles exist. For example, if you have a profile SMITH.TEST*.LNKLIB, entering SMITH.TEST2.LNKLIB will not display the profile.
- DISCRETE: Enter YES.
- GENERIC: Enter YES.

You should also enter YES in the categories that you want information displayed about the profile, such as ACCESS LIST, HISTORY, or STATISTICS.

You should see output similar to that in Figure 2-4 on page 2-21.

If you get a message stating you are not authorized, see your RACF security administrator.

```
INFORMATION FOR DATASET SMITH.TEST.LINKLIB

LEVEL    OWNER        UNIVERSAL ACCESS     WARNING     ERASE
-----    -----        ----------------     -------     -----
 00      SMITH            READ               NO         NO

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

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS            CREATION GROUP         DATASET TYPE
-------------        ----------------       -------------
   READ                   DEPTD60               NON-VSAM

VOLUMES ON WHICH DATASET RESIDES             UNIT
---------------------------------            ------
          21345                              SYSDA

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

SECURITY LEVEL
-----------------------------------------------
NO SECURITY LEVEL

CATEGORIES
-----------
NOCATEGORIES

CREATION DATE     LAST REFERENCE DATE     LAST CHANGE DATE
(DAY)  (YEAR)      (DAY)     (YEAR)        (DAY)   (YEAR)
-------------     ------------------     --------------
 070    85          070       85            070     85

ALTER COUNT    CONTROL COUNT    UPDATE COUNT    READ COUNT
-----------    -------------    ------------    ----------
 00000           00000            00002          00000

 ID           ACCESS               ACCESS COUNT
----         --------             --------------
JONES         UPDATE                 00009
WILLS         READ                   00015

PROGRAM       ID       ACCESS    ACCESS COUNT
--------   ---------  --------  --------------
NO ENTRIES IN CONDITIONAL ACCESS LIST

DFP INFORMATION

RESOWNER
--------
SMITH
```

Figure 2-4. Display of a Data Set Profile

Check the following fields for the most important security information about how the data set is protected:

- the LEVEL field (if used at your installation)
- the OWNER field
- the UNIVERSAL ACCESS field
- the WARNING field
- the SECURITY LEVEL field (if used at your installation)
- the CATEGORIES field (if used at your installation)
- the ID field and its related ACCESS and ACCESS COUNT fields
- the PROGRAM field and its related ID, ACCESS, and ACCESS COUNT fields

For detailed descriptions of the terms appearing in the output, see "Task MVS-5. Finding Out How a Data Set is Protected" on page 1-18.

Task MVS-20. Changing a Data Set's Universal Access Authority (UACC)

SITUATION: You have a data set containing research data, which you need to protect so that no one can tamper the data.

INFORMATION YOU NEED TO KNOW FIRST: You must know the name of the profile that protects your data set. See "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following 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
  TYPE              ===>    Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE ===>    YES if the profile is to be modeled
```

On the OPTION line, type 2. Enter the profile name and any other appropriate information. Press ENTER.

For a discrete profile, the profile name and data set name are the same.

Option 2 gives you the following panel:

```
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, ALTER, OR
                                    EXECUTE
   AUDIT SUCCESSES    ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   REMOVE NOTIFY      ===>          YES OR BLANK
   NOTIFY USER        ===>          USERID
   ERASE WHEN DELETED ===>          YES, NO OR BLANK
   RETENTION PERIOD   ===>          (TAPE ONLY) 1-65,534 DAYS
                                    OR 99,999 DAYS FOR NEVER
TO CHANGE OPTIONAL INFORMATION, ENTER YES:
   VOLUMES            ===>          SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>          DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Enter the UACC you want to assign to this profile.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets on MVS" on page A-2.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-24. Permitting an Individual or a Group to Use a Data Set" on page 2-39 for information on how to permit selected users or groups to access a data set.)

If you get a message stating you are not authorized, see your RACF security administrator.

For Example:

To change the UACC for profile USERID.PROJ.ONE to NONE, complete the panel as follows:

```
ICHP12                RACF - CHANGE DATA SET PROFILE
COMMAND ===>

   PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER DATA SET PROFILE INFORMATION TO BE CHANGED:

   OWNER              ===>            USERID OR GROUP NAME
   LEVEL              ===>            0-99
   FAILED ACCESSES    ===>            FAIL OR WARN
   UACC               ===> NONE       NONE, READ, UPDATE, CONTROL, ALTER, OR
                                      EXECUTE
   AUDIT SUCCESSES    ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   REMOVE NOTIFY      ===>            YES OR BLANK
   NOTIFY USER        ===>            USERID
   ERASE WHEN DELETED ===>            YES, NO OR BLANK
   RETENTION PERIOD   ===>            (TAPE ONLY) 1-65,534 DAYS
                                      OR 99,999 DAYS FOR NEVER
TO CHANGE OPTIONAL INFORMATION, ENTER YES:
   VOLUMES            ===>            SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>            DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Task MVS-21. Choosing Between Discrete and Generic Profiles

SITUATION: You need to protect one or more data sets, and no existing profile provides the exact protection needed.

If you need to determine how a particular data set is protected, see "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

If your installation has always-call support (ask your RACF security administrator), a generic profile might already exist under which the data set is protected. However, that profile might not provide the exact protection you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

- If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set.
- If a data set is protected by more than one generic profile, the *most specific* profile sets the level of protection for the data set.

PROCEDURE:

Step 1. Choose a *generic profile* for one of the following reasons:

- To protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
- If you have a single data set that might be deleted, then re-created, and you want the protection to remain the same, you can create a fully-qualified generic profile. The name of a fully-qualified generic profile matches the name of the data set it protects. Unlike a discrete profile, a fully-qualified generic profile is not deleted when the data set itself is deleted.

To create a generic profile, see "Task MVS-23. Creating a Generic Profile To Protect Data Sets" on page 2-34.

Step 2. Choose a *discrete profile* for the following reason:

- To protect one data set with unique security requirements. The name of a discrete profile matches the name of the data set it protects.

To create a discrete profile, see "Task MVS-22. Creating a Discrete Profile To Protect a Data Set" on page 2-29.

Notes:

1. All the members of a partitioned data set (PDS) are protected by one profile (the profile that protects the data set).
2. If your installation has always-call support, all the components of a VSAM data set are protected by one profile (the profile that protects the cluster name). You do not need to create profiles that protect the index and data components of a cluster. If your installation does *not* have always-call support, you must ensure that the index and data components of a VSAM cluster are protected the same way the cluster name is protected.

3. For a generic profile, unit and volume information is ignored because the data sets that are protected under the generic profile can be on many different volumes.

Task MVS-22. Creating a Discrete Profile To Protect a Data Set

SITUATION: You have a single data set that need to be protected with unique requirements.

If you need to determine how a particular data set is protected, see "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following panel:

```
ICHP10                  RACF - DATA SET SERVICES
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1 ADD         Add a profile       D DISPLAY    Display profile profile
   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
  TYPE               ===>   Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE  ===>   YES if the profile is to be modeled
```

On the OPTION line, type 1. Enter the profile name and any other appropriate information. Press ENTER.

Option 1 gives you the following 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, ALTER, OR
                                    EXECUTE
   AUDIT SUCCESSES    ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   INDICATOR          ===>          SET, NOSET, OR ONLY
   NOTIFY             ===>          USERID
   ERASE WHEN DELETED ===>          BLANK OR YES

TO ADD OPTIONAL INFORMATION, ENTER YES:

   OTHER VOLUMES      ===>          SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>          DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Enter the requested information about the profile you are creating. Press ENTER.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-24. Permitting an Individual or a Group to Use a Data Set" on page 2-39 for information on how to permit selected users or groups to access a data set.)

For Example:

To create a discrete profile for your data set, USERID.PROJ.ONE, with a UACC of NONE, complete the panel as follows:

```
ICHP11                  RACF - ADD DATA SET PROFILE
COMMAND ===>

   PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

   OWNER              ===>           USERID OR GROUP NAME
   LEVEL              ===>           0-99
   FAILED ACCESSES    ===>           FAIL OR WARN
   UACC               ===> NONE      NONE, READ, UPDATE, CONTROL, ALTER, OR
                                     EXECUTE
   AUDIT SUCCESSES    ===>           READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>           READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   INDICATOR          ===>           SET, NOSET, OR ONLY
   NOTIFY             ===>           USERID
   ERASE WHEN DELETED ===>           BLANK OR YES

TO ADD OPTIONAL INFORMATION, ENTER YES:

   OTHER VOLUMES      ===>           SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>           DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

For Example:

To create a discrete profile for group data set GROUPID.PROJ.ONE with a UACC of READ, complete the panel as follows:

```
ICHP11                    RACF - ADD DATA SET PROFILE
COMMAND ===>

   PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

   OWNER              ===>            USERID OR GROUP NAME
   LEVEL              ===>            0-99
   FAILED ACCESSES    ===>            FAIL OR WARN
   UACC               ===> READ       NONE, READ, UPDATE, CONTROL, ALTER, OR
                                      EXECUTE
   AUDIT SUCCESSES    ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   INDICATOR          ===>            SET, NOSET, OR ONLY
   NOTIFY             ===>            USERID
   ERASE WHEN DELETED ===>            BLANK OR YES

TO ADD OPTIONAL INFORMATION, ENTER YES:

   OTHER VOLUMES      ===>            SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>            DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Task MVS-23. Creating a Generic Profile To Protect Data Sets

SITUATION: You have several data sets that have the same security requirements and that have some identical characters in their names.

To create a generic profile for your user data set, the high level qualifier must be your userid.

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name you specify. (See "Enhanced Generic Names" on page A-4 for information on the rules for specifying generic characters.)

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following 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
  TYPE              ===>    Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE ===>    YES if the profile is to be modeled
```

On the OPTION line, type 1. Enter the profile name and any other appropriate information. Press ENTER.

Option 1 gives you the following 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, ALTER, OR
                                    EXECUTE
   AUDIT SUCCESSES    ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>          READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   INDICATOR          ===>          SET, NOSET, OR ONLY
   NOTIFY             ===>          USERID
   ERASE WHEN DELETED ===>          BLANK OR YES

TO ADD OPTIONAL INFORMATION, ENTER YES:

   OTHER VOLUMES      ===>          SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>          DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Enter the requested information about the profile you are creating. Press ENTER.

If you get a message stating you are not authorized, see your RACF security administrator.

If, after creating a generic profile, you want to create a data set that has more specific access requirements than allowed under the existing generic profile, create a discrete profile (or a more specific generic profile) for the data set.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-24. Permitting an Individual or a Group to Use a Data Set" on page 2-39 for information on how to permit selected users or groups to access a data set.)

For Example:

To create a generic profile USERID.* with a UACC of NONE and no recording of attempts to access the data set, complete the panel as follows:

```
ICHP11                    RACF - ADD DATA SET PROFILE
COMMAND ===>

   PROFILE NAME: <<<USERID.*>>>

ENTER OR CHANGE DATA SET PROFILE INFORMATION:

   OWNER              ===>            USERID OR GROUP NAME
   LEVEL              ===>            0-99
   FAILED ACCESSES    ===>            FAIL OR WARN
   UACC               ===> NONE       NONE, READ, UPDATE, CONTROL, ALTER, OR
                                      EXECUTE
   AUDIT SUCCESSES    ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   AUDIT FAILURES     ===>            READ, UPDATE, CONTROL, ALTER, OR NOAUDIT
   INDICATOR          ===>            SET, NOSET, OR ONLY
   NOTIFY             ===>            USERID
   ERASE WHEN DELETED ===>            BLANK OR YES

TO ADD OPTIONAL INFORMATION, ENTER YES:

   OTHER VOLUMES      ===>            SECURITY LEVEL/CATEGORIES ===>
   INSTALLATION DATA  ===>            DFP PARAMETERS            ===>
   ACCESS LIST        ===>
```

Task MVS-24. Permitting an Individual or a Group to Use a Data Set

SITUATION: You would like J.E. Jones, whose userid is JONES, to use a RACF-protected data set.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on MVS" on page A-5.

INFORMATION YOU NEED TO KNOW FIRST: You must know the name of the profile that protects the data set. See "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

You must also decide whether to use the profile that protects the data set.

- If the profile is a discrete profile, continue this procedure.
- If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.

   X  EXIT               Exit out of RACF.
```

On the OPTION line type, 1. Press ENTER.

Option 1 gives you the following 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
  TYPE              ===>    Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE ===>    YES if profile is to be modeled
```

On the OPTION line, type 4. Enter the profile name and any other appropriate information. Press ENTER.

Option 4 gives you the following 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.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following panel:

```
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 FROM WHICH ACCESS LIST IS TO BE COPIED:
PROFILE NAME  ===>
CLASS         ===>
GENERIC       ===>          YES if the profile name is generic
VOLUME SERIAL ===>          If a non-cataloged data set profile

TO ADD PROGRAM NAMES, ENTER YES ===>
```

Enter the userid and the access you wish to assign to that person or group.

For Example:

To add userid SMITH to the access list with READ authority to the profile USERID.PROJ.ONE, complete the panel as follows:

```
ICHP141             RACF - MAINTAIN DATA SET ACCESS LIST - ADD
COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL, or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===> SMITH   ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>

ENTER INFORMATION FOR PROFILE FROM WHICH ACCESS LIST IS TO BE COPIED:
PROFILE NAME  ===>
CLASS         ===>
GENERIC       ===>    YES if the profile name is generic
VOLUME SERIAL ===>    If a non-cataloged data set profile

TO ADD PROGRAM NAMES, ENTER YES ===>
```

For Example:

To add the userid, SMITH and the groupid GROUPA, to the access list with READ authority to the profile GROUPB.PROJ.ONE, complete the panel as follows:

```
ICHP141             RACF - MAINTAIN DATA SET ACCESS LIST - ADD
COMMAND ===>

PROFILE NAME: <<<GROUPB.PROJ.ONE>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL, or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===> SMITH   ===>         ===>         ===>         ===>
===> GROUPA  ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>

ENTER INFORMATION FOR PROFILE FROM WHICH ACCESS LIST IS TO BE COPIED:
PROFILE NAME  ===>
CLASS         ===>
GENERIC       ===>    YES if the profile name is generic
VOLUME SERIAL ===>    If a non-cataloged data set profile

TO ADD PROGRAM NAMES, ENTER YES ===>
```

Task MVS-25. Denying an Individual or a Group Use of a Data Set

SITUATION: A colleague who has left the department can still use a data set. For security reasons you wish to exclude the person from using the data set.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on MVS" on page A-5.

INFORMATION YOU NEED TO KNOW FIRST: You must know the name of the profile that protects your data set. See "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

You must also decide whether to use the profile that protects the data set.

- If the profile is a discrete profile, continue this procedure.
- If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Task MVS-19. Finding Out How a Data Set is Protected" on page 2-18.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following 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
  TYPE              ===>  Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE ===>  YES if profile is to be modeled
```

On the OPTION line, type 4. Enter the profile name and any other appropriate information. Press ENTER.

Option 4 gives you the following 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.
```

If you wish to remove ALL users or groups from the access list, on the OPTION line, type 3. Press ENTER.

If you wish to remove only certain users or groups from the access list, on the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
ICHP142     RACF - MAINTAIN DATA SET ACCESS LIST - REMOVE
COMMAND ===>

PROFILE NAME: <<<profile name>>>

ENTER USER/GROUP ID TO BE REMOVED:

===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>

TO REMOVE PROGRAM NAMES, ENTER YES ===>
```

Enter the userid(s) or groupid(s) you wish to remove from the access list.

For Example:

To remove userid SMITH from the access list of the profile USERID.PROJ.ONE, complete the panel as follows:

```
ICHP142     RACF - MAINTAIN DATA SET ACCESS LIST - REMOVE
COMMAND ===>

PROFILE NAME: <<<USERID.PROJ.ONE>>>

ENTER USER/GROUP ID TO BE REMOVED:

===> SMITH    ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>

TO REMOVE PROGRAM NAMES, ENTER YES ===>
```

Task MVS-26. Removing Protection From Your Data Set

SITUATION: You have a data set containing experimental data which has been published. You no longer feel it is necessary to protect the data.

Warning

When you delete a data set profile, anyone (RACF-defined or not) can access, change, and/or delete your data set. You can selectively "remove" protection by selectively permitting or denying access to your data set. For more information, see "Task MVS-24. Permitting an Individual or a Group to Use a Data Set" on page 2-39 and "Task MVS-25. Denying an Individual or a Group Use of a Data Set" on page 2-45.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 1. Press ENTER.

Option 1 gives you the following 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
  TYPE              ===>   Blank, MODEL, or TAPE
  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
  USE MODEL PROFILE ===>   YES if profile is to be modeled
```

On the OPTION line, type 3. Enter the profile name and any other appropriate information. Press ENTER.

Option 3 gives you the following panel:

```
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.
```

Press ENTER.

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected.

Chapter 3. Using RACF Commands On VM

This chapter includes the following tasks, which describe how to use RACF commands on VM:

ICH Messages

If the command fails, you will get a message. If the message ID begins with ICH, you can get an online explanation of the message by typing:

```
HELP command-name MSGID(message-id)
```

For example, to display the explanation for message ICH13002I (an RDEFINE message) enter the following:

```
HELP RDEFINE MSGID(ICH13002I)
```

Note: If you get a message, but do not get a message ID, do the following:

1. End the RACF command session (type the END command).
2. Enter the CMS command SET EMSG ON.
3. Re-start the RACF command session (type the RACF command).
4. Re-enter the RACF command that failed.
5. Re-enter the HELP command.

IKJ Messages

If you happen to make a mistake entering a RACF command in a RACF command session, you might start getting IKJ messages (such as "INVALID KEYWORD"). The system is prompting for keywords or values it recognizes as correct. To escape from the prompt sequence, enter

```
hx
```

This stops the prompt sequence and allows you to continue the RACF command session.

Task VM-1. Finding Out If and How You Are RACF-Defined

SITUATION: If RACF is installed on your VM system and you can log on, you are RACF-defined. If you want to find out *how* you are defined to RACF, list your RACF user profile. To list your RACF user profile, issue the LISTUSER command.

Note: To find out your authority to a minidisk, list the *minidisk profile* and check the field labeled YOUR ACCESS in the listing. See "Task VM-4. Finding Out How a Minidisk is Protected" on page 3-12.

First, log on to the system by entering your userid. If you are not aware that you have a userid, see your group or security administrator or someone in authority at your installation. Without a userid you cannot use the system.

> Be aware, if this is the first time you have ever logged on to the system, that you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the format of the assigned password.

PROCEDURE:

Step 1. After you have logged on to the system, enter a RACF command session by issuing the following command:

```
RACF
```

Step 2. To see how you are defined to RACF, issue the LISTUSER command:

```
LISTUSER
```

You will see output similar to that shown in Figure 3-1 on page 3-3 and Figure 3-2 on page 3-4.

Step 3. If, after you have determined what authority you have, you wish to terminate the RACF command session, enter the END command:

```
END
```

```
The following is the first part of the RACF information that
describes a user:

USER=AHLEE   NAME=A.H.LEE     OWNER=JONES  CREATED=88.096

DEFAULT-GROUP=PAYROLL PASSDATE=88.124   PASS-INTERVAL= 30

ATTRIBUTES=NONE

REVOKE DATE=NONE   RESUME DATE=NONE

LAST-ACCESS=88.130/13:47:18

CLASS AUTHORIZATIONS=NONE

NO-INSTALLATION-DATA

NO-MODEL-NAME

LOGON ALLOWED   (DAYS)          (TIME)

---------------------------------------------------------------

ANYDAY                           ANYTIME

The following part of the RACF information describes the RACF
group(s) the user belongs to and what the user can do as a
member of the group(s):

GROUP=PAYROLL AUTH=USE CONNECT-OWNER=MILL CONNECT-DATE=88.096

   CONNECTS= 04  UACC=NONE  LAST-CONNECT=88.130/13:47:18

   CONNECT ATTRIBUTES=NONE

   REVOKE DATE=NONE   RESUME DATE=NONE

The following is the second part of the RACF information that
describes a user:

SECURITY-LEVEL=NONE SPECIFIED

CATEGORY-AUTHORIZATION
 NONE SPECIFIED
```

Lee has none of the possible user attributes, but can still use RACF. For example, Lee can permit or deny access to his A-disk.

Lee belongs to one group, PAYROLL.

In the PAYROLL group, Lee has USE group authority, and can use any of resources that the group can use.

A detailed description of the output follows Example 2.

Figure 3-1. Output of LISTUSER Command on VM: Example 1

```
The following is the first part of the RACF information that
describes a user:

USER=SMITH   NAME=J.E.SMITH   OWNER=JONES  CREATED=88.096

DEFAULT-GROUP=SEARCH  PASSDATE=88.103   PASS-INTERVAL= 30

ATTRIBUTES=AUDITOR

REVOKE DATE=NONE   RESUME DATE=NONE

LAST-ACCESS=88.114/13:47:18

CLASS AUTHORIZATIONS=NONE

NO-INSTALLATION-DATA

NO-MODEL-NAME

LOGON ALLOWED   (DAYS)           (TIME)

-----------------------------------------------------------------

ANYDAY                           ANYTIME

The following part of the RACF information describes the RACF
group(s) the user belongs to and what the user can do as a
member of the group(s):

GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=88.096

   CONNECTS= 01   UACC=NONE   LAST-CONNECT=88.114/13:50:18

   CONNECT ATTRIBUTES=NONE

   REVOKE DATE=NONE   RESUME DATE=NONE

GROUP=PAYROLL AUTH=USE CONNECT-OWNER=MILL CONNECT-DATE=88.096

   CONNECTS= 00  UACC=NONE  LAST-CONNECT=88.114/13:55:18

   CONNECT ATTRIBUTES=NONE

   REVOKE DATE=NONE   RESUME DATE=NONE

The following is the second part of the RACF information that
describes a user:

SECURITY-LEVEL=NONE SPECIFIED

CATEGORY-AUTHORIZATION
 NONE SPECIFIED
```

Smith has the AUDITOR system-wide attribute. Not only can Smith control access to her A-disk, but, as system AUDITOR, she can audit security controls and create security reports.

Smith belongs to two groups, SEARCH and PAYROLL.

In the SEARCH group, Smith has JOIN group authority, and can assign group authorities to members of the group.

In the PAYROLL group, Smith has USE group authority, and can use any of the resources that the group can use.

A detailed description of the output follows this example.

Figure 3-2. Output of LISTUSER Command on VM: Example 2

Here are detailed descriptions of the terms appearing in the output:

USER
Your userid is the name the system knows you by. It is frequently a combination of such identifying information as your name, initials, personnel number, or department.

NAME
Your name as recorded in your user profile.

OWNER
The user ID or group name of the owner of your user profile. The owner of your profile can modify your profile.

CREATED
The date you were defined to RACF.

DEFAULT-GROUP
RACF connects each user to at least one group. If you are connected to only one group, that group is your default group and that group name appears in this field. If you are a member of more than one group, you can change this field in your user profile (using the ALTUSER command). When you log on again, the new group will be your current connect group.

PASSDATE
The date you last updated your password.

PASS-INTERVAL
The length of time in days your current password is valid. You must change your password before this interval expires.

ATTRIBUTES
The operating privileges and restrictions assigned to you. There are two types of attributes: user and connect. This field describes your system-wide attributes. See the CONNECT ATTRIBUTES field for your group-level attributes.

NONE	Allows no *special* operating privileges or restrictions. Users with NONE can still use RACF. In fact, most attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.
SPECIAL	Allows full authorization to all profiles in the RACF data base and allows you to perform all RACF functions except those requiring the AUDITOR attribute.
AUDITOR	Allows you to audit the use of system resources, to control the logging of detected accesses to resources, and to create security reports.
OPERATIONS	Allows you to have full authorization to all RACF-protected minidisks and to general resources that meet certain conditions (described in the *RACF Security Administrator's Guide*). OPERATIONS allows you to perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.
CLAUTH	Allows you to define profiles for any class specified in the class name.
REVOKE	Prohibits a user from entering the system. (You should never be able to see this attribute when you list your own profile.)

REVOKE DATE
This term appears twice in the output. On the user portion of the output, this is the date on which RACF prevents you from using the system. On the group portion of the output, this is the date on which RACF prevents you from using the system when you try to connect to this group.

RESUME DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF allows you to use the system again. In the group portion of the output, this is the date on which RACF allows you to use the system again when you are connected to this group.

LAST-ACCESS
The date is the last time you were on the on the system. RACF keeps records of all persons who have used the system, and what they have done, as well as recording unauthorized attempts to use of the system.

CLASS-AUTHORIZATIONS
Your installation assigns resources to various classes. The class appearing in this field is the class in which the user is authorized to assign RACF protection.

INSTALLATION-DATA
Additional information your installation maintains about you and your authority. If you need help to understand anything included here, see your RACF security administrator or the owner of your user profile.

MODEL-NAME
A profile used as a model for new data set profiles. (This term applies to MVS system only.)

LOGON-ALLOWED
The days of the week and/or hours in the day that RACF allows you to access the system from a terminal. These restrictions apply only to when you can log on to the system. If you are working on the system and an end-time occurs, RACF will not force you off the system. Also, these logon restrictions do not apply to batch jobs; you can still submit a batch job at any time.

The following portion is repeated once for each RACF group of which you are a member:

GROUP
The name of the group to which you are connected.

AUTH
The group authorities you have because you are a member of this group.

USE	Allows you to enter the system under the control of the specified group. You may use any of the resources the group may use.
CREATE	On MVS systems, allows you to RACF-protect group minidisks and control who can access them. It includes the privileges of the USE authority.
CONNECT	Allows you to connect RACF-defined users to the specified group and assign these users the USE, CREATE, or CONNECT authority. It includes the privileges of the CREATE authority.

JOIN — Allows you to define new users or groups to RACF and to assign group authorities. To define new users, you must also have the user attribute, CLAUTH(USER). JOIN authority includes all the privileges of the CONNECT authority.

CONNECT-OWNER
The owner of this group.

CONNECT-DATE
The date you were first connected to this group.

CONNECTS
The number of times you have been connected to this group.

UACC
The universal access authority for resources you create while connected to this group. If a user is not specifically listed in the access list describing a resource owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner specified in the UACC.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on VM" on page A-3.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. As owner of the copied minidisk, that user has control of the security characteristics of the copied minidisk, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. (For information on how to permit selected users or groups to access a minidisk, see "Task VM-6. Permitting an Individual or a Group to Use a Minidisk" on page 3-20.)

LAST-CONNECT
The last time you were connected to the group.

CONNECT-ATTRIBUTES
The operating privileges and restrictions assigned to you when you are connected to this group. Connect attributes are also called group-level attributes. The connect (group-level) attributes are:

NONE
SPECIAL
AUDITOR
OPERATIONS
REVOKE

For a description of each of these attributes, see the ATTRIBUTES field on page 3-5.

REVOKE DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF prevents you from using the system. In the group portion of the output, this is the date on which RACF prevents you from using the system when you try to connect to the group.

RESUME DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF allows you to use the system again. In the group portion of the output, this is the date on which RACF allows you to use the system again when you are connected to the group.

SECURITY-LEVEL
Your installation can define various security levels. The name appearing in this field is the security level assigned to you.

CATEGORY-AUTHORIZATION
Your installation can define various security categories. The names appearing in this field are the security categories assigned to you.

Task VM-2. Finding Out What Profiles You Have

SITUATION: You want to find the names of all of your current RACF minidisk profiles.

PROCEDURE:

Step 1. If you are not already in a RACF command session, issue the following command:

```
RACF
```

Step 2. To determine what minidisk profiles you have, issue the SEARCH command with the CLASS(VMMDISK) and MASK operands:

```
SEARCH CLASS(VMMDISK) MASK(your-userid.)
```

For example, if your userid is ADAMS, type:

```
SEARCH CLASS(VMMDISK) MASK(ADAMS.)
```

RACF will list all your minidisk profiles. For example, if two minidisks are protected with discrete profiles, you might see:

```
ADAMS.191
ADAMS.193
```

If you do not have any minidisk profiles, RACF will display a message stating that no entries meet the search criteria. Check that you have spelled everything correctly on the SEARCH command. If you have, inform your RACF security administrator that you have an unprotected minidisk, and ask that a RACF profile be created for it.

Step 3. If, after you have determined what profiles you have, you wish to terminate the RACF command session, enter the END command:

```
END
```

Task VM-3. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

Note: You may also change your password while logging on to the system. If your password has expired, RACF prompts you for a new password when you enter the old one. Before your password expires, you can clear the display, then enter the LOGON command with your userid. RACF will then prompt you for your password. At this time, you can enter both the current password and a new one.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may not allow you to re-use a previous password. See your RACF security administrator for an explanation of your installation's rules for passwords.

PROCEDURE:

Step 1. If you are not already in a RACF command session, issue the following command:

```
RACF
```

Step 2. **To change your password,** issue the PASSWORD command with the PASSWORD operand:

```
PASSWORD  PASSWORD(current-password  new-password)
```

For example, to change your password from "subject" to "testers," type:

```
PASSWORD  PASSWORD(subject  testers)
```

To change your password interval, issue the PASSWORD command with the INTERVAL keyword. Type:

```
PASSWORD  INTERVAL(interval-you-want)
```

For example, to change your password interval to 15 days, type:

```
PASSWORD  INTERVAL(15)
```

RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to be a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you may change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.

To change your password and password interval, issue the PASSWORD command with the PASSWORD and INTERVAL keywords. Type:

```
PASSWORD  PASSWORD(current-password  new-password)  INTERVAL(interval)
```

For example, to change the password from "subject" to "testers" and the interval to 15 days, type:

```
PASSWORD  PASSWORD(subject testers)  INTERVAL(15)
```

If you don't know what your current password interval is, issue the LISTUSER command and check the PASS-INTERVAL field. For more information, see "Task VM-1. Finding Out If and How You Are RACF-Defined" on page 3-2.

Step 3. If, after you have changed your password, you wish to terminate the RACF command session, enter the END command:

```
END
```

Task VM-4. Finding Out How a Minidisk is Protected

SITUATION: You are the owner of a minidisk (or you are responsible for the security protection of a minidisk), and you want to determine what protection the minidisk has. For example, you might want to find out what users and groups can access the minidisk.

INFORMATION YOU NEED TO KNOW FIRST: You need to know the virtual address of the minidisk.

The virtual address of an A-disk is, by convention, 191. To find the virtual address of one of your minidisks, enter the following command:

```
QUERY DISK n
```

where n is the letter by which you know the minidisk. For example, for the address of your A-disk, enter:

```
QUERY DISK A
```

The virtual address of the minidisk is under the column labeled CUU.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFLIST EXEC. This is described in "PROCEDURE USING THE RACFLIST EXEC" on page 3-13. Using RACFLIST does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), use the RACF commands described in "PROCEDURE USING RACF COMMANDS" on page 3-14.

PROCEDURE USING THE RACFLIST EXEC:

Enter the RACFLIST command, and RACF will display the following panel:

```
---------------------- LIST ACCESS TO DISKS OR READER --------------------

 Enter the required data and press ENTER and then press PF2:

 CURRENT PASSWORD   ===>          Enter your current password
 AUTHORIZED USERS   ===>          Enter an S for a list of authorized users
 STATISTICS         ===>          ENTER AN S FOR A STATISTICS REPORT
 HISTORY            ===>          Enter an S for a HISTORY report

 READER             ===>          Enter an S for a report for the READER
 DISKS:             ===>          Enter the disk addresses for which you
                    ===>          want a report
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authuser 11=Cmd line 12=Resources
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the AUTHORIZED USERS field, specify S if you want to display the access list of the minidisk profile.
- For the STATISTICS field, specify S if you want to display the number of times the minidisk was accessed by users.
- For the HISTORY field, specify S if you want to display information such as the date the minidisk profile was defined to RACF and the date on which the profile was last checked for UPDATE authority.
- Leave the READER field blank.
- For the DISKS fields, specify the virtual address of each minidisk for which you want information. (If you don't know the virtual address of the minidisk, see "INFORMATION YOU NEED TO KNOW FIRST" on page 3-12.)

Press PF2 to request that the information be listed. RACF displays a listing similar to that shown in Figure 3-3 on page 3-15.

After the information is displayed, clear your terminal screen, then press PF3 to leave RACFLIST.

PROCEDURE USING RACF COMMANDS:

Step 1. To enter a RACF command session, issue the following command:

```
RACF
```

Step 2. Find out if a discrete profile protects the minidisk by issuing the RLIST command as follows:

```
RLIST  VMMDISK  userid.virtual-address  ALL
```

(If you don't know the virtual address of the minidisk, see "INFORMATION YOU NEED TO KNOW FIRST" on page 3-12.)

For example, if a discrete profile protects JBROWN's A-disk, use the following command:

```
RLIST  VMMDISK  JBROWN.191  ALL
```

You will see one of the following on your screen:

- If the minidisk is protected by a discrete profile, a listing similar to that shown in Figure 3-3 on page 3-15.
- If the minidisk is not protected by a discrete profile, a message stating that no profile was found.

  Note: If generic profile checking is active, and you get the message that no profile was found, you must do Step 3 to check for generic profiles.

Step 3. To determine if the minidisk is protected by a generic profile, issue the RLIST command with the GENERIC operand as follows:

```
RLIST  VMMDISK   JBROWN.191  ALL  GENERIC
```

You will see one of the following on your screen:

- If the minidisk is not protected by a generic profile, a listing for the most specific generic profile that protects the minidisk (similar to that shown in Figure 3-3 on page 3-15).
- If the minidisk is not protected by a generic profile, a message stating that no profile was found

Step 4. If, after you have determined how the minidisk is protected, you wish to terminate the RACF command session, enter the END command:

```
END
```

```
CLASS          NAME
------         -----
VMMDISK        JBROWN.191

 LEVEL    OWNER        UNIVERSAL ACCESS     YOUR ACCESS      WARNING
 -----    -----        ----------------     -----------      -------
  00      JBROWN           READ               ALTER            NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
REVERIFY

 SECLEVEL
 --------
 NO SECLEVEL

 CATEGORIES
 ----------
 NO CATEGORIES

AUDITING
--------
NONE

NOTIFY
------
NO USER TO BE NOTIFIED

CREATION DATE     LAST REFERENCE DATE     LAST CHANGE DATE
(DAY)  (YEAR)      (DAY)     (YEAR)        (DAY)   (YEAR)
------------      ------------------      --------------
 070    85          070       85            070     85

ALTER COUNT    CONTROL COUNT    UPDATE COUNT    READ COUNT
-----------    -------------    ------------    ----------
 00000            00000            00002          00000

USER           ACCESS               ACCESS COUNT
----           ------               ------------
JBROWN         ALTER                   00009
```

Figure 3-3. Output of RLIST Command for a Minidisk Profile

Check the following fields for the most important security information about how the minidisk is protected:

- the LEVEL field (if used at your installation)
- the OWNER field
- the UNIVERSAL ACCESS field
- the WARNING field
- the SECLEVEL field (if used at your installation)
- the CATEGORIES field (if used at your installation)
- the USER field and its related ACCESS and ACCESS COUNT fields

Here are brief descriptions of the fields appearing in the output:

CLASS
The name of the class to which the resource belongs.

NAME
The name of the discrete or generic profile.

LEVEL
A security classification indicator used by each individual installation. If anything other than 00 appears in this field, see your RACF security administrator for an explanation of what the number means.

OWNER
Each RACF-defined minidisk has an owner. An owner may be a user or a group. When you RACF-protect a minidisk without specifying an owner, RACF names you the owner of the minidisk profile. The owner of the profile may modify the minidisk profile.

UNIVERSAL ACCESS
Each minidisk protected by RACF has a universal access authority (UACC). The UACC permits users or groups to use the minidisk in the manner specified in this field. In this example, the UACC is READ. Anyone may read this minidisk. (The only exception is if the user or group is specifically named in the access list with ACCESS of NONE.)

YOUR ACCESS
How you may access this minidisk.

If you must work with the listed minidisk but do not have the required authority, ask the owner (OWNER field) issue a PERMIT command to give you access to the minidisk.

WARNING
If this field contains YES, RACF permits a user to access this resource *even though his or her access authority is insufficient.* RACF issues a warning message *to the user who is attempting access;* you are notified only if your userid is the NOTIFY userid.

If this field contains NO, RACF does not permit a user with insufficient authority to access this resource.

INSTALLATION DATA
Any information your installation keeps in this minidisk profile.

APPLICATION DATA
Any information that RACF associates with the named resource.

SECLEVEL
Your installation can define its own security levels. This security level is a name associated with the numeric value shown in the LEVEL field earlier in this output. The security level displayed is the minimum security level you need to access a resource protected by this profile.

CATEGORIES
Your installation can define its own security categories. These names are the security categories you need to access a resource protected by this profile.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is NONE. RACF will not record any attempts to update the minidisk.

NOTIFY
The userid of a RACF-defined user that RACF notifies when denying access to a resource protected by this profile.

CREATION DATE
The date the profile was created.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The number of times the profile was altered (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the VMMDISK class, this value does not change.

CONTROL COUNT
The number of times the profile was successfully accessed with CONTROL authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the VMMDISK class, this value does not change.

UPDATE COUNT
The number of times the profile was successfully accessed with UPDATE authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the VMMDISK class, this value does not change.

READ COUNT
The number of times the profile was successfully accessed with READ authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the VMMDISK class, this value does not change.

USER, ACCESS, and ACCESS COUNT
Any specific users or groups permitted access to the minidisk.
These fields describe the access list. USER is the userid or group-id given the access authority listed in the ACCESS field. ACCESS COUNT is the number of times the user listed in the USER field accessed the minidisk (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the VMMDISK class, these values do not change.

Task VM-5. Changing a Minidisk's Universal Access Authority (UACC)

SITUATION: You have a minidisk containing research data, which you need to protect so that no one can tamper with the data.

PROCEDURE:

Step 1. Find the name of the profile that protects the minidisk. To do this, see "Task VM-4. Finding Out How a Minidisk is Protected" on page 3-12.

> Remember that changing the UACC for a generic profile changes the access to all minidisks protected by the profile.

Step 2. Decide which level of UACC to specify in the profile.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on VM" on page A-3.

Warnings

1. Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. (For information on how to permit selected users or groups to access a minidisk, see "Task VM-6. Permitting an Individual or a Group to Use a Minidisk" on page 3-20.)
2. If you are changing the UACC to restrict access, be certain that any user or group specifically mentioned in the access list has the access to the resource that you intend. For example, if you change the UACC to NONE, and there is a user specifically named in the access list with any authority, that user will still have that authority to the resource.

Step 3. If you are not already in a RACF command session, issue the following command:

```
RACF
```

Step 4. Change the UACC specified in the profile.

To change the UACC, issue the RALTER command as follows:

```
RALTER  VMMDISK  profile-name  UACC(access-authority)
```

Examples:

To change the UACC for minidisk ASMITH.191 to NONE, enter the following command:

```
RALTER  VMMDISK  ASMITH.191  UACC(NONE)
```

To change the UACC for the generic profile ASMITH.* to NONE, enter the following command:

```
RALTER  VMMDISK  ASMITH.*  UACC(NONE)
```

Step 5. If, after you have changed the UACC for the minidisk, you wish to terminate the RACF command session, enter the END command:

```
END
```

Task VM-6. Permitting an Individual or a Group to Use a Minidisk

SITUATION: You would like J.E. Jones, whose userid is JONES, to use your RACF-protected minidisk.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on VM" on page A-6.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in "PROCEDURE USING THE RACFPERM EXEC" on page 3-21. The RACFPERM EXEC displays a panel, but does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), use the RACF commands described in "PROCEDURE USING RACF COMMANDS" on page 3-22.

PROCEDURE USING THE RACFPERM EXEC:

Enter the RACFPERM command, and RACF will display the following panel:

```
---------------------  PERMIT ACCESS TO DISKS OR READER  --------------------

 Enter the required data and press ENTER and then press PF2:

 CURRENT PASSWORD  ===>          Enter your current password
 RESOURCE          ===>          DISK ADDRESS (191, 192, ETC.) OR RDR
 ACCESS AUTHORITY  ===>          DELETE  - TO REMOVE ACCESS AUTHORITY
                                 NONE    - TO PREVENT A USER FROM ACCESSING
                                 READ    - TO ALLOW READ/ONLY ACCESS
                                 UPDATE  - TO ALLOW WRITE ACCESS
                                 CONTROL - TO ALLOW MULTI-READ ACCESS
                                 ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                           allows user to assign authority)
 Enter the userids and/or groupids whose access authority you want to change:

 USERIDS AND/OR GROUPIDS:
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the RESOURCE field, specify the virtual address of the minidisk you want to grant access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify the access authority you want to grant.
- In the USERIDS AND/OR GROUPIDS fields, specify the userids or group ids (group names) to whom you want to grant access.

Press PF2 to execute the request.

After RACF displays some messages related to the request, clear your terminal screen, then press PF3 to leave RACFPERM.

PROCEDURE USING RACF COMMANDS:

Step 1. Find the name of the profile that protects the minidisk. To do this, see "Task VM-4. Finding Out How a Minidisk is Protected" on page 3-12.

Step 2. Decide which access authority to specify in the profile.

The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see "Access Authority for Minidisks on VM" on page A-3.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known.

Step 3. If you are not already in a RACF command session, issue the following command:

```
RACF
```

Step 4. Allowing access to a minidisk

To allow access to your minidisk, use the PERMIT command with the ACCESS operand. Type:

```
PERMIT  profile-name  CLASS(VMMDISK)  ID(userid or groupid)  ACCESS(level)
```

Examples:

To permit user Jones to read the user minidisk DCOLLINS.191, type:

```
PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(JONES) ACCESS(READ)
```

To permit users Jones and Moore to read the user minidisk DCOLLINS.191, type:

```
PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(JONES, MOORE)  +
   ACCESS(READ)
```

To permit group DEPTD60 to read the user minidisk DCOLLINS.191, type:

```
PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(DEPTD60) ACCESS(READ)
```

To permit groups DEPTD60 and DEPTD58 to read the user minidisk DCOLLINS.191, type:

```
PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(DEPTD60, DEPTD58) +
   ACCESS(READ)
```

Step 5. If, after you have permitted a user or group access to a minidisk, you wish to terminate the RACF command session, enter the END command:

```
END
```

Task VM-7. Denying an Individual or a Group Use of a Minidisk

SITUATION: A colleague who has left the department can still use a minidisk. For security reasons you wish to exclude the person from using the minidisk.

Note: For a description of when a change to a user's access occurs, see "When Profile Changes Take Effect on VM" on page A-6.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in "PROCEDURE USING THE RACFPERM EXEC" on page 3-24. Using RACFPERM does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), use the RACF commands described in "PROCEDURE USING RACF COMMANDS" on page 3-25.

PROCEDURE USING THE RACFPERM EXEC: **Enter the RACFPERM command, and RACF will display the following panel:**

```
---------------------  PERMIT ACCESS TO DISKS OR READER  -------------------

 Enter the required data and press ENTER and then press PF2:

  CURRENT PASSWORD  ===>          Enter your current password
  RESOURCE          ===>          DISK ADDRESS (191, 192, ETC.) OR RDR
  ACCESS AUTHORITY  ===>          DELETE  - TO REMOVE ACCESS AUTHORITY
                                  NONE    - TO PREVENT A USER FROM ACCESSING
                                  READ    - TO ALLOW READ/ONLY ACCESS
                                  UPDATE  - TO ALLOW WRITE ACCESS
                                  CONTROL - TO ALLOW MULTI-READ ACCESS
                                  ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                            allows user to assign authority)
 Enter the userids and/or groupids whose access authority you want to change:

  USERIDS AND/OR GROUPIDS:
  ===>            ===>            ===>            ===>
  ===>            ===>            ===>            ===>
  ===>            ===>            ===>            ===>
  ===>            ===>            ===>            ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the RESOURCE field, specify the virtual address of the minidisk you want to deny access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify DELETE or NONE.

  Note: DELETE removes the name of the user or group from the access list. However, this will deny access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group will still be able to access the minidisk. To ensure that the user or group will not be able to access the minidisk, specify NONE.
- In the USERIDS AND/OR GROUPIDS fields, specify the userids or group ids (group names) whom you want to deny access.

Press PF2 to execute the request.

After RACF displays some messages related to the request, clear your terminal screen, then press PF3 to leave RACFPERM.

PROCEDURE USING RACF COMMANDS:

Step 1. Find the name of the profile that protects the minidisk. To do this, see "Task VM-4. Finding Out How a Minidisk is Protected" on page 3-12.

Step 2. If you are not already in a RACF command session, issue the following command:

```
RACF
```

Step 3. Denying access to a minidisk.

You can deny access to a minidisk in two ways.

- One way is to remove the name of the user or group from the access list. However, this will deny access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group will still be able to access the minidisk. See "Removing the Individual or Group from the Access List" on page 3-26.
- The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. To assign an access of NONE is the best procedure to ensure the user or group will not be able to access the minidisk. See "Including the Individual or Group on the Access List with ACCESS(NONE)" on page 3-26.

Step 4. If, after you have denied a user or group access to a minidisk, you wish to terminate the RACF command session, enter the END command:

```
END
```

Removing the Individual or Group from the Access List: To deny access by removing a user or a group from the access list, issue the PERMIT command with the DELETE operand. Type:

```
PERMIT  profile-name  CLASS(VMMDISK)  ID(userid or groupid)  DELETE
```

Examples:

To deny user Jones use of user minidisk DLEWIS.191, type:

```
PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(JONES)  DELETE
```

To deny users Jones and Moore use of user minidisk DLEWIS.191, type:

```
PERMIT DLEWIS.191 CLASS(VMMDISK)  ID(JONES, MOORE) DELETE
```

To deny group DEPTD60 use of user minidisk DLEWIS.191, type:

```
PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(DEPTD60)  DELETE
```

To deny groups DEPTD60 and DEPTD58 use of user minidisk DLEWIS.191, type:

```
PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(DEPTD60,DEPTD58)  DELETE
```

Including the Individual or Group on the Access List with ACCESS(NONE): Including the user or group on the access list with ACCESS(NONE) is the best way to ensure that the user or group will not be able to access the minidisk.

To deny access by assigning a user or group an access of NONE, issue the PERMIT command with the ACCESS keyword as follows:

```
PERMIT profile-name  CLASS(VMMDISK) ID(userid or groupid)  ACCESS(NONE)
```

Examples:

To deny user Jones use of user minidisk KIRBY.191, type:

```
PERMIT  KIRBY.191  CLASS(VMMDISK) ID(JONES) ACCESS(NONE)
```

To deny users Jones and Moore the use of user minidisk KIRBY.191, type:

```
PERMIT KIRBY.191 CLASS(VMMDISK) ID(JONES, MOORE) ACCESS(NONE)
```

To deny group DEPTD60 use of user minidisk KIRBY.191, type:

```
PERMIT  KIRBY.191  CLASS(VMMDISK)  ID(DEPTD60)  ACCESS(NONE)
```

To deny groups DEPTD60 and DEPTD58 use of user minidisk KIRBY.191, type:

```
PERMIT KIRBY.191 CLASS(VMMDISK) ID(DEPTD60,DEPTD58) ACCESS(NONE)
```

Chapter 4. Using RACF ISPF Panels On VM

This chapter includes the following tasks, which describe how to use RACF ISPF panels on VM:

Some Notes about RACF ISPF Panels

RACF ISPF panels have a tutorial that gives you a general description of RACF. If you would like to view the tutorial, select the RACF option on the ISPF menu. On the next panel you see, select the tutorial option.

On each RACF ISPF panel, you can get online help by entering the HELP command (this is usually defined as PF1).

The panel illustrations contain the panel identifiers, which you can display by entering the ISPF command PANELID on the command line.

The panel illustrations use the convention

```
<<< field name >>>
```

to show variable, protected text fields. Variable, protected text fields contain the information previously entered on one panel that RACF displays on a subsequent panel.

Task VM-8. Finding Out If and How You Are RACF-Defined

SITUATION: If RACF is installed on your VM system and you can log on, you are RACF-defined. If you want to find out *how* you are defined to RACF, list your RACF user profile.

Note: To find out your authority to a minidisk, see the field labeled YOUR ACCESS in the display of the minidisk profile. See "Task VM-11. Finding Out How a Minidisk is Protected" on page 4-15.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.
   6  DUAL REGISTRATION  ADD, CHANGE, or DELETE VM users and/or minidisks
                         to both the RACF data base and the CP directory.
   7  SET VM EVENTS      Request auditing or controlling of VM events.
                         Disable or enable pre-logon CP commands.
                         List current settings.
   T  TUTORIAL           View a general description of RACF.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 4. Press ENTER.

Option 4 gives you the following 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   ===>
```

On the OPTION line, type D. In the USER ID field, type your userid. Press ENTER.

You will see output similar to that shown in Figure 4-1 on page 4-4. For detailed descriptions of the fields appearing in the output, see Figure 3-1 on page 3-3.

Your RACF security administrator creates and maintains your user profile.

If, after determining what your operating privileges and restrictions are, you need to change your user profile, see your RACF security administrator.

```
The following is the first part of the RACF information that
describes you as a user.

USER=your   NAME=your name     OWNER=the owner   CREATED=date you were defined
     userid                          of this profile     to RACF

 DEFAULT-GROUP=your     PASSDATE=date your    PASS-INTERVAL=length of time
              default           password was               your password
              group name        last updated               is valid

 ATTRIBUTES=your operating privileges and restrictions

 REVOKE DATE=date on which      RESUME DATE=date on which RACF allows
            RACF prevents you              you to use the system
            from using the system          again

 LAST-ACCESS=last date you used the system

 CLASS AUTHORIZATIONS=installation-assigned classes in which you
                      can define profiles.

 INSTALLATION-DATA=information your installation maintains about you

 LOGON ALLOWED=time during which you can access the system


The following portion of the output describes the RACF group(s)
you belong to and what you can do as a member of the group(s).


  GROUP=name  AUTH=your  CONNECT-OWNER=owner CONNECT-DATE=date you
       of         group              of this           were connected
       group      authority          group             to this group

    CONNECTS=number of times   UACC=universal    LAST-CONNECT=last time
             you were connected     access                  you were
             to this group          authority               connected

    CONNECT ATTRIBUTES=your operating privileges as a member of this group

    REVOKE DATE=date on which      RESUME DATE=date on which RACF
               RACF prevents you             allows you to access
               from accessing the system     the system again
               through this group            through this group

The following is the second part of the RACF information that
describes you as a user.

 SECURITY-LEVEL=your installation-assigned security level

 CATEGORY-AUTHORIZATION
  Your installation-assigned security categories
```

Figure 4-1. Display of a User Profile on VM

Task VM-9. Finding Out What Profiles You Have

SITUATION: You created a minidisk that needs protection but you do not know whether you currently have a profile that will protect the minidisk.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.
   6  DUAL REGISTRATION   ADD, CHANGE, or DELETE VM users and/or minidisks
                          to both the RACF data base and the CP directory.
   7  SET VM EVENTS       Request auditing or controlling of VM events.
                          Disable or enable pre-logon CP commands.
                          List current settings.
   T  TUTORIAL            View a general description of RACF.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
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    ===> VMMDISK
   RESOURCE NAME     ===>

   USE MODEL PROFILE ===>     YES if the profile is to be modeled
```

On the OPTION line, type S. In the RESOURCE CLASS field, type VMMDISK. Press ENTER.

Option S gives you the following panel:

```
ICHP29          RACF - SEARCH FOR GENERAL RESOURCE PROFILES          1 of 2
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 MASK1string.
                            Enter * to select undefined CATEGORYs

ENTER INPUT FILTER STRING:
   FILTER    ===>

TO ADD ADDITIONAL INFORMATION ENTER YES:

   Generate TSO CLIST                ===>
   Specify additional SEARCH criteria ===>
```

In the MASK1 field, type your userid. Press ENTER.

To narrow the list of profiles displayed, you can specify either of the following:

- MASK1, MASK2, or both
- FILTER

Note: You cannot specify both MASK and FILTER.

MASK1 specifies that RACF select profile names starting with this character string. MASK2 specifies that RACF select only those profile names containing this character string somewhere after the occurrence of MASK1. MASK1 and MASK2 together must not exceed 44 characters.

FILTER allows you to use generic characters (% and *).

For more information on using MASK and FILTER, see the description of the SEARCH command in the *RACF Command Language Reference*.

If you specify YES for the "Specify additional SEARCH criteria" field, RACF displays the following panel:

```
ICHP29A          RACF - SEARCH FOR GENERAL RESOURCE PROFILES          2 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

   TYPE      ===>          GENERIC, DISCRETE, WARNING,
                           TAPE (tape only) or ALL

SPECIFY ONE OF THE FOLLOWING:

   AGE       ===>          0-9999 DAYS
   EXPIRES   ===>          0-99999 DAYS
   LEVEL     ===>          0-99
   SECLEVEL  ===>
                           Enter * to select undefined SECLEVELs
   CATEGORY  ===>
                           Enter * to select undefined CATEGORYs
```

Enter the requested information in the fields on the panel. Press ENTER.

RACF will list all appropriate profiles (including only those profiles you are authorized to use). For example, if MASK1 is DCOLLINS and MASK2 is 19, then minidisk profiles DCOLLINS.191 and DCOLLINS.193 will be listed, but DCOLLINS.291 will not be selected.

If you do not have *any* profiles, RACF will display a message stating that no profiles exist for the minidisk.

For Example:

To find out what minidisk profiles have your userid as the high-level qualifier, complete the panel as shown:

```
ICHP29           RACF - SEARCH FOR GENERAL RESOURCE PROFILES          1 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

   MASK1     ===> DCOLLINS
                          MASK1 selects profile names starting with
                          the specified character string.
   MASK2     ===>
                          MASK2 selects profile names containing the
                          specified string somewhere after the MASK1string.
                          Enter * to select undefined CATEGORYs

ENTER INPUT FILTER STRING:
   FILTER    ===>

TO ADD ADDITIONAL INFORMATION ENTER YES:

   Generate TSO CLIST                ===>
   Specify additional SEARCH criteria ===>
```

If you specify YES for the "Specify additional SEARCH criteria" field, RACF displays the following panel:

```
ICHP29A          RACF - SEARCH FOR GENERAL RESOURCE PROFILES          2 of 2
COMMAND ===>

ENTER OPTIONAL SELECTION CRITERIA:

   TYPE      ===> ALL       GENERIC, DISCRETE, WARNING,
                            TAPE (tape only) or ALL

SPECIFY ONE OF THE FOLLOWING:

   AGE       ===>           0-9999 DAYS
   EXPIRES   ===>           0-99999 DAYS
   LEVEL     ===>           0-99
   SECLEVEL  ===>
                            Enter * to select undefined SECLEVELs
   CATEGORY  ===>
                            Enter * to select undefined CATEGORYs
```

RACF would list all the profiles with your userid as the high-level qualifier.

Task VM-10. Changing Your Password

SITUATION: You suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

Note: You may also change your password while logging on to the system. See "Task VM-1. Finding Out If and How You Are RACF-Defined" on page 3-2.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may also not allow you to re-use a previous password. See your RACF security administrator for an explanation of your installation's rules for passwords.

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                  RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET           ADD, CHANGE, DELETE, or DISPLAY the profile
                         for a 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.
   6  DUAL REGISTRATION  ADD, CHANGE, or DELETE VM users and/or minidisks
                         to both the RACF data base and the CP directory.
   7  SET VM EVENTS      Request auditing or controlling of VM events.
                         Disable or enable pre-logon CP commands.
                         List current settings.
   T  TUTORIAL           View a general description of RACF.

   X  EXIT               Exit out of RACF.
```

On the OPTION line, type 4. Press ENTER.

Option 4 gives you the following 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   ===>
```

On the OPTION line, type 4. Press ENTER.

Option 4 gives you the following panel:

```
ICHP44          RACF - CHANGE USER PASSWORD  - <<<userid>>>
COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>

   NEW PASSWORD      ===>

    INTERVAL         ===>
```

To change your password, enter the requested information. Press ENTER.

If you have chosen an incorrect password, you will get a message stating that the password has not been changed. See your RACF security administrator for an explanation of your installation's rules for passwords.

For Example:

To change your password from "subject" to "tester" complete the panel as follows:

```
ICHP44          RACF - CHANGE USER PASSWORD  - <<<userid>>>
COMMAND ===>

ENTER THE FOLLOWING:

   CURRENT PASSWORD  ===>  subject

   NEW PASSWORD      ===>  tester

   INTERVAL          ===>
```

Note: The passwords are shown in this book to illustrate how to enter them. On the system, the passwords are *not* displayed as you type them. This is to prevent others from seeing what they are.

Task VM-11. Finding Out How a Minidisk is Protected

SITUATION: You are the owner of a minidisk (or you are responsible for the security protection of a minidisk), and you want to determine what protection the minidisk has. For example, you might want to find out what users and groups can access the minidisk.

INFORMATION YOU NEED TO KNOW FIRST: You need to know the virtual address of the minidisk.

The virtual address of an A-disk is, by convention, 191. To find the virtual address of one of your minidisks, enter the following command:

```
QUERY DISK n
```

where n is the letter by which you know the minidisk. For example, for the address of your A-disk, enter:

```
QUERY DISK A
```

The virtual address of the minidisk is under the column labeled CUU.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFLIST EXEC. This is described in "PROCEDURE USING THE RACFLIST EXEC" on page 4-16. Using RACFLIST does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), and you want to use panels instead of commands, you must use the RACF ISPF panels, described in "PROCEDURE USING RACF ISPF PANELS" on page 4-17.

PROCEDURE USING THE RACFLIST EXEC:

Enter the RACFLIST command, and RACF will display the following panel:

```
---------------------  LIST ACCESS TO DISKS OR READER  --------------------

 Enter the required data and press ENTER and then press PF2:


 AUTHORIZED USERS   ===>          Enter an S for a list of authorized users
 STATISTICS         ===>          ENTER AN S FOR A STATISTICS REPORT
 HISTORY            ===>          Enter an S for a HISTORY report

 READER             ===>          Enter an S for a report for the READER
 DISKS:             ===>          Enter the disk addresses for which you
                    ===>          want a report
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authuser 11=Cmd line 12=Resources
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the AUTHORIZED USERS field, specify S if you want to display the access list of the minidisk profile.
- For the STATISTICS field, specify S if you want to display the number of times the minidisk was accessed by users.
- For the HISTORY field, specify S if you want to display information such as the date the minidisk profile was defined to RACF and the date on which the profile was last checked for UPDATE authority.
- Leave the READER field blank.
- For the DISKS fields, specify the virtual address of each minidisk for which you want information. (If you don't know the virtual address of the minidisk, see "INFORMATION YOU NEED TO KNOW FIRST" on page 4-15.)

Press PF2 to request that the information be listed.

After the information is displayed, clear your terminal screen, then press PF3 to leave RACFLIST.

PROCEDURE USING RACF ISPF PANELS:

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.
   6  DUAL REGISTRATION   ADD, CHANGE, or DELETE VM users and/or minidisks
                          to both the RACF data base and the CP directory.
   7  SET VM EVENTS       Request auditing or controlling of VM events.
                          Disable or enable pre-logon CP commands.
                          List current settings.
   T  TUTORIAL            View a general description of RACF.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
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     ===>

   USE MODEL PROFILE ===>     YES if the profile is to be modeled
```

On the OPTION line, type D, plus the following:

- For the RESOURCE CLASS field, enter VMMDISK.
- For the RESOURCE NAME field, enter

  `userid.virtual-address`

  where userid is your VM userid and virtual address is the address of the minidisk. For example, for SMITH's A-disk, enter SMITH.191.

Press ENTER.

Option D gives you the following panel:

```
ICHP28          RACF - DISPLAY GENERAL RESOURCE PROFILE
COMMAND ===>

     CLASS:  VMMDISK          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
    TVTOC           ===>          Tape Volume Table of Contents
```

Enter YES in the GENERIC field. You should also enter YES for the categories of information that you want displayed, for example, ACCESS LIST.

You should see output similar to that in Figure 4-2 on page 4-20.

If you get a message stating you are not authorized, see your RACF security administrator.

```
CLASS         NAME
------        -----
VMMDISK       JACKS.191

LEVEL    OWNER        UNIVERSAL ACCESS     YOUR ACCESS     WARNING
-----    -----        ----------------     -----------     -------
 00      JACKS            READ               ALTER           NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
REVERIFY

SECLEVEL
--------
NO SECLEVEL

CATEGORIES
----------
NO CATEGORIES

AUDITING
--------
NONE

NOTIFY
------
NO USER TO BE NOTIFIED

CREATION DATE     LAST REFERENCE DATE     LAST CHANGE DATE
(DAY)  (YEAR)      (DAY)     (YEAR)        (DAY)   (YEAR)
-------------     ------------------     --------------
 070    85          070       85            070     85

ALTER COUNT    CONTROL COUNT    UPDATE COUNT    READ COUNT
-----------    -------------    ------------    ----------
 00000           00000            00002          00000

 USER          ACCESS               ACCESS COUNT
 ----          ------               ------------
 JACKS         ALTER                   00009
```

Figure 4-2. Display of a Minidisk Profile

Check the following fields for the most important security information about how the minidisk is protected:

- the LEVEL field (if used at your installation)
- the OWNER field
- the UNIVERSAL ACCESS field
- the WARNING field

- the SECLEVEL field (if used at your installation)
- the CATEGORIES field (if used at your installation)
- the USER field and its related ACCESS and ACCESS COUNT fields

For detailed descriptions of the terms appearing in the output, see "Task VM-4. Finding Out How a Minidisk is Protected" on page 3-12.

Task VM-12. Changing a Minidisk's Universal Access Authority (UACC)

SITUATION: You have a minidisk containing research data, which you need to protect so that no one can tamper with the data.

INFORMATION YOU NEED TO KNOW FIRST: You must know the name of the profile that protects your minidisk. See "Task VM-11. Finding Out How a Minidisk is Protected" on page 4-15.

PROCEDURE: **Select the RACF option on the ISPF menu and RACF will display the following panel.**

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.
   6  DUAL REGISTRATION   ADD, CHANGE, or DELETE VM users and/or minidisks
                          to both the RACF data base and the CP directory.
   7  SET VM EVENTS       Request auditing or controlling of VM events.
                          Disable or enable pre-logon CP commands.
                          List current settings.
   T  TUTORIAL            View a general description of RACF.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
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     ===>

   USE MODEL PROFILE ===>     YES if the profile is to be modeled
```

On the OPTION line, type 2, plus the following:

- For the RESOURCE CLASS field, enter VMMDISK.
- For the RESOURCE NAME field, enter

  `userid.virtual-address`

  where userid is your VM userid and virtual address is the address of the minidisk. For example, for SMITH's A-disk, enter SMITH.191.

Press ENTER.

Option 2 gives you the following panel:

```
ICHP22              RACF - CHANGE GENERAL RESOURCE PROFILE
COMMAND ===>

   CLASS:  <<<VMMDISK>>>   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
   REMOVE NOTIFY     ===>            YES or Blank
   NEW NOTIFY        ===>            New Userid

   OPTIONAL INFORMATION ===>         ENTER YES TO CHANGE INFORMATION
```

Enter the UACC you want to assign to this profile. Press ENTER.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on VM" on page A-3.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. For information on how to permit selected users or groups to access a minidisk, see "Task VM-13. Permitting an Individual or a Group to Use a Minidisk" on page 4-26.

If you get a message stating you are not authorized, see your RACF security administrator.

For Example:

To change the UACC for minidisk profile USER5.191 to NONE, complete the panel as follows:

```
ICHP22              RACF - CHANGE GENERAL RESOURCE PROFILE
COMMAND ===>

   CLASS:  VMMDISK          PROFILE NAME: USER5.191

ENTER RESOURCE INFORMATION TO BE CHANGED:
   OWNER              ===>              Userid or group name
   LEVEL              ===>              0-99
   FAILED ACCESSES    ===>              FAIL or WARN
   UACC               ===> NONE         NONE, READ, UPDATE, CONTROL, or ALTER
   AUDIT SUCCESSES    ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
   AUDIT FAILURES     ===>              READ, UPDATE, CONTROL, ALTER, or NOAUDIT
   REMOVE NOTIFY      ===>              YES or Blank
   NEW NOTIFY         ===>              New Userid

   OPTIONAL INFORMATION ===>          ENTER YES TO CHANGE INFORMATION
```

Task VM-13. Permitting an Individual or a Group to Use a Minidisk

SITUATION: You would like J.E. Jones, whose userid is JONES, to use your RACF-protected minidisk.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in "PROCEDURE USING THE RACFPERM EXEC" on page 4-27. Using RACFPERM does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), and you want to use panels instead of commands, you must use the RACF ISPF panels, described in "PROCEDURE USING RACF ISPF PANELS" on page 4-28.

PROCEDURE USING THE RACFPERM EXEC:

Enter the RACFPERM command, and RACF will display the following panel:

```
---------------------  PERMIT ACCESS TO DISKS OR READER  -------------------

 Enter the required data and press ENTER and then press PF2:

 CURRENT PASSWORD  ===>          Enter your current password
 RESOURCE          ===>          DISK ADDRESS (191, 192, ETC.) OR RDR
 ACCESS AUTHORITY  ===>          DELETE  - TO REMOVE ACCESS AUTHORITY
                                 NONE    - TO PREVENT A USER FROM ACCESSING
                                 READ    - TO ALLOW READ/ONLY ACCESS
                                 UPDATE  - TO ALLOW WRITE ACCESS
                                 CONTROL - TO ALLOW MULTI-READ ACCESS
                                 ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                           allows user to assign authority)
 Enter the userids and/or groupids whose access authority you want to change:

 USERIDS AND/OR GROUPIDS:
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the RESOURCE field, specify the virtual address of the minidisk you want to grant access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify the access authority you want to grant.
- For the USERIDS AND/OR GROUPIDS fields, specify the userids or group ids (group names) to whom you want to grant access.

Press PF2 to execute the request.

After RACF displays some messages related to the request, clear your terminal screen, then press PF3 to leave RACFPERM.

PROCEDURE USING RACF ISPF PANELS:

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET            ADD, CHANGE, DELETE, or DISPLAY the profile
                          for a 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.
   6  DUAL REGISTRATION   ADD, CHANGE, or DELETE VM users and/or minidisks
                          to both the RACF data base and the CP directory.
   7  SET VM EVENTS       Request auditing or controlling of VM events.
                          Disable or enable pre-logon CP commands.
                          List current settings.
   T  TUTORIAL            View a general description of RACF.

   X  EXIT                Exit out of RACF.
```

On the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
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     ===>

   USE MODEL PROFILE ===>     YES if the profile is to be modeled
```

On the OPTION line, type 4, plus the following:

- For the RESOURCE CLASS field, enter VMMDISK.
- For the RESOURCE NAME field, enter

  `userid.virtual-address`

  where userid is your VM userid and virtual address is the address of the minidisk. For example, for SMITH's A-disk, enter SMITH.191.

Press ENTER.

Option 4 gives you the following panel:

```
ICHP24          RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST
OPTION ===>

   CLASS:  <<<VMMDISK>>>   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.
```

On the OPTION line, enter 1. Press ENTER.

Option 1 gives you the following panel:

```
ICHP241        RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - ADD
COMMAND ===>

   CLASS:  <<<VMMDISK>>>   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
```

Enter the userid or groupid and the access you wish to assign to that person or group.

The access can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on VM" on page A-3.

Warning

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known.

For Example:

To add the userid USER52 to the access list with READ authority to the minidisk profile USER4.191, complete the panel as follows:

```
ICHP241        RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - ADD
COMMAND ===>
     CLASS:  <<<VMMDISK>>>     PROFILE NAME: <<<USER4.191>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL, or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===>USER52   ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>

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
```

For Example:

To add the userid USER52 and the groupid TEST12 to the access list with READ authority to the profile USER4.191, complete the panel as follows:

```
ICHP241        RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - ADD
COMMAND ===>

     CLASS:  <<<VMMDISK>>>     PROFILE NAME: <<<USER4.191>>>

ENTER AUTHORITY TO BE GRANTED:

ACCESS AUTHORITY  ===> READ   NONE, READ, UPDATE, CONTROL, or ALTER

ENTER USER/GROUP ID TO BE ADDED:
===>USER52   ===>         ===>         ===>         ===>
===>TEST12   ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>

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
```

Task VM-14. Denying an Individual or a Group Use of a Minidisk

SITUATION: A colleague who has left the department can still use a minidisk. For security reasons you wish to exclude the person from using the minidisk.

WHICH PROCEDURE TO USE: You can choose between two procedures:

- If you're working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in "PROCEDURE USING THE RACFPERM EXEC" on page 4-35. Using RACFPERM does not require ISPF to be installed on your system.
- If you're working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), and you want to use panels instead of commands, you must use the RACF ISPF panels, described in "PROCEDURE USING RACF ISPF PANELS" on page 4-36.

PROCEDURE USING THE RACFPERM EXEC: **Enter the RACFPERM command, and RACF will display the following panel:**

```
---------------------  PERMIT ACCESS TO DISKS OR READER  -------------------

 Enter the required data and press ENTER and then press PF2:

 CURRENT PASSWORD  ===>          Enter your current password
 RESOURCE          ===>          DISK ADDRESS (191, 192, ETC.) OR RDR
 ACCESS AUTHORITY  ===>          DELETE  - TO REMOVE ACCESS AUTHORITY
                                 NONE    - TO PREVENT A USER FROM ACCESSING
                                 READ    - TO ALLOW READ/ONLY ACCESS
                                 UPDATE  - TO ALLOW WRITE ACCESS
                                 CONTROL - TO ALLOW MULTI-READ ACCESS
                                 ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                           allows user to assign authority)
 Enter the userids and/or groupids whose access authority you want to change:

 USERIDS AND/OR GROUPIDS:
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>
 ===>            ===>            ===>            ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 (twice) for online help.

On the panel, type in the following:

- For the CURRENT PASSWORD field, enter the password you logged on with. If this field does not appear on your system, go on to the next field.
- For the RESOURCE field, specify the virtual address of the minidisk you want to deny access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify DELETE or NONE.

  Note: DELETE removes the name of the user or group from the access list. However, this will deny access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group will still be able to access the minidisk. To ensure that the user or group will not be able to access the minidisk, specify NONE.
- In the USERIDS AND/OR GROUPIDS fields, specify the userids or group ids (group names) whom you want to deny access.

Press PF2 to execute the request.

After RACF displays some messages related to the request, clear your terminal screen, then press PF3 to leave RACFPERM.

PROCEDURE USING RACF ISPF PANELS:

Select the RACF option on the ISPF menu and RACF will display the following panel.

```
ICHP00                    RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET             ADD, CHANGE, DELETE, or DISPLAY the profile
                           for a 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.
   6  DUAL REGISTRATION    ADD, CHANGE, or DELETE VM users and/or minidisks
                           to both the RACF data base and the CP directory.
   7  SET VM EVENTS        Request auditing or controlling of VM events.
                           Disable or enable pre-logon CP commands.
                           List current settings.
   T  TUTORIAL             View a general description of RACF.

   X  EXIT                 Exit out of RACF.
```

On the OPTION line, type 2. Press ENTER.

Option 2 gives you the following panel:

```
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      ===>

   USE MODEL PROFILE ===>     YES if the profile is to be modeled
```

On the OPTION line, type 4, plus the following:

- For the RESOURCE CLASS field, enter VMMDISK.
- For the RESOURCE NAME field, enter

  `userid.virtual-address`

  where userid is your VM userid and virtual address is the address of the minidisk. For example, for SMITH's A-disk, enter SMITH.191.

Press ENTER.

Option 4 gives you the following panel:

```
ICHP24          RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST
OPTION ===>

   CLASS:  <<<VMMDISK>>>   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.
```

If you wish to remove ALL users or groups from the access list, type 3 on the OPTION line. Press ENTER.

If you wish to remove only certain users or groups from the access list, type 2 on the OPTION line. Press ENTER.

Option 2 gives you the following panel:

```
ICHP242        RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - REMOVE
COMMAND ===>

   CLASS:  <<<VMMDISK>>>   PROFILE NAME: <<<profile name>>>

ENTER USER/GROUP ID TO BE REMOVED:

===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
===>          ===>          ===>          ===>          ===>
```

Enter the userid(s) or groupid(s) you wish to remove from the access list.

For Example:

To remove userid USER43 from the access list of profile USER4.191, complete the panel as follows:

```
ICHP242        RACF - MAINTAIN GENERAL RESOURCE ACCESS LIST - REMOVE
COMMAND ===>

     CLASS:  <<<VMMDISK>>>     PROFILE NAME: <<<USER4.191>>>

ENTER USER/GROUP ID TO BE REMOVED:

===> USER43  ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
===>         ===>         ===>         ===>         ===>
```

Appendix A. Reference

This appendix includes the following:

Access Authority for Data Sets on MVS

For data sets on MVS, access authority can be one of the following:

NONE — Does not allow users to access the data set.

> **WARNING**
>
> Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Task MVS-10. Permitting an Individual or a Group to Use a Data Set" on page 1-32 for information on how to permit selected users or groups to access a data set.)

READ — Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE — Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL — For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER — ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list.* However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

On an always-call system, when specified in a generic profile, ALTER allows users to create new data sets that will be covered by that profile.

EXECUTE — For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Access Authority for Minidisks on VM

For minidisks on VM, access authority can be one of the following:

NONE — Does not allow users to access the minidisk.

> **WARNING**
>
> Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. (See "Task VM-6. Permitting an Individual or a Group to Use a Minidisk" on page 3-20 for information on how to permit selected users or groups to access a minidisk.)

READ — Allows users to access the minidisk for reading or copying only. This allows users to request an access mode of read (R) or read-read (RR) on the CP LINK command. (Note that users who can read files on a minidisk can copy or print them.)

UPDATE — Allows users to read from, copy from, or write to the minidisk. This allows users to request an access mode of write (W) or write-read (WR) on the CP LINK command.

CONTROL — Allows users to read from, copy from, or write to the minidisk. This allows users to request an access mode of multiple (M) or multiple-read (MR) on the CP LINK command.

ALTER — Allows users to read from, copy from, or write to the minidisk. This allows users to request an access mode of multiwrite (MW) on the CP LINK command.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

Enhanced Generic Names

The following tables show how to specify generic names:

Profile Name	ABC. % % F	ABC. DEF*	ABC. DEF.*	ABC.*.DEF	ABC.DEF.**	ABC.DEF*.**
Data sets protected by the profile	ABC.DEF ABC.XYF	ABC.DEF ABC.DEFG ABC.DEFGHI	ABC.DEF.GHI ABC.DEF.XY	ABC.DEF.DEF ABC.XY.DEF	ABC.DEF ABC.DEF.GHI ABC.DEF.GH.IJ	ABC.DEF ABC.DEFGH ABC.DEFG.HIJ ABC.DEF.GH.IJ
Data sets not protected by the profile	ABC.DEFGHI ABC.DEF.GHI	ABC.DEF.GHI ABC.DEFG.HI	ABC.DEFGHI ABC.DEF.GH.IJ	ABC.DEF ABC.DEF.GHI ABC.XY.XY.DEF	ABC.DEFG ABC.DEFG.HIJ	ABCD.EFG
How RACF displays the name after enhanced generic naming is deactivated	ABC.% % F	ABC.DEF*	ABC.DEF.*	ABC.*.DEF	ABC.DEF:	ABC.DEF*
Data sets protected by the profile after enhanced generic naming is deactivated	Same as before	none	none	Same as before	none	Same as before

Figure A-1. Generic profile names created with enhanced generic naming active.

Profile Name	ABC.% % F	ABC.DEF*	ABC.DEF.*	ABC.*.DEF
Data sets protected by the profile	ABC.DEF ABC.XYF	ABC.DEF ABC.DEFGHI ABC.DEFG.HIJ ABC.DEF.GH.IJ	ABC.DEF ABC.DEF.GHI ABC.DEF.GHI.JKL	ABC.DEF.DEF ABC.XYZ.DEF
Data sets not protected by the profile	ABC.DEFG ABC.DEF.GHI	ABCD.EFG	ABC.DEFG ABC.DEFG.HIJ	ABC.DEF ABC.DEF.GHI ABC.XYZ.XYZ.DEF
How RACF displays the name after enhanced generic naming is activated	ABC.% % F	ABC.DEF*.**	ABC.DEF.*.**	ABC.*.DEF
Data sets protected by the profile after enhanced generic naming is activated	Same as before	Same as before	Same as before	Same as before

Figure A-2. Generic profile names created prior to RACF 1.8.1, or with enhanced generic naming inactive.

When Profile Changes Take Effect on MVS

If a user is currently using your data set, changing the access of that user may not affect the current access until that user logs on again.

Your change will affect the user's access immediately in the following cases:

- If the user is not logged on. You can check to see if a user is logged on with the TSO SEND command:

  ```
  SEND 'message-text' USERID(userid)
  ```

- If the user is logged on and has not yet opened the data set (for example, to browse or edit it).

If the user is logged on and has opened the data set, and you change his access, two situations could occur:

- If the profile is a discrete profile, the user's access changes after closing the data set.
- If the profile is a generic profile, the user's access changes after *both* the following occur:
  - The user closes the data set.
  - The copy of the generic profile that is kept in his address space is changed.

  The copy of the generic profile is changed when the user logs off and on again or when the SETROPTS GENERIC REFRESH command is issued.

When Profile Changes Take Effect on VM

If a user is currently using your minidisk, changing the access of that user may not affect the current access until that user logs on again.

Your change will affect the user's access immediately in the following cases:

- If the user is not logged on. You can check to see if a user is logged on with the CP QUERY command:

  ```
  QUERY userid
  ```

- If the user is logged on and has not yet linked to the minidisk. You can check to see if a user is linked to your minidisk with the CP QUERY LINKS command:

  ```
  QUERY LINKS virtual-address
  ```

If the user is logged on and has linked to the minidisk, and you change his access, two situations could occur:

- If the profile is a discrete profile, the user's access changes after detaching the minidisk.
- If the profile is a generic profile, the user's access changes after *both* the following occur:
  - The user detaches the minidisk.
  - The copy of the generic profile that is kept in virtual storage is changed.

  The copy of the generic profile is changed when the user logs off and on again or when the SETROPTS GENERIC REFRESH command is issued.

Glossary

For definitions of terms not in this glossary, see the *Dictionary of Computing*, SC20-1699.

access. The manner in which files or data sets are referred to by the computer. In RACF, the ability to obtain the use of a protected resource.

access authority. An authority that relates to a request for a type of access to protected resources. The access authorities are NONE, READ access, UPDATE access, CONTROL access (for VSAM data sets), ALTER access, and EXECUTE access (for programs in an MVS private load library).

access control to load modules. A RACF function on MVS that allows only authorized users to load and/or execute specified load modules.

access list. A list within a profile of all authorized users and their access authorities.

accessor environment element (ACEE). A description of the current user including userid, current connect group, user attributes, group authorities. An ACEE is constructed during user identification and verification.

ACEE. See accessor environment element.

ACI bit map. The area that CP checks for information about whether to call RACF when a security-related VM event occurs. The information can specify whether RACF is to audit the event, or to perform access checking related to the event, or both.

alphanumeric. The set of characters that includes alphabetic (A through Z), numeric (0 through 9), and national (#, $, and @) characters.

always-call. On MVS, a data management function that calls RACF whenever a data set is accessed (whether the data set is RACF-indicated or not) or DASD space is allocated for a data set.

automatic data set protection (ADSP). On MVS, a user attribute that causes all permanent data sets created by the user to be automatically defined to RACF with a discrete RACF profile.

automatic profile. On MVS, a TAPEVOL profile that RACF creates when a RACF-defined user protects a tape data set. The TAPEVOL profile created in this manner is called an automatic profile because, when RACF deletes the last data set on the volume, RACF automatically deletes the TAPEVOL profile. Also see non-automatic profile.

attribute. See user attribute.

authority. The ability to perform a function on a RACF-defined user, group, or resource. See access authority, group authority, class authority.

authorization checking. The action of determining if a user is permitted access to a RACF-protected resource.

base segment. A logical field in the RACF data base. Also called RACF segment.

category. An installation-defined name corresponding to a department or area within an organization with similar security requirements. Also called security category.

class. A collection of RACF-defined entities with similar characteristics.

class authority. An authority that allows a user to define entities to RACF in the classes defined in the class descriptor table.

class descriptor. RACF-supplied control block for all the resource classes in the class descriptor table (which is all the classes except the USER, GROUP, and DATASET classes).

class descriptor table. A table consisting of an entry for each class except the USER, GROUP, and DATASET classes. The table is generated by specifying the ICHERCDE macro once for each class.

class name. The name that identifies a RACF class of entities. The class names are USER, GROUP, DATASET, and those class names found in the class descriptor table.

conditional access list. On MVS, a second access list within a resource profile that associates a program name with each userid and the corresponding access authority. The user can access the data set at the specified access authority while executing the associated program. See also access list.

connect profile. A description of a RACF-defined user's relationship to a group, including group authority and group-related user attributes.

CST (CMS sub-tasking). An interface program that enables CMS to execute programs written to run in an OS/VS environment.

current connect group. The group with which a user is associated during a terminal session or batch job.

data security. The protection of data from unauthorized disclosure, modification, or destruction, whether accidental or intentional.

data security monitor (DSMON). A RACF auditing tool that produces reports that enable an installation to verify its basic system integrity and data security controls.

data set profile. A description of a RACF-defined data set, including data set name, owner, volume serial number, universal access authority, security level, and other data.

default group. The group with which a user is associated when a group name is not specified on the TSO LOGON command or batch JOB statement. (On a VM system, you cannot specify a group name.)

delegation. The act of giving other users or groups authorities to perform RACF operations.

discrete profile. A description of a single RACF-defined resource that belongs either to the DATASET class or to one of the general resource classes. This description includes the authorized users, the access authority of each user, the location of the data set (device type and volume serial number), the number of accesses to the data set, and other information.

dual registration. An interface that allows the security administrator of a VM system to add a user to the CP system directory and the RACF data base simultaneously.

entity. A user, group, or resource (for example, a DASD data set or VM minidisk) that is defined to RACF.

erase-on-scratch. The physical overwriting of data on a DASD data set when the data set is deleted (scratched).

field access. Authority to access data in a RACF profile at the segment or field level.

FMID. See function modification identifier. A seven-character identifier that is used in MVS, VS/1, and related program products to identify the release of the product.

function modification identifier (FMID). A seven-character identifier that is used in MVS, VS/1, and related program products to identify the release of the product.

general resource. Any system resource, other than an MVS data set, that is defined in the class descriptor table (CDT). On MVS, general resources include DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, installation-defined resource classes, and so forth. On VM, general resources include terminals, minidisks, virtual unit record devices, RSCS nodes, and so forth.

general resource profile. The RACF protection information associated with a general resource or group of general resources. This information can include the resource profile name, owner, volume serial number, universal access authority, security level, and other data.

generation data group (GDG). A collection of data sets with the same base name, such as PAYROLL, that are kept in chronological order. Each data set is called a generation data set.

generic profile. A description of one or more RACF-protected resources that belong either to the DATASET class or to one of the general resource classes and have similar names and similar access-authorization requirements. This description includes the authorized users, the access authority of each user, and other information.

global access checking. The ability to allow an installation to establish an in-storage table of default values for authorization levels for selected resources. RACF refers to this table prior to performing normal RACHECK processing, and grants the request without performing a RACHECK if the requested access authority does not exceed the global value. Global access checking can grant the user access to the resource, but it cannot deny access.

group. A collection of RACF users who can share access authorities for protected resources.

group authority. An authority that relates to a type of function a user can perform in a group. The group authorities are USE, CREATE, CONNECT, and JOIN.

group data set. On MVS, a data set defined to RACF where either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF group name.

group id. One to eight alphanumeric characters, beginning with an alphabetic, #, $, or @ character, that identifies a group to RACF.

group profile. A description of a RACF-defined group, including group name, superior group name, owner, and users in the group.

group-related user attribute. A user attribute assigned at the group level that allows the user to control the resource, group, and user profiles associated with the group and its subgroups. Some of the group-related user attributes are group-SPECIAL, group-AUDITOR, and group-OPERATIONS.

group terminal option. Users within a group are allowed to LOGON to TSO only from those terminals to which they have been specifically authorized access by the owner of the group.

list-of-groups checking. The function of allowing a user to access all resources available to all groups of which the user is a member, regardless of the specified group to which the user is logged on.

logging. The recording of data about specific events.

modeling. The ability for a user or an installation to define a sample "model" profile that RACF uses when defining a new profile. Each profile model can contain defaults for fields such as the universal access authority, level, owner, auditing flags, access list, erase indicator, security classification information, and installation-defined data.

MVS. Implies MVS/370, MVS/XA, and MVS/ESA.

non-automatic profile. On MVS, a TAPEVOL profile that RACF creates in response to an RDEFINE command or when tape data set protection is not active. A TAPEVOL profile created in this manner is called a non-automatic profile because RACF never deletes the profile except in response to the RDELETE command. Also see automatic profile.

operator identification card (OIDCARD).. A small card with a magnetic stripe encoded with unique characters and used to verify the identity of a terminal operator to RACF on an MVS system.

owner. The user or group who creates a profile (or is named the owner of a profile). The owner can modify, list, or delete the profile. A group can be named the owner of a profile.

password. A one to eight alphanumeric character string that a user specifies to meet security requirements when entering the system or accessing protected data sets.

profile. A description of the characteristics of a RACF-defined entity. A profile resides on the RACF data base. Also see connect profile, data set profile, group profile, and user profile.

profile list. A list of profiles indexed by class (for general resources) or by the high-level qualifier (for DATASET profiles) and built in storage by the RACF routines.

program access to data sets (PADS). A RACF function on MVS that allows an authorized user or group of users to access a data set at a specified level while running a certain program. The conditional access list of the data set associates each user ID or group name with a program name.

program control. Program control is a RACF option on MVS that consists of two parts: access control to load modules, and program access to data sets. See also access control to load modules and program access to data sets.

protected resource. A resource that is defined to RACF for the purpose of controlling access to the resource. Some of the resources that can be protected by RACF include DASD and tape data sets, VM minidisks, DASD volumes, tape volumes, terminals, IMS/VS transactions, IMS/VS transaction groups, and any other resources defined in the class descriptor table.

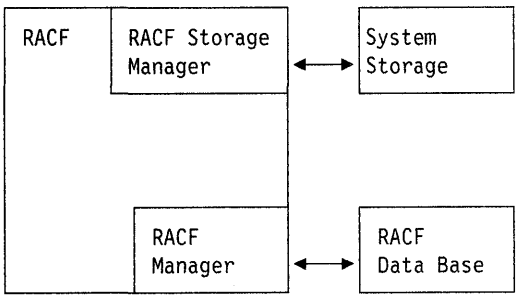
RACF. Resource Access Control Facility.

RACF data base. A collection of interrelated or independent data items stored together without unnecessary redundancy, to serve Resource Access Control Facility (RACF).

RACF-indicated. On MVS systems, a data set is RACF-indicated when RACF sets an indicator in the DSCB for a non-VSAM DASD data set, in the catalog entry for a VSAM data set, or in the tape volume profile for a tape data set. If a data set is RACF-indicated, a user can access the data set only if a RACF profile or an entry in the global access checking table exists for that data set. If a user requests access to a RACF-indicated data set, RACF first checks for an entry in the global access checking table, then a discrete profile and, finally, a generic profile when verifying access authorization. An error condition exists if a data set is RACF-indicated, but there is no entry in the global access checking table and the data set is not protected by a discrete or generic profile. On a system without RACF, a user cannot access a RACF-indicated data set unless the indicator is turned off.

RACF-protected. A resource is RACF-protected if it has either a discrete profile or an applicable generic profile. A data set that is RACF-protected by a discrete profile must also be RACF-indicated.

RACF manager. The routines within RACF that provide access to the RACF data base. Contrast with **RACF storage manager**.



RACF report writer. A RACF function that prints out RACF SMF records and produces reports on system use and resource use from information found in the RACF SMF records.

RACF segment. The portion of a profile that contains basic information needed to define an entity (user, group, data set, or general resource) to RACF.

RACF storage manager. The routines within RACF that obtain and release system storage on behalf of the rest of RACF. Contrast with **RACF manager**.

RBA (relative byte address). The address of an index block or index control block in the RACF data base.

resource. A facility of the computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs.

Resource Access Control Facility (RACF). A program product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, and logging detected unauthorized attempts to enter the system and detected accesses to protected resources.

security. See data security.

security category. An installation-defined name corresponding to a department or area within an organization with similar security requirements.

security level. An installation-defined name that corresponds to an numerical security level (the higher the number, the higher the security level).

standard access list. See access list.

TSO segment. The logical area of a RACF profile containing TSO/E logon information.

TVTOC. On MVS, the tape volume table of contents (TVTOC) is information about a tape data set that RACF stores in the TAPEVOL profile for the volume on which the data set resides. The TVTOC includes the data set name, data set sequence number, creation date, and an indicator as to whether a discrete tape data set profile exists.

universal access authority (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities.

user. A person who requires the services of a computing system.

user attribute. A characteristic of a user that defines the type of functions the user can perform on entities. The user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE.

user data set. On MVS, a data set defined to RACF where either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF userid.

user identification. See userid.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the system during TSO or VM logon or batch job processing. RACF identifies the user by the userid and verifies the user by the password and/or operator identification card (MVS only) supplied during logon processing or the password supplied on a batch JOB statement.

user name. One to twenty alphanumeric characters that represent a RACF user.

user profile. A description of a RACF-defined user including the userid, user name, default group name, password, owner, access authority, attributes, security level.

userid. A code that uniquely identifies a user to the system. A userid is one to eight alphanumeric or national characters. On TSO and for MVS batch jobs, userids can only be seven characters and must begin with an alphanumeric or national character.

verification. See user identification and verification.

VM. Implies VM/SP with or without the High Performance Option and VM/XA System Product.

VM event. The use of a CP command, DIAGNOSE function, or a user request related to communication among virtual machines (such as spool file open).

volume set. The collection of volumes on which a multivolume data set resides. A volume set is represented in one RACF profile.

Index

A

C

D

E

F

G

H

I

L

M

N

O

P

V

W

Y

Resource Access
Control Facility
(RACF) General
User's Guide

READER'S
COMMENT
FORM

SC28-1341-3

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

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 comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

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 or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) General User's Guide

SC28-1341-3 S370-34

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 NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 950
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

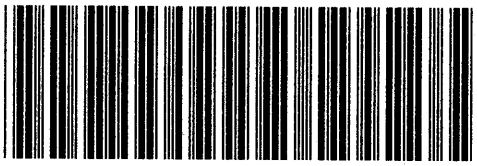
Printed in U.S.A.

IBM®

Program Number
5740-XXH

File Number
S370-34

SC28-1341-3



Printed in U.S.A.