# VMSECURE User's Guide

January 31, 1986

Release 2.1

VM Software, Inc.
2070 Chain Bridge Road
Suite 355
Vienna, Virginia 22180
(703) 442-9314

This document was prepared to assist licensed users of VM Software, Inc.'s VMSECURE system; its contents may not be used for any other purpose without prior written permission. The material contained herein is supplied without representation or warranty of any kind. VM Software, Inc., therefore, assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.



Printed in the United States of America.

# SUMMARY OF CHANGES

The VMSECURE User's Guide has been updated to provide information about new features included in VMSECURE Release 2.1. It includes detailed information on using the QUERY subcommand.

Changes and new material in this book are identified by vertical bars in the left margin.

# PREFACE

The VMSECURE User's Guide is intended primarily for the individual who has limited data processing experience; however, some VM/SP experience is required.

This book contains nine chapters describing the procedures and subcommands available to the general VMSECURE user, a glossary, and an index.

Chapter 1, "Overview," contains an overview of the VMSECURE capabilities and authorization levels.

Chapter 2, "Using the USER Subcommand," describes how to issue the USER subcommand and perform the functions available through the User Selection Menu.

Chapter 3, "Using the MAINT Subcommand," describes the capabilities of the MAINT subcommand, for users who do not have 3270 display terminals.

Chapter 4, "Using the QUERY Subcommand," describes the uses of the QUERY subcommand available to users.

Chapter 5, "Encryption Capabilities," contains an overview of the NBS Data Encryption Standard and the VMSECURE encryption and decryption components.

Chapter 6, "VMCIPHER Command Reference," describes the VMCIPHER command, which encrypts and decrypts data.

Chapter 7, "VMXDEF Command Reference," describes the VMXDEF command, which allows OS simulation application programs running under CMS to use VMCIPHER on input or output files without program modification.

Chapter 8, "VMXSUBS Subroutines," describes the three subroutines that encrypt or decrypt blocks of data.

Chapter 9, "Using the CMS HELP Facility," explains how to use the online HELP facility to obtain information on subcommands and system messages.

## NOTATIONAL CONVENTIONS

The following conventions are used in this book to define the VMSECURE subcommand syntax:

1. When truncation of a parameter name is permitted, the shortest acceptable version of the name is represented by uppercase letters. For example:

   Query

   indicates that Q, QU, QUE, QUER, and QUERY are all valid specifications for the QUERY subcommand.

2. Uppercase letters, asterisks (*), and parentheses must be entered exactly as shown.

3. Lowercase letters represent information that must be supplied by the user.

4. Information contained within brackets represents an option that can be included or omitted.

5. Vertical lists that are enclosed in brackets represent alternatives, at least one of which may be given. For example:

   ```
   +   +
   | A |
   | B |
   +   +
   ```

6. Vertical lists that are not enclosed in brackets represent alternatives, at least one of which must be given. For example:

   X
   Y

The following additional conventions are used in this book:

7. Examples are shown with user entries in lowercase and system entries in uppercase. System messages are shown in uppercase, even though they may appear in mixed case on your terminal screen.

8. Messages in this book were generated with a setting of TEXT for the CP SET EMSG command. Only the

message text (not the message code) is displayed. For example:

```
USERID NOT SPECIFIED.
R(00024);
```

rather than:

```
VMXSYS366E USERID NOT SPECIFIED.
R(00024);
```

When you use a setting of TEXT, you can refer to the "Message Cross-Reference" section in the VMSECURE Messages and Codes for an alphabetical cross-reference of the messages.

## RELATED PUBLICATIONS

For the general user:

IBM Virtual Machine/System Product:

CE Command Reference for General Users, SC19-6211

## COMMENTS AND SUGGESTIONS

VM Software, Inc. welcomes comments and suggestions for improving this book. For this purpose, a Reader's Comment form is provided at the end of the book. If the form is missing, please send your comments to:

VM Software, Inc.
Technical Publications
2070 Chain Bridge Road, Suite 355
Vienna, Virginia 22180

# CONTENTS

## LIST OF ILLUSTRATIONS

# 1.0 OVERVIEW

The basis of any VM security product is sound directory management. Toward this end, VMSECURE, a directory and disk space management and security system for the VM environment, provides the following:

- Authorization levels that allow different classes of users to perform specific levels of directory modification
- Customizing the validation of data modifications such as account numbers, passwords, and distribution codes through user exits
- Monitoring password violations within VMSECURE functions
- Enforcing periodic logon password changes
- Providing last logon information that displays at logon time
- Performing mass changes of logon and link passwords
- Monitoring links to minidisks
- Protecting against overlapping minidisks
- Audit reports.

VMSECURE also provides a database of installation-defined rules that controls access to virtual machines and minidisks and the transfer of data between virtual machines. The Rules facility performs the following functions:

- Intercepts the following CP commands and determines whether the command request should be accepted or rejected based on an applicable rule found in the rules database: AUTOLOG, LINK, LOGON, SPOOL, TAG, and TRANSFER.
- Intercepts the VMSECURE GROUP subcommand; the VMSCHEDULE CANCEL, QUERY, and SCHEDULE subcommands; and the VMTAPE CATALOG, LIST, and MOUNT subcommands. Determines whether the above subcommands should be accepted or rejected based on an applicable rule in the rules database.

Creates rules dynamically when invalid passwords for the AUTOLOG and LINK commands reach the maximum defined by your installation.

Allows your site to determine how to handle excessive invalid logon attempts.

Maintains rules at three levels: system, security group, and user.

Provides last logon information that displays at logon time and provides information as to when a userid was last logged on .

Provides history information by virtual machine about successful and unsuccessful attempts to access your virtual machine or its minidisks.

Allows you to specify time of day and dates that virtual machines and minidisks can be accessed.

Coordinates directory maintenance and rules modifications by removing rules for userids that are deleted from the directory and changing rule references when the userid changes.

The three authorization levels available with VMSECURE are directory administrator, directory manager, and general user. A VMSECURE **directory administrator** can modify any field in any userid's directory entry. Most installations establish one directory administrator, but there is no restriction on the number of directory administrators allowed. The directory administrator can also perform directory manager and general user functions for other users.

A VMSECURE **directory manager** can create and modify userids assigned to him and manipulate minidisks belonging to those userids. The ability to modify statements in the directory entry is limited to editing comment statements in the directory. A typical installation may authorize the manager of each user department to modify the userids in his department. A particular userid can be assigned to only one directory manager. A directory manager may also perform general user functions for users.

A VMSECURE **general user** can perform limited modifications on his own directory entry and can remove links made by other userids to his minidisks.

Information in this book is based on typical use. Any unusual use of this system may produce unpredictable results. If you have unusual circumstances, have your VMSECURE system administrator contact your Technical Support Representative at VM Software, Inc.

# 2.0 USING THE USER SUBCOMMAND

When you log on to VM, a virtual machine is created for you. This virtual machine is the functional equivalent of a computer with its associated devices. The characteristics of your virtual machine are defined in your directory entry. These characteristics include such attributes as your userid, logon password, minidisk passwords, size and location of your minidisks, and links to other minidisks.

Use the USER subcommand to modify certain characteristics of your virtual machine. The USER subcommand requires a 3270 display terminal. ALL USER subcommand functions are presented to you with a full-screen display: you fill in the necessary data fields without concern for command syntax. Use the MAINT subcommand, documented in "Using the MAINT Subcommand" on page 37, to perform the same functions with a line mode terminal.

The following sections describe how to issue the USER subcommand, use the full-screen displays, and use the special function keys.

## 2.1 USER SUBCOMMAND

To modify characteristics of your virtual machine using a 3270 display terminal, issue the following command:

```
vmsecure user
```

A full-screen menu displays the 11 user functions available with the USER subcommand.

The remainder of this section provides an overview of the 11 functions available with the USER subcommand.

Selection 1: Logon Storage Size and Password

Use Selection 1 to change the amount of virtual storage your userid is allocated at logon. Virtual storage can be modified after logon with the CP DEFINE STORAGE command.

Use Selection 1 to change your logon password.

Selection 2: Minidisk Link Mode and Passwords

Use Selection 2 to modify the link mode and read, write, or multiple passwords for your minidisks.

*Selection 3: Virtual Machine Options*

Use Selection 3 to select or remove various attributes associated with your userid: REALTIMER, ECMODE, BMX, SVCOFF, VMSAVE, ISAM, and CPUID. None of these attributes is necessary for normal CMS operation.

*Selection 4: Logical Line Editing Symbols*

Use Selection 4 to modify the terminal logical line editing symbols set for your userid at logon. The symbols that can be modified are: line end, line delete, character delete, and escape character.

*Selection 5: IPL System Name and Parameters*

Use Selection 5 to specify the system to be IPLed at logon.

*Selection 6: Screen Colors and Highlighting*

Use Selection 6 to modify the color and highlighting features set for your userid at logon. Color and highlighting settings affect only IBM 3279 color display terminals.

*Selection 7: Define a Link to Another User's Minidisk*

Use Selection 7 to set up a directory link to another user's minidisk. Directory links are performed for you at logon.

*Selection 8: Review/Remove Links By Other Users*

Use Selection 8 to review and optionally remove any directory links that other users may have defined to one of your minidisks. This selection is particularly useful when you determine that data on your minidisk should no longer be shared with other users.

*Selection 9: Account Number and Distribution Code*

Use Selection 9 to change the account number to which your usage is charged or to change the

distribution code associated with your spooled output.

*Selection 10: Delete a Link to Another User's Minidisk*

Use *Selection 10* to delete your directory link to another user's minidisk.

*Selection 11: Review the Directory Entry*

Use *Selection 11* to review all directory control statements in your directory entry. *Selection 11* provides information about existing directory links and all virtual addresses associated with your virtual machine. This information is needed for *Selections 2, 7, 8, and 10.*

## 2.2 ACCESSING THE USER SELECTION MENU

The USER subcommand enables the user to display the User Selection Menu and select a function to be executed. To access the menu, you need the full-screen capability of an IBM 3270 display terminal. To invoke the USER subcommand, complete the following steps:

1. Log on to your userid.

2. Type VMSECURE USER and press ENTER.

3. When prompted, type your logon password and press ENTER to display the User Selection Menu shown in Figure 1. The menu enables you to select a function. Each function is explained in detail in this chapter.

   The screen that is displayed follows:

```
+-------------------------------------------------------------------------------
| Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So
|
|                          * * * User Selection Menu * * *
|
|                        Userid: JONES         Manager: CSMGR
|
|                     + - - - - - - - - - - - - - - - - - - - - - - +
|                     |                                             |
|                     |  Selection:           For Device: 191       |
|                     |                                             |
|                     + - - - - - - - - - - - - - - - - - - - - - - +
|
|                                   Selections:
|
| 1 Logon Storage Size and Password     7 Define a Link to Another Use
| 2 Minidisk Link Mode and Passwords    8 Review/Remove Links By Other
| 3 Virtual Machine Options             9 Account Number and Distribut
| 4 Logical Line Editing Symbols       10 Delete a Link to Another Use
| 5 IPL System Name and Parameters     11 Review the Directory Entry
| 6 Screen Colors and Highlighting
| ------------------------------------------------------------------------------
| PA1: Cancel      PF1: Help        PF3: Quit        PF10: Print
+-------------------------------------------------------------------------------
```

Figure 1. User Selection Menu

4. In the SELECTION field, type the number that corresponds to your selection.

5. VMSECURE displays the default virtual device address, 191, in the FOR DEVICE field. A virtual device address is required for Selections 2, 7, 8, and 10. If a virtual device address other than 191 is desired, type that address in the field.

6. Press ENTER to display the screen associated with the specified function.

## 2.3 USING THE FULL-SCREEN DISPLAYS

When a screen is initially displayed, the cursor is positioned at the first non-blank data entry field. To perform a function, enter the data requested on the screen.

Some fields on the screen may already have a value; these are default values provided when VMSECURE can anticipate the values you might want to enter. Default values can be overridden by placing the cursor at the field and entering the desired value.

Some fields on the screen are left blank. In most cases, you do not have to fill in each field since VMSECURE can calculate the necessary values from data you have already provided.

Most of the screens require that you enter at least one value. If VMSECURE determines that no fields were modified, the function is not performed and the menu is redisplayed.

When you have finished entering data, press ENTER. If VMSECURE determines that you have left an essential field blank (that is, remaining values cannot be determined until a value is supplied for that field), the cursor is repositioned at that field. You must do one of the following:

Enter a value to continue.

Press PA1 to cancel the USER subcommand.

Press PF3 to quit the screen without performing the function.

At the bottom of each screen is a list of the special function keys available to that screen and their meanings.

Some USER subcommand functions require a virtual address specification. If a virtual address is not specified, 191 is assumed. If you wish to specify a virtual address other than 191, specify the address in the FOR DEVICE field on the menu.

It is important to note that the functions performed with the USER subcommand are made to a copy of your directory entry. Therefore, should you decide that you

do not want to save any changes, you can use PA1 from the menu to cancel all changes. PA1 indicates that all changes made to the copy of your directory entry are to be discarded.

## 2.4 SPECIAL FUNCTION KEYS

Within the VMSECURE user screens, the following keys perform special functions:

**----->|** Forward tab key. Moves the cursor to the beginning of the next data entry field.

**|<-----** Reverse tab key. Moves the cursor back to the beginning of your current field or, if the cursor is already at the start of a field, to the beginning of the previous field.

**ENTER** Sends screen data to VMSECURE. If changes to the screen data are valid, VMSECURE modifies a copy of your directory entry. If no changes are made to the selected screen, the menu is redisplayed. If a field is incomplete or invalid when ENTER is pressed, the cursor is repositioned in that field and the system may display a status message at the bottom of the screen. When ENTER is pressed from the User Selection Menu, your directory entry is updated online.

**PA1** Cancels the VMSECURE session and returns the user to the CMS environment. The PA1 key restores the user's directory entry to its original contents at the beginning of the VMSECURE session. Since Selection 8, Review/Remove Links by Other Users, modifies directory entries other than the requesting userid, the PA1 key ends the VMSECURE session but does not cancel any changes made from this screen.

**PA2** Changes the password display mode on screens containing a password field. Pressing PA2 initially makes the current password visible to the user. PA2 may be disabled at your site by the VMSECURE system administrator.

**Note:**

Any data keyed but not ENTERed is lost when PA2 is pressed.

**CLEAR** Refreshes the screen to its initial values.

| | |
|---|---|
| **PF1** | Displays online help information for the current screen. |
| **PF3** | Quits the current screen without performing any updates. If you have made changes during the current VMSECURE session and press PF3 while the User Selection Menu is displayed, you receive a message instructing you to press PA1 to cancel changes made during this VMSECURE session or to press ENTER to complete the changes. |
| **PF10** | Prints the current screen and sends screen data to VMSECURE. Fields in non-display mode are not printed. |
| **PF12** | Ends the VMSECURE session after performing any updates on the current screen. The User Selection Menu is not redisplayed. |

## 2.5 CHANGING LOGON STORAGE SIZE AND PASSWORD

Use Selection 1, Logon Storage Size and Password, to change the logon password and the default logon storage size for your virtual machine. The screen associated with this selection is shown below:

```
+-------------------------------------------------------------------------------
| Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So
|
|                  Selection 1:  Logon Storage Size and Password
|
|                                Userid: JONES
|
|                  + - - - - - - - - - - - - - - - - - - - - - - - - - +
|                  |                                                   |
|                  |  Storage Size: 1M          Password:              |
|                  |                                                   |
|                  + - - - - - - - - - - - - - - - - - - - - - - - - - +
|
|
|
|                  Note: Press PA2 to reverse password display mode.
|
|
|  ---------------------------------------------------------------------------
|  PA1: Cancel       PF1: Help          PF3: Quit          PF10: Print
+-------------------------------------------------------------------------------
```

Figure 2. Logon Storage Size and Password Screen

**Procedure:**

1. To change your logon storage size, type the desired storage in the STORAGE SIZE field.

   **Notes:**

   CP will round the specified storage size to a multiple of 4K. The directory entry will contain the storage size you specified, but a CP QUERY VIRTUAL STORAGE command will show the storage size as a multiple of 4K.

   The last character must be K or M (1M=1024K).

   Minimum size is 8K; maximum size is 16M. The directory entry for your userid may define your maximum size as less than 16M. If the size you specify is less than 8K, the directory entry

will contain the storage size you specified, but a CP QUERY VIRTUAL STORAGE command will show a storage size of 8K.

2. To change your logon password, type a one- to eight-character password in the PASSWORD field.

   **Notes:**

   When the Logon Storage Size and Password screen is displayed, the password is in non-display mode. To view the password, press PA2. Any change to the screen that has not been processed by ENTER is lost when PA2 is pressed.

   If your site has implemented password suppression, or the Password Encryption facility, you cannot view your password at a terminal, and the screen is slightly different from the one shown in Figure 2 on page 14. When you change your logon password, you are prompted to reenter it for verification.

   You cannot change your logon password to NOLOG; NOLOG is a special password that prevents a userid from being logged on. NOLOG should be used only by directory administrators to deactivate a userid but still allow access to its minidisks.

   Your installation may have controls to ensure that your new password is not one you have used in the past.

3. Press ENTER to verify field entries.

4. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.6 CHANGING MINIDISK LINK MODE AND PASSWORDS

Use Selection 2, Minidisk Link Mode and Passwords, to change the link mode for the minidisk specified on the User Selection Menu and to change the read, write, and multiple passwords associated with the minidisk. By specifying a password for a minidisk, you make it possible to share your CMS files with other users. The screen associated with this selection is shown below:

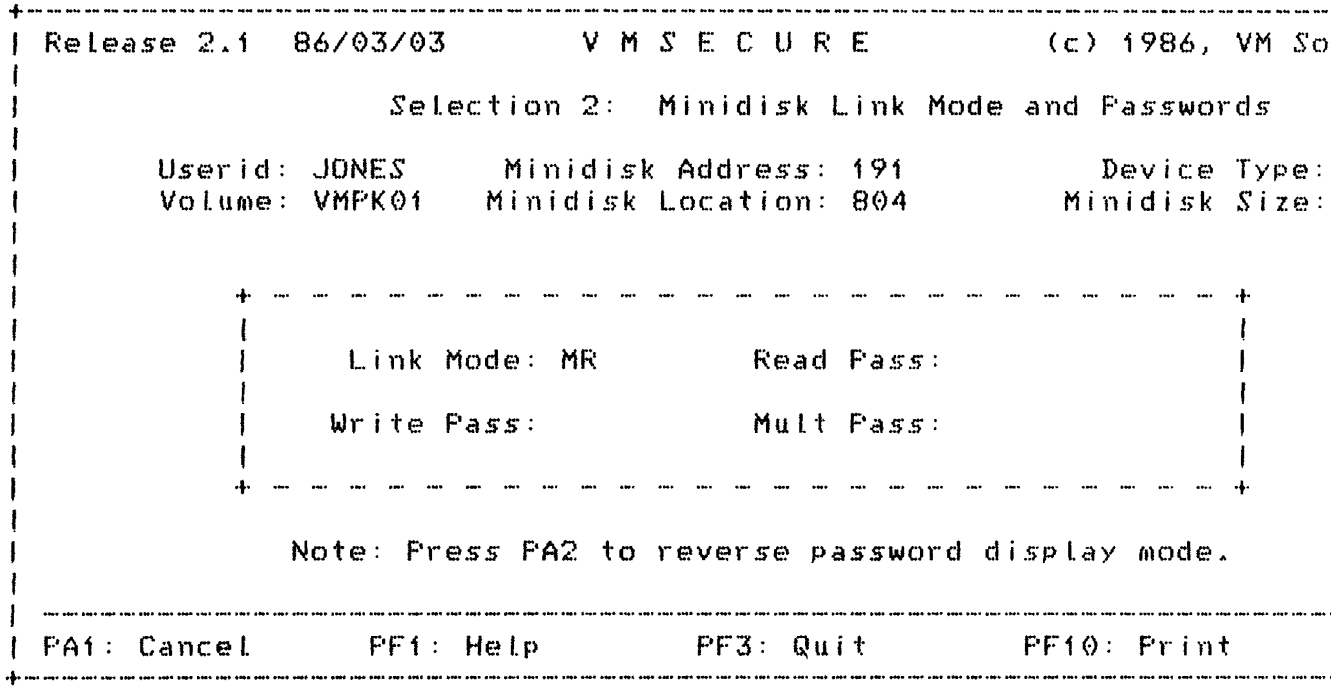



Figure 3. Minidisk Link Mode and Passwords Screen

**Procedure:**

1. To change the link mode, one of the following codes is required in the LINK MODE field:

   **R** Read-only link. The read-only link is established as long as no other user has the minidisk in write mode. If there is an existing write link to the minidisk, no link is granted.

   **RR** Read-only link. The read-only link is established even if another user has the minidisk linked in read or write mode.

**W** Write link. The write link is established only if there are no other current links to the minidisk. If there is an existing read or write link, no link is granted.

**WR** Write and read link. A write link is established if available. Otherwise a read-only link is granted.

**M** Multiple link. A write link is established if no user already has a write link to the minidisk. If a user has a write link, no link is granted.

**MR** Multiple read link. A write link is established if no user already has a write link to the minidisk. If a user has a write link, a read link is granted. (Unpredictable results can occur if a user has a read link to a minidisk that is being updated by a user who has a write link.)

**MW** Multiple write link. A write link is granted in all cases. (More than one user writing to the same minidisk can result in a permanent loss of data.)

**V** Virtual reserve release. This specifies use of CP virtual reserve/release support in I/O operations when it is appended to the right of the access mode, as in MWV.

2. To change any or all of the passwords appearing on the screen, type changes in the READ PASS, WRITE PASS, and MULT PASS fields.

**Notes:**

A valid password entry is one to eight characters in length and contains no blanks, left parentheses, or right parentheses.

A read password must exist before a write password can be entered; both read and write passwords must exist before a multiple password can be entered.

When the screen displays, the password is in non-display mode. To view the password, press PA2. Any change to the screen that has not

been processed by ENTER is lost when PA2 is pressed. If your site has implemented password suppression or the Password Encryption facility, you cannot view passwords at your terminal.

When you are in non-display mode and enter a password with fewer characters than the existing password, press ERASE EOF to clear the remainder of the old password.

3. Press ENTER to verify field entries.

4. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.7 SETTING VIRTUAL MACHINE OPTIONS

Use Selection 3, Virtual Machine Options, to select (ON) or remove (OFF) options associated with your userid and to enter a virtual CPUID to be associated with your virtual machine. The screen associated with this selection is shown below:

```
+-------------------------------------------------------------------------------
| Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So
|
|                        Selection 3:  Virtual Machine Options
|
|                                    Userid: JONES
|
|
|                 + - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|                 |                                                         |
|                 |   REAL TIMER: OFF       ECMODE: OFF      BMX: OFF       |
|                 |                                                         |
|                 |       SVCOFF: OFF       VMSAVE: OFF     ISAM: OFF       |
|                 |                                                         |
|                 |                          CPUID:                         |
|                 |                                                         |
|                 + - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|
|    Note: Specify ON or OFF or enter the desired CPUID value in hexa
|
| ------------------------------------------------------------------------------
| PA1: Cancel       PF1: Help          PF3: Quit          PF10: Print
+-------------------------------------------------------------------------------
```

Figure 4. Virtual Machine Options Screen

None of these options is necessary for normal CMS operation. Some of the options result in increased system overhead. For more information, refer to the documentation on the CP SET command in IBM VM/SP: CP Command Reference for General Users or check with your VMSECURE directory manager.

The options and their definitions are listed below:

REAL TIMER — When this option is ON, the timer for the virtual machine is updated during virtual processor run time **and** wait time. When the option is OFF, the timer reflects only virtual processor run time.

| | |
|---|---|
| ECMODE | When this option is ON, the virtual machine is allowed to run in extended control mode. The option is required for certain operating systems and virtual machines. When the option is OFF, the virtual machine runs in basic control mode. |
| BMX | When this option is ON, virtual machine I/O channels are simulated as block multiplexer channels instead of as selector channels. |
| SVCOFF | When this option is ON, CP handles all SVC interrupts for the virtual machine. |
| VMSAVE | When this option is ON, virtual machine registers and real storage contents are saved on DASD space if the virtual machine is terminated. |
| ISAM | When this option is ON, special channel command word translation routines are provided to permit OS/PCP, MFT, and MVT ISAM operation. |
| CPUID | With the previous virtual machine options, valid entries on the VMSECURE screen are ON or OFF. For the CPUID field, only one- to six-character hexadecimal entries are valid. This value is reflected in the information stored by the STIDP instruction. See the SET command in the CP Command Reference for General Users or check with your VMSECURE directory manager for further information. |

**Procedure:**

1. To activate an option, tab to the desired field, clear the field, and type ON. To deactivate, type OFF or simply clear the field.

2. To change the CPUID, type the new CPUID in the CPUID field. To remove a CPUID, clear the field.

3. Press ENTER to verify field entries.

4. Press ENTER again to initiate the update, or press PF3 to quit (cancel the changes).

**Note:**

Your new virtual machine options become your default values the next time you log on. The CP *SET* command can be used to change any of these values for your current *session*.

## 2.8 SELECTING LOGICAL LINE EDITING SYMBOLS

Use Selection 4, Logical Line Editing Symbols, to change the terminal logical line editing symbols established by default when you log on to VM. To determine the defaults in effect at your installation, issue the CP QUERY TERMINAL command. The screen associated with this selection is shown below.

```
+-------------------------------------------------------------------------------
| Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So
|
|                     Selection 4:  Logical Line Editing Symbols
|
|                                   Userid: JONES
|
|
|                  + - - - - - - - - - - - - - - - - - - - - - - - - - - +
|                  |                                                     |
|                  |           Line End: ON          Line Delete: ON     |
|                  |                                                     |
|                  |  Character Delete: ON    Escape Character: ON       |
|                  |                                                     |
|                  + - - - - - - - - - - - - - - - - - - - - - - - - - - +
|
|   Note: Specify symbols with a single character, a two-digit hexadec
|         value, or ON or OFF.
|
| ------------------------------------------------------------------------------
| PA1: Cancel       PF1: Help         PF3: Quit         PF10: Print
+-------------------------------------------------------------------------------
```

Figure 5. Logical Line Editing Symbols Screen

**Procedure:**

1. To change a symbol, tab to the desired field and type one of the following for each symbol changed:

   The desired symbol

   The hexadecimal representation of the symbol

   ON to select the system default symbol

   OFF to disable a specific line editing function.

2. Press ENTER to verify field entries.

3. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

**Note:**

Your new selections become your default values the next time you log on. The CP TERMINAL command can be used to change any of these values for your current session.

## 2.9 SELECTING IPL SYSTEM NAME AND PARAMETERS

Use *Selection 5, IPL System Name and Parameters*, to define, change, or remove the name of the system loaded at logon as well as the parameters to be passed to that system. The screen associated with this selection is shown below:

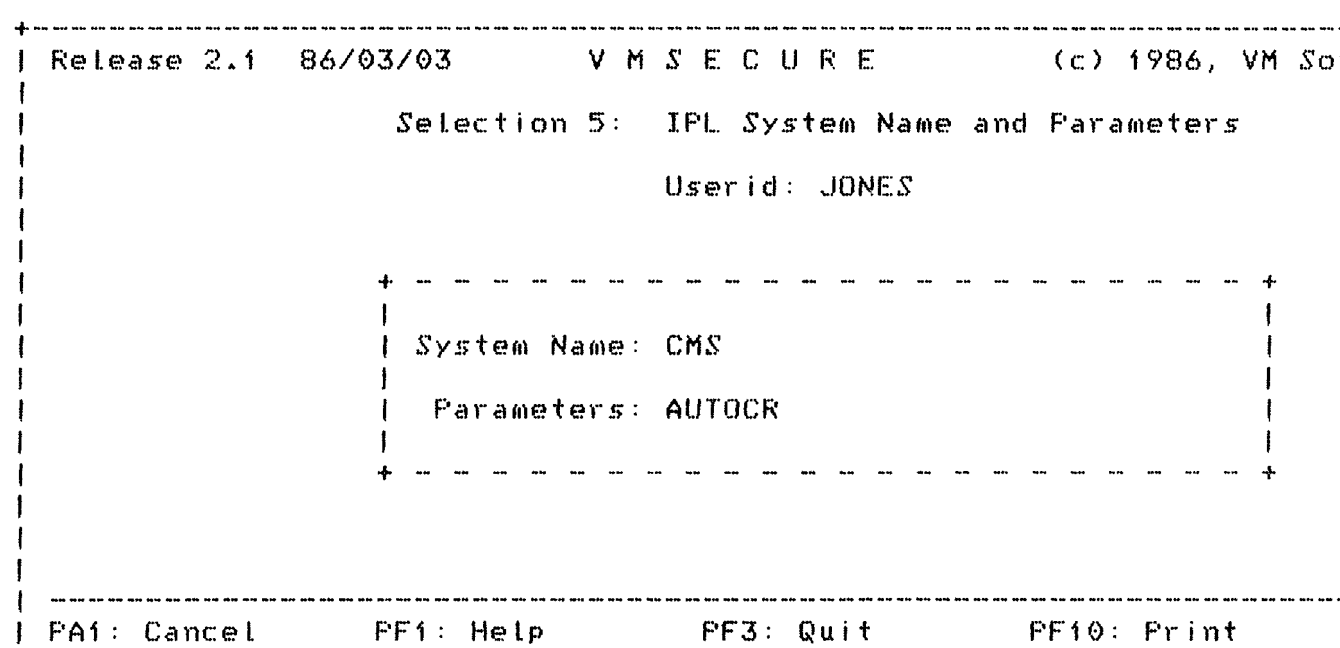



Figure 6. IPL System Name and Parameters Screen

**Procedure:**

1. To change the system loaded at logon, type a one- to eight-character system name (CMS, for example) **or** the three-digit virtual device address of the system minidisk in the SYSTEM NAME field.

2. To specify or change associated system parameters, type up to 30 characters of data to be passed to the system at IPL time in the PARAMETERS field. For example, AUTOCR is the parameter that performs an automatic "carriage return" after IPL to allow your PROFILE EXEC to execute without intervention.

3. Press ENTER to verify field entries.

4. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.10 CHANGING SCREEN COLORS AND HIGHLIGHTING

Use Selection 6, Screen Colors and Highlighting, to change the IBM or installation-defined default colors and highlighting on IBM 3279 color display terminals. These changes are effective when CP is managing the screen formats. Non-color terminal display is not affected by any changes made to your directory entry via this screen. The screen associated with this selection is shown below:

```
Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So

                  Selection 6:  Screen Colors and Highlighting

                                Userid: JONES


                    -Areas-   -Color- -Highlight-
                Input Area:  DEFAULT   NONE
                Status Area: DEFAULT   NONE
                  CP Output: DEFAULT   NONE
                  VM Output: DEFAULT   NONE
              Input Redisplay: DEFAULT   NONE

      Colors - DEFault          GREen                  Highlighting - NON
               BLUe             TURquois(e)                           BLI
               RED              YELlow                                REV
               PINk             WHIte                                 UND

PA1: Cancel       PF1: Help         PF3: Quit         PF10: Print
```

Figure 7. Screen Colors and Highlighting Screen

Colors or highlighting can be selected for any of the following:

**Input Area** The field at the lower left of the screen where commands are entered. It includes one entire line above the status area and all of the next line before the status area.

**Status Area** The field at the lower right of the screen where one of six system status

messages displays: RUNNING, VM READ, NOT ACCEPTED, MORE..., HOLDING, or CP READ.

| | |
|---|---|
| CP Output | Information displayed as the result of a CP command, such as the response to a QUERY USERS command. |
| VM Output | Information displayed by an operating system (such as CMS) that is running in your virtual machine, such as the response to a QUERY DISK command. |
| Input Redisplay | Information entered in the input area that is redisplayed in the upper portion of the screen after ENTER is pressed. |

**Procedure:**

1. To select colors or highlighting, tab to the desired fields and type the selected options.

   **Notes:**

   Colors available for display are shown on the screen in Figure 7 on page 25. The minimum abbreviations are shown in uppercase.

   You can remove highlights or set default colors by clearing the fields.

2. Press ENTER to verify field entries.

3. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.11 DEFINING A LINK TO ANOTHER USER'S MINIDISK

Use Selection 7, Define a Link to Another User's Minidisk, to add to your directory entry a link to a minidisk that belongs to another user. When this function is selected, the virtual address of the link to be defined must be specified in the FOR DEVICE field on the menu. VM performs the link automatically at logon. The screen associated with this selection is shown below:

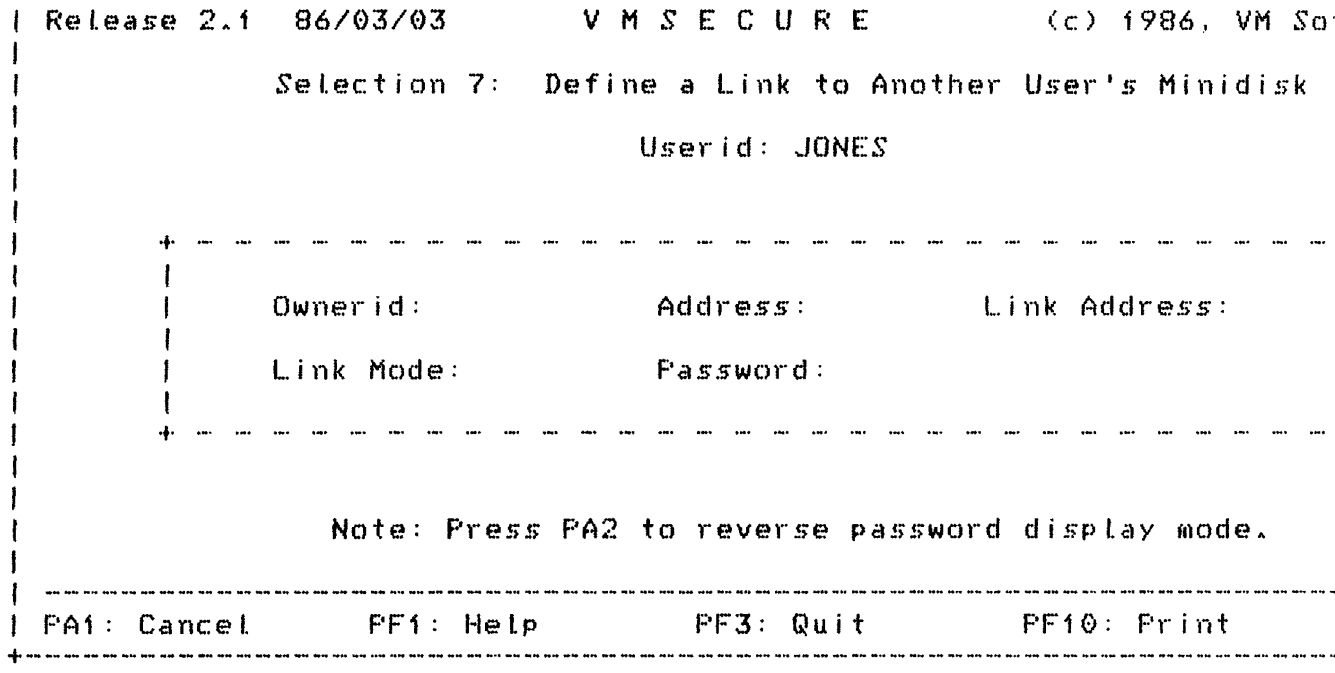



Figure 8. Define a Link to Another User's Minidisk Screen

**Procedure:**

To specify a Link, complete the following steps:

1. In the OWNERID field, type the userid that owns the minidisk to which you want to Link.

2. In the ADDRESS field, type the owner's virtual device address for the minidisk (for example, 191).

3. The LINK ADDRESS field displays the virtual address you entered on the menu. This is the virtual address at which you want to Link the specified

minidisk. You can change the Link address, if you desire.

4. In the LINK MODE field, type the mode in which you wish to Link this minidisk. Link modes are explained in the section "Changing Minidisk Link Mode and Passwords" on page 16.

5. In the PASSWORD field, type the owner's Link password for the minidisk.

**Notes:**

A read password is required for R and RR Link modes; a write password is required for W and WR Link modes; a multiple password is required for M, MR, and MW Link modes.

If the password for the desired minidisk is ALL, no password need be specified.

If the userid whose minidisk is being linked has not specified a password, the Link cannot be completed. If the Rules facility is installed, a rule must exist that allows you to Link to the other user's minidisk. If no rule is found, the installation-defined default is applied.

6. Press ENTER to initiate the update or press PF3 to quit (cancel the changes).

## 2.12 REVIEWING OR REMOVING LINKS BY OTHER USERS

Use Selection 8, Review/Remove Links by Other Users, to review or remove links to your minidisk that have been specified in other directory entries. The screen associated with this selection is shown below:

```
+-------------------------------------------------------------------------------
| Release 2.1  86/03/03        V M S E C U R E          (c) 1986, VM So
|
|                Selection 8:  Review/Remove Links by Other Users
|
|                      Userid: JONES            Minidisk: 191
|
|
|        +- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
|        |   Userid    Vaddr          Userid    Vaddr          Userid    Vadd
|        |   --------  -----          --------  -----          --------  ----
|        |   ALICE     205
|        |
|        |
|        |
|        +- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
|
|         Note: To remove another user's link to your minidisk, clear
|               corresponding field and press the ENTER key.
|
|-------------------------------------------------------------------------------
| PA1: Cancel       PF1: Help          PF3: Quit          PF10: Print
+-------------------------------------------------------------------------------
```

Figure 9. Review/Remove Links by Other Users Screen

The USERID field above the box displays your userid. The USERID fields within the box display the userids having a link to the minidisk shown in the MINIDISK field. The VADDR fields display the virtual addresses assigned to the minidisk when linked by the specified userids.

**Procedure:**

To remove a link, complete the following steps:

1. Position the cursor at the selected userid and press the ERASE EOF key.

2. Repeat step 1, as necessary, to remove other links.

3. Press ENTER when all links to be removed have been cleared.

4. Press ENTER again to display any additional links.

**Notes:**

1. When you exit VMSECURE after removing a link to your minidisk, you may receive the message DIRECTORY NOT CHANGED. This is because removing a link does not update your directory entry; it changes the directory entry of the userid that was linked to your minidisk.

2. CP links established with the CP LINK command are not displayed. Only directory links can be removed via VMSECURE. To determine who is currently linked to your minidisk, use the CP QUERY LINKS command.

## 2.13 CHANGING ACCOUNT NUMBER AND DISTRIBUTION CODE

Use Selection 9, Account Number and Distribution Code, to change the account number to which your usage is charged or to change the distribution code associated with your spooled output. The screen associated with this selection is shown below:

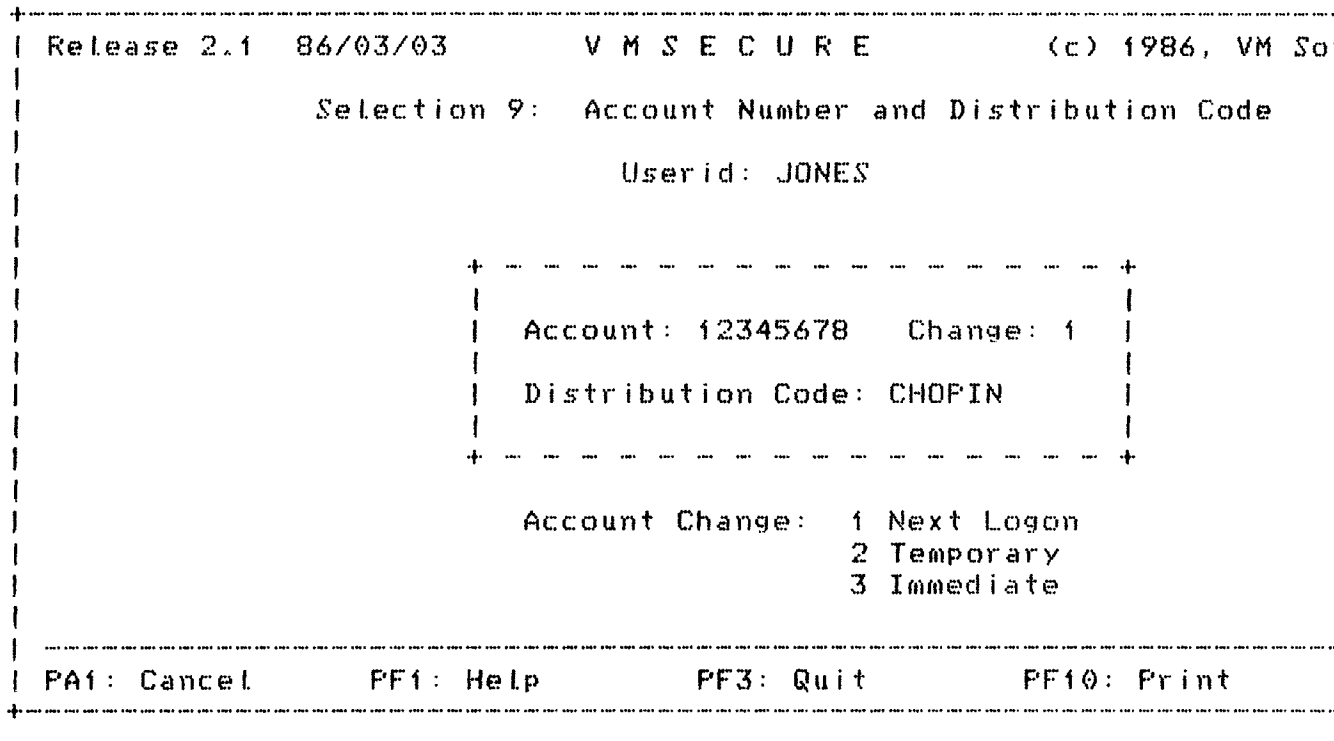



Figure 10. Account Number and Distribution Code Screen

**Procedure:**

1. To change your account number, type the new one- to eight-character account number in the ACCOUNT field.

2. If you change the account number, you must type an account change code in the CHANGE field. Valid entries are as follows:

   **1** Indicates the change will be in effect the next time you log on.

   **2** Indicates the change is in effect immediately and remains in effect until you log off.

**3** Indicates the change is in effect immediately and is permanent.

**Notes**:

Account number changes may be limited depending on installation-supplied exit routines.

If VMACCOUNT is installed at your installation, there is no CHANGE field on the screen and the account change is in effect immediately and is permanent (change code 3).

3. To change your distribution code, type a one- to eight-character word to be associated with your printer or punch output.

**Notes**:

Distribution code changes may be limited depending on installation-supplied exit routines.

If you delete your distribution code, your userid is supplied as the default distribution code.

4. Press ENTER to verify field entries.

5. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.14 DELETING A LINK TO ANOTHER USER'S MINIDISK

Use Selection 10, Delete a Link to Another User's Minidisk, to delete the link in your directory entry to another user's minidisk. When this function is selected, the virtual address of the link to be deleted must be specified in the FOR DEVICE field on the menu. The screen associated with this selection is shown below:

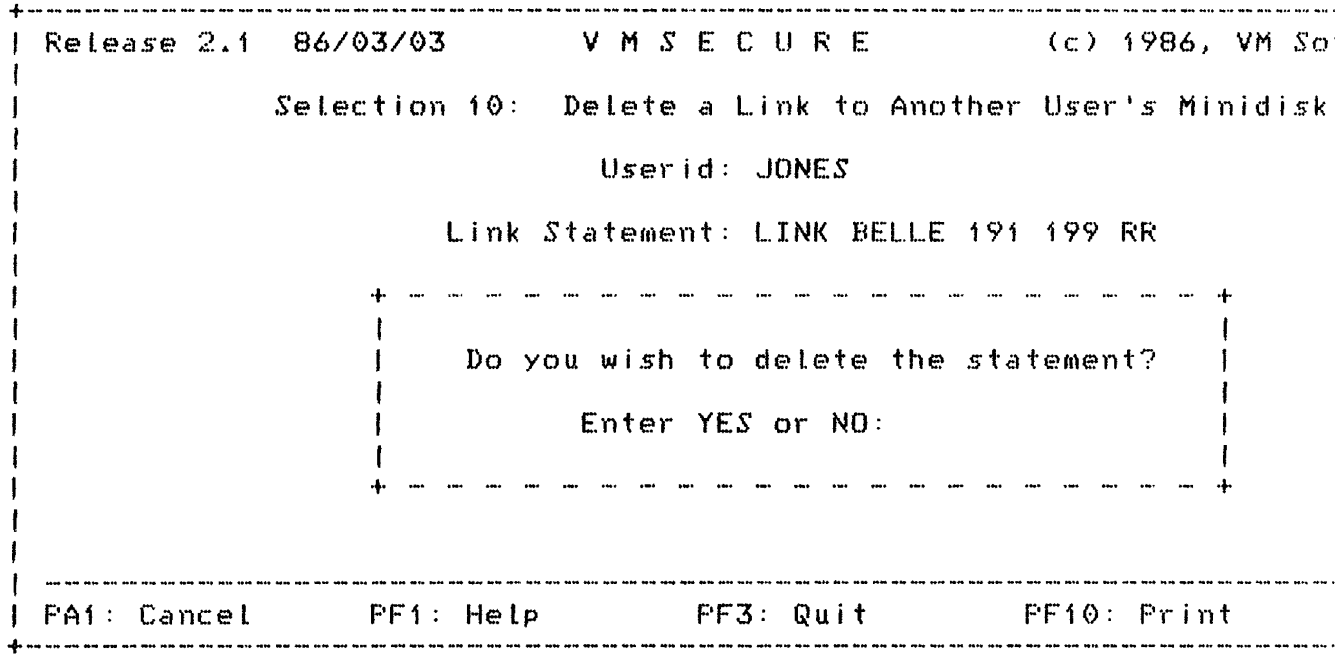



Figure 11. Delete a Link to Another User's Minidisk Screen

**Procedure:**

1. To delete the link specified, enter YES. Specify NO if you do not want to delete the link.

2. Press ENTER to verify field entries.

3. Press ENTER again to initiate the update or press PF3 to quit (cancel the changes).

## 2.15 REVIEWING YOUR DIRECTORY ENTRY

Use Selection 11, Review the Directory Entry, to use XEDIT to view a file that contains a copy of your directory entry. The XEDIT screen associated with this selection is illustrated below:

```
|
|
|   FINANCE  DIRECT   A0 V 80      TRUNC=72  SIZE=19 LINE=0 COL=1 ALT
|
|   |...+....1....+....2....+....3....+....4....+....5....+....6....+
|   00000 * * * TOP OF FILE * * *
|   00001 USER FINANCE ******** 1M 1M G 64
|   00002 *PW= 85/12/13 FINANCE
|   00003 *ED= 86/01/13 09:48:10 ACCTMGR  MANAGE  85/12/13
|   00004 *HS 01/24/86 10:49:27 Accepted Logon from 513
|   00005 *HS 01/23/86 06:18:13 Rejected Link by SNOOP to 191 (RR)
|   00006 *HS 01/22/86 10:01:15 Accepted Logon from 513
|   00007 *HS 01/21/86 10:23:18 Accepted Logon from 513
|   00008 *FL= *
|   00009 *LL= 10:49:27 EST Wednesday  01/22/86 from      5A2
|   00010 * Userid = FINANCE; Ext = 2048; Dept = 107; Mail Stop = 5E
|   00011 ACCOUNT 20000000 RECEIVE
|   00012 IPL CMS PARM AUTOCR
|   00013 OPTION ECMODE
|   00014 CONSOLE 009 3215
|   00015 SPOOL 00C 2540 READER *
|   00016 SPOOL 00D 2540 PUNCH A
|   00017 SPOOL 00E 1403
|   00018 LINK MAINT 190 190 RR
|   00019 LINK MAINT 19E 19E RR
|   00020 MDISK 191 3375 312 1 VMPK99 MR ********
|   00021 MDISK 192 3375 955 2 VMPK99 MR ********
|   00022 * * * END OF FILE * * *
|
|   ====>
|                                                  X E D I T   1 FIL
```

Figure 12. Sample XEDIT Directory Entry File

**Procedure:**

1. After selecting function 11, a screen similar to the one shown above displays. Review the information. No changes can be made to this screen.

2. To exit this XEDIT file, type FILE or QUIT after the command arrow (====>), or press PF3.

**Notes:**

The filename is your userid, the filetype is DIRECT, and the filemode is A0.

Because the file is written to disk, a read/write link to an A-disk is required. When you quit the file, it is erased from your minidisk. The function overwrites any existing file with the same fileid.

A brief description of the special directory comments used by VMSECURE follows. For more information, see your directory manager.

***ED=** Edit statement. Records the date and time your directory entry was last updated, the userid that performed the update, and the VMSECURE subcommand that was issued. For userids created after VMSECURE Release 2.1 was installed, the userid creation time and date are listed along with the userid of the directory manager who created the userid. For userids already existing when Release 2.1 was installed, the last subcommand issued for the userid and the time and date the userid was edited with VMSECURE Release 2.1 running are listed.

***FL=** Flag statement. Specifies the status of your logon password.

***HS=** History statement. Records successful and unsuccessful attempts to access your virtual machine and minidisks.

***LL=** Last Logon statement. Records the date, time, and terminal address for the last time your userid was logged on. The information recorded is displayed at next logon for your verification.

***PW=** Password History statement. Records the date your logon password was last changed.

# 3.0 USING THE MAINT SUBCOMMAND

The MAINT subcommand enables users who do not have 3270 display terminals to perform VMSECURE functions. The MAINT functions described in this chapter correspond to the full-screen USER subcommand. Use the MAINT subcommand to modify certain characteristics of your virtual machine.

## 3.1 MAINT SUBCOMMAND

The MAINT subcommand allows you to modify certain characteristics of your virtual machine.

Each MAINT function is explained in the following sections. Issue the MAINT subcommand by completing the following steps:

1. Log on to your userid.

2. Type "VMSECURE MAINT function" and press ENTER.

3. When prompted, type your logon password and press ENTER. For certain functions, you will be prompted for further information necessary to complete the subcommand.

4. If the syntax and information are correct, the directory will be updated and you will receive the message:

```
DIRECTORY UPDATED ONLINE.
R;
```

The general syntax of the MAINT subcommand line is shown below. Each subfunction is summarized.

The format of the MAINT subcommand line is:

| | |
|---|---|
| VMSECURE MAInt | function |

Any of the following are valid for "function":

ACCOUNT newacct <IMMED|NEXTLOG|TEMP>

Use the ACCOUNT function to change the account number to which your usage is charged.

DEFINE vaddr1 vaddr2

Use the DEFINE function to change the virtual address of one of your minidisks to a new address. "vaddr1" specifies the existing virtual address of the minidisk, and "vaddr2" specifies the new address.

DELETE vaddr

Use the DELETE function to delete your directory link to another user's minidisk. "vaddr" specifies the virtual address of the directory link you wish to remove.

DISTRIB newdist

Use the DISTRIB function to change the distribution code associated with your spooled output.

HELP|?

Use the HELP function to display a brief list of the MAINT subcommand functions and their operands.

IPL <sysname|vaddr <PARM parameters>>

Use the IPL function to specify the system to be IPLed at logon and any parameters to be passed to the IPLed system.

LINK ownerid ownervaddr yourvaddr <mode>

Use the LINK function to set up a directory link to another user's minidisk. Directory links are performed for you at logon.

MDPW <vaddr>

Use the MDPW function to display the passwords for your minidisks. If a virtual address is not specified, passwords for all your minidisks are displayed. Your installation may choose to mask minidisk passwords.

MGRID

Use the MGRID function to determine who your directory manager is.

MINIDISK vaddr

Use the MINIDISK function to modify the link mode and read, write, or multiple passwords for your minidisks. "vaddr" specifies the virtual address of one of your minidisks.

OPTION optname ON|OFF

Use the OPTION function to select (ON) or remove (OFF) various attributes associated with your userid: REALTIMER, ECMODE, BMX, SVCOFF, VMSAVE, ISAM, and CPUID. None of these attributes is necessary for normal CMS operation.

PASSWORD

Use the PASSWORD function to change your logon password.

REVIEW

Use the REVIEW function to review all directory control statements in your directory entry. The REVIEW function provides information about existing directory links and all virtual addresses associated with your userid. This information is needed for the DEFINE, DELETE, LINK, MINIDISK, MDFW, RLINK, and SCRATCH functions.

RLINK vaddr

Use the RLINK function to review and optionally remove any directory links that other users may have defined to one of your minidisks. This function is particularly useful when you determine that data on your minidisk should no longer be shared with other users.

SCRATCH vaddr

Use the SCRATCH function to scratch and format one of your minidisks. "vaddr" specifies the virtual address of the minidisk.

STORAGE sizeK|sizeM

Use the STORAGE function to change the amount of virtual storage your userid is set up with at logon. Virtual storage can be modified after logon with the CP DEFINE STORAGE command.

TERMINAL keyword ON|OFF|char|hex

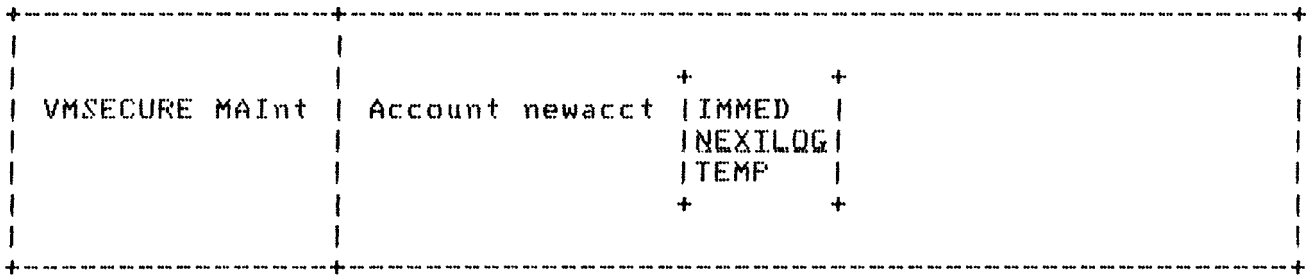
Use the TERMINAL function to modify the terminal logical line editing symbols set for your userid at logon. The symbols that can be modified are: line end, line delete, character delete, and escape character.

The following sections describe each of the MAINT functions in detail.

## 3.2 MODIFYING YOUR ACCOUNT NUMBER

Use the ACCOUNT function to alter your virtual machine's account number.

The format of the ACCOUNT function is:




where:

newacct specifies the new account number you wish to have. Your installation may have restrictions on what account numbers you can use.

IMMED specifies that the new account number is effective immediately and is permanent.

NEXTLOG specifies that the new account number will become effective the next time you log on and will be permanent. NEXTLOG is the default.

TEMP specifies that the new account number is effective immediately, but only until you log off. When you log on again, your old account number will be in effect.

Usage Notes:

1. If VMACCOUNT is installed at your installation, temporary (TEMP) and next logon (NEXTLOG) account number changes are disabled. The only valid account number change when VMACCOUNT is installed is effective immediately and is permanent (IMMED).

2. Account number changes may be limited depending on installation-supplied exit routines.

Examples:

1. To change your account number permanently to 01555000 and to have the change become effective immediately, enter the following:

```
vmsecure maint account 01555000 immed
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

2. To change your account number to 01555002, effective immediately and remaining in effect until logoff, enter the following:

```
vmsecure maint account 01555002 temp
ENTER YOUR LOGON PASSWORD:

R;
```

3. To change your account number to 02003001, effective when you next log on, enter the following:

```
vmsecure maint account 02003001
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

**Note**: You do not have to specify NEXTLOG on the command line because it is the default.

## 3.3 CHANGING THE VIRTUAL ADDRESS OF YOUR MINIDISK

Use the DEFINE function to change the virtual address of one of your minidisks. Directory links to this minidisk are updated to reflect the new virtual address. Minidisk passwords for the minidisk remain unchanged.

The format of the DEFINE function is:

| | |
|---|---|
| VMSECURE MAInt | DEFine vaddr1 vaddr2 |

where:

vaddr1 specifies the old virtual address of the minidisk

vaddr2 specifies the new virtual address of the minidisk.

Example:

To change the virtual address of one of your minidisks from 194 to 242, enter the following:

```
vmsecure maint define 194 242
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

## 3.4 DELETING A LINK TO ANOTHER USER'S MINIDISK

Use the DELETE function to remove a link to another user's minidisk from your directory entry.

The format of the DELETE function is:

| | |
|---|---|
| VMSECURE MAInt | Delete vaddr |

where:

vaddr — specifies the virtual address of the minidisk link you are deleting from your directory entry.

Example:

To delete virtual address 205, which is a link in your directory to another user's minidisk, enter the following:

```
vmsecure maint delete 205
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

## 3.5 MODIFYING YOUR DISTRIBUTION CODE

Use the DISTRIB function to alter your virtual machine's distribution code. This change does not take effect until the next session logon.

The format of the DISTRIB function is:

| | |
|---|---|
| VMSECURE MAInt | DIstrib newdist |

where:

newdist specifies the new one- to eight-character distribution code being assigned to your virtual machine.

Usage Note:

Distribution code changes may be limited depending on installation-supplied exit routines.

Example:

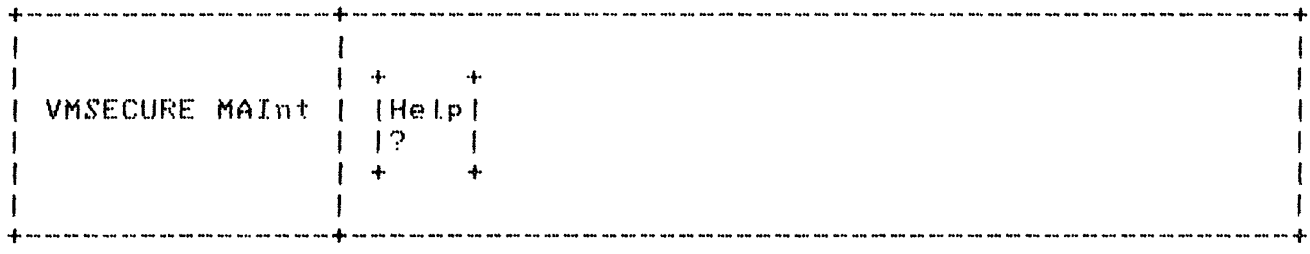
To change your distribution code to JSBACH, enter the following:

```
vmsecure maint distrib jsbach
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

## 3.6 DISPLAYING HELP INFORMATION

Use the HELP function to view a brief list of the MAINT subcommand functions and their operands.

The format of the HELP function is:




Usage Note:

Enter VMSECURE MAINT, VMSECURE MAINT HELP, or VMSECURE MAINT ? to display the MAINT subcommand functions.

Example:

To display the MAINT HELP screen, enter the following:

```
vmsecure maint help
ENTER YOUR LOGON PASSWORD:

THE VMSECURE MAINT SUBCOMMAND PARAMETERS ARE:

Account newacct (NEXTLOG|TEMP|IMMED)
DEFine vaddr1 vaddr2
Delete vaddr
DIstrib newdist
(Help|?)
Ipl (sysname|vaddr (PARM parameters...))
Link ownerid vaddr1 vaddr2 (mode)
MDpw (vaddr)
MGrid
MInidisk vaddr
Option keyword ON|OFF
Password
Review
RLink vaddr
SCratch vaddr
Storage sizeK|sizeM
Terminal keyword ON|OFF|char|hex

R;
```

## 3.7 MODIFYING IPL SYSTEM NAME AND PARAMETERS

Use the IPL function to add, remove, or change the IPL system name (or device address) and the parameters passed to the system when it is invoked during logon time.

The format of the IPL function is:

| | |
|---|---|
| VMSECURE MAInt | Ipl <sysname\|vaddr <PARM parameters>> |

where:

*sysname* specifies the name of the saved system you wish to IPL automatically at logon. If not specified, no system will be IPLed automatically at logon.

vaddr specifies the virtual address of the device you wish to IPL at logon.

PARM parameters
specifies the parameters you wish to pass to the IPLed system. An example is the AUTOCR parameter for CMS. If not specified, no parameters are passed at IPL time.

Usage Note:

If you enter VMSECURE MAINT IPL with no optional parameters, the IPL statement in your directory entry is deleted.

Example:

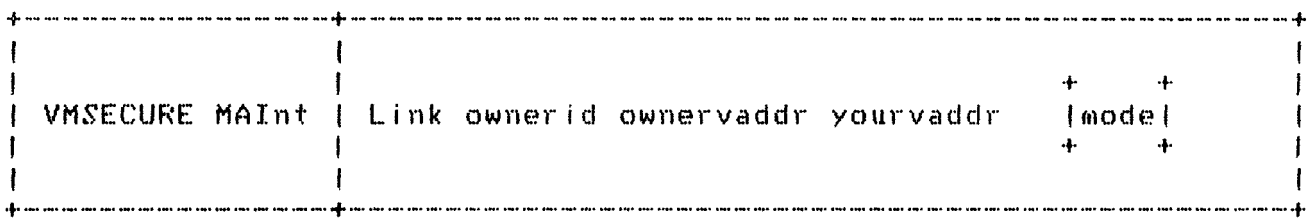
To change the system IPLed at logon, enter the following:

```
vmsecure maint ipl cms parm autocr
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

## 3.8 ADDING A DIRECTORY LINK TO ANOTHER USER'S MINIDISK

Use the LINK function to add a directory link to another user's minidisk. VM performs the link automatically at logon.

The format of the LINK function is:




where:

ownerid specifies the userid that owns the minidisk to which you are linking.

ownervaddr specifies the owner's virtual address for the minidisk to which you are linking.

yourvaddr specifies the virtual address for the linked minidisk as it is defined to your virtual machine.

mode specifies the mode in which you wish to link the minidisk. Valid link modes are R, RR, W, WR, M, MR, and MW. If no mode is specified, the default link mode is R. For more information about link modes, refer to the section "Changing Minidisk Link Mode and Passwords" on page 16.

Example:

To add a directory link to userid FINANCE's 191 minidisk and give it a virtual address of 195 on your machine with a link mode of RR, enter the following:

```
vmsecure maint link finance 191 195 rr
ENTER YOUR LOGON PASSWORD:

ENTER THE READ LINK PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

Usage Notes:

1. A read password is required for R and RR link modes; a write password is required for W and WR link modes; a multiple password is required for M, MR, and MW link modes.

2. If the password for the desired minidisk is ALL, no password prompt is displayed.

3. If the userid whose minidisk is being linked has not specified a password, the link cannot be completed. If the Rules facility is installed, a rule must exist that allows you to link to the other user's minidisk. If no rule is found, the installation-defined default is applied.

## 3.9 DISPLAYING LINK PASSWORDS

Use the MDPW function to display the link passwords for a specific minidisk or for all minidisks owned by your virtual machine.

The format of the MDPW function is:

| | |
|---|---|
| VMSECURE MAInt | MDpw <vaddr> |

where:

vaddr — specifies the optional virtual device address of a minidisk. If not specified, passwords for all minidisks are displayed.

Usage Notes:

1. The minidisk passwords are displayed in the following order: read, write, and multiple.

2. If password suppression or the Password Encryption facility is implemented at your site, you cannot view passwords at a terminal. The output of MAINT MDPW is asterisks.

Example:

To display the link passwords for your 191 minidisk, enter the following:

```
vmsecure maint mdpw 191
ENTER YOUR LOGON PASSWORD:

MINIDISK '191' HAS PASSWORDS: ALL FIN307 MGRBGT
R;
```

## 3.10 DETERMINING YOUR DIRECTORY MANAGER

Use the MGRID function to determine your directory manager.

The format of the MGRID function is:

| | |
|---|---|
| VMSECURE MAInt | MGrid |

There are no parameters.

Example:

For userid FINANCE to determine his directory manager, the following would be entered:

```
vmsecure maint mgrid
ENTER YOUR LOGON PASSWORD:

USER 'FINANCE' ASSIGNED TO DIRECTORY MANAGER 'FINEMGR'.
R;
```

## 3.11 MODIFYING YOUR MINIDISK LINK MODE OR PASSWORDS

Use the MINIDISK function to change or remove the link mode and passwords on one of your minidisks.

The format of the MINIDISK function is:

| | |
|---|---|
| VMSECURE MAInt | MInidisk vaddr |

where:

vaddr — specifies the virtual address of the minidisk.

Usage Note:

The *system* prompts for a new link mode and three passwords. If you do not wish to change the indicated parameter, enter an equal sign (=). To remove the parameter, press ENTER. The remaining passwords, if any, will be removed.

Example:

To change the link mode of your 191 minidisk to R and keep the passwords the same, enter the following:

```
vmsecure maint minidisk 191
ENTER YOUR LOGON PASSWORD:

ENTER NEW LINK MODE VALUE:
r
ENTER THE READ LINK PASSWORD:
=
ENTER THE WRITE LINK PASSWORD:
=
ENTER THE MULT LINK PASSWORD:
=
DIRECTORY UPDATED ONLINE.
R;
```

## 3.12 MODIFYING DIRECTORY OPTIONS

Use the OPTION function to add, remove, or change a directory option for your virtual machine.

The format of the OPTION function is:

| | |
|---|---|
| VMSECURE MAInt | Option optname ON\|OFF |

where:

optname — specifies the name of the option being modified. The valid names are: REALTIMER, ECMODE, BMX, SVCOFF, VMSAVE, ISAM, and CPUID. Refer to the section "Setting Virtual Machine Options" on page 19.

ON|OFF — specifies whether the option should be added (ON) to or removed (OFF) from your virtual machine's directory entry.

Usage Notes:

1. Option names can be abbreviated. The minimum abbreviations are indicated below with capital letters:

   BMX
   CPUID
   Ecmode
   Isam
   Realtimer
   Svcoff
   VMsave

2. If CPUID ON is specified, you are prompted to enter the six-digit hexadecimal CPUID value.

3. None of the options is necessary for normal CMS operation. Use of some of these options may increase system overhead. For more information, refer to the documentation on the CP SET command in IBM VM/SP: CP Command Reference for General Users or check with your VMSECURE directory manager.

4. Your new virtual machine options become your default values the next time you log on. The CP SET command can be used to change any of these values for your current session.

Examples:

1. To activate the REALTIMER option for your virtual machine, enter the following:

```
vmsecure maint option realtimer on
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

2. To specify a new CPUID of 123456, enter the following:

```
vmsecure maint option cpuid on
ENTER YOUR LOGON PASSWORD:

ENTER SECOND PARAMETER FOR CPUID:
123456
DIRECTORY UPDATED ONLINE.
R;
```

## 3.13 CHANGING YOUR VIRTUAL MACHINE'S LOGON PASSWORD

Use the PASSWORD function to change your virtual machine's logon password.

The format of the PASSWORD function is:

| | |
|---|---|
| VMSECURE MAInt | Password |

There are no parameters.

Usage Notes:

1. VMSECURE prompts for your current logon password, then prompts for your new password.

2. You cannot change your logon password to NOLOG; NOLOG is a special password that prevents a userid from being logged on. NOLOG should be used only by directory administrators to deactivate a userid, but still allow access to its minidisks.

3. Your installation may have controls to ensure that your new password is not one you have used in the past.

Example:

To change your logon password, enter the following:

```
vmsecure maint password
ENTER YOUR LOGON PASSWORD:

ENTER A NEW LOGON PASSWORD:

REENTER YOUR NEW LOGON PASSWORD FOR VERIFICATION:

DIRECTORY UPDATED ONLINE.
R;
```

## 3.14 REVIEWING YOUR DIRECTORY ENTRY

Use the REVIEW function to cause a copy of your directory entry with passwords removed to be sent to your virtual machine. Before using the function, you must have a read/write minidisk accessed as your A-disk.

The format of the REVIEW function is:

| | |
|---|---|
| VMSECURE MAInt | Review |

There are no parameters.

Usage Notes:

1. The XEDIT command is automatically invoked to view the file that has been copied to your A-disk. No changes can be made to this screen.

2. The filename is your userid, the filetype is DIRECT, and the filemode is A0. This function overwrites any existing file with the same fileid.

3. To exit this XEDIT file, type FILE or QUIT after the command arrow (=====>).

Example:

Review a copy of your directory entry by entering the following:

```
vmsecure maint review
ENTER YOUR LOGON PASSWORD:
```

The following file is displayed:

```
FINANCE  DIRECT   A0 V 80      TRUNC=72  SIZE=19 LINE=0 COL=1 ALT=0
|...+....1....+....2....+....3....+....4....+....5....+....6....+...
00000 * * * TOP OF FILE * * *
00001 USER FINANCE ******** 1M 1M G 64
00002 *PW= 85/12/13 FINANCE
00003 *ED= 86/01/13 09:48:10 ACCTMGR  MANAGE   85/12/13
00004 *HS 01/24/86 10:49:27 Accepted Logon from 513
00005 *HS 01/23/86 06:18:13 Rejected Link by SNOOP to 191 (RR)
00006 *HS 01/22/86 10:01:15 Accepted Logon from 513
00007 *HS 01/21/86 10:23:18 Accepted Logon from 513
00008 *FL= *
00009 *LL= 10:49:27 EST Wednesday  01/22/86 from      5A2
00010 * Userid = FINANCE; Ext = 2048; Dept = 107; Mail Stop = 5E
00011 ACCOUNT 20000000 RECEIVE
00012 IPL CMS PARM AUTOCR
00013 OPTION ECMODE
00014 CONSOLE 009 3215
00015 SPOOL 00C 2540 READER *
00016 SPOOL 00D 2540 PUNCH A
00017 SPOOL 00E 1403
00018 LINK MAINT 190 190 RR
00019 LINK MAINT 19E 19E RR
00020 MDISK 191 3375 312 1 VMPK99 MR ********
00021 MDISK 192 3375 955 2 VMPK99 MR ********
00022 * * * END OF FILE * * *
====>
                                                X E D I T   1 FILE
```

A brief description of the special directory comments used by VMSECURE follows. For more information, see your directory manager.

***ED=** Edit statement. Records the date and time your directory entry was last updated, the userid that performed the update, and the VMSECURE subcommand that was issued. For userids created after VMSECURE Release 2.1 was installed, the userid creation time and date are listed along with the userid of the user who created the userid. For userids already existing when Release 2.1 was installed, the last subcommand issued for the userid and the time and date the userid was edited with VMSECURE Release 2.1 running are listed.

***FL=** Flag statement. Specifies the status of your logon password.

***HS=** History statement. Records successful and unsuccessful attempts to access your virtual machine and minidisks.

***LL=** Last Logon statement. Records the date, time, and terminal address for the last time your userid was logged on. The information recorded is displayed at next logon for your verification.

***PW=** Password History statement. Records the date your logon password was last changed.

## 3.15 REMOVING DIRECTORY LINKS TO YOUR VIRTUAL MACHINE

Use the RLINK function to review and optionally to remove directory links established by other users to one of your minidisks.

The format of the RLINK function is:

| | |
|---|---|
| VMSECURE MAInt | RLink vaddr |

where:

vaddr specifies the virtual device address of your minidisk.

Usage Notes:

1. For each existing directory minidisk link you are prompted with the following message:

   REMOVE 'userid vaddr' LINK?

   where "userid vaddr" is the userid who has a directory link to you at the virtual address indicated.

   Reply YES if you wish to remove the link from the userid's directory entry or NO if you wish to leave the link in place.

2. If you do not wish to be prompted for any other links that may exist, reply END.

Example:

To review but not delete other users' links to your 191 minidisk, enter the following:

```
vmsecure maint rlink 191
ENTER YOUR LOGON PASSWORD:

REPLY 'YES' OR 'NO' TO THE FOLLOWING PROMPTS.
TERMINATE PROMPTING BY REPLYING 'END'.
REMOVE 'FINANCE 205' LINK?
no
REMOVE 'ADMIN   192' LINK?
no
THERE WERE 0 LINKS REMOVED.
R;
```

## 3.16 SCRATCHING ONE OF YOUR MINIDISKS

Use the SCRATCH function to scratch one of your minidisks. When you scratch a minidisk, VMSECURE automatically formats the scratched minidisk, erasing all files and data on the minidisk. The space occupied by the formatted minidisk is returned to the pool of available disk space. Directory links to the minidisk being scratched are automatically removed from other users' directory entries.

The format of the SCRATCH function is:

| | |
|---|---|
| VMSECURE MAInt | SCratch vaddr |

where:

vaddr specifies the virtual address of the minidisk you are deleting from your directory entry.

Example:

To scratch your 242 minidisk, enter the following:

```
vmsecure maint scratch 242
ENTER YOUR LOGON PASSWORD:

SCRATCHING MINIDISK '242'.
MINIDISK ON VOLUME 'VMPK11', DEVICE TYPE '3375'.
AT LOCATION '599', SIZE '4', LABELED 'DSK194'.
MINIDISK IS 1% UTILIZED WITH 8 FILES.

DO YOU WISH TO SCRATCH THE MINIDISK?
ENTER YES OR NO:
yes
DIRECTORY UPDATED ONLINE.
R;
```

## 3.17 MODIFYING STORAGE SIZE

Use the STORAGE function to change the logon storage size of your virtual machine. This change does not take effect until the next logon session.

The format of the STORAGE function is:

```
+---------------------+-----------------------------------------------------+
|                     |                                                     |
| VMSECURE MAInt | Storage sizeK | sizeM                                    |
|                     |                                                     |
+---------------------+-----------------------------------------------------+
```

where:

*size* specifies the new logon storage size expressed in units of K (1024 bytes) or M (1024K bytes).

Usage Notes:

1. The new virtual storage size must be in multiples of 4K. The minimum size is 8K and the maximum is 16M. The last character must be K or M (1M=1024K). If the size you specify is less than 8K, the directory entry will contain the storage size you specified, but a CP QUERY VIRTUAL STORAGE command will show a storage size of 8K.

2. You cannot specify a storage size greater than the installation-specified maximum for your virtual machine. Your directory administrator must make the change to increase your storage size above the current maximum.

Example:

To increase your logon storage size to 2M, enter the following:

```
+-------------------------------------------------------------------------+
|                                                                         |
| vmsecure maint storage 2m                                               |
| ENTER YOUR LOGON PASSWORD:                                              |
|                                                                         |
| DIRECTORY UPDATED ONLINE.                                               |
| R;                                                                      |
|                                                                         |
+-------------------------------------------------------------------------+
```

## 3.18 MODIFYING LOGICAL LINE EDITING SYMBOLS

Use the TERMINAL function to change or remove the optional logical line editing symbols assigned to your virtual machine at logon time. These changes do not take effect until the next session logon.

The format of the TERMINAL function is:

| | |
|---|---|
| VMSECURE MAInt | Terminal keyword ON<br>OFF<br>char<br>hex |

where:

keyword — specifies which of the line editing symbols is being set and must be one of the following values: CHARDEL, LINEDEL, LINEND, or ESCAPE.

ON — specifies that the default line editing symbol should be used.

OFF — specifies that no line editing symbol should be used.

char — specifies the character to be used as the line editing symbol.

hex — specifies the two-digit hexadecimal value to be used as the line editing symbol.

Example:

To activate the default line delete character for your virtual machine, enter the following:

```
vmsecure maint term linedel on
ENTER YOUR LOGON PASSWORD:

DIRECTORY UPDATED ONLINE.
R;
```

# 4.0 USING THE QUERY SUBCOMMAND

The QUERY subcommand provides you with information about the following:

Account number of your userid

CP privilege class or classes of your userid.

## 4.1 QUERY SUBCOMMAND

Use the QUERY subcommand to display directory entry information about your virtual machine.

The format of the QUERY subcommand is:

| | |
|---|---|
| VMSECURE QUERY | ACcount <userid><(option())><br>Class <userid><(option())><br><br>Option:<br>STACK<FIFO\|LIFO> |

where:

ACCOUNT <userid>
: specifies that your account number, as it appears in your directory entry, is displayed.

CLASS <userid>
: specifies that your CP privilege class(es), as listed in your directory entry, is displayed.

Option:

STACK
: specifies that the query output is stacked in your program stack in FIFO or LIFO order. The default stack order is FIFO.

Usage Notes:

1. Since you can query only information about your userid, the "userid" parameter can be omitted.

2. Dynamic changes made to your account number are not reflected in the QUERY output.

Examples:

1. To query the account number listed in your directory entry, enter:

```
vmsecure query account
38104400
R;
```

2. To query your CP privilege class, enter:

```
vmsecure query class
G
R;
```

# 5.0 ENCRYPTION CAPABILITIES

VMSECURE provides a software implementation of the National Bureau of Standards (NBS) Data Encryption Standard (DES) to protect proprietary or sensitive data from accidental or intentional disclosure.

VMSECURE's encryption and decryption capabilities provide a cost-effective means of protecting valuable data. Whether this data is stored on a minidisk or tape, or transmitted across public telecommunications lines, it can be protected against theft or disclosure through the use of cryptographic techniques employed by VMSECURE.

No CMS or CP modifications are required to use any portion of VMSECURE's encryption or decryption capabilities. In addition, many existing applications programs can use VMSECURE- encrypted data without modification.

## 5.1 THE NBS DATA ENCRYPTION STANDARD

The National Bureau of Standards Data Encryption Standard (DES) is an encryption algorithm that can produce unintelligible data from normal data and later restore the data to original form. In VMSECURE, the VMCIPHER command performs encryption and decryption of files (see the chapter "VMCIPHER Command Reference" on page 75).

DES is the encryption of a 64-bit (8-byte) piece of data. This data and a cipher key are sent through the DES "black box," generating encrypted 64-bit data. The cipher key is a character string that is the basis on which the encrypted data is generated. The encrypted data, if put back through the algorithm with the same key, produces the original 64-bit data.

For more information on the methods used in the DES algorithm, refer to the Department of Commerce/NBS FIPS publication #46, Data Encryption Standard.

```
+-------------------------------------------------------------------------+
|                                                                         |
|                                  CAUTION                                |
|                                                                         |
|     Files encrypted by VMCIPHER cannot be decrypted without the         |
|                                 original                                |
|    cipher key.  If the key is lost, VMCIPHER cannot decrypt the         |
|                                  file.                                  |
|                                                                         |
+-------------------------------------------------------------------------+
```

## 5.2 ENCRYPTION AND DECRYPTION COMPONENTS

The VMSECURE cryptography provides three different components for employing DES to protect sensitive data. Each of these follows the same algorithm and is compatible with the output of the others.

The VMCIPHER command encrypts or decrypts CMS minidisk files.

The VMXDEF command allows OS simulation programs to read and write encrypted data to disk and tape with **no modifications to the existing programs.**

VMXSUBS is a set of callable subroutines provided for programmers who wish to develop their own DES applications.

## 5.3 VMCIPHER PROCESSING

VMCIPHER offers two processing modes: RECORD mode and FILE mode. In RECORD mode, the encryption of a record is based on the unciphered text (the clear text) and the cipher key. Each record is handled as a separate encryption process. Preceding records have no effect on the encryption of later records; in RECORD mode identical records of clear text produce identical enciphered records (the cipher text). RECORD mode allows the use of random file access methods (BDAM).

In FILE mode, the encryption of a record is based on the clear text, the cipher key, and the previous record's cipher text. Therefore, two identical records of clear text in the same file produce different records of cipher text. FILE mode encryption obscures the form of the data as well as its contents. Only

sequential file access methods can be used to read files encrypted in FILE mode.

Multiple encryptions in either or both modes enhance the security of any file, as does the frequent change of cipher keys.

## 6.0 VMCIPHER COMMAND REFERENCE

The VMCIPHER command is designed to perform encryption and decryption of CMS files according to the National Bureau of Standards Data Encryption Standard (DES). The VMCIPHER command is similar to the standard CMS COPYFILE command in format and operation.

The format of the VMCIPHER command is:


where:

fileid1 specifies the filename, filetype, and filemode of the input file for encryption or decryption. Pattern matching is not allowed.

fileid2 specifies the filename, filetype, and filemode of the output (CMS minidisk) file to receive the results of the encryption or decryption process. "fileid2" is optional and, if not specified, defaults to the input file ("fileid1"), destroying the original contents of "fileid1". An equal sign (=) in any field of "fileid2" indicates that it is the same as the corresponding field in "fileid1".

Options:

ENcrypt specifies that encryption is to be performed on the input file. This is the default value.

DEcrypt specifies that decryption is to be performed on the input file.

FILe specifies that encryption or decryption is to be performed in FILE mode. This is the default value.

RECord specifies that encryption or decryption is to be performed in RECORD mode.

REPlace overrides the protection of an existing CMS file with the same file identifiers as "fileid2". If not specified, an existing file cannot be altered. REPLACE is required when "fileid2" is specified and already exists on the minidisk.

Usage Notes:

1. VMCIPHER checks the console and program stacks for data. If anything other than blanks exists in either stack, that data is used as the cipher key. If both stacks are empty, the user is prompted for a cipher key that is suppressed or masked on input. The key can be any character string from 1 to 40 characters in length.

2. The cipher key is used by VMSECURE **exactly** as entered unless there is a CMS user input translation table. (See the IBM VM/SP: CMS User's Guide for further information on user input translate tables.)

3. A cipher key entered in all uppercase letters produces different output from the same key in upper and lowercase or in all lowercase.

4. Multiple encryptions can be performed on any file. To decrypt a file created by multiple encryptions, decrypt using the cipher keys in reverse order--that is, last one first.

5. **Do not lose the cipher key.** The file cannot be decrypted without it.

Examples:

1. Encrypt a file containing confidential salary data in FILE mode using the input fileid as the output fileid and the word "cash" (all lowercase) as the cipher key.

```
vmcipher salary data a
ENTER ENCRYPTION KEY FOR FILE:

R;
```

The file SALARY DATA A now contains encrypted data. To decrypt the file, enter the following:

```
vmcipher salary data a (decrypt
ENTER ENCRYPTION KEY FOR FILE:

R;
```

2. Encrypt SALARY DATA A in FILE mode using the new file GARBLED DATA A for output and the word "mixup" as the cipher key:

```
vmcipher salary data a garbled data a
ENTER ENCRYPTION KEY FOR FILE:

R;
```

To decrypt the file GARBLED DATA A enter the subcommand shown below. The result of this entry is two identical decrypted files--SALARY DATA A and GARBLED DATA A.

```
vmcipher garbled data a (de
ENTER ENCRYPTION KEY FOR FILE:

R;
```

This command puts the decrypted data into the file GARBLED DATA A.

3. Encrypt SALARY DATA A in RECORD mode and replace the old GARBLED DATA A file with the encrypted file:

```
vmcipher salary data a garbled = = (record replace
ENTER ENCRYPTION KEY FOR FILE:

R;
```

Next, decrypt the GARBLED DATA A file and replace the old SALARY DATA A with decrypted data by entering the following:

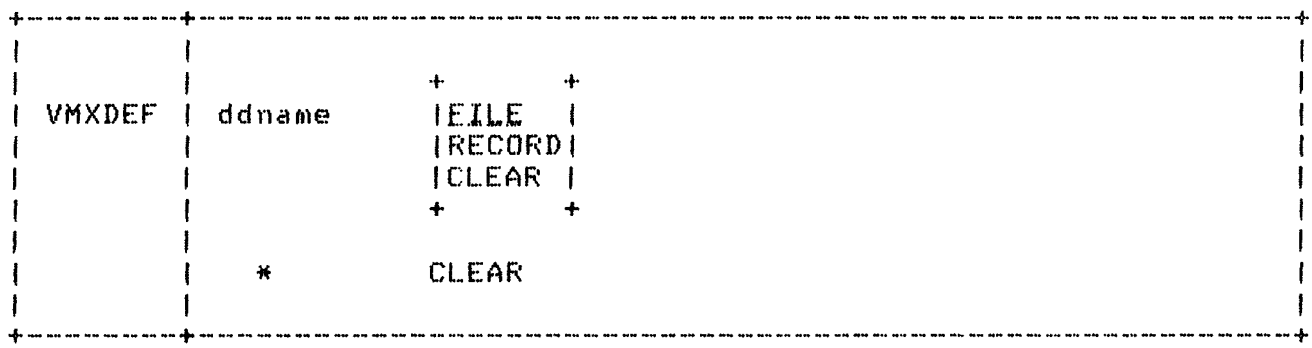
```
vmcipher garbled data a salary = = (de rec rep
ENTER ENCRYPTION KEY FOR FILE:

R;
```

## 7.0 VMXDEF COMMAND REFERENCE

The VMXDEF command allows OS simulation programs running under CMS to use VMCIPHER on their input and output files without program modification. VMXDEF does this by intercepting all input and output (I/O) and performing encryption and decryption as part of the normal I/O. There is also a VMXDEF option that removes the I/O intercepts.

After issuing the application's FILEDEFs, issue VMXDEF once for each data set (FILEDEF) to be encrypted or decrypted and then run the user program. On each read from a data set, the data is decrypted before it is passed to the user program and encrypted before being written back out.

The format of the VMXDEF command is:




where:

ddname specifies the "ddname" of the data set to be encrypted or decrypted. Specifying 'VMCIPHER' as the ddname causes an error.

FILE specifies that encryption or decryption is to be performed in FILE mode. This is the default encryption and decryption mode.

RECORD specifies that encryption or decryption is to be performed in RECORD mode.

* specifies that all ddnames are to be cleared. This operand is valid only if the CLEAR operand is also specified.

CLEAR removes the I/O intercepts. If "ddname" is specified, the I/O intercept is removed for that ddname. If an '*' is specified, all I/O intercepts are removed, all VMXDEF user storage is returned to CMS, and the VMCIPHER ddname is cleared.

Usage Notes:

1. This technique can only be used under CMS for programs that use OS simulation I/O (FILEDEF, OPEN, CLOSE, GET, PUT, etc.). It cannot be used for programs that use CMS I/O (FSREAD, FSWRITE, RDTAPE, etc.) or DOS simulation I/O (DTF, ASSIGN, etc.).

2. The FILEDEFs must be issued prior to using the VMXDEF command.

3. Before issuing the VMXDEF command, make sure a GLOBAL is run on the VMCIPHER text library by issuing the following command:

   GLOBAL TXTLIB VMCIPHER

4. The operand keywords cannot be abbreviated.

5. VMXDEF issues a dummy FILEDEF for the ddname VMCIPHER during its operation.

6. VMXDEF supports I/O to the following devices: DUMMY, TAPE, and DISK. Any other device causes a user abend.

Examples:

1. Issue FILEDEFs for the newly encrypted (in FILE mode) minidisk file and the standard output file for the salary update program. Next issue VMXDEF for the encrypted input file giving the cipher key SECURE. This enables the salary update program to read the encrypted data. The program output is not encrypted. After issuing the FILEDEFs and running VMXDEF, run the program. These steps are outlined in the following example:

```
filedef 5 disk salary data a
R;

filedef 6 disk update output a
R;

vmxdef 5 file
ENTER ENCRYPTION KEY FOR 'FT05F001' ID:
secure
R;

load salupdat (clear start)
R;
```

2. Have a billing program read a newly encrypted (in RECORD mode) data file and write encrypted output to the file ENBILL DATA A1. First issue the FILEDEFs, then run VMXDEF twice, once for each encrypted file used. The cipher key is MONEY. After running the billing program, clear all intercepts using the '* CLEAR' parameters. These steps are outlined in the following example:

```
filedef 5 disk billing data a
R;

filedef 6 disk enbill data a
R;

vmxdef 5 record
ENTER ENCRYPTION KEY FOR 'FT05F001' ID:
money
R;

vmxdef 6 record
ENTER ENCRYPTION KEY FOR 'FT06F001' ID:
money
R;

load billing (clear start)
R;

vmxdef * clear
R;
```

# 8.0 VMXSUBS SUBROUTINES

The VMXSUBS subroutines are used to encrypt or decrypt blocks of data using the National Bureau of Standards Data Encryption Standard (DES) algorithm. The subroutines are as follows:

**VMXCRYPT** encrypts and decrypts blocks of data in FILE or RECORD mode.

**VMXKINIT** initializes the cipher key used for data encryption and decryption.

**VMXKREAD** reads in the cipher key from the console.

These subroutines are designed for CMS and OS application programmers who wish to do encryption within their programs. For security, this package includes a CMS subroutine to read the cipher key from the console and masks or suppresses the display. All subroutines are written in assembler and use standard OS subroutine linkage. Programmers using assembler should call these routines using the OS CALL macro with the VL option.

The subroutines can be used to encrypt different portions of a data record using different keys. Thus, users can access data fields based on the cipher key.

Usage Notes:

1. These subroutines reside in the VMCIPHER text library. A GLOBAL must be run on the text library before loading the user program. Issue the following command:

   ```
   GLOBAL TXTLIB VMCIPHER
   ```

2. All subroutines have a six-byte synonym to allow valid FORTRAN calling sequences.

## 8.1 VMXCRYPT SUBROUTINE

The VMXCRYPT subroutine encrypts and decrypts blocks of data in either FILE or RECORD mode. See the section "VMCIPHER Processing" on page 72 for an explanation of FILE and RECORD modes.

The format of the VMXCRYPT subroutine is:

```
CALL VMXCRYPT (id,buffer,length,type)
```

where:

id — specifies the unique doubleword identifier of the data set being processed. This parameter corresponds to the "id" passed to the VMXKINIT routine and determines which cipher key is used. If VMXKINIT has not been called to initialize the key for the ID, a user abend occurs. The "id" X'FFFFFFFF' is reserved; if used, it causes a user abend.

buffer — specifies the area in memory containing the text to be encrypted or decrypted.

length — specifies a fullword containing the number of bytes in "buffer" to encrypt or decrypt.

type — specifies a fullword of characters describing the operation to be performed. If the type passed is invalid, a user abend occurs. Valid entries are as follows:

| | |
|---|---|
| ENFM | Encrypt in FILE mode |
| DEFM | Decrypt in FILE mode |
| ENRM | Encrypt in RECORD mode |
| DERM | Decrypt in RECORD mode |

Usage Note:

For FORTRAN compatibility, use the six-byte synonym VMXCRY.

## 8.2 VMXKINIT SUBROUTINE

The VMXKINIT subroutine initializes the cipher key used for data encryption and decryption. VMXKINIT must be called at least once for each file to be encrypted or decrypted. Subsequent calls with the same fileid reinitialize the cipher key associated with that fileid.

The format of the VMXKINIT subroutine is:

```
CALL VMXKINIT (id,key)
```

where:

id — specifies the unique doubleword identifier of the data set associated with this key. This doubleword can be any binary value, but the ddname is recommended. This allows for handling of multiple data sets with different cipher keys. The "id" X'FFFFFFFF' is reserved; if used, it causes a user abend.

key — specifies a 40-character field containing the cipher key. The key is not modified by this subroutine.

Usage Note:

For FORTRAN compatibility, use the six-byte synonym VMXKIN.

## 8.3 VMXKREAD SUBROUTINE

The VMXKREAD subroutine reads in the cipher key from the console. If there is an entry in either the console stack or the program stack, the key is read from the stack. If there are no stacked lines and there is a valid real terminal, the console is prompted for a password with masking or suppression depending on the type of terminal. If no cipher key or a cipher key of blanks is entered, the read process is repeated.

The format of the VMXKREAD subroutine is:

```
+-------------------------------------------------------------------------------+
|                                                                               |
| CALL VMXKREAD (id,key)                                                        |
|                                                                               |
+-------------------------------------------------------------------------------+
```

where:

id — specifies the unique doubleword identifier of the data set associated with the password to be read. This doubleword can be any binary value, but the ddname is recommended. This allows for handling of multiple data sets with different cipher keys. This "id" is displayed as part of the cipher key prompting message. The "id" X'FFFFFFFF' is reserved; if used, it causes a user abend.

key — specifies a 40-character field that is filled in with the cipher key by VMXKREAD from console input and padded with blanks. The key is translated using the existing CMS input translate table.

Usage Note:

For FORTRAN compatibility, use the six-byte synonym VMXKRE.

## 8.4 USING VMXSUBS SUBROUTINE CALLS IN FORTRAN PROGRAMS

The following is an example of a FORTRAN program using the VMXSUBS subroutines to read clear text data and encrypt it in FILE mode to an output file:

```
      INTEGER KEYBUF(10),BUFFER(20),TYPE(1),LENGTH
      REAL*8 ID
C
      DATA ID/'VMTEST  '/
      DATA TYPE/'ENFM'/
      DATA LENGTH/80/
C
      CALL VMXKRE(ID,KEY)
      CALL VMXKIN(ID,KEY)
C
10    READ(5,200,END=20) BUFFER
      CALL VMXCRY(ID,BUFFER,LENGTH,TYPE)
      WRITE(4,200) BUFFER
      GOTO 10
20    STOP
C
200   FORMAT(20A4)
      END
```

Figure 13. Example Using VMXSUBS in a FORTRAN Program

The program calls VMXKREAD to read the cipher key and calls VMXKINIT to initialize the key buffer with the input cipher key before the encryption process begins. After reading a buffer of text, VMXCRYPT is called to encrypt the data in FILE mode (ENFM). Changing the definition of the variable TYPE in the DATA statement changes the mode or allows the same program to decrypt data.

After encryption, the buffer is written to a new file.

## 8.5 USING VMXSUBS SUBROUTINE CALLS IN ASSEMBLER PROGRAMS

The following is an example of the assembler language statements necessary to use the VMXSUBS subroutines. In this example, the encryption key is read from the terminal and is used to encrypt a 200-character buffer in FILE mode. The CALL instruction is the standard OS CALL macro. Note that this is not a complete program.

```
                .
                .
                .
         CALL   VMXKREAD,(ID,KEY),VL      READ KEY FROM THE TERMINAL
         CALL   VMXKINIT,(ID,KEY),VL      INIT KEY WITH OUR ID
*
         CALL   VMXCRYPT,(ID,BUFFER,LENGTH,TYPE),VL    ENCRYPT THE|D
*
                .
                .
ID       DC     CL8'VMTEST'          ENCRYPTION ID
KEYBUF   DS     CL40                 ENCRYPTION KEY
TYPE     DC     CL4'ENFM'            SELECT ENCRYPTION IN FILE MODE
LENGTH   DC     F'200'               LENGTH OF BUFFER
BUFFER   DS     CL200                DATA BUFFER TO ENCRYPT
                .
                .
```

Figure 14. Example Using VMXSUBS in an Assembler Program

# 9.0 USING THE CMS HELP FACILITY

## 9.1 HELP COMMAND

The CMS HELP command provides information on the VMSECURE user subcommands and system messages. The information presented by the HELP files is the same text as the documentation provided in this book, the VMSECURE Rules Facility Guide, and VMSECURE Messages and Codes.

## 9.2 VIEWING THE VMSECURE HELP MENU

To display the contents of the VMSECURE HELP menu, enter the following CMS command:

```
help vmsecure
```

## 9.3 HELP AND VMSECURE USER SUBCOMMANDS

It is possible to bypass the menus entirely and go directly to the information on the specific topic in which you are interested.

For the description of a particular VMSECURE subcommand, enter:

```
help vmsecure subcmd
```

where "subcmd" is the subcommand you wish to see. Help information is available for the following subcommands:

```
GROUP
HISTORY
MAINT
MANAGE
RULEMAP
RULES
USER
```

## 9.4 HELP AND VMSECURE SYSTEM MESSAGES

HELP files describing VMSECURE system messages can be viewed by issuing a HELP command line and specifying the desired system message number.

For example, to get a description of a particular VMSECURE system message, enter:

```
help vmxnnnc
```

where "vmxnnnc" is a system message identifier consisting of the letters 'vmx', the three digit message number (including leading zeros), and the one letter severity code.

For example:

```
help vmx106i
```

provides information on message VMX106I.

Additional details on using the HELP facility can be found in the IBM VM/SP: CMS User's Guide, SC19-6210.

# GLOSSARY

**Cipher Key**: A character string used by VMSECURE when encrypting and decrypting data.

**Cipher Text**: Unintelligible, encrypted data.

**Clear Text**: Readable, non-encrypted data.

**Configuration File**: A file maintained by the VMSECURE system administrator that indicates certain system defaults and authorizations.

**DASD**: Direct access storage device or disk used for storage of users' files.

**Decrypt**: To restore encrypted data to its original, readable form.

**Default**: The value supplied by VMSECURE if one is not entered by the user.

**Directory**: A file that defines each virtual machine's configuration. Userid, virtual storage, and password are defined in the directory.

**Directory Administrator**: A user with ADMIN authorization in the VMSECURE configuration file who can modify the directory entries of all the userids at the site.

**Directory Entry**: A group of statements in the directory that define a particular virtual machine.

**Directory Manager**: A user with MANAGE authorization in the VMSECURE configuration file who can modify the directory entries of the userids in his security group.

**Directory Statements**: Special purpose statements that define virtual machine attributes (such as userid and password) and configuration (such as unit record devices and minidisks).

**Encrypt**: The process of converting clear text into cipher text.

**Field**: An area on a selection screen in which you can enter data.

**HELP Facility**: A CMS facility that allows users to obtain online information about commands, subcommands, and system messages, including those for VMSECURE.

**Menu**: A screen display that lists VMSECURE functions available to the user.

**Password Encryption Facility**: An optional VMSECURE feature that allows a site to encrypt logon and link passwords and maintain them in an encrypted form in the online directory and in the VMSECURE directory database.

**Product Interface**: A feature of VMSECURE that allows other VM Software, Inc. products to use the Rules facility to enhance their data security.

**Rule**: In VMSECURE, a rule put into a rules file to control access to virtual machines and minidisks and to control the transfer of data. The rule specifies the action to be taken, the userid making the request, and the command or subcommand affecting the request.

**Rules Database**: Installation-defined rules that control access to virtual machines and minidisks and the transfer of data between virtual machines.

**Rules Facility**: Files residing on the VMSECURE rules minidisk that allow an installation to control access to virtual machines and minidisks and the transfer of data.

**Rules File**: A file of rule statements created by users, security group managers, and security administrators to control access to virtual machines and minidisks and the transfer of data. These files reside on the Rules minidisk of VMSECURE. Rules created at the system level override all other rules. Rules created by security group managers override the rules of users in their respective security groups.

***Scratch***: When a disk is scratched, all data is erased and the disk space is reformatted. The disk space is then added back to the available space for reallocation.

***Service Virtual Machine***: A virtual machine running a program that provides system-wide services.

***System Administrator***: A user with all levels of authorization in the VMSECURE configuration file who is designated by the site to administer all directories at the site. May also be the security administrator.

**User Exit**: Same as "exit routine." A point in the operation of VMSECURE at which a user-written routine can be given control.

**Vaddr**: Virtual device address.

**Virtual Machine**: A functional simulation of a computer and its associated devices.

**VMACCOUNT**: An accounting, reporting, and capacity management system, available from VM Software, Inc.

**VMBACKUP**: A minidisk dump and restore system, available from VM Software, Inc.

**VMCIPHER**: A command that allows users to encrypt and decrypt data in CMS files.

**VMSCHEDULE**: A scheduling system designed for the CMS environment, available from VM Software, Inc.

**VMTAPE**: A system for managing any number of tape volumes and tape drives, available from VM Software, Inc.

## Special Characters



## A



## C



## D

+---+
| N |
+---+



+---+
| O |
+---+



+---+
| P |
+---+



+---+
| Q |
+---+



+---+
| R |
+---+



+---+
| S |
+---+

I



U



V

## READER'S COMMEN

Your views about this publication can help improve its usefulness. P
help us by filling out and returning this form. If you include your
and address, we will respond.

Please return this sheet to

VM Software, Inc.
Technical Publications
2070 Chain Bridge Road
Suite 355
Vienna, VA 22180

Did you find errors or misleading information in this book? If so, sp
by page.

Did you find any part(s) of the book hard to understand? If so, which
part(s) and how can we improve them?

Is the documentation complete on all facets of the system? If not, wh
material is missing and where should it be placed?

How can we change this book to make it more useful to you? (If you ne
more room, please write on the back.)