

VMS SES
Installation Guide and
Release Notes
Version 5.3-1

Order Number: QS-970AA-IG

June 1990

This manual describes installation and upgrade procedures, new and changed features, problems and restrictions, and documentation notes for Version 5.3-1 of the VMS Security Enhancement Service.

Revision/Update Information: This manual supersedes the previous version, Version 5.2, of the *VMS SES Installation Guide and Release Notes*.

Operating System and Version: VMS Version 5.3-1

Software Version: SEVMS Version 5.3-1

June 1990

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation.

Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

Any software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license. No responsibility is assumed for the use or reliability of software or equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Restricted Rights: Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

© Digital Equipment Corporation 1990. All rights reserved.

Printed in U.S.A.

The Reader's Comments form at the end of this document requests your critical evaluation to assist in preparing future documentation.

The following are trademarks of Digital Equipment Corporation:

DEC	DIBOL	UNIBUS
DEC/CMS	EduSystem	VAX
DEC/MMS	IAS	VAXcluster
DECnet	MASSBUS	VMS
DECsystem-10	PDP	VT
DECSYSTEM-20	PDT	
DECUS	RSTS	
DECwriter	RSX	

This document was prepared with VAX DOCUMENT, Version 1.2.

Contents

PREFACE

v

Part I INSTALLATION GUIDE

CHAPTER 1 INSTALLATION INSTRUCTIONS 1-1

1.1 INTRODUCTION 1-1

1.2 REMOVING SEVMS VERSION 5.2 1-2

1.3 INSTALLING VMS VERSION 5.3-1 1-2

1.4 INSTALLING SEVMS VERSION 5.3-1 1-3

1.5 TYPICAL INSTALLATION PROCEDURE 1-5

1.5.1 Note about SEVMS Audit Server Database 1-7

CHAPTER 2 INSTALLATION FILES 2-1

2.1 REPLACEMENT FILES 2-1

2.2 COMMAND DEFINITION FILES 2-3

2.3 SEVMS FILES 2-4

2.4 OBSOLETE FILES 2-5

CHAPTER 3 PROBLEM REPORTS	3-1
----------------------------------	------------

Part II RELEASE NOTES

CHAPTER 4 NEW AND CHANGED FEATURES	4-1
---	------------

4.1	FILE CLASSIFICATION NOT DISPLAYED FOR DIRECTORY COMMAND ACROSS NETWORK	4-1
4.2	SYMBOLIC DEFINITION FILES FOR LANGUAGES AVAILABLE	4-1
4.3	CHANGE TO FILE NAME — SEVMS_SMB.EXE BECOMES SEVMS\$SMB.EXE	4-1
4.4	CHANGE TO RECOMMENDED PRIVILEGES FOR MAIL ACCOUNTS	4-2
4.5	NEW FUNCTIONALITY — CLASSIFICATION OF LOCAL INTERACTIVE TERMINALS	4-2
4.5.1	Definition of Local Interactive Terminals	4-2
4.5.2	Classification of Logins to Local Interactive Terminals	4-2
4.5.2.1	SET CLASS/TERMINAL • 4-3	
4.5.2.2	SHOW CLASS/TERMINAL • 4-4	
4.6	RECLASSIFICATION OF TERMINALS DURING INTERACTIVE USE	4-5
4.7	NEW DCL COMMANDS IMPLEMENTED TO SET AND SHOW CLASSIFICATIONS ASSOCIATED WITH TERMINALS	4-5
4.8	NEW QUALIFIER ADDED TO SET CLASS COMMANDS — /REMOVE	4-6
4.9	CHANGES TO ANALYZE/AUDIT COMMAND	4-6
4.9.1	New Qualifier — /FACILITY=SEVMS	4-6
4.9.2	New Keywords for /EVENT_TYPE Qualifier	4-6
4.9.3	New Keywords for /SELECT Qualifier	4-8

4.10	PARTIAL WILDCARDING (*) SUPPORT ADDED FOR SHOW CLASS COMMAND	4-8
------	---	-----

CHAPTER 5	PROBLEMS AND RESTRICTIONS	5-1
------------------	----------------------------------	------------

5.1	INSTALLATION PROCEDURE NOTE	5-1
5.2	MAILING DOWN TO PRIVILEGED ACCOUNTS	5-1
5.3	DISCONNECT TERMINAL CHARACTERISTIC NOT FULLY SUPPORTED	5-1
5.4	SYSTEM DISK CLASSIFICATION RESTRICTION	5-2
5.5	STORAGE LIBRARY SYSTEM (SLS) — NOTE FOR USE WITH SEVMS	5-2

CHAPTER 6	PROBLEMS RESOLVED	6-1
------------------	--------------------------	------------

6.1	MAIL — PROBLEMS RESOLVED	6-1
6.2	SET AUDIT — PROBLEMS RESOLVED	6-1
6.3	CAPTIVE ACCOUNT/LOGINOUT PROBLEM RESOLVED	6-2
6.4	ANALYZE/AUDIT COMMAND — /EVENT_TYPE=PRINT FUNCTIONALITY RESTORED	6-2
6.5	CLASSIFICATION OF TEMPLATE DEVICE	6-2
6.6	RMS CHANNEL UNAVAILABLE	6-3
6.7	\$CREPRC RETURNS BADPARAM ERROR	6-3

Contents

6.8	SEVMS LAT PRINT SYMBIONT — DEFINE/FORM/LENGTH SUPPORT	6-3
-----	---	-----

6.9	SHOW CLASS/NODE COMMAND — WILDCARD (*) PROBLEM RESOLVED	6-3
-----	---	-----

INDEX

FIGURES

1-1	Typical SEVMS Version 5.3-1 Installation Procedure	1-5
-----	--	-----

Preface

This document describes installation and upgrade procedures, new and changed features, problems and restrictions, and documentation notes for the VMS Security Enhancement Service.

The VMS Security Enhancement Service (VMS SES) is a software security consulting package. It provides many features of mandatory access controls and security auditing for the VMS operating system.

The VMS SES software security consulting package is composed of the following components:

- Services performed by a DIGITAL consultant
- Licensed software
- Documentation

VMS SES provides the services of a trained DIGITAL consultant who supports the customer in several areas, such as: assisting in planning security policies and controls, training users, and installing the licensed software.

The licensed software component of this product is called SEVMS. SEVMS provides a tool set for devising a system-wide security policy to help safeguard users, data, and software from security threats. Since this manual describes the features of the licensed software, the term SEVMS is used throughout this manual to reference this software. SEVMS is also the VMS facility name for the licensed software and is used as a prefix for many of the software components.

A documentation set which describes the SEVMS software and how it is installed, used, and managed is provided with the VMS SES package.

Intended Audience

This manual is intended for installers and security managers of the SEVMS (Security Enhanced VMS) system. It is assumed that users of this manual have a working knowledge of VMS and basic system management experience.

Document Structure

The information in this manual is divided into the following chapters:

- **Installation Notes** — This chapter describes the procedure for installing SEVMS, lists the files provided by the installation, and outlines the procedure for reporting problems.
- **Release Notes** — This chapter describes new and changed features, problems and restrictions, and documentation notes for SEVMS.

Associated Documents

This manual should be used in conjunction with the other manuals of the SES document set and the manuals of the VMS document set. References will be made throughout this manual to VMS SES manuals and VMS manuals.

SES Document Set

This manual is one of three manuals that form the VMS Security Enhancement Service (SES) document set. This document set consists of the following manuals:

- *VMS SES User's Guide* — This manual describes the mandatory protection mechanisms provided by the SEVMS software, the interaction of these mechanisms with VMS discretionary protection mechanisms, and the use of commands and utilities which are unique to SEVMS. It is intended for all SEVMS users.
- *VMS SES Security Manager's Guide* — This manual describes the configuration, management, and operation of SEVMS. It is intended for use by system administrators and security officers. This manual assumes that the reader is familiar with basic VMS security practices and the VMS documentation which describes VMS security.
- *VMS SES Installation Guide and Release Notes* — This manual is intended as a supplemental manual of the SES documentation set. It provides information concerning the installation (but not configuration) of SEVMS on a VMS system. It also contains release notes which summarize omitted features, resolved problems, new features, and known problems and restrictions for the current release of the SEVMS software.

Together, these manuals form complete documentation about SEVMS. For information about related VMS features and functions, the user should refer to the manuals of the VMS document set.

VMS Documentation Set

The VMS documentation set has two main divisions:

- VMS Base Documentation Set
- VMS Extended Documentation Set

The VMS Base Documentation Set is a desk-top set for users of small standalone systems and low-end Local Area VAXclusters, and for general users of large VAX systems. The Base Documentation Set contains concise, easy to find, information about performing day-to-day tasks.

This documentation set contains the following components:

- Overview of VMS Documentation
- VMS New Features Manual
- VMS General User's Manual
- VMS System Manager's Manual

- VMS Mini-Reference Manual
- VMS License Management Manual

The VMS Extended Documentation Set is a full documentation set for users who need more detail about any VMS component to perform daily tasks. The Extended Documentation Set also meets the needs of system managers of large VAX systems and of system and application programmers.

This documentation set contains the following components:

- General User Subkit
- System Management Subkit
- Programming Subkit

These manuals are supplemented by several other forms of VMS documentation: Release Notes, Obsolete Features Kit, Software Installation and Operations Guides, online help information, and other optional documentation.

Refer to the *Overview of VMS Documentation* booklet in the VMS documentation set for complete information about the VMS documentation set.

Relationship Between VMS and SEVMS Documentation

The documentation for SEVMS is intended to be used along with the documentation for VMS. While the SES documentation set addresses issues specific to the SEVMS product, issues of a more general nature pertaining to VMS are addressed in the VMS documentation set. Therefore, you can consider the manuals of the SES document set to be an extension of your existing VMS document set. As such, SES manuals do not repeat information already contained in existing VMS documentation. Instead, references are made throughout SES manuals to several of the manuals in the VMS document set, when appropriate. The following VMS documentation is most frequently referenced by the SES manuals:

- *VMS System Management Subkit*
- *Guide to VMS System Security*
- *VMS DCL Dictionary*
- *VMS Release Notes*
- *VMS Audit Analysis Utility Manual*

Conventions

This section describes the VMS and SEVMS conventions which are used in this manual.

VMS Conventions Used In This Manual

Throughout this manual, the following standard conventions are used in examples of commands:

Convention	Meaning
[]	Square brackets indicate that the enclosed item is optional.
{ }	Braces enclose a list from which one element must be chosen.
<>	Angle brackets indicate that item is to be replaced by a specific instance of the named quantity.
	The OR symbol separates alternatives within braces or brackets.
...	An ellipsis indicates that the preceding item(s) can be repeated one or more times.
:=	A "colon equals" indicates the item to its left is defined as the item to its right.

Unless otherwise indicated in the examples, commands are terminated by pressing the `Return` key.

Colons (:) and equals signs (=) are used interchangeably in descriptions of DCL command qualifiers.

SEVMS Conventions Used In This Manual

SEVMS mandatory access controls introduce a number of new protection attributes and relationships. Among these are the concepts of hierarchical *levels* and non-hierarchical *categories*. Categories form discrete mathematical *sets*.

The *operators* used to indicate the relationship between numeric quantities (*scalar*) differ from the operators used to indicate the relationship between non-numeric quantities (*sets*), although their meanings are similar. The operators used in this manual are described and compared in the following table.

Operator	Scalar Interpretation for Security Levels	Operator	Set Interpretation for Security Categories
<	is less than	⊂	is a proper subset of
≤	is less than or equal	⊆	is a subset of
=	is equal to	≡	is identical to
>	is greater than	⊃	is a proper superset of
≥	is greater than or equal	⊇	is a superset of
≠	is not equal to	≠	is not identical to

In informal discussions of the relationship between two classifications, the scalar relationships may be used to refer to both the scalar (level) and set (categories) portions of the classification. For instance, the informal statement "A's classification is equal to B's" means "A's level = B's level AND A's categories ≡ B's categories".

Dominates describes a relationship between two classifications. "A's classification dominates B's" means "A's level \geq B's level AND A's categories \supseteq B's categories".

Part I Installation Guide

This part of the manual describes the installation of SEVMS. It contains the following sections:

- Instructions for installing SEVMS Version 5.3-1.
- A detailed list of the files provided by the installation.
- Information needed by DIGITAL when you report software problems.

1

Installation Instructions

This section tells you how to install SEVMS Version 5.3-1. It is intended for a reader who has system management experience.

1.1 Introduction

SEVMS Version 5.3-1 installs as an upgrade to VMS Version 5.3-1. Therefore, you must first be sure that VMS Version 5.3-1 is installed on your system before attempting to install SEVMS Version 5.3-1. Once you are assured that your system is running VMS Version 5.3-1, you can proceed with the installation of SEVMS Version 5.3-1 as detailed in this chapter.

Caution: During the entire installation procedure, there should be no other user activity on your system. In particular, when SEVMS is not running, classifications are not checked or enforced.

- If you are installing SEVMS on your system for the first time, you must do the following things:
 - 1 Install, or upgrade your system to, VMS Version 5.3-1.
 - 2 Install SEVMS Version 5.3-1.
- If your system is presently running a version of SEVMS, you must do the following things:
 - 1 **Either** restore your system to VMS and then *upgrade* it to VMS Version 5.3-1 – **Or** *install* VMS Version 5.3-1.
 - 2 Install SEVMS Version 5.3-1.

Instructions for removing SEVMS Version 5.2 to restore your system to VMS Version 5.2 are contained in this chapter in Section 1.2.

For complete instructions on updating from VMS Version 5.2 to VMS Version 5.3-1, refer to the appropriate installation and operations guides which were supplied with your media kit, the *VMS Release Notes* and the *VMS System Management Subkit—Setup Volume*.

Instructions for installing SEVMS Version 5.3-1 are contained in this chapter in Section 1.4.

Summary:

- **Your system must be running VMS Version 5.3-1 prior to installation of SEVMS Version 5.3-1.**
- **If you are going to install SEVMS Version 5.3-1 on a cluster, all nodes should be running VMS Version 5.3-1. Rolling upgrades to SEVMS Version 5.3-1 are NOT recommended.**

Installation Instructions

- **There should be no user activity on the system during the installation procedure.**

1.2 Removing SEVMS Version 5.2

This section contains information for SEVMS customers who are currently running SEVMS Version 5.2.

In preparation for the successful installation of VMS Version 5.3-1 and SEVMS Version 5.3-1, customers who are running SEVMS Version 5.2 must first restore their system to VMS Version 5.2 by removing SEVMS.

To accomplish this, you must restore the VMS Version 5.2 files that were replaced by SEVMS Version 5.2 files when SEVMS was installed. This can be done by invoking the command procedure SEVMS\$RESTORE_VMS.COM, which is located by default in the SYS\$SYSROOT:[SEVMS\$SAVED] directory.

Note: Before removing SEVMS Version 5.2 you may wish to note security auditing information such as the file name of the log file and the resource wait mode because you will need to reset auditing characteristics when Version 5.3-1 is installed. See Section 1.5.1 for more information.

The SEVMS\$RESTORE_VMS.COM command procedure contains a record of all VMS images which are replaced by SEVMS images when SEVMS is installed. Running this command procedure restores the VMS images which were previously saved during the SEVMS installation. This command procedure was supplied when SEVMS Version 5.2 was installed.

Restoring VMS Version 5.2

To restore the VMS Version 5.2 files, proceed as follows:

- 1 Log into the system manager's account.
- 2 Invoke the SEVMS\$RESTORE_VMS command procedure, which is located in SYS\$SYSROOT:[SEVMS\$SAVED]. This procedure provides user prompts. Follow the instructions given in these prompts.

This command procedure automatically restores the VMS system images to their appropriate system directories.

At the end of this procedure, your system is restored to VMS Version 5.2.

1.3 Installing VMS Version 5.3-1

After restoring your system to VMS Version 5.2, you are now ready to upgrade your system to VMS Version 5.3-1.

For complete instructions on updating from VMS Version 5.2 to VMS Version 5.3-1, refer to the appropriate installation and operations guide which you received with your media kit, the *VMS Release Notes* and the *VMS System Management Subkit—Setup Volume*.

After you have upgraded your system, proceed to Section 1.4 for information about installing SEVMS Version 5.3-1.

1.4 Installing SEVMS Version 5.3-1

This section contains information to guide you through the installation of SEVMS Version 5.3-1.

To prepare for the installation and for further details regarding installation and related activities, please refer to the previous sections of this chapter and the *VMS SES Security Manager's Guide*.

Pre-Installation Notes

Please note the following information before beginning to install SEVMS:

- To *install* SEVMS, a minimum of **12,000 free blocks** is required on the system disk.
- To *run* SEVMS, a minimum of **9500 free blocks** is required on the system disk.

Installation Procedure

To install SEVMS, perform the following steps:

- 1 Back up your system disk. Refer to the following manuals of the "VMS System Management Subkit" for information about this procedure: *Guide to Maintaining a VMS System*, *VMS Backup Utility Manual*, and *Guide to VMS System Security*.

- 2 Install the SEVMS product kit with VMSINSTAL.

To install the kit, do the following:

- a. Log in to the system manager account (SYSTEM).
- b. Invoke the VMSINSTAL procedure—specifying the product name /version and the location of the distribution media.

This procedure provides user prompts. Follow the instructions given in the user prompts.

An example installation session is shown in Figure 1-1, in Section 1.5. Refer to this example as you install the product kit.

- 3 Set the SYSGEN parameter CLASS_PROT to 1. This enables mandatory control checks (after the system is rebooted.)

An example of setting CLASS_PROT follows:

```
$ MCR SYSGEN
SYSGEN> USE CURRENT
SYSGEN> SET CLASS_PROT 1
SYSGEN> WRITE CURRENT
SYSGEN> EXIT
```

CLASS_PROT should also be set to 1 in MODPARAMS.DAT so that AUTOGEN will maintain its value. See the *VMS System Management Subkit* for more information about AUTOGEN.

- 4 Add the following line to the *beginning* of your SYSTARTUP_V5.COM (system startup) command file (it is important that this line be placed as the first line of the file):

```
$(SYS$STARTUP:SEVMS$STARTUP.COM
```

Installation Instructions

- 5 Reboot the system after the installation is completed. **The system must be rebooted before the SEVMS software can be used.**
- 6 Update any alternate copies of DCLTABLES.EXE.

The installation procedure only updates the first DCLTABLES.EXE it encounters when looking for SYS\$SYSROOT:[SYSLIB]DCLTABLES.EXE. If there are other command tables in other directories or other directory roots (e.g. [SYSn], or [SYSn.SYSCOMMON], etc.), the installation procedure does not update them.

To update other copies of DCLTABLES.EXE, issue the following commands after the installation procedure is complete:

```
$ BACKUP/SELECT=(INIT.CLD,SET.CLD,SHOW.CLD,AUDIT.CLD,RUN.CLD) -  
    ddcu:SEVMS531.A/SAVE SET []  
$ SET COMMAND/TABLE=dcltable/OUTPUT=dcltable/ INIT.CLD,SET.CLD, -  
    SHOW.CLD,AUDIT.CLD,RUN.CLD
```

- *ddcu*: is the device the SEVMS distribution media is mounted on.
- *dcltable* is the full file specification of the command table to be updated.

- 7 Rebuild the stand-alone BACKUP kit.

Because the SEVMS kit contains updated BACKUP.EXE and STABACKUP.EXE images, you must re-build your stand-alone kit in order to use the updated version of stand-alone BACKUP.

For details on how to build a stand-alone BACKUP kit, refer to the *VMS Backup Utility Manual* in the "VMS System Management Subkit".

- 8 Back up and restore your system disk if you wish to be able to classify the system disk or any files on the system disk. Refer to the *Guide to Maintaining a VMS System*, *VMS Backup Utility Manual*, and *Guide to VMS System Security* for information about this procedure. Also, refer to the "Protecting Volumes" section of the *VMS SES Security Manager's Guide* for further information about backing up and restoring your system disk.
- 9 Refer to the *VMS SES Security Manager's Guide* for information about post-installation tasks that must be performed before labelled protection is fully enabled.

POST-INSTALLATION NOTE: Due to a bug in VMSINSTAL.COM, the SEVMS installation procedure is unable to set the appropriate file protection on the following files:

```
SYS$COMMON: [SYSLIB]SEVMS$SMB_HDRFRM.DAT  
SYS$COMMON: [SYSLIB]SEVMS$SMB_LIB.TLB
```

After the SEVMS installation is complete, please enter the following commands to change the protection and ownership of these two files:

```
$ SET FILE/OWNER=[1,4]/PROTECTION=(SYSTEM:RWE,OWNER,GROUP,WORLD) -  
    _$ SYS$COMMON: [SYSLIB]SEVMS$SMB_HDRFRM.DAT  
$ SET FILE/OWNER=[1,4]/PROTECTION=(SYSTEM:RWE,OWNER,GROUP,WORLD) -  
    _$ SYS$COMMON: [SYSLIB]SEVMS$SMB_LIB.TLB
```

This problem will be fixed in a future release of VMS.

Note: Since this kit replaces several base VMS components (detailed in Section 1.5), installing VMS Version 5.3-1 or RMS Journaling, after installing SEVMS, will negate the SEVMS installation.

1.5 Typical Installation Procedure

This section contains the output of a typical SEVMS Version 5.3-1 installation. It is provided only as an **example** of an installation. In a specific installation, details may vary.

Figure 1-1 Typical SEVMS Version 5.3-1 Installation Procedure

```

$ @SYSSUPDATE:VMSINSTAL SEVMS531 MUA0:

VMS Software Product Installation Procedure V5.3-1
It is 24-OCT-1989 at 12:07.
Enter a question mark (?) at any time for help.
* Are you satisfied with the backup of your system disk [YES]?

The following products will be processed:
    SEVMS V53.1
        Beginning installation of SEVMS V53.1 at 12:09
%VMSINSTAL-I-RESTORE, Restoring product saveset A...
%VMSINSTAL-I-REMOVED, The product's release notes have been successfully moved to SYSSHELP.
%SEVMS-I-KITINFO, Installation kit version V53.1

+-----+
! This installation will copy any standard VMS system files it replaces      !
! into the [SEVMS$SAVED] directory, if they aren't already there. This      !
! allows them to be restored, at a later date, to apply VMS updates.        !
+-----+

Would you like to continue [YES]?

%VMSINSTAL-I-SYSDIR, This product creates system disk directory VMI$ROOT:[SEVMS$SAVED].
%VMSINSTAL-I-SYSDIR, This product creates system disk directory VMI$ROOT:[SYSS$STARTUP]/PROTECTION=(GR,WO).
%CREATE-I-EXISTS, VMI$ROOT:[SYSS$STARTUP] already exists

%COPY-S-COPIED, VMI$ROOT:[SYSEXE]AUTHORIZE.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]AUTHORIZE.EXE;25 (159 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]DIRECTORY.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]DIRECTORY.EXE;25 (94 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]BACKUP.EXE;26 copied to VMI$ROOT:[SEVMS$SAVED]BACKUP.EXE;26 (191 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]INIT.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]INIT.EXE;25 (81 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]LOGINOUT.EXE;33 copied to VMI$ROOT:[SEVMS$SAVED]LOGINOUT.EXE;33 (140 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSSLDR]IO_ROUTINES.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]IO_ROUTINES.EXE;4 (71 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSSLDR]MESSAGE_ROUTINES.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]MESSAGE_ROUTINES.EXE;1
(25 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSSLDR]LOGICAL_NAMES.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]LOGICAL_NAMES.EXE;1
(19 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSSLDR]SYSDEVICE.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]SYSDEVICE.EXE;1 (16 blocks)

```

Figure 1-1 Cont'd on next page

Installation Instructions

Figure 1-1 (Cont.) Typical SEVMS Version 5.3-1 Installation Procedure

```
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]SYSTEM_PRIMITIVES.EXE;2 copied to VMI$ROOT:[SEVMS$SAVED]SYSTEM_PRIMITIVES.EXE;2
(38 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]SECURITY.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]SECURITY.EXE;1 (18 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]PAGE_MANAGEMENT.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]PAGE_MANAGEMENT.EXE;4
(76 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]PROCESS_MANAGEMENT.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]PROCESS_MANAGEMENT.EXE
(76 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]NETDRIVER.EXE;3 copied to VMI$ROOT:[SEVMS$SAVED]NETDRIVER.EXE;3 (41 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSS$LDR]RMS.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]RMS.EXE;4 (312 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]F11BXQP.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]F11BXQP.EXE;25 (132 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]STABACKUP.EXE;26 copied to VMI$ROOT:[SEVMS$SAVED]STABACKUP.EXE;26 (401 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]SHOW.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]SHOW.EXE;25 (203 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]SETAUDIT.EXE;7 copied to VMI$ROOT:[SEVMS$SAVED]SETAUDIT.EXE;7 (41 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]SECURESHR.EXE;23 copied to VMI$ROOT:[SEVMS$SAVED]SECURESHR.EXE;23 (121 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]SECURESHRP.EXE;23 copied to VMI$ROOT:[SEVMS$SAVED]SECURESHRP.EXE;23 (121 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]MOUNTSHR.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]MOUNTSHR.EXE;25 (172 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]OPCOM.EXE;43 copied to VMI$ROOT:[SEVMS$SAVED]OPCOM.EXE;43 (72 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]MAILSHR.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]MAILSHR.EXE;1 (114 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]MAILSHRP.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]MAILSHRP.EXE;1 (70 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]SYSINIT.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]SYSINIT.EXE;25 (109 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]NETACP.EXE;2 copied to VMI$ROOT:[SEVMS$SAVED]NETACP.EXE;2 (147 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]REMACP.EXE;3 copied to VMI$ROOT:[SEVMS$SAVED]REMACP.EXE;3 (17 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]JOBCTL.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]JOBCTL.EXE;1 (120 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSLIB]MAIL.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]MAIL.EXE;1 (114 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]MAIL_SERVER.EXE;9 copied to VMI$ROOT:[SEVMS$SAVED]MAIL_SERVER.EXE;9
(21 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSMGR]RTTLOAD.COM;3 copied to VMI$ROOT:[SEVMS$SAVED]RTTLOAD.COM;3 (3 blocks)
%COPY-S-COPIED, VMI$ROOT:[SYSEXE]SHUTDOWN.COM;1 copied to VMI$ROOT:[SEVMS$SAVED]SHUTDOWN.COM;1 (30 blocks)
%SEVMS-I-DATEXISTS, VMI$ROOT:[SYSLIB]SEVMS$SMB_HDFRM.DAT already exists - it will not be replaced.
%SEVMS-I-LIBEXISTS, VMI$ROOT:[SYSLIB]SEVMS$SMB_LIB.TLB already exists - it will not be replaced.
+-----+
!
! To complete the installation, after the VMSINSTAL procedure is complete,
! you need to do the following things:
!
! 1. Set the SYSGEN parameter CLASS_PROT to 1.
! 2. Add @SYSSSTARTUP:SEVMS$STARTUP.COM to the beginning of
! the system startup command file.
! 3. Reboot your system.
! 4. Please refer to the SEVMS Security Manager's Guide
! for instructions on post-installation procedures
! that must be performed before labelled protection
! is fully enabled.
!
+-----+
%VMSINSTAL-I-MOVEFILES, Files will now be moved to their target directories...
Installation of SEVMS V53.1 completed at 12:22
VMSINSTAL procedure done at 12:22
```

1.5.1 Note about SEVMS Audit Server Database

The SEVMS audit server process uses a database file named AUDIT_SERVER.DAT to store auditing characteristics, such as the location of the security audit log file. (Refer to Section 6.2.1.1 of the *Guide to VMS System Security* for more information about this file.) The format of the file was changed in SEVMS Version 5.2, and is similarly changed in versions which follow.

If the Version 5.3-1 audit server is started with a Version 5.1 (or prior) database file, the process will exit with an RMS-F-RET error status. The installation procedure attempts to prevent this problem from occurring, but, in some cases, additional manual steps must be taken.

To avoid this problem, the old database file must be renamed or deleted so that the audit server is forced to create a new database file. If the installation procedure detects a database file with an improper format (i.e. a database file from SEVMS Version 5.1 or prior), it will display the following warning and question:

```

+-----+
!
! The current audit server database file is not compatible with this version !
! of SEVMS and will be deleted if you answer YES to the next question.      !
! Answering NO will cause this procedure to exit, allowing you to take other !
! actions (such as renaming the file) before invoking it again.             !
!
+-----+
* Delete VMI$ROOT:[SYSMGR]AUDIT_SERVER.DAT; [YES]?

```

- If you answer "YES" to the preceding question, the database file of the root into which you are installing SEVMS will be deleted. At the time you reboot the system, you may wish to use SET AUDIT commands to reset the auditing information stored in the database to that of your system specific values. (Refer to Section 6.2.1.1 of the *Guide to VMS System Security* for a description of this information.)
- If you answer "NO" to the preceding question, the installation procedure will exit, allowing you to take other actions before restarting the installation. You may wish to do this if the database is being shared by SEVMS Version 5.1 (and prior) systems, or if you failed to note the auditing information before upgrading to SEVMS Version 5.3-1.

If SEVMS is being installed on a system which is a member of a cluster, and an incompatible database file is found, the installation procedure will display an additional "post-installation procedure" step - to remind you to check the database files in other system roots.

Incompatible database files can be identified by the number of keys in the file. Version 5.1 (and prior) database files have one key; Version 5.2 (and later) database files have two keys. A DIRECTORY/FULL command will display the number of keys in a file.

2

Installation Files

The files installed by the SEVMS kit fall into the following categories:

- Files that replace their VMS equivalents.
- Command definition files which add SEVMS commands.
- New files that exist only as a part of SEVMS.

The following sections provide lists of the files contained in each category, including a brief description of each file.

2.1 Replacement Files

The following files are SEVMS versions of standard VMS files. As SEVMS files are installed into the system, the latest versions of the VMS files being replaced are copied into the `SYS$SYSROOT:[SEVMS$SAVED]` directory. Previous versions of these files are also left in the `SYS$SYSROOT:[SYSEXE]`, `SYS$SYSROOT:[SYS$LDR]`, and `SYS$SYSROOT:[SYSLIB]` directories.

The VMS files replaced by the SEVMS installation can be manually purged from the `SYS$SYSROOT:[SYSEXE]`, `[SYS$LDR]`, and `[SYSLIB]` directories after the installation.

- **ANALAUDIT.EXE**
Provides auditing analysis capability of audit records in audit archive file.
- **AUDIT_SERVER.EXE**
Formats audit messages and records audit information in appropriate audit archive file.
- **AUTHORIZE.EXE**
Supports classification qualifiers on ADD, REMOVE, MODIFY. Supports display of classification labels. Supports definition and display of classification names.
- **BACKUP.EXE**
Supports save and restoration of file classification.
- **DIRECTORY.EXE**
Supports display of file classification.
- **F11BXQP.EXE**
Provides proper mandatory access checks for files.
- **INIT.EXE**
Supports initialization of a disk volume with access classification.

Installation Files

- **JOBCTL.EXE**
Causes batch jobs to run at the classification of the submitting process.
- **LOGINOUT.EXE**
Supports /SECURITY qualifier on log in as well as additional access checks.
- **MAILSHR.EXE, MAILSHRP.EXE, MAIL_SERVER.EXE and MAIL.EXE**
Supports sending of mail to classified directories.
- **MOUNTSHR.EXE**
Supports new access checks on MOUNT.
- **NETACP.EXE**
Passes a classification when initiating a DECnet connection, and uses this classification in selecting a target process when receiving a connection.
- **NETDRIVER.EXE**
Uses the expanded structures that contain the classification of the process initiating a DECnet connection.
- **OPCOM.EXE**
Supports recognition of modification of user's SECURITY by means of AUTHORIZE, supports display of file classification in security alarms, supports new printed-file alarms, and provides an interface with the audit server.
- **REMACP.EXE**
Uses the classification of the remote terminal (RT) device to allow /disallow an incoming SET HOST connecton.
- **RMS.EXE**
Contains support for auditing by classification.
- **RTTLOAD.COM**
Runs the REMACP image with BYPASS and DOWNGRADE privileges to allow it to process SET HOST requests from processes of any classification.
- **SECURESHR.EXE, SECURESHRP.EXE**
Supports new system services.
- **SETAUDIT.EXE**
Supports SET AUDIT command for auditing of DOWNGRADE operations.
- **SHOW.EXE**
Supports display of new privileges.
- **SHUTDOWN.COM**

Provides a clean shutdown of auditing by doing the following: turning off auditing, flushing all buffered audit records, closing the operator log, and closing the archive file.

- STABACKUP.EXE

Supports save and restoration of file classification.

- STAENCBACKUP.EXE

For systems with encryption, supports save and restoration of file classification.

Note: STAENCBACKUP.EXE will only be installed on systems that already have encryption installed.

- IO_ROUTINES.EXE, MESSAGE_ROUTINES.EXE, LOGICAL_NAMES.EXE, SYSDEVICE.EXE, SYSTEM_PRIMITIVES.EXE, SECURITY.EXE, PAGE_MANAGEMENT.EXE, PROCESS_MANAGEMENT.EXE

New system image modules with miscellaneous changes.

- SYSINIT.EXE

Reads the classification information when mounting the boot volume.

2.2 Command Definition Files

The command definition files listed below add the indicated commands and qualifiers to the system command table (DCLTABLES.EXE).

- ANALYZE.CLD
 - ANALYZE/AUDIT
- INIT.CLD
 - INITIALIZE/SECURITY
- SET.CLD
 - SET AUDIT/SECURITY
 - SET CLASS
 - SET *object*/CLASS
 - SET TEMPLATE
- SHOW.CLD
 - SHOW AUDIT/SECURITY
 - SHOW CLASS
 - SHOW CLASS/PROCESS
 - SHOW *object*/CLASS
 - SHOW TEMPLATE
- RUN.CLD
 - RUN/PRIVILEGE=DOWNGRADE

— RUN/PRIVILEGE=UPGRADE

2.3 SEVMS Files

The files listed below are unique to SEVMS.

- SEVMS\$DEF.ADA, SEVMS\$DEF.BAS, SEVMS\$DEF.FOR, SEVMS\$DEF.H, SEVMS\$DEF.MAR, SEVMS\$DEF.PAS, SEVMS\$DEF.PLI, SEVMS\$DEF.R32

Symbolic definition files provided for various languages.

- SETSHOAUD.EXE

Implements the AUDIT SET command.

- SETSHOCLASS.EXE

Implements the SET and SHOW CLASS commands.

- SEVMS\$\$SMB_HDRFRM.DAT

Template versus category data base for secure print symbiont. (See note below)

Note: If `SYSLIBRARY:SEVMS_SMB_HDRFRM.DAT` exists (from an earlier SEVMS installation) it will be renamed to `SEVMS$$SMB_HDRFRM.DAT` and not replaced.

If `SYSLIBRARY:SEVMS$$SMB_HDRFRM.DAT` already exists on the target disk, it will not be replaced.

- SEVMS\$\$SMB_LIB.TLB

Template text library for secure print symbiont.

Note: If `SYSLIBRARY:SEVMS_SMB_LIB.TLB` exists (from an earlier SEVMS installation), it will be renamed to `SEVMS$$SMB_LIB.TLB` and not replaced.

If `SYSLIBRARY:SEVMS$$SMB_LIB.TLB` already exists on the target disk, it will not be replaced.

- SEVMS\$STARTUP.COM

Startup command file for SEVMS.

- SEVMS.HLP

Updates to the HELP facility for SEVMS.

- SEVMS\$SETSHOWAUDIT.EXE

Enables file audit according to classification.

- SEVMS\$RESTORE_VMS.COM

This command procedure is used prior to performing a VMS upgrade. It contains a record of all VMS images which are replaced by SEVMS images when SEVMS is installed. Running this command procedure restores the VMS images which were previously saved during SEVMS installation.

- SEVMS\$\$SMB.EXE

The secure print symbiont.

Note: If `SYSSYSTEM:SEVMS_SMB.EXE` exists (from an earlier SEVMS installation), it will be deleted during installation.

- `SEVMS$LATSYM.EXE`

A secure print symbiont which supports LAT print devices.

- `SEVMS$SETSHOTEMPLATE.EXE`

Provides support for the SET/SHOW TEMPLATE commands.

- `SEVMS$SMB_TEST.MAR`

Used to aid in the development of customer-supplied formatting routines (which are used in conjunction with the `.FORMAT_LINE` template directive of the SEVMS print symbiont).

2.4 Obsolete Files

This section lists the obsolete files from previous versions of SEVMS.

The following files are no longer used by SEVMS; these files can be deleted after installation:

- `SEVMS_SETSHOSMB.EXE`

3

Problem Reports

Problems can be submitted to the nearest delivery center using the SEVMS problem report form included with your SES documentation set.

Besides the standard information needed with any problem report (description of problem, sequence of events leading to problem, short command file and/or program to reproduce problem), please include the following SEVMS-specific information (where applicable):

- Crash dump, if available, with output from SDA SHOW CRASH, SHOW STACK.
- An indication of the relative classifications of the subjects and objects involved, if the problem concerns enforcement of mandatory controls.
- If possible, a sanitized version of the code related to the problem.

Part II Release Notes

This part of the manual contains release notes for SEVMS. Release notes are included in the SEVMS documentation set to supplement its manuals with the latest changes to the software and documentation.

The information in this part is divided into the following sections:

- **New and Changed Features**
- **Problems and Restrictions**
- **Problems Resolved**
- **Notes to Documentation**

4 New and Changed Features

This section contains information pertaining to the new and changed features of SEVMS Version 5.3-1. A brief description of each new or changed feature is provided, including a reference to where more information can be found on the topic.

4.1 File Classification Not Displayed For DIRECTORY Command Across Network

For SEVMS Version 5.3-1, the classification of files will not be displayed when a DIRECTORY/FULL or DIRECTORY/SECURITY command is issued for a directory on another network node.

In previous versions of SEVMS, when these commands were issued, a classification of "0" (i.e. `SECURITY=(LEVEL=UNCLASSIFIED)` on most systems) was always displayed, regardless of the actual classification of the file(s).

4.2 Symbolic Definition Files For Languages Available

This version of SEVMS provides symbolic definition files for various languages (listed below). The files provide definitions of SEVMS-specific values that are useful to system programmers.

The following symbolic definition files have been added to the SEVMS kit and reside in the `SYS$COMMON:[SYSLIB]` directory on the system:

- SEVMS\$DEF.ADA
- SEVMS\$DEF.BAS
- SEVMS\$DEF.FOR
- SEVMS\$DEF.H
- SEVMS\$DEF.MAR
- SEVMS\$DEF.PAS
- SEVMS\$DEF.PLI
- SEVMS\$DEF.R32

4.3 Change to File Name — SEVMS_SMB.EXE Becomes SEVMS\$SMB.EXE

Beginning with SEVMS Version 5.3-1, the name of the executable file previously called SEVMS_SMB.EXE has been changed. The new name for this file is SEVMS\$SMB.EXE.

Reminder: `START/QUEUE/PROCESSOR=SEVMS_SMB` commands must be changed to `START/QUEUE/PROCESSOR=SEVMS$SMB`.

4.4 Change to Recommended Privileges for MAIL Accounts

In Version 5.2 of SEVMS, it was recommended in 'Section 5.11' of the *VMS SES Security Manager's Guide* that default mail accounts be given DOWNGRADE privilege as both a "default" and an "authorized" privilege. This recommendation has been changed for Version 5.3-1.

For this version of SEVMS, it is recommended that the MAIL\$SERVER account be given DOWNGRADE privilege only as an "authorized" privilege.

4.5 New Functionality — Classification of Local Interactive Terminals

Previous versions of SEVMS used a terminal's device classification to determine the allowable range of classifications that a user could specify when logging in. This functionality has been changed for SEVMS Version 5.3-1.

For this version of SEVMS, a local terminal can still be classified with a terminal device classification - but, in addition, it can be given a *log-in classification range* which specifies the classification range of log-ins allowed on that terminal.

This change has been implemented so that terminals can be single level devices when users are not logged-in. This is important at sites where output to multi-level devices must be labeled (as with the SEVMS secure print symbiont).

4.5.1 Definition of Local Interactive Terminals

Local interactive terminals are terminals that are connected to asynchronous, serial line multiplexers on interfaces which reside on VAX processor buses or are provided as part of the processors themselves. These include all interfaces listed in Table 8-1 of the *VMS I/O User's Reference Manual: Part I* except for LAT terminal interfaces. These local terminals have the following device types:

- TT
- TX
- OP
- CS

4.5.2 Classification of Logins to Local Interactive Terminals

As in previous versions of SEVMS, SEVMS Version 5.3-1 allows local interactive terminals to have a device classification (similar to any other device). This classification is referred to as the *terminal device classification*. In previous versions of SEVMS, the terminal device classification was used to determine the range of classifications a user was allowed to specify when logging in on a local interactive terminal, as

well as the classification of a terminal when no users were logged-in to the terminal.

New for SEVMS Version 5.3-1 is the concept that terminals can now also be given a *log-in classification range*. The log-in classification range establishes a specific range of classifications which can be used for log-ins to a terminal.

When a log-in classification range is established for a terminal, it is used, rather than the terminal device classification, to determine the classification range for user log-ins. For the duration of the user's interactive session, the terminal is reclassified to the user's log-in classification (as described in Section 4.6). A terminal's log-in classification range is *not* used for other access control purposes.

If no log-in classification range is established for a terminal, the terminal device classification is used for specifying the terminal's classification range for user log-ins, as well as the terminal's classification when no users are logged-in.

The log-in classification ranges associated with each local interactive terminal are stored in a database file on the system. SEVMS uses the information in the database file when determining the range of classifications allowed for log-in to a terminal. If no log-in classification range record exists for a given terminal in the database, then log-in to that terminal will be constrained by the device classification of the terminal.

The database file used to store the log-in classification ranges for terminals is called `SYSS$COMMON:[SYSEXEXE]SEVMS$LOGIN_CLASS.DAT`. This is also the file which is used to contain classifications for LAT and network connections.

The `SET CLASS/TERMINAL` and `SHOW CLASS/TERMINAL DCL` commands are used to maintain this database. These commands are described in the following sections.

4.5.2.1 SET CLASS/TERMINAL

The `SET CLASS/TERMINAL` command is used to create and modify log-in classification ranges for local interactive terminals in the `SEVMS$LOGIN_CLASS.DAT` database file. When this command is used with the `/REMOVE` qualifier, it enables a user to delete an unwanted log-in classification range from the database file.

A user must have `WRITE` access to `SYSS$COMMON:[SYSEXEXE]SEVMS$LOGIN_CLASS.DAT` to execute this command. By default, this means the user must have `SYSTEM` privilege (`SYSPRV`).

The format of this command is as follows:

```
SET CLASS/TERMINAL [ /SECRECY=<classification-range>
                    /INTEGRITY=<classification-range> ] <terminal-name>
```

New and Changed Features

The *<terminal-name>* must have one of following formats:

Format	Device Type
<i><node-name></i> \$(<i><device-name></i> [:])	a specific device on a specific cluster node
<i><device-name></i> [:]	a device on a system which is not part of a cluster

Wildcards are not allowed in the command line.

While terminal devices are not cluster accessible, the *<node-name>*\$(*<device-name>*[:]) format is used to uniquely identify each device on the cluster in the shared cluster database. It is the same format that is returned by the **DVI\$_DISPLAY_DEVNAM** item of the **\$GETDVI** system service, except that the colon is optional. The *<device-name>*[:] form is intended for use on systems which are not clustered and the **SCSNODE SYSGEN** parameter is null. It will not match any terminal on a system where **SCSNODE** is defined.

If the device name specified in the terminal name is not one of the types listed in Section 4.5.1, **SET CLASS/TERMINAL** will return the following error:

```
"%SET-F-INVDEV, device is invalid for requested operation"
```

No check for existence of a node is made, since a node may not be a member of the cluster at the time the database is loaded. No check for existence of a device is made, since the database might be loaded before a controller is installed.

When **SET CLASS/TERMINAL** stores the terminal name in the database, it always includes the colon (:). The colon is optional in the command line.

4.5.2.2 SHOW CLASS/TERMINAL

The **SHOW CLASS/TERMINAL** command is used to display login classification ranges for local interactive terminals. A user must have **READ** access to **SY\$COMMON:[SYSEXE]SEVMS\$LOGIN_CLASS.DAT** to execute this command. By default, this means that the user must have **SYSTEM** privilege (**SYSPRV**). The format of this command is as follows:

```
SHOW CLASS/TERMINAL <terminal-name>
```

where *<terminal-name>* must have one of following formats:

Format	Device types(s)
<code><node-name>\${<device-name> [:]}</code> ¹	a specific device on a specific cluster node
<code><device-name>[:]</code> ¹	a device on a system which is not part of a cluster
<code><node-name>\${}</code> ²	all terminal devices on the specified node
*	all terminal devices on all nodes

¹Partial wildcarding of the `<device-name>` is allowed (i.e. `<partial-device-name>*`).

²Partial wildcarding of the `<node-name>` is allowed (i.e. `<partial-node-name>*`).

As is shown in the above table, full and partial wildcarding of the *terminal-name* is allowed. Note that the wildcard must always be at the end of the full or partially specified *terminal-name*.

Refer to Section 4.10 and to the "DCL Commands" section of the *VMS SES User's Guide* for additional information about full and partial wildcarding of SHOW CLASS commands.

The following example illustrates the use of the SHOW CLASS /TERMINAL command with a full wildcard to display all terminal devices on all nodes.

```
$ SHOW CLASS/TERMINAL *
Terminal classifications on 19-FEB-1990 13:31:31.25
Terminal: ANODE$TXA3:
Class: SECRECY=(LEVEL=SECRET, CATEGORY=(NONE))
Terminal: ZNODE$OPA0:
Class: SECRECY=(LEVEL=TOP_SECRET, CATEGORY=(A))
```

4.6 Reclassification of Terminals During Interactive Use

While a terminal is being used interactively (i.e. between the time a user logs in upon a terminal and the time the user's process deallocates it), the terminal is reclassified to the user's process' classification. After interactive use, the terminal's device classification is reset to its prior value. This is necessary because a terminal could be classified differently than the user's process. For example, a terminal device could have a device classification of SECRET, but be authorized in the log-in classification database for log-ins within the range SECRET through TOP_SECRET. If the terminal was not reclassified, a TOP_SECRET process logged-in at the terminal could not open a channel and write to it.

4.7 New DCL Commands Implemented To Set and Show Classifications Associated With Terminals

For SEVMS Version 5.3-1, two new commands have been implemented to set and show classifications associated with terminals. The SET CLASS /TERMINAL and SHOW CLASS/TERMINAL commands are now available in this release of SEVMS.

Refer to Section 4.5 of this chapter for a detailed description of the functions and use of these SEVMS commands.

4.8 New Qualifier Added to SET CLASS Commands — /REMOVE

A new qualifier, /REMOVE, has been added to the SEVMS SET CLASS commands. This qualifier affects the existing SET CLASS/SERVER (and SET CLASS/SERVER/PORT) and SET CLASS/NODE commands, and can also be used with the new SET CLASS/TERMINAL command (described in Section 4.5).

This qualifier enables a user to delete an unwanted record from the SEVMS\$LOGIN_CLASS.DAT database file.

Examples of the using this qualifier with each applicable SET CLASS command are provided below.

```
$SET CLASS/SERVER server-name/REMOVE
$SET CLASS/SERVER/PORT=port-name server-name/REMOVE
$SET CLASS/NODE/LINK=link-type node-name/REMOVE
$SET CLASS/TERMINAL terminal-name/REMOVE
```

4.9 Changes to ANALYZE/AUDIT Command

The following SEVMS-specific changes have been made to the VMS ANALYZE/AUDIT command.

4.9.1 New Qualifier — /FACILITY=SEVMS

An SEVMS-specific qualifier has been added to the VMS ANALYZE /AUDIT command. This qualifier, /FACILITY=SEVMS, can be used in conjunction with the /EVENT_TYPE qualifier and is required when specifying SEVMS event types. The syntax for using this command is shown below.

```
$ANALYZE/AUDIT/FACILITY=SEVMS/EVENT_TYPE=sevms_event_type-keyword file-name
```

4.9.2 New Keywords for /EVENT_TYPE Qualifier

The following SEVMS-specific keywords have been added to the /EVENT_TYPE qualifier of the VMS ANALYZE/AUDIT command:

- PRINTED_FILE — selects attempts to print files
- LABEL_BYPASS — selects attempts to bypass page labeling using PRINT/PASSALL command
- CHANGE_CLASS — selects attempts to change the classification of objects using SET CLASS command (i.e. \$CHANGE_CLASS system service)

In addition, the `/EVENT_TYPE=ALL` qualifier has been changed . It now displays all SEVMS information as well as all VMS information. To display all SEVMS information only (without VMS information), use the new `/FACILITY=SEVMS` qualifier in conjunction with this keyword.

The `/EVENT_TYPE` qualifier specifies the general class of event to be used in selecting audit records from the audit archive file. The syntax of this command, when used to select SEVMS-specific event types, is shown below.

```
$ANALYZE/AUDIT/FACILITY=SEVMS/EVENT_TYPE=sevms_event_type-keyword file-name
```

The *sevms_event_type-keyword* is specified from one of the choices listed above. The `/FACILITY=SEVMS` qualifier is required for this command.

The following examples show the use of two of the keywords of the `/EVENT_TYPE` qualifier, and the results which are displayed when each is used. An explanation follows each example.

```
$ANALYZE/AUDIT/FACILITY=SEVMS/EVENT_TYPE=CHANGE_CLASS AUDIT.LOG
```

Date / Time	Type	Subtype	Node	Username	ID	Term
6-MAR-1990 14:23:00.60	CHANGE	CHANGE_SUBTYP_SU	TURBO	RUSNER	00000163	
6-MAR-1990 14:23:10.29	CHANGE	CHANGE_SUBTYP_SU	TURBO	RUSNER	00000163	
6-MAR-1990 14:27:26.81	CHANGE	CHANGE_SUBTYP_SU	TURBO	RUSNER	0000012C	
6-MAR-1990 14:33:30.21	CHANGE	CHANGE_SUBTYP_SU	TURBO	MAIL\$SERVER	00000173	

This command specifies that SEVMS audit records which contain attempts to change the classification of objects by use of the `SET CLASS` command or the `$CHANGE_CLASS` system service be displayed for analysis. It specifies that the information be selected from the records in audit archive file named `AUDIT.LOG`. In this case, the `AUDIT.LOG` records show that there were several such attempts: they all occurred on node `TURBO`, the user was `RUSNER` in all cases except for the last one, which was `MAIL$SERVER`. The date and time for each is recorded, as well as the event which caused the audit record.

```
$ANALYZE/AUDIT/FACILITY=SEVMS/EVENT_TYPE=LABEL_BYPASS AUDIT.LOG
```

Date / Time	Type	Subtype	Node	Username	ID	Term
6-MAR-1990 14:42:24.59	PRINT	PRINT_SUBTYP_NOP	TURBO	SYSTEM	00000174	

This command specifies that SEVMS audit records which contain attempts to bypass the page labeling on files through use of the `PRINT/PASSALL` command be displayed for analysis. It specifies that the information be selected from the records in audit archive file named `AUDIT.LOG`. In this case, the `AUDIT.LOG` file contained only one record of such an attempt: it occurred on node `TURBO`, by user `SYSTEM`, on the day and time shown.

4.9.3 New Keywords for /SELECT Qualifier

The SEVMS-specific keywords SYMBIONT_PROCESS_ID and QUEMGR_JOB_NUMBER have been added to the /SELECT qualifier of the VMS ANALYZE/AUDIT command.

These keywords replace the SYMBIONT_ID and JOBNUM keywords used with the /SELECT qualifier in SEVMS Version 5.2.

The /SELECT qualifier specifies the criteria to be used when selecting event records. The syntax of this command is shown below.

```
$ANALYZE/AUDIT/SELECT=keyword=value file-name
```

The *keyword* is specified from one of the choices described above.

4.10 Partial Wildcarding (*) Support Added for SHOW CLASS Command

For this version of SEVMS, support has been added for the partial wildcarding of SHOW CLASS commands. This new feature can be used with the SHOW CLASS/NODE, SHOW CLASS/SERVER, and SHOW CLASS/TERMINAL commands.

This feature enables a user to specify a partial name with a wildcard (*) to display node, server, and terminal classification information. For example, this new feature could be used to display the classification of all terminal names beginning with TX by specifying TX* in the command line. The following example illustrates this idea:

```
$ SHOW CLASS/TERMINAL OP*

Terminal classifications on 22-MAY-1990 05:56:15.66

Terminal: OPA11:
Class: SECRECY=(LEVEL=SECRET,CATEGORY=(NONE))

Terminal: OPA8:
Class: SECRECY=(LEVEL=CONFIDENTIAL,CATEGORY=(NONE))
```

This feature does not support partial wildcarding for port names, however (i.e. SHOW CLASS/SERVER/PORT).

Refer to the *VMS SES User's Guide* "DCL Commands" section for further information.

5

Problems and Restrictions

This section contains information about problems and restrictions which apply to Version 5.3-1 of SEVMS. A brief description of each problem or restriction is provided, including a reference to where more information can be located on the topic.

5.1 Installation Procedure Note

Due to a bug in VMSINSTAL.COM, the SEVMS installation procedure is unable to set the appropriate file protection on the following files:

```
SYS$COMMON: [SYSLIB] SEVMS$SMB_HDRFRM.DAT
SYS$COMMON: [SYSLIB] SEVMS$SMB_LIB.TLB
```

After the SEVMS installation is complete, please enter the following commands to change the protection and ownership of these two files:

```
$ SET FILE/OWNER=[1,4]/PROTECTION=(SYSTEM:RWE,OWNER,GROUP,WORLD) -
  _$ SYS$COMMON:[SYSLIB]SEVMS$SMB_HDRFRM.DAT
$ SET FILE/OWNER=[1,4]/PROTECTION=(SYSTEM:RWE,OWNER,GROUP,WORLD) -
  _$ SYS$COMMON:[SYSLIB]SEVMS$SMB_LIB.TLB
```

This problem will be fixed in a future release of VMS.

5.2 Mailing Down to Privileged Accounts

In SEVMS Version 5.2, there was a restriction (described in the VMS SES Version 5.2 Cover Letter) associated with mailing down to privileged accounts. This restriction stated that if a user can receive mail through DECnet, then the user's default MAIL directory must be classified with the user's maximum authorized classification.

This restriction is still in effect for SEVMS Version 5.3-1.

5.3 DISCONNECT Terminal Characteristic Not Fully Supported

SEVMS does not provide full support for terminals which are set to DISCONNECT. Setting a terminal with this characteristic causes it to be accessed through a virtual terminal. This allows a user to switch from one (user-owned) process to another (user-owned) process without logging out of the terminal. The use of virtual terminals also allows users to connect to disconnected processes when they log in.

SEVMS allows a user logging-in to connect only to a process with a classification identical to that specified (or defaulted to) in that log-in. SEVMS does not, however, support similar limitations on the use of the DCL CONNECT command.

Problems and Restrictions

Terminals on SEVMS systems should not be set to DISCONNECT unless some other means are used to insure that there can be no change in classification. For instance, since VMS already ensures that a process being connected to belongs to the same user, terminals can be set DISCONNECT if all users have single level accounts.

This restriction applies to this version, and all prior versions, of SEVMS.

5.4 System Disk Classification Restriction

When classifying the system disk, the empty, but classified, disk **must** be created on an SEVMS Version 5.x system.

5.5 Storage Library System (SLS) — Note for Use With SEVMS

If SLS (Storage Library System) is to be installed on the same system as SEVMS, you must first contact the SEVMS support center for your area.

6 Problems Resolved

This section contains information pertaining to problems in previous versions of SEVMS which have been resolved in Version 5.3-1 of SEVMS.

This section discusses only those resolved problems which may be significant to the customer.

6.1 MAIL — Problems Resolved

- In prior versions of SEVMS, newly created MAIL.MAI and message files were classified using the classification of the sending process.

For this version of SEVMS, these files are now classified using the classification of the recipient process' default mail directory.

- In prior versions of SEVMS, MAIL messages sent by a privileged, higher-classified user to a lower-classified user could not be selected for reading by the lower-classified user.

This problem has been resolved in this version of SEVMS. The lower-classified user can now select MAIL messages sent by a privileged, higher-classified user.

6.2 SET AUDIT — Problems Resolved

- When the /ENABLE or /DISABLE qualifier is used with the SET AUDIT/SECURITY or SET AUDIT/INTEGRITY command, a classification qualifier must also be used.

In prior versions of SEVMS, an error message should have been generated, but was not, when the SET AUDIT/SECURITY or SET AUDIT/INTEGRITY commands were issued with the /ENABLE or /DISABLE qualifier and a classification qualifier was not included.

For this version of SEVMS, this problem has been resolved. An error is now generated if a classification qualifier is not included when /ENABLE or /DISABLE is used.

- The /SECURITY and /INTEGRITY qualifier cannot be used with the SET AUDIT command at the same time.

In prior versions of SEVMS, an error message should have been generated, but was not, when the SET AUDIT command was issued with both the /SECURITY and /INTEGRITY qualifiers. Instead, the classification specified would arbitrarily be used as an INTEGRITY classification.

Problems Resolved

For this version of SEVMS, this problem has been resolved. An error is now generated if the /SECRECY and /INTEGRITY qualifiers are entered in the same command line.

6.3 Captive Account/LOGINOUT Problem Resolved

In SEVMS Version 5.2, a user cannot log in through a captive account. (Captive accounts are accounts that have the CAPTIVE flag specified in the UAF record.)

This problem has been fixed in Version 5.3-1 of SEVMS.

6.4 ANALYZE/AUDIT Command — /EVENT_TYPE=PRINT Functionality Restored

The /EVENT_TYPE=PRINT qualifier of the ANALYZE/AUDIT command was removed from Version 5.2 of SEVMS. The functionality of this qualifier has been restored in Version 5.3-1 of SEVMS - however, the keyword name portion of the qualifier has been changed to PRINTED_FILE (i.e. /EVENT_TYPE=PRINTED_FILE). Refer to Section 4.9.2 for details about this new keyword name and its functionality.

This qualifier is used to produce an audit report which selects all records written to the security audit log file that were generated as a result of PRINT events.

The alternate method to achieve identical results to the (former) /EVENT_TYPE=PRINT qualifier, which was recommended and described in the Version 5.2 Release Notes, is still valid and can also be used. An updated version of this alternate method is included in this release note.

Alternate Method

To produce an audit report which selects all records written to the security audit log file that are generated as a result of PRINT events, you can use the /SELECT qualifier of ANALYZE/AUDIT command. When this qualifier is used with the SYMBIONT_PROCESS_ID or QUEMGR_JOB_NUMBER keywords and the wildcard character (*), it produces the same results as the new /EVENT_TYPE=PRINTED_FILE (formerly /EVENT_TYPE=PRINT) qualifier.

The syntax for these commands is as follows:

```
$ANALYZE/AUDIT/SELECT=SYMBIONT_PROCESS_ID=* file-name
```

OR

```
$ANALYZE/AUDIT/SELECT=QUEMGR_JOB_NUMBER=* file-spec
```

6.5 Classification of Template Device

In previous versions of SEVMS, there was a problem which prevented the classification of template devices. This problem has been corrected in SEVMS Version 5.3-1.

6.6 RMS Channel Unavailable

For SEVMS Version 5.2, a problem existed (when classifying files) which sometimes resulted in the following error message:

```
-RMS-F-CHN, assign channel system service request failed  
-SYSTEM-F-NOIOCHAN, no I/O channel available
```

This problem has been corrected in this version of SEVMS.

6.7 \$CREPRC Returns BADPARAM Error

In versions of SEVMS prior to Version 5.3-1, there was a problem in the \$CREPRC system service which sometimes caused a SS\$_BADPARAM error to be returned when a classification was specified. This problem has been corrected in this version of SEVMS.

6.8 SEVMS LAT Print Symbiont — DEFINE/FORM/LENGTH Support

A change has been made to the maximum value supported for DEFINE /FORM/LENGTH of the SEVMS LAT print symbiont.

In SEVMS Version 5.2, the SEVMS LAT print symbiont (SEVMS\$LATSYM.EXE) would hang when a form length was set to greater than 131.

In SEVMS Version 5.3-1, form lengths up to (and including) 255 are now supported.

6.9 SHOW CLASS/NODE Command — Wildcard (*) Problem Resolved

In prior versions of SEVMS, when the SHOW CLASS/NODE * command was issued, the * was not echoed back if no node was found for a particular LINK type.

This problem has been corrected for this version of SEVMS.

Index

A

Audit server database
 in SEVMS Version 5.1 • 1–7
 in SEVMS Version 5.2 • 1–7
AUDIT_SERVER.DAT • 1–7

C

Changed features • 4–1
Command definition files • 2–3
Command syntax
 of SEVMS commands • viii
 of VMS commands • viii
Conventions
 SEVMS • viii
 VMS • viii

D

DIGITAL consultant
 services provided by • v
Documentation
 associated SEVMS manuals • vi
 associated VMS manuals • vi, vii
 description of • v
 relationship of VMS and SEVMS manuals • vii
Document structure • v
Dominate
 definition of • viii

F

Features
 new and changed • 4–1
Files
 provided by installation • 2–1
 replaced by installation • 2–1
 SEVMS files provided by installation • 2–4

I

Installation • 1–1
 caution • 1–1
 files provided by SEVMS • 2–1
 replacement files • 2–1
 sample of • 1–5
 SEVMS files provided • 2–4
Intended audience • v

L

Licensed software
 of VMS Security Enhancement Service • v

N

New features • 4–1

O

Obsolete files • 2–5
Operator
 definition of • viii

P

Problem reports • 3–1
Problems • 5–1
Problems resolved • 6–1

Q

Quality Assurance Report (QAR) • 3–1

Index

R

Release notes • 3–1 to 6–3
Restrictions • 5–1

S

Scalar
 definition of • viii

Security category
 conventions used • viii

Security Enhancement Service • v
 see also VMS SES

Security level
 conventions used • viii

Security manager
 use of this manual • v

SES
 see VMS SES

SES Documentation
 description of • v

SES Installation Guide and Release Notes Manual
 structure of • v

Set
 definition of • viii

SEVMS
 conventions of • viii
 definition of • v

SEVMS documentation
 associated manuals • vi

SEVMS Version 5.2
 removing • 1–2

SEVMS Version 5.3-1
 files provided by installation • 2–4
 installation of • 1–3
 sample installation • 1–5

Software Performance Report (SPR) • 3–1

Subset
 definition of • viii

System manager
 use of this manual • v

U

Using this manual • v

V

VMS
 conventions of • viii

VMS documentation
 associated manuals • vi

VMS Security Enhancement Service
 see also VMS SES
 definition of • v

VMS SES
 description of • v

VMS SES documentation • v

VMS SES software security consulting package
 components of • v
 definition of • v

Reader's Comments

Please use this postage-paid form to comment on this manual. If you require a written reply to a software problem and are eligible to receive one under Software Performance Report (SPR) service, submit your comments on an SPR form.

Thank you for your assistance.

I rate this manual's:	Excellent	Good	Fair	Poor
Accuracy (software works as manual says)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Completeness (enough information)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clarity (easy to understand)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Organization (structure of subject matter)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Figures (useful)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Examples (useful)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Index (ability to find topic)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Page layout (easy to find information)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

I would like to see more/less _____

What I like best about this manual is _____

What I like least about this manual is _____

I found the following errors in this manual:

Page	Description
_____	_____
_____	_____
_____	_____
_____	_____

Additional comments or suggestions to improve this manual:

I am using Version _____ of the software this manual describes.

Name/Title _____ Dept. _____

Company _____ Date _____

Mailing Address _____

Phone _____

FOLD HERE AND TAPE. DO NOT STAPLE.

digitalTM



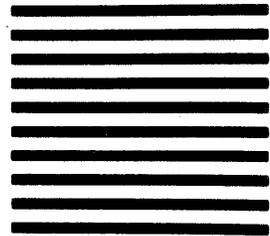
No Postage
Necessary
if Mailed in the
United States

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 33 MAYNARD, MA

POSTAGE WILL BE PAID BY ADDRESSEE

Digital Equipment Corporation
Advanced Technology Products & Services
110 Spitbrook Road, ZK03-3/Z34
Nashua, NH 03062

ATTENTION: Release Engineering SEVMS



FOLD HERE AND TAPE. DO NOT STAPLE.