VMS Security Enhancement Service Documentation Set

Version 5.3-1

Order Number: QS-970AA-GZ

June 1990

Contents:

- *VMS SES Installation Guide and Release Notes*
- *VMS SES User's Guide*
- *VMS SES Security Manager's Guide*

Digital Equipment Corporation

VMS SES
Installation Guide and Release Notes
Version 5.2

Order Number: QS-970AA-IG

November 1989

This manual describes installation and upgrade procedures, new and changed features, problems and restrictions, and documentation notes for Version 5.2 of the VMS Security Enhancement Service.

Revision/Update Information:	This manual supersedes the Version 5.1 *VMS SES Installation Guide and Release Notes*.
Operating System and Version:	VMS Version 5.2
Software Version:	SEVMS Version 5.2

Digital Equipment Corporation

Contents

Preface

This document describes installation and upgrade procedures, new and changed features, problems and restrictions, and documentation notes for Version 5.2 of 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.

- 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, Version 5.2*
- *VMS Audit Analysis Utility Manual*

Conventions

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

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".

1 Installation Instructions

This section tells you how to install SEVMS Version 5.2. It is intended for a reader who has system management experience.

1.1 Introduction

SEVMS Version 5.2 installs as an upgrade to VMS Version 5.2. Therefore, you must first be sure that VMS Version 5.2 is installed on your system before attempting to install SEVMS Version 5.2. Once you are assured that your system is running VMS Version 5.2, you can proceed with the installation of SEVMS Version 5.2 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 5.2.
  2. Install SEVMS Version 5.2.

- 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 5.2 - **Or** *install* VMS Version 5.2.
  2. Install SEVMS Version 5.2.

Instructions for removing SEVMS Version 5.1 to restore your system to VMS Version 5.1 are contained in this chapter in Section 1.2.

For complete instructions on updating from VMS Version 5.1 to VMS Version 5.2, refer to the appropriate installation and operations guides which were supplied with your media kit, the *VMS Release Notes, Version 5.2* and the *VMS System Management Subkit—Setup Volume*.

Instructions for installing SEVMS Version 5.2 are contained in this chapter in Section 1.4.

Summary:

- **Your system must be running VMS Version 5.2 prior to installation of SEVMS Version 5.2.**
- **If you are going to install SEVMS Version 5.2 on a cluster, all nodes should be running VMS Version 5.2. Rolling upgrades to SEVMS Version 5.2 are NOT recommended.**

1.4 Installing SEVMS Version 5.2

This section contains information to guide you through the installation of SEVMS Version 5.2.

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
```

Figure 1-1 Typical SEVMS Version 5.2 Installation Procedure

```
$ @SYS$UPDATE:VMSINSTAL  SEVMS052  MUA0:

VMS Software Product Installation Procedure V5.2

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 V5.2

       Beginning installation of SEVMS V5.2 at 12:09

%VMSINSTAL-I-RESTORE, Restoring product saveset A...
%SEVMS-I-KITINFO, Installation kit version V5.2

+----------------------------------------------------------------------------+
! 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].


%COPY-S-COPIED, VMI$ROOT:[SYSEXE]AUTHORIZE.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]AUTHORIZE.EXE;25 (159 block

%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$ROOT:[SYS$LDR]IO_ROUTINES.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]IO_ROUTINES.EXE;4 (71 blo

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]MESSAGE_ROUTINES.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]MESSAGE_ROUTINES.EXE
(25 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]LOGICAL_NAMES.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]LOGICAL_NAMES.EXE;1
(19 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]SYSDEVICE.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]SYSDEVICE.EXE;1 (16 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]SYSTEM_PRIMITIVES.EXE;2 copied to VMI$ROOT:[SEVMS$SAVED]SYSTEM_PRIMITIVES.E
(38 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]SECURITY.EXE;1 copied to VMI$ROOT:[SEVMS$SAVED]SECURITY.EXE;1 (18 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]PAGE_MANAGEMENT.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]PAGE_MANAGEMENT.EXE;4
(76 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]PROCESS_MANAGEMENT.EXE;4 copied to VMI$ROOT:[SEVMS$SAVED]PROCESS_MANAGEMENT
(76 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$LDR]NETDRIVER.EXE;3 copied to VMI$ROOT:[SEVMS$SAVED]NETDRIVER.EXE;3 (41 blocks)

%COPY-S-COPIED, VMI$ROOT:[SYS$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 block

%COPY-S-COPIED, VMI$ROOT:[SYSEXE]SHOW.EXE;25 copied to VMI$ROOT:[SEVMS$SAVED]SHOW.EXE;25 (203 blocks)
```

Figure 1-1 Cont'd. on next page

To avoid the 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, 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 preceeding question, the database file in 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 *VMS Guide to System Security* for a description of this information.)

If you answer "NO" to the preceeding 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 systems, or if you failed to note the auditing information before upgrading to SEVMS Version 5.2.

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 a fifth "post-installation procedure" step to remind you to check the database files in other system roots.

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

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 SECRECY 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

2.3 SEVMS Files

The files listed below are unique to SEVMS.

- 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 SYS$LIBRARY:SEVMS_SMB_HDRFRM.DAT exists (from an earlier SEVMS installation) it will be renamed to SEVMS$SMB_HDRFRM.DAT and not replaced.**
If SYS$LIBRARY:SEVMS$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 SYS$LIBRARY:SEVMS_SMB_LIB.TLB exists (from an earlier SEVMS installation), it will be renamed to SEVMS$SMB_LIB.TLB and not replaced.**
If SYS$LIBRARY:SEVMS$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

  Secure print symbiont.

- SEVMS$LATSYM.EXE

  A secure print symbiont which supports LAT print devices.

- SEVMS$SETSHOTEMPLATE.EXE

  Provides support for the SET/SHOW TEMPLATE commands.

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.