VSI OpenVMS

Enhanced Password Management Installation and User Guide

Document Number: DO-DPWDIG-01A

Publication Date: December 2021

Revision Update Information: This is a new manual.

Operating System and Version: VSI OpenVMS Integrity Version 8.4-2L3
VSI OpenVMS Alpha Version 8.4-2L2
VSI OpenVMS x86-64 Version 9.1

VMS Software, Inc. (VSI)
Burlington, Massachusetts, USA

Enhanced Password Management Installation and User Guide

Legal Notice

Preface

This document describes how to install the VSI OpenVMS Enhanced Password Management software, define a password policy, and implement that policy. Hereafter in this document, VSI OpenVMS Enhanced Password Management is referred to as VSI Password Management.

1. About VSI

VMS Software, Inc. (VSI) is an independent software company licensed by Hewlett Packard Enterprise to develop and support the OpenVMS operating system.

VSI seeks to continue the legendary development prowess and customer-first priorities that are so closely associated with the OpenVMS operating system and its original author, Digital Equipment Corporation.

2. Introducing VSI Password Management

The password is the most common authentication method that you can use to determine if a user has permission to access a system, resource, or a file. It acts as a primary defense against unauthorized access. The effectiveness of this defense is governed by a set of principles that define the password policy of your site or system.

One of the basic concepts of a password policy is a list of requirements that the system, application, or website uses to gain access. For example, a common set of criteria is a password that must include at least one uppercase character, one lowercase character, one digit, and one symbol.

With VSI Password Management software, VSI OpenVMS now provides system or security managers with additional tools to define and implement a site-wide password policy. This manual provides installation, conceptual, and usage information to implement that policy.

Note

As a sample password policy, this document references aspects of the US Department of Defense (DoD) password policy. The summary of DoD requirements is listed in Appendix C of this document.

---

3. Prerequisites

VSI Password Management can be installed on the following VSI OpenVMS versions:

- VSI OpenVMS for Integrity Servers Version 8.4-2L3
- VSI OpenVMS Alpha Version 8.4-2L2
- VSI OpenVMS x86-64 9.1

You must install the VSI VMS NOTARY Version 2.0 patch kit prior to installing VSI Password Management. All VSI OpenVMS patch kits now require the VSI VMS NOTARY V2.0 patch kit.

VSI Password Management operates for local authorization using either UAF login or ACME login.

4. Intended Audience

This manual is for experienced system or security managers, who have the responsibility to manage the security of an OpenVMS system and have full system management privileges.

Important

Extreme care should be exercised when using this software because it provides the ability to change the password behavior for all OpenVMS accounts.

---

5. Related OpenVMS Documentation

See the list below for OpenVMS manuals that you will find helpful when implementing the VSI Password Management software.

- *VSI OpenVMS Guide to System Security*
- *VSI OpenVMS System Manager's Manual, Volume 1: Essentials*
- *VSI OpenVMS System Manager's Manual, Volume 2: Tuning, Monitoring, and Complex Systems*
- *VSI OpenVMS System Management Utilities Reference Manual, Volume 1: A-L*
- *VSI OpenVMS System Management Utilities Reference Manual, Volume 2: M-Z*
- *VSI OpenVMS Programming Concepts Manual, Volume II*
- *VSI OpenVMS User's Manual*

The full VSI OpenVMS documentation set can be found on the VMS Software Documentation webpage at https://docs.vmssoftware.com/.

6. VSI OpenVMS Enhanced Password Management Support

VSI supports VSI OpenVMS Enhanced Password Management running on VSI OpenVMS Integrity Version 8.4-2L1, VSI OpenVMS Integrity Version 8.4-2L3, VSI OpenVMS Alpha Version 8.4-2L1, VSI OpenVMS Alpha Version 8.4-2L2, and VSI OpenVMS x86-64 9.1. Please contact your support channel for help with this product.

7. VSI Encourages Your Comments

You may send comments or suggestions regarding this manual or any VSI document by sending electronic mail to the following Internet address: `<docinfo@vmssoftware.com>`. Users who have OpenVMS support contracts through VSI can contact `<support@vmssoftware.com>` for help with this product.

8. Typographical Conventions

The following conventions are used in this manual:

Convention	Meaning
Ctrl/*X*	A sequence such as **Ctrl/*X*** indicates that you must hold down the key labeled Ctrl while you press another key or a pointing device button.
PF1 *X*	A sequence such as **PF1 *X*** indicates that you must first press and release the key labeled PF1 and then press and release another key (***X***) or a pointing device button.
Enter	In examples, a key name in bold indicates that you press that key.
. . .	A horizontal ellipsis in examples indicates one of the following possibilities:- Additional optional arguments in a statement have been omitted.- The preceding item or items can be repeated one or more times.- Additional parameters, values, or other information can be entered.
. . .	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being discussed.
( )	In command format descriptions, parentheses indicate that you must enclose choices in parentheses if you specify more than one. In installation or upgrade examples, parentheses indicate the possible answers to a prompt, such as: `Is this correct? (Y/N) [Y]`
[ ]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for directory specifications and for a substring specification in an assignment statement. In installation or upgrade examples, brackets indicate the default answer to a prompt if you press **Enter** without entering a value, as in: `Is this correct? (Y/N) [Y]`
|	In command format descriptions, vertical bars separate choices within brackets or braces. Within brackets, the choices are optional; within braces, at least one choice is required. Do not type the vertical bars on the command line.
{ }	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
bold type	Bold type represents the name of an argument, an attribute, or a reason. In command and script examples, bold indicates user input. Bold type also represents the introduction of a new term.
italic type	Italic type indicates important information, complete titles of manuals, or variables. Variables include information that varies in system output (Internal error *number*), in command lines (/PRODUCER=*name*), and in command parameters in text (where *dd* represents the predefined code for the device type).
UPPERCASE TYPE	Uppercase type indicates a command, the name of a routine, the name of a file, or the abbreviation for a system privilege.
`Example`	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies website addresses, UNIX command and pathnames, PC-based commands and folders, and certain elements of the C programming language.

Convention	Meaning
--	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.
numbers	All numbers in text are assumed to be decimal unless otherwise noted. Nondecimal radixes, binary, octal, or hexadecimal, are explicitly indicated.

Chapter 1. Installing VSI Password Management

This chapter describes the steps to install the VSI Password Management software. Please read the installation procedure completely before installing the patch kit.

Note

This chapter provides an example installation performed on an OpenVMS for Integrity Server system. Installing this kit on an OpenVMS Alpha system is performed with the same commands and procedure.

1.1. Installing the Kit

To install the VSI Password Management patch kit, perform the following steps:

1. **Log on to SYSTEM.** The installation procedure copies files onto the system disk. You must be logged into the SYSTEM account (or another fully privileged account) to perform the installation.

2. **Read the Release Notes.** It is important to read the Release Notes because they provide details that will help you install and use the product.

3. **Check OpenVMS Version.** Ensure your system is running a supported version of VSI OpenVMS.

   ```
   $ SHOW SYSTEM /NOPROCESS
   ```

4. **Confirm that you recently backed up your system disk.**

5. **Locate your VSI Password Management kit file**. If the file type is ZIPEXE, run the file to extract the PCSI files.

   For I64 systems:

   ```
   Directory SYS$SYSROOT:[SYSMGR]
   VSI-I64VMS-VMS842L1I_PWDMGMT-V0100--4.PCSI$COMPRESSED;1
   VSI-I64VMS-VMS842L1I_PWDMGMT-V0100--4.PCSI$COMPRESSED_VNC;1
   ```

   For Alpha systems:

   ```
   VSI-AXPVMS-VMS842L2A_PWDMGMT-V0100--4.PCSI$COMPRESSED;1
   VSI-AXPVMS-VMS842L2A_PWDMGMT-V0100--4.PCSI$COMPRESSED_VNC;1
   ```

Note

You must install the VSI VMS NOTARY Version 2.0 patch kit prior to installing the VSI Enhanced Password Management Software kit. See the *VSI OpenVMS Enhanced Password Management Cover Letter and Release Notes* for more information.

---

6. **Execute the PCSI kit with the following command:**

   ```
   $ PRODUCT INSTALL *PWDMGMT
   ```

Note

VSI provides separate kits for the Integrity and Alpha VSI Password Management software. Using the asterisk in the PRODUCT INSTALL command guarantees that the PCSI procedure will select and install the correct kit for your specific architecture.

The system will produce output similar to the following:

```
Performing product kit validation of signed kits ...
%PCSI-I-VSIVALPASSED, validation of $1$DGA110:[UAF.KITS]
    VSI-I64VMS-VMS842L1I_PWDMGMT-V0100--4.PCSI$COMPRESSED;1 succeeded

The following product has been selected:
    VSI I64VMS VMS842L1I_PWDMGMT V1.0      Patch (remedial update)

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected
product and for any products that may be installed to satisfy
software dependency requirements.

Configuring VSI I64VMS VMS842L1I_PWDMGMT V1.0:
   VSI OpenVMS V8.4-2L1 PWDMGMT V1.0

Recovery data will be saved which will allow you to un-install
this kit.  In the past, kit installations provided some level
of recovery capability by renaming all replaced files to
file_name.ext_OLD.  If you wish, you can continue to do this.

Note that this will triple the disk space required for
this kit - one for the installed files, once for the saved
recovery data and once for the file_name.ext_OLD files.

Do you wish to have replaced files renamed
to file_name.ext_OLD [NO] ?:

Files will not be renamed

* This product does not have any configuration options.

    <<System disk backup>>

VMS Software, Inc. recommends that you backup your system disk
before installing any patches.

This ECO kit will make functional changes to your system.
Before installing this kit you should make a backup copy
of your system disk.  Without a backup copy you will not
be able to restore your system to a pre-kit installation
state should the need arise.

Do you want to continue? [YES]

<<No reboot required, but additional actions required>>
```

```
This ECO kit does not require a system reboot.

However, there are additional steps that must be performed to use
the images provided by this kit on the installing system and also
on all nodes of a VMSCluster using this system disk as a shared
common system disk.  Refer to the PCSI kit release notes,
SYS$HELP:VMS842L1I_PWDMGMT-V0200.RELEASE_NOTES, Section 8.3,
"Special Installation Instructions", for required
post-installation actions.

    Do you want to continue? [YES]

Execution phase starting ...

The following product will be installed to destination:
    VSI I64VMS VMS842L1I_PWDMGMT V1.0      DISK$CAMHUD:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...40%...50%...60%...80%...90%...100%

The following product has been installed (and a recovery data set
 created):
    VSI I64VMS VMS842L1I_PWDMGMT V1.0      Patch (maintenance update)

VSI I64VMS VMS842L1I_PWDMGMT V1.0: VSI OpenVMS V8.4-2L1 PWDMGMT V1.0

    <<Release notes available>>

The PCSI kit release notes are copied to the system disk during
kit installation and are available as a standard text file
which may be read using the TYPE command or in an editor:

  SYS$HELP:VMS842L1I_PWDMGMT-V0200.RELEASE_NOTES

Additional documentation for the Enhanced Password Management
software is copied to the system disk during kit installation.
These are PDF files which may be read by a browser:

  SYS$HELP:PWDMGMT_RELNOTES.PDF    Contains cover letter and
                                   additional release notes for
                                   enhanced password functionality

  SYS$HELP:PWDMGMT_USERGUIDE.PDF   Contains installation, setup,
                                   and user information for
                                   enhanced password functionality
------------------------------------------------------------------
                   *** NOTE ***

  This kit requires the ACME_SERVER to be restarted
  for all functionality to be present.  Use the command:

      $ SET SERVER ACME_SERVER /RESTART

  at an appropriate time for your system configuration requirements
  as described in Section 8.3 of the PCSI kit release notes,
  SYS$HELP:VMS842L1I_PWDMGMT-V0200.RELEASE_NOTES.  Additional
  information for other post-installation steps is explained there.
------------------------------------------------------------------
```

VSI Password Management is now installed.

7. **Log out of your account and log back in** to ensure that the VSI Password Management is enabled on your system.

Important

A properly configured cluster will have a single authorization file and password policy implemented cluster-wide. If your cluster has multiple system disks, ensure that VSI Password Management software is installed on one node per system disk using steps 1-6.

1.2. Removing VSI Password Management Patch Kit

VSI Password Management is a patch kit and can be removed by using the PCSI UNDO PATCH command. Enter:

```
$ PRODUCT UNDO PATCH *
```

A menu displays a list of products that you can remove from the system. For example:

```
PRODUCT UNDO PATCH

One recovery data set has been found.  All patches listed will be rolled
 back as a unit.

The following patches have been selected to uninstall:

RECOVERY DATA SET 001 created 18-OCT-2018 14:23:42.68
   ----------------------------- --------------------------
   PATCH                         APPLIED TO
   ----------------------------- --------------------------
   VSI I64VMS PWDMGMT V1.0       VSI I64VMS VMS V8.4-2
   ----------------------------- --------------------------

Do you want to continue? [YES]

Processing RECOVERY DATA SET 001 ...
Portion done: 0%...10%...20%...30%...40%...60%...80%...90%…100%
```

Note

The ability to remove a PATCH with this command is not available once you install any other full product using the PRODUCT INSTALL command.

Chapter 2. Understanding VSI Password Management

This chapter describes the aspects of password management and components of the VSI Password Management software.

2.1. Aspects of a Password Policy

This section describes the following aspects of a password policy:

- Password length and complexity
- Password dictionary check
- Password lifetime
- Password history
- Minimum password lifetime
- Login failure behavior

2.1.1. Password Length and Complexity

The VSI Password Management kit supports generated passwords of up to 32 characters. It also supplies sample source code for a password policy module that demonstrates how to implement the following password complexity characteristics:

- The minimum number of upper-case characters in a password
- The minimum number of lower-case characters in a password
- The minimum number of special characters in a password
- The minimum number of numbers in a password
- The minimum number of categories that must be included in a password (categories include upper-case characters, lower-case characters, special characters, and numbers)
- The minimum percentage by which a password must be changed

Please refer to Appendix C for a complete list of DoD requirements that can be met by VSI OpenVMS with VSI Password Management software.

2.1.2. Password Dictionary Check

Most operating systems, including VSI OpenVMS, contain a user-modifiable **password dictionary** of the most common passwords and reject new passwords that can be found in the dictionary. OpenVMS provides a standard dictionary of English words. The system manager can supplement this list.

For more information about expanding the system password dictionary, see the section "Using Passwords to Control System Access" in the *VSI OpenVMS Guide to System Security*.

The sample DoD policy requires a dictionary lookup, but does not specify the dictionary contents.

2.1.3. Password Lifetime

Password lifetime is a rule that defines the maximum time between password changes.

The sample DoD policy requires that the password change every 60 days.

2.1.4. Password History

Password history is a rule that prevents password reuse. The operating system stores a number of hashed password values for a specified period and disallows password reuse until the age-out time has passed.

By default, OpenVMS retains the last 60 passwords for 365 days. If an OpenVMS user changes the password more than the maximum number of password history slots in the specified period, the operating system forces the user to use generated passwords.

The sample DoD policy requires the operating system to retain the last 5 passwords.

2.1.5. Minimum Password Lifetime

Minimum password lifetime is a principle that prevents users from reusing their current password simply by changing their password the number of times needed to overcome the password history limit. OpenVMS defends against this behavior by forcing the user to use generated passwords when the password history record fills. Using the defaults listed in section 2.1.4, a user who changed his or her password 61 times in 24 hours would be forced to choose a generated password on the sixty-first password change and would then be subject to generated passwords for the next 364 days.

In spite of this, if your security policy requires a minimum time between password changes, defining the system logical name LGI$PASSWORD_NOCHANGE_DAYS to a small positive integer will enforce that number of 24-hour periods before the user is allowed to change passwords.

The sample DoD policy requires a one-day minimum between password changes.

2.1.6. Login Failure Behavior

Login failure behavior covers all aspects of the password policy in response to incorrect passwords as follows:

- The number of incorrect passwords before the system disconnects a user
- The time frame in which incorrect passwords are counted
- The point at which the account is disabled when it is subjected to multiple incorrect password attempts.

The sample DoD policy requires the operating system to automatically lock an account after three unsuccessful logon attempts in 15 minutes.

2.2. Components of the VSI OpenVMS Enhanced Password Management Kit

The VSI Password Management kit includes the following components:

- Policy definition command file
- Password policy module
- Mixed-character password generator

2.2.1. Policy Definition

To define a policy, you need to run SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM to modify per-user records, SYSGEN parameters, and logical names as listed and defined in Appendix A. The command procedure changes the following system settings and logicals:

- User account parameters: SYSUAF.
- SYSGEN parameters: MODPARAMS.DAT.
- Logical names: See Appendix A for a list of logical names used by a password policy module that are modified.

2.2.2. Password Policy Module

You can define a password policy module by building and installing a policy module shareable image, naming it VMS$PASSWORD_POLICY.EXE. OpenVMS supports customer-written password policy modules to allow you to provide password rules designed specifically for your systems. VSI has supplied the source file, SYS$EXAMPLES:VMS$PASSWORD_POLICY.C, which can be used as is or as a basis for your site-specific version of SYS$EXAMPLES:VMS$PASSWORD_POLICY.EXE.

Note

VSI does not mandate the use of the supplied password policy module, nor does it overwrite any previously defined password policy module.

2.2.3. Mixed-character Password Generator

Traditionally, VMS has supported case-blind passwords from a limited character set of uppercase letters A-Z, the digits 0-9 , the dollar sign ($), and the underscore (_). User accounts may have the `PWDMIX` flag set, which enforces case-sensitivity in passwords and allows any character that can be entered from the keyboard in a valid password. The traditional OpenVMS password generator produces passwords containing only letters.

This kit supplies an additional mixed-character password generator. The new password generator is the default for `SET PASSWORD/GENERATE` for accounts with the `PWDMIX` flag set in their account record. The mixed-character generator makes no attempt to generate pronounceable or memorable passwords.

In addition, the `SET PASSWORD/GENERATE` command now supports a new qualifier, /ALGORITHM=keyword. The valid keywords are:

- ALPHABETIC
- MIXED_CHARACTER

Within the `AUTHORIZE` utility, use the ADD or MODIFY commands with the /GENERATE_PASSWORD qualifier to select either the traditional alphabetic generator or mixed-character generator.

The /GENERATE_PASSWORD qualifier uses the account's PWDMIX flag to choose between the traditional alphabetic password generator and the new mixed-character generator. Unlike DCL's SET PASSWORD/GENERATE command, the only way to select a generator is to toggle the PWDMIX flag.

For more information about the AUTHORIZE utility, see the *VSI OpenVMS System Management Utilities Reference Manual, Volume 1: A-L* .

Chapter 3. Implementing a New Password Policy

This chapter explains how to plan and implement VSI Enhanced Password software. It is important to note that VSI Password Management provides the system or security manager with three options to set up your OpenVMS password policy:

Your Situation...	This means that you...
You do not currently have or use a site-specific password policy module and do not plan to add one.	• Do not have the LGI$MIN* logical names that define password complexity rules. • Do not need to use the section of VMS$DEFINE_PASSWORD_POLICY.COM that sets those logical names. • Can use VMS$DEFINE_PASSWORD_POLICY.COM file to set user parameters and SYSGEN parameters affecting the password policy. • Do not set the SYSGEN parameter LOAD_PWD_POLICY.
You plan to use the VSI provided password policy module in SYS$EXAMPLES:.	• Should complete the password policy worksheet in its entirety. • Can define password complexity rules using the LGI$MIN* logical names. • Can use the full functionality of the VMS$DEFINE_PASSWORD_POLICY.COM file to set user parameters, SYSGEN parameters, and logical names affecting the password policy.
You have your own password policy module and want to use it with VSI Password Management software.	• Should complete the Password Policy worksheet in its entirety. • Can borrow logic from VMS$PASSWORD_POLICY.C program in SYS$EXAMPLES:. • Can only use the LGI$MIN* logical names if your password policy module makes use of them. • Can use VMS$DEFINE_PASSWORD_POLICY.COM file to set user parameters and SYSGEN parameters affecting the password policy.

3.1. Select an Optional Password Policy Module

Traditionally, the OpenVMS operating system has allowed an optional user-written password policy to check proposed new passwords against site-specific rules by creating the shareable image SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE. Within this kit, VSI provides a robust example program written in C located in the SYS$EXAMPLES: directory. Rudimentary example programs in BLISS and Ada are also supplied in the same directory.

The image must contain the following two entry points:

- *policy_plaintext* which is called with the user name and proposed password as a text string
- *policy_hash* which is called with the username and the quadword hash value of the new password.

If either policy routine returns a non-success status, the proposed password is considered to have failed policy validation.

The VSI Password Management software expands the user-written policy support in the following ways:

1. Support for a new optional routine to allow the ability to verify the amount of change between the previous password and the current proposed password. The new routine is called `policy_changes` and is called with the `old password`, `proposed new password`, and the `user name` as arguments. The routine is optional in the sense that if a password policy module is defined and this routine is not present, no error messages will be issued and the system will make no calls to `policy_changes`.

2. Addition of the following new and more focused message SS$_PWDPOLICY:

   ```
   %SYSTEM-E-PWDPOLICY, password fails policy requirements; please choose another string
   ```

3. A fully-implemented sample password policy module written in C and a pre-built image from the C sources. The example code is SYS$EXAMPLES:VMS$PASSWORD_POLICY.C. The image file is SYS$EXAMPLES:VMS$PASSWORD_POLICY.EXE

4. SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM contains support for the logical names that control the sample program. If you opt to modify or not use the VSI-supplied password policy sources or module, you may safely ignore those settings that are not applicable.

Your site may already have a policy module in operation. If so, you may wish to make modifications to your site source code to take advantage of the additional support described above. You may freely borrow from or add to the existing source code in SYS$EXAMPLES:VMS$PASSWORD_POLICY.C.

3.2. Defining a Password Policy

It is important to plan your password policy before implementing. This should be done to comply with your specific company security protocols and rules. Use the following worksheet to determine how best to implement your password policy.

Password Policy Worksheet

Policy Parameter	Value
Per-User Defined Parameter: Attributes defined for each user	
Minimum Password Length (in characters)	
Maximum Password Lifetime (in days)	
Allow Mixed-Case/Character Passwords (Y/N)	
System-Wide SYSGEN parameters: Existing SYSGEN parameters. For more information, *see HP OpenVMS System Management Utilities Reference Manual: M–Z*	
LGI_PWD_TMO: (seconds)	
LGI_RETRY_LIM: (attempts)	
LGI_RETRY_TMO: (seconds)	
LGI_BRK_LIM: (failures before triggering break-in evasion)	
LGI_BRK_TMO: (seconds added to the break-in evasion timeout)	
LGI_HID_TIM: (seconds of evasive action)	
LGI_BRK_TERM: (Boolean) Normally 0 unless system has hardwired terminals.	
LGI_BRK_DISUSER: (Boolean) Disables accounts when break-in detected. *Use caution because this can be used to mount a denial-of-service attack against the system.*	
LOAD_PWD_POLICY: (Boolean) Must be set to use loadable password policy module.	
Logical Names: Control password history and password complexity as provided by the sample password policy module provided. Unless specified, the system treats undefined logical names as zero.	
LGI$PASSWORD_NOCHANGE_DAYS (days)	
SYS$PASSWORD_HISTORY_LIFETIME (days) {default 365}	
SYS$PASSWORD_HISTORY_LIMIT (entries) {default 60}	
LGI$MIN_PASSWORD_UC_CHAR (characters)	
LGI$MIN_PASSWORD_LC_CHAR (characters)	
LGI$MIN_PASSWORD_NUMERIC (characters)	
LGI$MIN_PASSWORD_SYMBOLS (characters)	
LGI$MIN_PASSWORD_CATEGORIES (categories) Categories allows a more free-form way to get complexity. The chosen password must contain characters from at least n of the above categories. Note that *categories = 4* is equivalent to setting all 4 complexity logical names to 1.	
LGI$PWD_PERCENT_CHANGE (integer percentage) When matched on a per-character basis, at least n% of the characters must differ between the old and the new password. Rounded up.	

3.3. Using the VSI Password Management Menu

This section explains how to use the VSI Password Management Menu. Appendix B provides more examples and detailed explanations about each option.

Invoke the Password Policy menu by running VMS$DEFINE_PASSWORD_POLICY.COM located in the SYS$MANAGER: directory as in the following example:

```
$ @SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY
```

The system responds. Note that the system reports whether your system is running UAF_LOGIN or ACME_LOGIN.

```
This system is running UAF LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

Option:
```

Option 1: Summary Report to a File

Option 1 creates the file VMS$PASSWORD_POLICY_REPORT.TXT, which is a report of the current settings of password policy related per-user SYSUAF parameters, SYSGEN parameters, and logical names:

```
OpenVMS Password Policy Summary Report - 11-JAN-2019 11:37

Per-User SYSUAF Parameters:

Minimum Password Length:           15
Password Lifetime:                 30
Allow Mixed-Char Pwds:            Yes
------------------------------------------------------------
SYSGEN Parameters:

-- Login Behavior --
LGI_PWD_TMO:           30
LGI_RETRY_LIM:          3
LGI_RETRY_TMO:         20

-- Breakin Detection and Evasion --
LGI_BRK_LIM:          5
LGI_BRK_TMO:        300
LGI_HID_TIM:        300
LGI_BRK_TERM:         1 (Should be 0 for systems without
                         hardwired terminals.)
LGI_BRK_DISUSER:      0

-- User-Defined Password Policy --
LOAD_PWD_POLICY:      0
------------------------------------------------------------

Password Policy Logical Names:
```

```
-- OS Behavior --

Logical Name                    Mode Value  Table Name                 CW
------------------------------ ---- ------ -------------------------- --
LGI$PASSWORD_NOCHANGE_DAYS                  (Not defined)
SYS$PASSWORD_HISTORY_LIFETIME            365 (Default Value)
SYS$PASSWORD_HISTORY_LIMIT                60 (Default Value)

-- Password Policy Module Behavior --

Logical Name                    Mode Value  Table Name                 CW
------------------------------ ---- ------ -------------------------- --
LGI$MIN_PASSWORD_UC_CHAR                    (Not defined)
LGI$MIN_PASSWORD_LC_CHAR                    (Not defined)
LGI$MIN_PASSWORD_NUMERIC          E       4 LNM$SYSCLUSTER_TABLE       T
LGI$MIN_PASSWORD_SYMBOLS          E       4 LNM$SYSTEM_TABLE           F
LGI$MIN_PASSWORD_CATEGORIES                 (Not defined)
LGI$PWD_PERCENT_CHANGE            E      50 LNM$SYSCLUSTER_TABLE       T
```

Option 2: Per-User SYSUAF Settings

Option 2 shows the proposed policy values for controlling length, lifetime, and mixed nature of each user's password (not the logged in user's current SYSUAF settings) with the option to change the policy values as in the following example:

```
Per-User SYSUAF Parameters:

Minimum Password Length:           15
Password Lifetime:                 90
Allow Mixed-Char Pwds:            Yes

Change values? (Y/N):
```

Note

If your cluster has multiple SYSUAF.DAT files, you need to run VMS$DEFINE_PASSWORD_POLICY.COM on any system that has a separate SYSUAF.DAT file. You first need to select Option 2 (Per-User SYSUAF Settings) and Option 6 (Scan SYSUAF.DAT for non-compliant accounts).

When SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM is initially invoked, the Password Policy related Per-user SYSUAF settings are determined by the value of these fields in the SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.DAT. If you exit without saving the changes, the Per-User SYSUAF settings will not be written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_POLICY.DAT.

Option 3: SYSGEN Parameters

Option 3 provides the current values of the SYSGEN parameters with the option to change values as in the following example:

```
SYSGEN Parameters:

-- Login Behavior --
LGI_PWD_TMO:           30
```

```
LGI_RETRY_LIM:          3
LGI_RETRY_TMO:         20

-- Breakin Detection and Evasion --
LGI_BRK_LIM:            5
LGI_BRK_TMO:          300
LGI_HID_TIM:          300
LGI_BRK_TERM:           1  (Should be 0 for systems without
                            hardwired terminals.)
LGI_BRK_DISUSER:        0

-- User-Defined Password Policy --
LOAD_PWD_POLICY:        0

Change values? (Y/N):
```

Option 4: Password Policy Parameters

Option 4 provides the current values of the password policy logical names with the option to change values as in the following example:

```
Password Policy Logical Names:

-- OS Behavior --

Logical Name                    Mode Value  Table Name                 CW
------------------------------ ---- ------ -------------------------- --
LGI$PASSWORD_NOCHANGE_DAYS                  (Not defined)
SYS$PASSWORD_HISTORY_LIFETIME            365 (Default Value)
SYS$PASSWORD_HISTORY_LIMIT                60 (Default Value)

-- Password Policy Module Behavior --

Logical Name                    Mode Value  Table Name                 CW
------------------------------ ---- ------ -------------------------- --
LGI$MIN_PASSWORD_UC_CHAR                    (Not defined)
LGI$MIN_PASSWORD_LC_CHAR                    (Not defined)
LGI$MIN_PASSWORD_NUMERIC          E       4 LNM$SYSCLUSTER_TABLE       T
LGI$MIN_PASSWORD_SYMBOLS          E       4 LNM$SYSTEM_TABLE           F
LGI$MIN_PASSWORD_CATEGORIES                 (Not defined)
LGI$PWD_PERCENT_CHANGE            E      50 LNM$SYSCLUSTER_TABLE       T
```

Option 5: Save Current Settings

If you have made changes to any of the parameters, Option 5 saves the new settings. It also reports the change status of the parameters as in following example:

```
Saving SYSUAF policy parameters...
Appending SYSGEN parameters to SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT...
***
***   SYSGEN parameters must be copied to MODPARAMS.DAT
***   on each node of the cluster
***
Saving Password Policy logical names to
SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM...
3 values written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM
You may wish to add "@SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM"
```

```
to your system startup procedures.
```

Due to the specific nature of the various types of policy data, the save option writes values to three distinct locations:

1. For the Per-User SYSUAF parameters, the modified values are written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_POLICY.DAT, a data file read by VMS$DEFINE_PASSWORD_POLICY.COM. In this way, the values are preserved from one invocation of VMS$DEFINE_PASSWORD_POLICY.COM to the next. The actual work of updating SYSUAF.DAT is described in Option 6 below.

2. The SYSGEN parameters are saved by appending all of the parameters to SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT. To ensure that the parameter values are preserved across reboot, the 9 parameters must be copied to MODPARAMS.DAT on each system root on all system disks and AUTOGEN must be run on all nodes.

3. The policy logical names are written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM. To ensure the logical names are defined after a reboot, your system startup procedures should invoke this command file.

Option 6: Scan SYSUAF.DAT for non-compliant accounts

Option 6 creates a command procedure (VMS$UPDATE_UAF.COM in the current default directory) to modify your system authorization file (SYSUAF.DAT) that lists all of the non-compliant accounts on your system and provides appropriate commands to bring those accounts into compliance. It is important that you review this file before executing it to ensure that:

Note

As a rule, it is best not to modify any account that does not represent an interactive user.

---

1. The proposed changes are appropriate for each account on your system. For example, some software products may not be designed to handle longer passwords or case-sensitive passwords.

2. Forcing immediate password expiration on all modified accounts is appropriate. The VMS $UPDATE_UAF.COM procedure header contains instructions on changing the default from forcing password expiration to not forcing password expiration as shown in the following example. Note that some software accounts may not operate properly if the password is expired.

The following example shows a fragment of a sample generated command procedure:

```
$! Created by the VMS$CHECK_UAF utility on 11-JAN-2019 13:37:34.17
$!
$! Examine this procedure before execution. Only local
$! knowledge can determine if all proposed changes are
$! valid for your particular system.
$!
$! The default is to pre-expire the password of all accounts
$! modified by this procedure. To not pre-expire passords, swap
$! the comment character on the next two lines:
$ Prexpire = "/PWDEXPIRED"
$! Prexpire = ""
$!
```

```
$ Set NoOn
$ Auth := $AUTHORIZE
$!
$! Policy Parameters in effect:
$!    Password Lifetime:   90 00:00
$!    Minimum password length 15
$!    Account must allow mixed-case passwords.
.
.
.
$!******** USER1 ********
$!    PwdLiftime  non-compliant: (None)
$!    Min pwd len non-compliant: 10
$!    Account does not support mixed-case passwords.
$!
$ AUTH MOD USER1 'Prexpire'/PWDLIFETIME="90-00:00"/PWDMINIMUM=15/
FLAGS=(PWDMIX)
```

Note

If your cluster has multiple SYSUAF.DAT files you need to run VMS$DEFINE_PASSWORD_POLICY.COM on any system that has a separate SYSUAF.DAT file. You first need to select Option 2 (Per-User SYSUAF Settings) and Option 6 (Scan SYSUAF.DAT for non-compliant accounts).

Option 7: Exit (^Z)

Option 7 exits the command procedure. If you have modified parameters during this session and have not saved them, the system asks if you wish to save at this time. A **NO** answer discards any modified changes.

3.4. Implementing the Policy on the System

This section provides a checklist to properly analyze your site's current password policies.

1. Select a password policy module. See Section 3.1.

   - If you are building a password policy module, copy the necessary source to somewhere other than the SYS$EXAMPLES: directory. The supplied source files may be replaced by future upgrades or patch kits. Moving the files to another location ensures they will not be overwritten.
   - Instructions for building the policy shareable image are documented in the header comments of VMS$PASSWORD_POLICY.C.
   - If you have an existing custom password policy program, you can use logic from SYS$EXAMPLES:VMS$PASSWORD_POLICY.C to take advantage of new features introduced by the VSI Enhanced Password Management software.
   - You will need to build one copy of the password policy module for each architecture in your cluster: Itanium and Alpha.
   - Do not copy the new image to SYS$LIBRARY: at this time. (This is addressed in Step 11 below.)

2. Complete the password policy worksheet in Section 3.2.

3. Execute the VSI Password Management command procedure by entering:

   ```
   @SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY
   ```

4. Select Option 1: Summary Report to a File. Examine the generated report, VMS$PASSWORD_POLICY_REPORT.TXT, to compare existing policy values against the password policy worksheet completed in Step 2 above.

Note

Using values from the policy worksheet that are not the default may influence the password policy source code.

---

5. Based on your worksheet values, perform the following steps:

   a. Choose Options 2-4 in VMS$DEFINE_PASSWORD_POLICY.COM to change parameters as defined in your worksheet.

      i. If you were not previously using a password policy module, set the SYSGEN parameter LOAD_PWD_POLICY to 1.

      ii. If you want to disable a password policy module, set the SYSGEN parameter LOAD_PWD_POLICY to 0.

   b. Choose Option 5 in VMS$DEFINE_PASSWORD_POLICY.COM to save modified values.

   c. Choose Option 6 in VMS$DEFINE_PASSWORD_POLICY.COM to scan SYSUAF for non-compliant accounts.

6. Perform the necessary post-save operations as documented in Option 5: Save Current Settings. See Section 3.3.

   - If SYSGEN changes were made, the changes should be made on all other nodes in the OpenVMS cluster. Add the needed SYSGEN changes to SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT.

     To see the parameters so that you can add them to the other MODPARAMS.DAT files, use the DIFF command on the cluster member where SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM was run:

     ```
     $ DIFF SYS$SYSTEM:MODPARAMS.DAT
     ```

   - If any new logical names were defined by VMS$DEFINE_PASSWORD_POLICY.COM, add the following command to your system startup (e.g. SYS$MANAGER:SYLOGICALS.COM):

     ```
     $ @SYS$MANAGER:VMS$DEFINE_PASSWORD_LOGICALS.COM
     ```

     This ensures the password policy related logical names are redefined following a system reboot.

7. Perform the file review of VMS$UPDATE_UAF.COM containing non-compliant accounts, editing it as explained in Appendix B. Once you are satisfied with your edits, execute VMS$UPDATE_UAF.COM to perform the required modifications.

8. **IMPORTANT:** Notify users of pending changes. The following aspects of implementing a password policy may have significant impact on the user experience:

   - New minimum password lengths and expiration times.
   - Expiration of passwords for all modified accounts.
   - Users who are switching from not having the PWDMIX flag set to having the PWDMIX flag set need to enter their current password in upper case and all subsequent passwords in matching case.

     Note that there are consequences to changing an account from PWDMIX set to PWDMIX clear. It is usually necessary to set the user's password to an all-uppercase value at the same time.
   - Setting PWDMIX implies use of the mixed-character password generator by default.

9. Ensure that the relevant SYSGEN parameters (ACTIVE and CURRENT) are consistent across all cluster members.

Note

Unless you are currently using a password policy module, do not set LOAD_PWD_POLICY to 1 in the ACTIVE parameters at this time. See Step 14.

---

10. **IMPORTANT:** Ensure that all password policy-related logical names are defined cluster-wide.

11. On each system disk, copy the architecture-appropriate version of VMS$PASSWORD_POLICY.EXE to SYS$COMMON:[SYSLIB] as follows:

```
$ COPY VMS$PASSWORD_POLICY.EXE SYS$COMMON:[SYSLIB]/PROT=(W:RE)
```

12. **IMPORTANT:** The three global routines used by SET PASSWORD let you obtain the user's original password in plaintext, the proposed new plaintext password, and its equivalent quadword hash value. All security administrators should be aware of this feature because its subversion by a malicious privileged user will compromise the system's security.

    VSI recommends that security auditing and alarms be placed on the policy module shareable image to ensure that any changes to this function are made visible to the security administrator as in the following examples. For more information, see the *OpenVMS Guide to System Security*.

```
$ SET SECURITY/ACL=(AUDIT=SECURITY,ACCESS=W+D+C+S) -
   SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE

$ SET SECURITY/ACL=(ALARM=SECURITY,ACCESS=W+D+C+S) -
   SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE

$ SET SECURITY/ACL=(AUDIT=SECURITY,ACCESS=W+D+C+S) -
   SYS$COMMON:[000000]SYSLIB.DIR

$ SET SECURITY/ACL=(ALARM=SECURITY,ACCESS=W+D+C+S) -
   SYS$COMMON:[000000]SYSLIB.DIR

$ SET SECURITY/ACL=(AUDIT=SECURITY,ACCESS=W+D+C+S) -
   SYS$SPECIFIC:[000000]SYSLIB.DIR

$ SET SECURITY/ACL=(ALARM=SECURITY,ACCESS=W+D+C+S) -
```

```
SYS$SPECIFIC:[000000]SYSLIB.DIR
```

13. On each node of the cluster, run the INSTALL utility as follows:

```
$ INSTALL ADD SYS$LIBRARY:VMS$PASSWORD_POLICY/OPEN/HEAD/SHARE
```

Note

If you already have a policy module installed, use the REPLACE command (instead of ADD).

14. If you were not previously using a password policy module, on each node set the ACTIVE SYSGEN parameter LOAD_PWD_POLICY to 1.

15. Restart the ACME server.

```
$ SET SERVER ACME/RESTART
```

Note

The ACME server must be restarted any time a password policy module is updated and installed even if you are not using ACME Login. Some parts of the system call ACME directly via the SYS$ACM system service.

16. You may want to add the following code snippet to the end of your SYSTARTUP_VMS.COM. This step is optional if it is already addressed in your system start up files, or if a password policy module is not needed.

```
$ if f$getsyi("LOAD_PWD_POLICY")
$ then
$  if f$search("SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE") .nes. ""
$  then
$   if .not. -
$_  f$file_attributes("SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE","KNOWN")
$   then
$    INSTALL ADD SYS$LIBRARY:VMS$PASSWORD_POLICY.EXE/OPEN/HEADER/SHARE
$    endif
$   endif
$ SET SERVER ACME/RESTART
$ endif
```

Appendix A. Definitions of Enhanced Password Policy Parameters

This appendix provides the list of parameters and their definitions used by the Enhance Password Management software to set a password policy.

Table A.1. Password Policy Settings

Parameter Name	Definition
Per-User SYSUAF Settings	
Minimum Password Length:	Number of characters in the password.
Password Lifetime:	Lifetime of password in days.
Allow Mixed-Char Pwds:	Mixed-character allowed (true or false)
Password Policy SYSGEN Parameters	
LGI_PWD_TMO	LGI_PWD_TMO specifies, in seconds, the period of time a user has to enter the correct system password (if used). LGI_PWD_TMO also establishes the timeout period for users to enter their personal account passwords at login time. Also, when using the SET PASSWORD command, LGI_PWD_TMO specifies the period of time the system waits for a user to type in a new password, an old password, and the password verification. LGI_PWD_TMO is a DYNAMIC parameter.
LGI_RETRY_LIM	LGI_RETRY_LIM specifies the number of retry attempts allowed users attempting to log in. If this parameter is greater than 0, and a legitimate user fails to log in correctly because of typing errors, the user does not automatically lose the carrier. Instead (provided that LGI_RETRY_TMO has not elapsed), by pressing the Return key, the user is prompted to enter the user name and password again. Once the specified number of attempts has been made without success, the user loses the carrier. As long as neither LGI_BRK_LIM nor LGI_BRK_TMO has elapsed, the user can dial in again and reattempt login. LGI_RETRY_LIM is a DYNAMIC parameter.
LGI_BRK_LIM	LGI_BRK_LIM specifies the number of failures that can occur at login time before the system takes action against a possible break-in. The count of failures applies independently to login attempts by each user name, terminal, and node. Whenever login attempts from any of these sources reach the break-in limit specified by LGI_BRK_LIM, the system assumes it is under attack and initiates evasive action as specified by the LGI_HID_TIM parameter.

Parameter Name	Definition
	The minimum value is 1. The default value is usually adequate. LGI_BRK_LIM is a DYNAMIC parameter.
LGI_BRK_TMO	LGI_BRK_TMO specifies the length of the failure monitoring period. This time increment is added to the suspect's expiration time each time a login failure occurs. Once the expiration period passes, prior failures are discarded, and the suspect is given a clean slate. LGI_BRK_TMO is a DYNAMIC parameter.
LGI_HID_TIM	LGI_HID_TIM specifies the number of seconds that evasive action persists following the detection of a possible break-in attempt. The system refuses to allow any logins during this period, even if a valid user name and password are specified. LGI_HID_TIM is a DYNAMIC parameter.
LGI_BRK_TERM	LGI_BRK_TERM causes the terminal name to be part of the association string for the terminal mode of break-in detection. When LGI_BRK_TERM is set to off (0), the processing considers the local or remote source of the attempt, allowing break-in detection to correlate failed access attempts across multiple terminal devices. When set to on (1), LGI_BRK_TERM assumes that only local hard-wired or dedicated terminals are in use and causes breakin detection processing to include the specific local terminal name when examining and correlating break-in attempts. Ordinarily, LGI_BRK_TERM should be set to off (0) when physical terminal names are created dynamically, such as when network protocols like LAT and Telnet are in use. LGI_BRK_TERM is a DYNAMIC parameter.
LGI_BRK_DISUSER	LGI_BRK_DISUSER turns on the DISUSER flag in the UAF record when an attempted break-in is detected, thus permanently locking out that account. The parameter is off (0) by default. You should set the parameter (1) only under extreme security watch conditions, because it results in severely restricted user service. LGI_BRK_DISUSER is a DYNAMIC parameter.
LOAD_PWD_POLICY	LOAD_PWD_POLICY controls whether the SET PASSWORD command attempts to use site-specific password policy routines, which are contained in the shareable image SYS$LIBRARY:VMS$PASSWORD_ POLICY.EXE.

Parameter Name	Definition
	The default is 0, which indicates not to use policy routines.
Password Policy Logical Names	
LGI$PASSWORD_NOCHANGE_DAYS	The minimum number of 24-hour periods that must pass before a password change is allowed. The default is undefined, which is equivalent to 0 days. This parameter is used mostly to attempt to prevent users from overrunning the password history list, however the OpenVMS password history list is both deep (60 values) and long-lived (365 days) by default and filling the history record forces the user into generated passwords. Unless your security policy requires a non-zero value, the OpenVMS defaults should provide adequate security. See also SYS$PASSWORD_HISTORY_LIFETIME and SYS$PASSWORD_HISTORY_LIMIT.
SYS$PASSWORD_HISTORY_LIFETIME	Number of days for password history entries to age out. Default is 365. Allowed range is 1 to 28000 days. **Note** SYS$PASSWORD_HISTORY_LIFETIME must be larger than the UAF parameter PWDLIFETIME. If you set the SYS$PASSWORD_HISTORY_LIFETIME value to less than PWDLIFETIME, passwords will expire out of the history file before they expire in SYSUAF. This defeats the purpose of the password history file. There is a correspondence between the lifetime of a password history list and the number of passwords allowed on the list. For example, if you increase the password history lifetime to 4 years and your passwords expire every 2 weeks, you would need to increase the password history limit to at least 104 (4 years times 26 passwords a year). The password history lifetime and limit can be changed dynamically, but they should be consistent across all nodes on the cluster. Sites using secondary passwords may need to double the password limit to account for the secondary password storage. See also SYS$PASSWORD_HISTORY_LIMIT.
SYS$PASSWORD_HISTORY_LIMIT	The number of previous password entries per user kept in the password history file. Default is 60 entries. Allowed range is 1 to 2000 entries.

Parameter Name	Definition
	There is a correspondence between the lifetime of a password history list and the number of passwords allowed on the list. For example, if you increase the password history lifetime to 4 years and your passwords expire every 2 weeks, you would need to increase the password history limit to at least 104 (4 years times 26 passwords a year). The password history lifetime and limit can be changed dynamically, but they should be consistent across all nodes on the cluster. Sites using secondary passwords may need to double the password limit to account for the secondary password storage. See also SYS$PASSWORD_HISTORY_LIFETIME.
LGI$MIN_PASSWORD_UC_CHAR	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source form in SYS$EXAMPLES:. If defined as a (small) positive integer, the password policy module will require a new password to have at least that many upper case characters when a password is changed. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS$PASSWORD_POLICY is not installed and enabled, defining this logical has no effect.
LGI$MIN_PASSWORD_LC_CHAR	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source form in SYS$EXAMPLES:. If defined as a (small) positive integer, the password policy module will require a new password to have at least that many lower case characters when a password is changed. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS$PASSWORD_POLICY is not installed and enabled, defining this logical has no effect.
LGI$MIN_PASSWORD_NUMERIC	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source form in SYS$EXAMPLES:. If defined as a (small) positive integer, the password policy module will require a new password to have at least that many digits (0-9) characters when a password is changed. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS$PASSWORD_POLICY is not installed and enabled, defining this logical has no effect.
LGI$MIN_PASSWORD_SYMBOLS	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source

Parameter Name	Definition
	form in SYS$EXAMPLES:. If defined as a (small) positive integer, the password policy module will require a new password to have at least that many non-alphanumeric (other than A-Za-z0-9) characters when a password is changed. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS$PASSWORD_POLICY is not installed and enabled, defining this logical has no effect.
LGI$MIN_PASSWORD_CATEGORIES	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source form in SYS$EXAMPLES:. If defined as a (small) positive integer, the password policy module will require a new password to contain characters from at least that many characters. The maximum value is 4. The four categories are upper case, lower case, numeric and symbols. This logical name allows for a more flexible password complexity policy than setting specific category targets. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS $PASSWORD_POLICY is not installed and enabled, defining this logical has no effect.
LGI$PWD_PERCENT_CHANGE	Logical name supported by the example VMS$PASSWORD_POLICY supplied in C source form in SYS$EXAMPLES:. If defined as a positive integer from zero to 100, the SET PASSWORD command will verify that the characters in each position change when matching the new password against the old password. At startup this logical is undefined, which makes it equivalent to 0 and is therefore ignored. If VMS$PASSWORD_POLICY is not installed and enabled, defining this logical has no effect. For example, user with a 15-character minimum password length and LGI$PWD_PERCENT_CHANGE defined as 50 [percent]. The code will check that at least 8 (50% rounded up) characters have changed. See the following table.

Old Password	Proposed New	Changes	Passes?
OldMacDonald123	OldMacDonald124	1	No
OldMacDonald123	HadAFarm1234567	15	Yes
OldMacDonald123	3OldMacDonald12	15	Yes

OldMacDonald123	NewMacDonald321	6	No

Appendix B. Enhanced Password Menu Examples

This appendix provides examples that you may find helpful when using the Enhanced Password Menu.

Note

During the current session, if you have changed any values for Options 2, 3, and 4, the system displays the following message:

```
*** Modified, but as-yet-unsaved parameters exist in this session. ***
```

If you choose to Exit the command procedure (using Option 7), you will receive the following message:

```
Option: 7
*** Modified, but as-yet-unsaved parameters exist in this session. ***

Option: *EXIT*
*** Modified parameters have not been saved! Save them now? (Y/N):
```

Not saving the parameters at this time discards all of your setting and returns parameter settings to those values set prior to running the command procedure.

Option 1: Summary Report to a File

Option 1 creates the file VMS$PASSWORD_POLICY_REPORT.TXT, which is a report of the current settings of password policy related to Per-User SYSUAF parameters, SYSGEN parameters, and logical names

```
This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)


*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option: 1
Summary report written to SYS$SYSDEVICE:[ADMIN]VMS
$PASSWORD_POLICY_REPORT.TXT;1
<cr> to continue
```

The following example shows the contents of VMS$PASSWORD_POLICY_REPORT.TXT:

```
$ TYPE VMS$PASSWORD_POLICY_REPORT.TXT
```

```
OpenVMS Password Policy Summary Report - 12-OCT-2018 14:12

This system is running ACME LOGIN.

Per-User Parameters:

Minimum Password Length:           15
Password Lifetime:                100
Allow Mixed-Char Pwds:            Yes
------------------------------------------------------------------
SYSGEN Parameters:

-- Login Behavior --
LGI_PWD_TMO:           30
LGI_RETRY_LIM:          3
LGI_RETRY_TMO:         20

-- Breakin Detection and Evasion --
LGI_BRK_LIM:            5
LGI_BRK_TMO:          300
LGI_HID_TIM:          300
LGI_BRK_TERM:           0
LGI_BRK_DISUSER:        0

-- User-Defined Password Policy --
LOAD_PWD_POLICY:        1
  Policy Image: SYS$COMMON:[SYSLIB]VMS$PASSWORD_POLICY.EXE;1  (installed)
------------------------------------------------------------------
Password Policy Logical Names:

-- OS Behavior --

Logical Name                    Mode Value     Table Name             CW
------------------------------ ---- --------- ---------------------- --
LGI$PASSWORD_NOCHANGE_DAYS                    (Not defined)
SYS$PASSWORD_HISTORY_LIFETIME           365   (Default Value)
SYS$PASSWORD_HISTORY_LIMIT               60   (Default Value)

-- Password Policy Module Behavior --

Logical Name                    Mode Value     Table Name             CW
------------------------------ ---- --------- ---------------------- --
LGI$MIN_PASSWORD_UC_CHAR          E       1    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_LC_CHAR                  1    *modified*
LGI$MIN_PASSWORD_NUMERIC          E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_SYMBOLS          E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_CATEGORIES               (Not defined)
LGI$PWD_PERCENT_CHANGE            E      50    LNM$SYSCLUSTER_TABLE    T
```

When SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM is initially invoked, the Password Policy related Per-user SYSUAF settings are determined by the value of these fields in the SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.DAT.

The Password Policy related SYSGEN parameters and Logical Names are determined by examining the live system. When settings are changed via Option 2 (Per-User SYSUAF Settings), Option 3 (SYSGEN Parameters) and Option 4 (Password Policy Logical Names), these changes will be reflected in the Summary Report even if the changes have not been applied to the live system.

Option 2: Per-User SYSUAF Settings

Option 2 provides settings controlling length, lifetime, and mixed nature of the user's password in the SYSUAF.DAT file with the option to change values as in the following example. The settings specified will affect the outcome of Option 6 (Scan SYSUAF.DAT for non-compliant accounts).

```
VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)


*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option: 2

Per-User Parameters:

Minimum Password Length:          10
Password Lifetime:               100
Allow Mixed-Char Pwds:           Yes

Change values? (Y/N): Y
Minimum Password Length [10]: 15
Maximum Password Lifetime (Days) [100]:
Allow mixed-character passwords (Y/N) [Y]:

Per-User Parameters:

Minimum Password Length:          15
Password Lifetime:               100
Allow Mixed-Char Pwds:           Yes

Modified values

<cr> to continue

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)


*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option:
```

When SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM is initially invoked, the Password Policy related Per-User SYSUAF settings are determined by the value of these fields in the SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.DAT. If you exit without saving the changes, the Per-User SYSUAF settings will not be written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_POLICY.DAT.

The first time SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM is run and SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.DAT does not exist, a set of default parameters is used.

Option 3: SYSGEN Parameters

Option 3 displays the current values of the Password Policy related SYSGEN parameters with the option to change values as in the following example:

```
$ @SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

Option: 3

SYSGEN Parameters:

-- Login Behavior --
LGI_PWD_TMO:           30
LGI_RETRY_LIM:          4
LGI_RETRY_TMO:         20

-- Breakin Detection and Evasion --
LGI_BRK_LIM:            5
LGI_BRK_TMO:          300
LGI_HID_TIM:          300
LGI_BRK_TERM:           0
LGI_BRK_DISUSER:        0

-- User-Defined Password Policy --
LOAD_PWD_POLICY:        1
  Policy Image: SYS$COMMON:[SYSLIB]VMS$PASSWORD_POLICY.EXE;1  (installed)

Change values? (Y/N):
```

If you respond NO to the "Change values? (Y/N)” question, no parameters will be changed, and you will be returned to the main menu. If you respond YES to this question, you will be prompted, one parameter at a time, to enter a new value for each SYSGEN parameter. Simply pressing the ENTER key without entering any value will leave the current value, shown in brackets, unchanged. When the value for the last parameter, which is the LOAD_PWD_POLICY, is entered, the screen will be cleared

and the proposed changes will then be displayed, and you will be asked “Update active and current SYSGEN parameters? (Y/N)”:

```
Change values? (Y/N): Y

Type ? for help with any parameter

LGI_PWD_TMO? [30]
LGI_RETRY_LIM? [3] 4   <-- (note this parameter is being changed)
LGI_RETRY_TMO? [20]
LGI_BRK_LIM? [5]
LGI_BRK_TMO? [300]
LGI_HID_TIM? [300]
LGI_BRK_TERM? [0]
LGI_BRK_DISUSER? [0]
LOAD_PWD_POLICY? [0] 1  <-- (note this parameter is being changed)
                            (screen clears here)

SYSGEN Parameters:

-- Login Behavior --
LGI_PWD_TMO:           30
LGI_RETRY_LIM:          4
LGI_RETRY_TMO:         20

-- Breakin Detection and Evasion --
LGI_BRK_LIM:            5
LGI_BRK_TMO:          300
LGI_HID_TIM:          300
LGI_BRK_TERM:           0
LGI_BRK_DISUSER:        0

-- User-Defined Password Policy --
LOAD_PWD_POLICY:        1
  Policy Image: SYS$COMMON:[SYSLIB]VMS$PASSWORD_POLICY.EXE;1  (installed)

Update active and current SYSGEN parameters? (Y/N): Y
Update cluster-wide? (Y/N): N
```

If the system is a member of a cluster and you respond YES to the question “Update active and current SYSGEN parameters? (Y/N)”, the command procedure will next ask you “Update cluster-wide? (Y/N)”. Based on your response to these 2 questions the command procedure will display the outcome of changing the ACTIVE and CURRENT SYSGEN parameters:

Note

Users may see repeated values in the system display for ACTIVE and CURRENT SYSGEN parameters, as shown in the following example. This is expected behavior. The system displays all of the values that have been changed cluster-wide.

```
Updating ACTIVE SYSGEN parameters...

Updating CURRENT SYSGEN parameters...
Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_PWD_TMO           30         30     0      255      Sec       D
```

```
Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_RETRY_LIM          4          3     0      255      Tries     D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_RETRY_TMO         20         20     2      255      Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_BRK_LIM            5          5     1      255      Fails     D

Parameter Name   Current    Default    Min     Max      Unit      Dynamic
--------------   -------    -------    ---     ---      ----      -------
LGI_BRK_TMO          300        300      0   5184000    Sec       D

Parameter Name   Current    Default    Min     Max      Unit      Dynamic
--------------   -------    -------    ---     ---      ----      -------
LGI_HID_TIM          300        300      0  1261440000  Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_BRK_TERM           0          1     0        1      Boolean   D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_BRK_DISUSER        0          0     0        1      Boolean   D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LOAD_PWD_POLICY        1          0     0        1      Boolean   D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_PWD_TMO           30         30     0      255      Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_RETRY_LIM          4          3     0      255      Tries     D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_RETRY_TMO         20         20     2      255      Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_BRK_LIM            5          5     1      255      Fails     D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_BRK_TMO          300        300     0    5184000    Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
--------------   -------    -------   ---      ---      ----      -------
LGI_HID_TIM          300        300     0   1261440000  Sec       D

Parameter Name   Current    Default   Min      Max      Unit      Dynamic
```

```
--------------   -------    -------   ---     ---       ----      -------
LGI_BRK_TERM           0          1     0      1        Boolean   D

Parameter Name   Current    Default   Min     Max       Unit      Dynamic
--------------   -------    -------   ---     ---       ----      -------
LGI_BRK_DISUSER        0          0     0       1       Boolean   D

Parameter Name   Current    Default   Min     Max       Unit      Dynamic
--------------   -------    -------   ---     ---       ----      -------
LOAD_PWD_POLICY        1          0     0       1       Boolean   D
<cr> to continue

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)


*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option:
```

Option 4: Password Policy Logical Names

Option 4 provides the current values of the Password Policy related Logical Names with the option to change values as in the following example. Note that all logicals defined by this procedure will be cluster-wide logicals placed in the LNM$SYSCLUSTER_TABLE. Any of the logicals can be changed dynamically and should be consistent across all nodes on a cluster.

```
$ @VMS$DEFINE_PASSWORD_POLICY.COM

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

Option: 4

Password Policy Logical Names:

-- OS Behavior --
```

```
Logical Name                    Mode Value     Table Name            CW
------------------------------ ---- --------- --------------------- --
LGI$PASSWORD_NOCHANGE_DAYS                    (Not defined)
SYS$PASSWORD_HISTORY_LIFETIME           365   (Default Value)
SYS$PASSWORD_HISTORY_LIMIT               60   (Default Value)

-- Password Policy Module Behavior --

Logical Name                    Mode Value     Table Name             CW
------------------------------ ---- --------- ---------------------- --
LGI$MIN_PASSWORD_UC_CHAR          E       1    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_LC_CHAR          E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_NUMERIC          E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_SYMBOLS          E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_CATEGORIES                    (Not defined)
LGI$PWD_PERCENT_CHANGE            E      50    LNM$SYSCLUSTER_TABLE    T

Change values? (Y/N):
```

If you respond NO to the “Change values? (Y/N) question":, you will be returned to Main Menu. If you respond YES to this question, you will be given the opportunity to modify each logical name. Enter return if no change is desired for a particular logical name.

```
Enter ? for help.

LGI$PASSWORD_NOCHANGE_DAYS? ():
SYS$PASSWORD_HISTORY_LIFETIME? (365):
SYS$PASSWORD_HISTORY_LIMIT? (60):
LGI$MIN_PASSWORD_UC_CHAR? (1):
LGI$MIN_PASSWORD_LC_CHAR? (0): 1  <-- (note this parameter is being changed)
LGI$MIN_PASSWORD_NUMERIC? (0):
LGI$MIN_PASSWORD_SYMBOLS? (0):
LGI$MIN_PASSWORD_CATEGORIES? ():
LGI$PWD_PERCENT_CHANGE? (50):

Update any modified logical names? (Y/N): y
```

If you do not want to update the logicals on the live system, respond NO to the question “Update any modified logical names? (Y/N)”. If you answer YES, the display will mention which previously defined logicals were updated.

```
Updating LGI$MIN_PASSWORD_LC_CHAR ...
%DCL-I-SUPERSEDE, previous value of LGI$MIN_PASSWORD_LC_CHAR has been superseded
```

The current values of the logical names are then redisplayed. Note that if you answered NO to the question “Update any modified logical names? (Y/N)”, the redisplay will reflect the changes made to the logicals in the procedure which were never defined on the live system. If you do not like these settings, re-execute Option 4 to fix the settings.

```
Password Policy Logical Names:

-- OS Behavior --

Logical Name                    Mode Value     Table Name             CW
------------------------------ ---- --------- ---------------------- --
LGI$PASSWORD_NOCHANGE_DAYS                    (Not defined)
SYS$PASSWORD_HISTORY_LIFETIME           365   (Default Value)
SYS$PASSWORD_HISTORY_LIMIT               60   (Default Value)
```

```
-- Password Policy Module Behavior --

Logical Name                     Mode Value     Table Name             CW
-------------------------------- ---- --------- ---------------------- --
LGI$MIN_PASSWORD_UC_CHAR           E       1    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_LC_CHAR           E       1    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_NUMERIC           E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_SYMBOLS           E       0    LNM$SYSCLUSTER_TABLE    T
LGI$MIN_PASSWORD_CATEGORIES                     (Not defined)
LGI$PWD_PERCENT_CHANGE             E      50    LNM$SYSCLUSTER_TABLE    T
<cr> to continue:


This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)


*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option:
```

To ensure the logicals are defined properly at system boot time execute Option 5 (Save Current Settings). This will cause the current settings of the Password Policy related Logical Names to be written to SYS$COMMON:[SYSMGR] VMS$DEFINE_PASSWORD_LOGICALS.COM on the system where the VMS$DEFINE_PASSWORD_POLICY.COM command procedure was invoked. The VMS$DEFINE_PASSWORD_LOGICALS.COM command procedure is designed to be invoked by SYS$MANAGER:SYLOGICALS.COM at system startup by adding the following command to SYLOGICALS.COM:

```
$ @SYS$MANAGER:VMS$DEFINE_PASSWORD_LOGICALS.COM
```

Option 5: Save Current Settings

Option 5 performs the SAVE function and reports the outcome of the SAVE operation. It displays an appropriate message similar to the following when no changes are required:

```
VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

Option: 5
No change in SYSUAF parameters. No save operation required.
```

```
No change in SYSGEN parameters. No save operation required.
Password Policy logical names unchanged.  No save operation required.
<cr> to continue
```

If any modifications have been detected in Per-User SYSUAF settings, SYSGEN parameters, or Password Policy logical names, this option saves the modified settings. What is actually saved depends on what was changed. Modified Per-User SYSUAF settings is written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_POLICY.DAT. By storing the values in this file, the current Per-User SYSUAF settings are available the next time the VMS$DEFINE_PASSWORD_POLICY.COM command procedure is invoked. See the following example of what is displayed when only Per-User SYSUAF settings are modified:

```
Option: 5
Saving SYSUAF policy parameters...
No change in SYSGEN parameters. No save operation required.
Password Policy logical names unchanged.  No save operation required.
<cr> to continue
```

Modified SYSGEN parameters causes the SAVE function to append the current settings of Password Policy related SYSGEN parameters to the SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT file. This change is only applied to the system where the SYS$MANAGER:VMS$DEFINE_PASSWORD_POLICY.COM procedure was invoked. The SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT file on all other nodes in a cluster need to be manually updated to reflect any SYSGEN parameters changes made cluster-wide. See the following example of what is displayed when only SYSGEN parameters are modified:

```
VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option: 5
No change in SYSUAF parameters. No save operation required.
Appending SYSGEN parameters to SYS$SPECIFIC:[SYSEXE]MODPARAMS.DAT...***
*** SYSGEN parameters must be copied to MODPARAMS.DAT on each node of the cluster ***

Password Policy logical names unchanged.  No save operation required.
<cr> to continue
```

When Password Policy related Logical Names are modified, the SAVE function creates the command procedure SYS$COMMON:[SYSMGR]SYS$VMS$DEFINE_PASSWORD_LOGICALS.COM reflecting the current settings defined in Option 4 of the procedure. The following example shows what is displayed when only Password Policy related Logical Names are modified

```
VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)
```

```
*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option: 5
No change in SYSUAF parameters. No save operation required.
No change in SYSGEN parameters. No save operation required.
Saving Password Policy logical names to SYS$COMMON:[SYSMGR]VMS
$DEFINE_PASSWORD_LOGICALS.COM...
5 values written to SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM
You may wish to add "@SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM"
 to your system startup procedures.
<cr> to continue
```

The SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM procedure is designed to be invoked by SYS$MANAGER:SYLOGICALS.COM. The following example shows the file contents of this command procedure.

```
$ TYPE SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM
! ----  SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM  ----
! created by VMS$DEFINE_PASSWORD_POLICY.COM on  6-OCT-2018 23:42:54.69

$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 90 SYS$PASSWORD_HISTORY_LIMIT
$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 1 LGI$MIN_PASSWORD_UC_CHAR
$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 0 LGI$MIN_PASSWORD_LC_CHAR
$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 0 LGI$MIN_PASSWORD_NUMERIC
$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 0 LGI$MIN_PASSWORD_SYMBOLS
$ ASSIGN/CLUSTER/EXECUTIVE_MODE/NAME_ATTRIBUTES=NO_ALIAS 50 LGI$PWD_PERCENT_CHANGE
```

Note that if in Option 4 you answered NO to the question “Update any modified logical names? (Y/N)”, the logical definitions in VMS$DEFINE_PASSWORD_LOGICALS.COM will differ from the live system.

To ensure SYS$COMMON:[SYSMGR]VMS$DEFINE_PASSWORD_LOGICALS.COM is invoked during system startup, add the following command to SYS$MANAGER:SYLOGICALS.COM. Make sure that this command procedure is invoked on every node in a cluster.

```
$ @SYS$MANAGER:VMS$DEFINE_PASSWORD_LOGICALS.COM
```

Option 6: Scan SYSUAF.DAT

Option 6 creates the command procedure VMS$UPDATE_UAF.COM that contains the AUTHORIZE commands for fixing all accounts that do not meet your current password policy settings. It uses the current Per-User SYSUAF settings defined in Option 2 for determining the criteria to use. The system displays something similar to the following example when you select YES to the question "Scan SYSUAF for non-compliant accounts using these values?”.

```
$ @VMS$DEFINE_PASSWORD_POLICY.COM

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

Option: 6
```

```
Per-User Parameters:

Minimum Password Length:          15
Password Lifetime:               100
Allow Mixed-Char Pwds:           Yes

Scan SYSUAF for non-compliant accounts using these values? yes
Maximum password lifetime: "100-"
Minimum password length: 15
Mixed password required: 1
19 records written to $1$DGA1:[ADMIN]VMS$UPDATE_UAF.COM;

<cr> to continue
```

It is important that you review the VMS$UPDATE_UAF.COM file to ensure that:

1. Your choices meet your site password policy.
2. You want to implement that policy for every account on the system. Based on site needs, you may want to exclude certain accounts from inclusion in the password policy.

Note

If your cluster has multiple SYSUAF.DAT files, you need to run VMS$DEFINE_PASSWORD_POLICY.COM on every system disk with its own SYSUAF.DAT file. You first need to select Option 2 (Per-User SYSUAF Settings) and Option 6 (Scan SYSUAF.DAT for non-compliant accounts).

Option 7: Exit (^Z)

Option 7 indicates that you want to exit the command procedure. If there are unsaved changes, you will see the following message and prompt that allows you to save the changes before exiting the command procedure when you use ^Z to exit instead of typing the number 7.

```
$ @VMS$DEFINE_PASSWORD_POLICY.COM

This system is running ACME LOGIN.

VMS$DEFINE_PASSWORD_POLICY Main Menu:

 1)     Summary Report to a file
 2)     Per-User SYSUAF Settings
 3)     SYSGEN Parameters
 4)     Password Policy Logical Names
 5)     Save Current Settings
 6)     Scan SYSUAF.DAT for non-compliant accounts
 7)     Exit (^Z)

*** Modified, but as-yet-unsaved parameters exist in this session. ***
Option: 7
Option: *EXIT*
*** Modified parameters have not been saved!  Save them now? (Y/N):
```

Answer NO if you do not want to save any changes. Answer YES to save all changes. The SAVE operation will function identically to Option 5 (Save Current Settings). To learn more about what is saved, refer to the section the section called “Option 5: Save Current Settings” in this appendix.

Appendix C. DoD Password Policy Requirements as Provided by VSI

In 2017, NIST (National Institute of Standards and Technology) significantly modified their policy on memorized secrets (passwords). For more information about changes in the policy, see the Memorized Secret Authenticators section in the NIST Special Publication 800-63B.

This appendix contains the DoD password policy requirements with each item categorized by its implementation in the VSI Password Management software.

1. OpenVMS provides by default. No management action required.
2. OpenVMS provides, but requires management of system or UAF settings.
3. Requirements provided by VSI Password Management software.
4. Not possible to provide in the base operating system. These items may be possible with 3rd-party software.
5. Outside the scope of VSI Password Management.

DoD Requirements by VSI Password Management Category
A. OpenVMS provides by default. No management action required.
1. The operating system must store only encrypted representations of passwords.
2. The operating system must prohibit password reuse for a minimum of five generations.
3. The operating system must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
4. The operating system must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
5. The operating system must allow the use of a temporary password for system logons with an immediate change to a permanent password.
6. The operating system must prevent the use of dictionary words for passwords.
B. OpenVMS provides, but requires management of system or UAF settings.
1. The operating system must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period
2. The operating system must transmit only encrypted representations of passwords.
3. Operating systems must enforce 24 hours/1 day as the minimum password lifetime.
4. Operating systems must enforce a 60-day maximum password lifetime restriction.
5. The operating system must enforce a minimum 15-character password length.
6. The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes occur.

DoD Requirements by VSI Password Management Category
C. Requirements provided by the VSI Password Management software.
1. The operating system must enforce password complexity by requiring that at least one upper-case character be used. 2. The operating system must enforce password complexity by requiring that at least one lower-case character be used 3. The operating system must require the change of at least 50% of the total number of characters when passwords are changed. 4. The operating system must enforce password complexity by requiring that at least one special character be used.
D. Not possible to provide in the base operating system. These items may be possible with 3rd-party software.
1. The operating system must use multifactor authentication for network access to privileged accounts. 2. The operating system must use multifactor authentication for network access to non-privileged accounts. 3. The operating system must use multifactor authentication for local access to privileged accounts. 4. The operating system must use multifactor authentication for local access to non-privileged accounts.
E. Outside the scope of VSI Password Management
1. The operating system must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.