
VMS Authentication Module Administration and User's Guide

December 2006

This manual provides the system manager with the procedures for installing, managing, and using the VAM family of software products.

Revision/Update: This manual supersedes the *VMS Authentication Module Administration and User's Guide, V1.1*.

Operating System/Version: OpenVMS VAX V7.3 and higher
OpenVMS Alpha V6.2 and higher
OpenVMS I64 8.2 and higher

MultiNet Version: V4.4 and later
TCPware Version: V5.6-2 and later
UCX Version: V4.0 ECO 5 and later
TCP/IP Services Version: V5.0 and later

**RSA Authentication
Manager Version:** V6.0 and later

Software Version: V2.0

**Process Software
Framingham, Massachusetts
USA**

The material in this document is for informational purposes only and is subject to change without notice. It should not be construed as a commitment by Process Software. Process Software assumes no responsibility for any errors that may appear in this document.

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

The following third-party software may be included with your product and will be subject to the software license agreement.

Portions Copyright © 1993 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Hewlett-Packard Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission. THE SOFTWARE IS PROVIDED "AS IS" AND HEWLETT-PACKARD CORPORATION DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL HEWLETT-PACKARD CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Confidence Inspired, e-Titlement, Intelli-Access, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority, and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.

All other goods and/or services mentioned are trademarks of their respective companies Secure Shell (SSH). Copyright © 2000. This License agreement, including the Exhibits ("Agreement"), effective as of the latter date of execution ("Effective Date"), is hereby made by and between Data Fellows, Inc., a California corporation, having principal offices at 675 N. First Street, 8th floor, San Jose, CA 95112170 ("Data Fellows") and Process Software, Inc., a Massachusetts corporation, having a place of business at 959 Concord Street, Framingham, MA 01701 ("OEM").

All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective holders.

Copyright ©1997, 1998, 1999, 2000 Process Software Corporation. All rights reserved. Printed in USA.

Copyright ©2006 Process Software. All rights reserved. Printed in USA.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Portions copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Portions copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

If the examples of URLs, domain names, internet addresses, and web sites we use in this documentation reflect any that actually exist, it is not intentional and should not to be considered an endorsement, approval, or recommendation of the actual site, or any products or services located at any such site by Process Software. Any resemblance or duplication is strictly coincidental.

Contents

Preface

About VMS Authentication Module	vii
Introducing This Guide.....	vii
What You Need to Know Beforehand	vii
How This Guide Is Organized	vii
Online Help.....	viii
Accessing the VAM Public Mailing List	viii
Obtaining Customer Support	ix
License Information.....	ix
Maintenance Services	ix
Reader's Comments Page.....	ix
Documentation Set.....	x
Conventions Used.....	xi

Chapter 1 Before You Begin

Introduction.....	1-1
Steps to Get VAM Up and Running.....	1-1
Prepare for Installation	1-2
Hardware Requirements	1-2
Software Requirements.....	1-2
Disk Space and Global Pages	1-2
General Requirements	1-2
Where to Install VAM.....	1-2
Release Notes and Online Documentation	1-3

Chapter 2 Installing and Configuring VAM

Introduction.....	2-1
Load the Software.....	2-1
Start VMSINSTAL	2-1
Sample Installation	2-2
Installing VAM for the First Time on a Common VMScLuster System Disk.....	2-3
Installing VAM on Mixed Platform Clusters.....	2-4

Post-Installation Steps	2-4
Post-Installation File Protections	2-4
Post-Installation Using the VAM Callable Module	2-4
Post-Installation Using the VAM OpenVMS LOGINOUT Callouts	2-4
Configuration Keywords When Using LOGINOUT Callouts	2-5
General Logical Names	2-5
Logging Control Logicals	2-5

Chapter 3 Using SecurID and VAM

Introduction	3-1
Post-Installation Steps	3-1
SECURID Authentication	3-1
The VAM SecurID LGI Callouts	3-2
Sample VAM SecurID Login	3-2
Controlling Access to the Callout	3-2
SecurID Configuration Keywords'	3-3
SecurID Logical Names	3-3
SecurID Files Used by VAM	3-3

Chapter 4 Using LDAP and VAM

Introduction	4-1
Post-Installation Steps	4-1
The VAM LDAP LGI Callouts	4-2
Sample VAM LDAP Login	4-2
Controlling Access to the Callout	4-2
VAM LDAP Configuration Keywords	4-2
Configuring VAM LDAP Server Search Criteria	4-3
Specifying Servers Using the LDAP_SERVER Keywords	4-3
Specifying Searches Using the LDAP_SEARCH Keywords	4-4
Fetching User Attributes	4-5
Using TLS/SSL with VAM	4-6
Sample LDAP Configuration	4-6
VAM LDAP Support Tools	4-8

Chapter 5 Using LOCALUAF and VAM

Introduction	5-9
Post-Installation Steps	5-9
Controlling LOCALUAF Access to the Application	5-9

Chapter 6 Using the VAM API

Introduction.....	6-1
The VAM API.....	6-1
The API Authentication Philosophy.....	6-1
Compiling a VAM Application.....	6-2
Linking A VAM Application.....	6-2
VAM Application Special Note.....	6-2
VAM API Functions.....	6-3
VMSAuthenticate.....	6-4
IOCallback.....	6-7
InfoCallback.....	6-9
TimeoutCallback.....	6-10
ScreenClearCallback.....	6-11

Chapter 7 Using VAM with SSH

Introduction.....	7-1
Configuring VAM in SSH.....	7-1
Configuring VAM.....	7-1
Configuring SSH.....	7-1

Preface

About VMS Authentication Module

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to both user-written applications and the OpenVMS system overall using SecurID and/or LDAP. It can be incorporated into an OpenVMS-based platform in two ways:

- Via an API that the user incorporates into a specific application to control access to that application
- On a system-wide basis via use of the LGI callouts for OpenVMS LOGINOUT.EXE.

Chapters three through six describe the two mechanisms and how they are implemented.

Introducing This Guide

This guide describes the VMS Authentication Module (VAM) software. It covers the following topics: software installation, configuration, and server monitoring and control.

What You Need to Know Beforehand

Before using VAM, you should be familiar with:

- Computer networks in general
- OpenVMS operating system and file system
- The TCP/IP stack (MultiNet, TCPware, or HP's OpenVMS TCP/IP software) you're using

How This Guide Is Organized

This guide has the following contents:

- Chapter 1, *Before You Begin*, explains what you need to prepare for an installation.
- Chapter 2, *Installing and Configuring VAM*, provides a step-by-step procedure for executing the software installation and configuring general VAM options.
- Chapter 3, *Using SecurID and VAM*, explains how to configure VAM for using RSA SecurID authentication.
- Chapter 4, *Using LDAP and VAM*, explains how to configure VAM for using LDAP authentication.
- Chapter 5, *Using LOCALUAF and VAM*, explains how to configure VAM for using the local UAF file for authentication.
- Chapter 6, *Using the VAM API*, describes how to integrate the VAM API into a user-written application.

Online Help

There is no online help for VAM.

Accessing the VAM Public Mailing List

Process Software maintains two public mailing lists for VAM customers:

- **Info-VAM@process.com**
- **VAM-Announce@process.com**

The **Info-VAM@process.com** mailing list is a forum for discussion among VAM system managers and programmers. Questions and problems regarding VAM can be posted for a response by any of the subscribers. To subscribe to info-VAM, send a mail message with the word “SUBSCRIBE” in the body to Info-VAM-request@process.com.

You can retrieve the Info-VAM archives by anonymous FTP to <ftp.multinet.process.com>. The archives are located in the directory `[.MAIL_ARCHIVES.INFO-VAM]`.

The **VAM-Announce@process.com** mailing list is a one-way communication (from Process Software to you) used for the posting of announcements relating to VAM (patch releases, product releases, etc.). To subscribe to VAM-Announce, send a mail message with the word “SUBSCRIBE” in the body to VAM-Announce-request@process.com.

Obtaining Customer Support

You can use the following customer support services for information and help about VAM and other Process Software products if you subscribe to our Product Support Services. (If you bought VAM products through an authorized Process Software reseller, contact your reseller for technical support.) Contact Technical Support directly using the following methods:

- **Electronic Mail**

E-mail relays your question to us quickly and allows us to respond, as soon as we have information for you. Send e-mail to support@process.com. Be sure to include your:

- Name
- Telephone number
- Company name
- Process Software product name and version number
- Operating system name and version number

Describe the problem in as much detail as possible. You should receive an immediate automated response telling you that your call was logged.

- **Telephone**

If calling within the continental United States or Canada, call Process Software Technical Support toll-free at 1-800-394-8700. If calling from outside the continental United States or Canada, dial +1-508-628-5074. Please be ready to provide your name, company name, and telephone number.

- **World Wide Web**

There is a variety of useful technical information available on our World Wide Web home page, <http://www.process.com> (select **Support**).

License Information

Please read and understand the *Software License Agreement* before installing the product.

Maintenance Services

Process Software offers a variety of software maintenance and support services. Contact us or your distributor for details about these services.

Reader's Comments Page

The *VAM Administration and User's Guide* includes Reader's Comments as the last page. If you find an error in this guide or have any other comments about it, please let us know. Return a completed copy of the Reader's Comments page, or send e-mail to techpubs@process.com.

Please make your comments specific, including page references whenever possible. We would appreciate your comments about our documentation.

Documentation Set

The documentation set for VAM consists of the following:

- ***Administration and User's Guide*** — For system managers, general users, and those installing the software. The guide provides installation and configuration instructions for the VAM products.
- ***Release Notes*** for the current version of VAM — For all users, system managers, and application programmers. The *Release Notes* are available online on your VAM media and are accessible before or after software installation.

Conventions Used

Convention	Meaning
host	Any computer system on the network. The local host is your computer. A remote host is any other computer.
monospaced type	System output or user input. User input is in bold type . Example: Is this configuration correct? YES Monospaced type also indicates user input where the case of the entry should be preserved.
italic type	Variable value in commands and examples. For example, <i>username</i> indicates that you must substitute your actual username. Italic text also identifies documentation references.
[<i>directory</i>]	Directory name in an OpenVMS file specification. Include the brackets in the specification.
[optional-text]	(Italicized text and square brackets) Enclosed information is optional. Do not include the brackets when entering the information. Example: START/IP line address [info] This command indicates that the <i>info</i> parameter is optional.
{ <i>value</i> <i>value</i> }	Denotes that you should use only one of the given values. Do not include the braces or vertical bars when entering the value.
Note!	Information that follows is particularly noteworthy.
CAUTION!	Information that follows is critical in preventing a system interruption or security breach.
key	Press the specified key on your keyboard.
Ctrl/key	Press the control key and the other specified key simultaneously.
Return	Press the Return or Enter key on your keyboard.

Chapter 1

Before You Begin

Introduction

This chapter introduces you to and prepares you for the VMS Authentication Module (VAM) product installation, configuration, startup, and testing. It is for the OpenVMS system manager or technician responsible for product installation and configuration.

Steps to Get VAM Up and Running

To get VAM up and working, you must perform the following steps:

Table 1-1 Getting VAM Up and Running

1	Load the license pack.	
2	Install the software.	See Chapter 2, <i>Installing and Configuring VAM</i>
3	Configure the VAM environment.	See Chapter2, <i>Installing and Configuring VAM</i>

Prepare for Installation

VAM installation involves using the VMSINSTAL procedure. Preparing for installation involves:

- Understanding the hardware and software requirements
- Determining if you have sufficient disk space and global pages for the installation
- Determining where to install the software

Hardware Requirements

VAM has no special hardware requirements beyond those stated in the Software Product Description for TCPware, MultiNet or HP's TCP/IP Services.

Software Requirements

VAM supports OpenVMS/VAX version 7.3; OpenVMS Alpha version 6.2, 7.0, 7.1, 7.2-1, 7.2-2, 7.3, 7.3-1, 7.3-2, 8.2, 8.3; OpenVMS I64 version 8.2, 8.2-1, 8.3; MultiNet version 4.4 or later, TCPware version 5.6-2 or later, UCX version 4.0 ECO 5 and later, and TCP/IP Services version 5.0 and later.

Disk Space and Global Pages

Disk space and global page requirements are documented in the release notes.

General Requirements

Check at this point that you:

- Have OPER, SYSPRV, or BYPASS privileges
- Can log in to the system manager's account
- Are the only user logged in (recommended)
- Backed up your system disk on a known, good, current, full backup (recommended)
- Need to reinstall VAM after performing a major VMS upgrade
- Ensure MultiNet, TCPware or TCP/IP Services (or UCX) is currently running.

Where to Install VAM

Install VAM in a location depending on the following:

- Generally, on your system disk, but you can install VAM anywhere, just answer the question when it appears. This is also where you would keep your "common" files. Node-specific files should always be on your system disk.
- If the machine is in a single platform cluster, on a common disk.
- If the machine is in a mixed platform cluster, once on the Alpha system disk (or disks), once on the I64 system disk (or disks), and once on the VAX common system disk.

Release Notes and Online Documentation

The VAM *Release Notes* provide important information on the current release.

- The Release Notes is a text file which can be obtained in one of three ways:
 - By performing a partial installation
 - During the full installation
 - After the installation

To perform a partial installation (see Example 1-1):

1 Invoke VMSINSTAL at the system prompt:

```
$ @SYSSUPDATE:VMSINSTAL VAM020 directory-spec OPTIONS N
```

The *directory-spec* is the location of the distribution savesets.

2 Press **Return** at the prompt

```
Are you satisfied with the backup of your system disk [YES]?
```

3 Select the option by number as to whether you want to display or print the *Release Notes*, or both.

4 If you requested a printout, enter the queue name for the printer. The default is SYSS\$PRINT.

5 Press **Return** at the prompt

```
Do you want to continue the installation [NO]?:
```

```
This will print the VAM V2.0 Release Notes.      (Note that if you enter YES at the prompt,
you proceed with the full installation.)
```

6 You see the message

```
Product's release notes have been moved to SYS$HELP.
```

7 If you want to read or print the *Release Notes* after you exit the installation, you can access the VAM020.RELEASE_NOTES files in the SYS\$HELP directory, as in:

```
$ TYPE SYS$HELP:VAM020.RELEASE_NOTES
```

Note! For this command to work as desired, do not redefine the SYS\$HELP directory logical.

Example 1-1 Performing a Partial Installation to Obtain the Release Notes

```
$ @SYSSUPDATE:VMSINSTAL VAM020 DKA300:[MYDIR] OPTIONS N [1]
```

```
OpenVMS AXP Software Product Installation Procedure V7.1
```

```
It is 13-MAY-2006 at 11:01.
```

```
Enter a question mark (?) at any time for help.
```

```
* Are you satisfied with the backup of your system disk [YES]? Return [2]
```

```
The following products will be processed:
```

```
VAM V2.0
```

```
Beginning installation of VAM V2.0 at 11:01
```

```
%VMSINSTAL-I-RESTORE, Restoring product save set A ...
```

```
Release notes included with this kit are always copied to SYS$HELP.
```

Before You Begin

Additional Release Notes Options:

1. Display release notes
2. Print release notes
3. Both 1 and 2
4. None of the above

* Select option [2]: **Return** [3]

* Queue name [SYS\$PRINT]: **Return** [4]

Job VAM020 (queue SYS\$PRINT, entry 1) started on SYS\$PRINT

* Do you want to continue the installation [NO]? **Return** [5]

%VMSINSTAL-I-REMOVED, Product's release notes have been moved to
SYS\$HELP. [6]

VMSINSTAL procedure done at 11:02

\$TYPE SYS\$HELP:VAM020.RELEASE_NOTES [7]

Installing and Configuring VAM

Introduction

This chapter takes you through the VMS Authentication Manager (VAM) product installation procedure and certain post-installation tasks. It is for the OpenVMS system manager, administrator, or technician responsible for product installation.

To prepare for installation, see Chapter 1, *Before You Begin*.

Note! Once you have installed VAM, you need to reinstall it after you have done a major OpenVMS upgrade.

To install VAM:

- 1 Load the software.
- 2 Run the VMSINSTAL procedure.
- 3 Install other products, if needed, and perform post-installation tasks.

Load the Software

VAM is downloaded from the Process Software FTP site. Information on downloading the software will be supplied to users by Process Software.

The VAM software must be installed from the system manager's account.

If you install VAM on a VMS cluster that has a common system disk, install the software on only one node in the cluster. Be sure to configure VAM on all systems in a VMS cluster that has a common system disk, even though it only needs to be installed once.

Start VMSINSTAL

VMSINSTAL is the OpenVMS installation program for layered products. VMSINSTAL prompts

you for any information it needs. Table 2-1 shows the steps to follow.

Table 2-1 Starting VMSINSTAL

Step	For this task...	Enter this response...
1	Make sure that you are logged in to the system manager's account, and invoke VMSINSTAL	@SYSS\$UPDATE:VMSINSTAL
2	Determine if you are satisfied with your system disk backup	Return or Y (Yes) or N (No)
3	Determine where the distribution volumes will be mounted	The disk (and directory) where you want the software to be mounted.
4	Enter the products you want processed from the first distribution volume set	VAM020
5	Enter the installation options you wish to use (such as obtaining the <i>Release Notes</i>)	Return for no options or N for <i>Release Notes</i> .
6	Specify the device where you want the files installed.	Return if accepting default of SYSS\$SYSDEVICE:

Sample Installation

```
$ @sys$update:vmsinstal VAM020 dka600:
```

```
OpenVMS Software Product Installation Procedure V8.2
```

```
It is 16-JUN-2006 at 14:09.
```

```
Enter a question mark (?) at any time for help.
```

```
%VMSINSTAL-W-NOTSYSTEM, You are not logged in to the SYSTEM account.
```

```
%VMSINSTAL-W-ACTIVE, The following processes are still active:
```

```
DECW$SERVER_0
```

```
DECW$TE_043B
```

```
* Do you want to continue anyway [NO]? y
```

```
* Are you satisfied with the backup of your system disk [YES]?
```

```
The following products will be processed:
```

```
VAM V2.0
```

```

Beginning installation of VAM V2.0 at 14:09

%VMSINSTAL-I-RESTORE, Restoring product save set A ...

                VMS Authentication Module (R)

ALL RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES

This licensed material is the valuable property of Process Software.
Its use, duplication, or disclosure is subject to the restrictions set
forth in the License Agreement.

Other use, duplication or disclosure, unless expressly provided for in
the license agreement, is unlawful.

* What device do you want to install VMS Authentication Module on
[SYS$SYSDEVICE]:

* Do you want to purge files replaced by this installation [YES]?

The installation will now proceed with no further questions.

*****

To complete this installation, you must refer to the documentation
and the Release Notes for post-installation instructions.

*****

%VMSINSTAL-I-MOVEFILES, Files will now be moved to their target
directories...

                Installation of VAM V2.0 completed at 14:09

                Adding history entry in VMI$ROOT:[SYSUPD]VMSINSTAL.HISTORY

                Creating installation data file: VMI$ROOT:[SYSUPD]VAM020.VMI_DATA

                VMSINSTAL procedure done at 14:10

$

```

Installing VAM for the First Time on a Common VMScluster System Disk

No special preparation is required after installing VAM on one node of a VMScluster with a common system disk.

Installing VAM on Mixed Platform Clusters

VAM has no files which can be shared between cluster systems of different architectures.

Post-Installation Steps

The following sections describe the post-installation setup required to enable the various forms of authentication. Specific configuration of the authentication methods (e.g., LDAP) are covered in subsequent chapters

For both the VAM callable module and the VAM OpenVMS LOGINOUT callouts, the file VAM:VAM_CONFIG.TEMPLATE must be copied (if it doesn't already exist) to VAM:VAM_CONFIG.DAT. This file contains the configurable options for VAM, and may be edited as needed by the system manager.

Post-Installation File Protections

The following files must have at least the the following protection and ownership. Failure to have these protections will result in authentication attempts failing. Note that the SECURID file is created automatically with these protections.

VAM_CONFIG.DAT	[SYSTEM]	(RWED,RWED,,)
SECURID.	[SYSTEM]	(R,R,,)
SDCONF.REC	[SYSTEM]	(RWED,RWED,,)

Post-Installation Using the VAM Callable Module

To use the VAM callable module, the system manager must add the line

```
@<install_device>: [VAM] VAM_STARTUP
```

to the SYSTARTUP_VMS.COM file.

Beyond that, no further configuration on the client system is required.

The user will be responsible for using the provided VAM API to integrate VAM into the desired application(s).

Post-Installation Using the VAM OpenVMS LOGINOUT Callouts

The OpenVMS system requires further configuration to enable the LOGINOUT callouts.

- Edit VAM:VAM_CONFIG.DAT and set the appropriate configuration keywords as desired.
- The dynamic SYSGEN parameter LGI_CALLOUTS must be set to "1":
- Next, the system manager must determine which authentication methods (LDAP and/or SecurID) users are to be required to use. See chapters 3 and 4 for information on configuring the LGI callouts for these methods.

Note! Including the LGI parameter on the VAM_STARTUP command line will enable both the VAM

LGI callouts and the VAM callable module.

Configuration Keywords When Using LOGINOUT Callouts

The following keywords, found in VAM:CONFIG.DAT, are used to control access using the OpenVMS LOGINOUT callouts.

LGI_AUTH_METHODS

Contains a priority-ordered list of the authentication methods to be used. For example, “LDAP,SECURID” will cause the VAM LGI interface to attempt first LDAP and then SECURID authentication when called.

FALLTHROUGH_TO_VMS

If set to 1, allows VAM to fall through to using normal VMS authentication if the SecurID and/or LDAP servers are all unreachable.

General Logical Names

These logical names are defined on all VAM systems. They are defined in VAM:VAM_SPECIFIC_STARTUP.COM when the VAM_STARTUP command procedure is executed.

VAM

This logical points to the *<install_device>*:[VAM] directory.

VAM_ROOT

This logical points to *<install_device>*:[VAM.]. It may be used, for example, to specify the log file directory: VAM_ROOT:[LOG].

Logging Control Logicals

The following logical names are used to affect logging for the VAM software. The logicals are located in the VAM_SPECIFIC_STARTUP command procedure and are normally commented out. This logging is used to debug VAM installations, and should generally be used only when recommended by Process Software.

VAM_LOGFILE

This logical determines the location and name of the file used to log VAM transactions and errors.

VAM_CURRENT_TRACE_LEVEL

This logical determines the level of detail in the VAM log. The level is a combination of the following bit masks:

TRACE_EXECUTION (1) - traces general steps the VAM module is performing.

TRACE_EXECUTION_DEEP (2) - verbose tracking of the VAM module processing.

TRACE_INFO (4) - Tracks informational messages generated by the VAM module

TRACE_ERROR (8) - Logs errors encountered by the VAM module

Using SecurID and VAM

Introduction

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to both user-written applications and the OpenVMS system overall using SecurID. It can be incorporated into an OpenVMS-based platform in two ways:

- Via an API that the user incorporates into a specific application to control access to that application. The VAM API is described in detail in chapter 6, “*Using the VAM API*”.
- On a system-wide basis via use of the LGI callouts for OpenVMS LOGINOUT.EXE.

SSH logins are not affected by the VAM LGI callouts.

The system console (OPA0:) is never required to use the LDAP LGI Callout interface, in order to prevent being locked-out of the system in the event of a network failure that prevents the VMS system from talking with the SecurID RSA Authentication Manager system(s).

Post-Installation Steps

The following sections describe the post-installation setup required to enable SecurID authentication. The VAM SecurID support must be configured for both the callable module (API) and LOGINOUT (LGI) callout support.

SECURID Authentication

The SDCONF.REC file must be obtained from the ACE/Server system or from another VMS system running VAM. This file is to be copied to the `<install_device>:[VAM]` directory. This is a binary file, so it must be transferred via ftp in binary mode from a non-VMS system.

When configuring the OpenVMS system as an agent host in the RSA Authentication Manager, the system must be described as a “UNIX AGENT”

The VAM SecurID LGI Callouts

VAM may be incorporated into the OpenVMS login mechanism to control access to the entire system. VAM provides an OpenVMS shareable image, which the system manager can incorporate, using supported OpenVMS mechanisms, into the OpenVMS LOGINOUT mechanism. This image uses the SecurID protocols to supplement the standard OpenVMS login processing and provides the necessary user authentication to access the system as part of the login process.

Note! This section assumes the user has basic knowledge of how SecurID authentication works.

Sample VAM SecurID Login

The following example shows a login to a system for a user that has not yet established a PIN

```
$ SET HOST VOODOO
```

```
Welcome to OpenVMS (TM) IA64 Operating System, Version V8.2-1
```

```
Username: johndoe
```

```
Enter PASSCODE:
```

```
You must select a new PIN.
```

```
Do you want the system to generate  
your new PIN? (y/n) [n] n
```

```
Enter a new PIN between 4 and 8 alphanumeric  
characters:
```

```
Re-enter new PIN to confirm:
```

```
PIN accepted. Wait for the tokencode to  
change, then enter a new PASSCODE:
```

```
PASSCODE accepted.
```

```
Welcome to OpenVMS IA64 V8.2-1
```

```
Last interactive login on Monday, 23-JAN-2006 12:04:50.21
```

```
Last non-interactive login on Friday, 2-DEC-2005 07:33:34.74
```

```
You have 1 new Mail message.
```

```
VOODOO_$
```

Controlling Access to the Callout

The system manager configures the system to use the LGI callouts. This may be done in two ways:

- Set the configuration keyword **REQUIRE_SECURID**. If set, all users are required to attempt SecurID authentication.
- Add the rights identifier **VAM_LGI_SECURID** to the system rights database. This identifier may then be granted to those users that will be required to use SecurID authentication.

SecurID Configuration Keywords'

The following keywords are used to configure SecurID for VAM. These keywords are set in VAM:VAM_CONFIG.DAT.

ALLOW_DECNET_LOGIN

If set to a non-zero value, determines DECnet CTERM (RTAnn:) devices are required log in using SecurID

ALLOW_DECTERM_LOGIN

If set to a non-zero value, determines that DECTerm (FTAnn:) devices are required log in using SecurID

REQUIRE_SECURID

When set, all users will be required to attempt SecurID authentication.

SECURID_HONOR_VMS_MODAL

If this keyword is set to 1, the VMS login modals (e.g., allowed login date and times) will be honored. By default, the modals as defined by the ACE server are used

SecurID Logical Names

The following logical names are used to configure SecurID access for VAM. These may be found in VAM:VAM_SPECIFIC_STARTUP.COM.

RSATRACELEVEL

This logical name is used to determine the level of detail in the SecurID logfile. This is a number from 1 to 65535, where 1 is the lowest level of tracing. This logical should never normally be defined, as it can have a severe impact on performance.

RSATRACEDEST

This logical defines the location and name of the SecurID log file. If this isn't defined, output will go to the user's terminal.

SecurID Files Used by VAM

The following files, used by SecurID processing, are found in the VAM directory. They should not normally be manipulated by the system manager:

SDSTATUS.12

This file is used by SecurID to keep track of the status of the RSA Authentication Manager servers and replicas. Each time a successful connection is made to a SecurID server, this file is rewritten.

SECURID.

This is the SecurID "node secret" file. It's created after the first successful SecurID session.

Using LDAP and VAM

Introduction

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to both user-written applications and the OpenVMS system overall using LDAP. It can be incorporated into an OpenVMS-based platform in two ways:

- Via an API that the user incorporates into a specific application to control access to that application. The VAM API is described in detail in chapter 6, “*Using the VAM API*”.
- On a system-wide basis via use of the LGI callouts for OpenVMS LOGINOUT.EXE.

SSH logins are not affected by the VAM LGI callouts.

The system console (OPA0:) is never required to use the LDAP LGI Callout interface, in order to prevent being locked-out of the system in the event of a network failure that prevents the VMS system from talking with the LDAP server system(s).

Note! This chapter assumes the user is familiar with LDAP in general; of the specifics of the user’s LDAP installation; and if using TLS/SSL, of certificates and how to obtain and use them. Due to the breadth and depth of the topics above, this chapter will not attempt to present a tutorial on those topics.

Post-Installation Steps

The following sections describe the post-installation setup required to enable the various forms of authentication.

VAM uses configuration keywords, set in the VAM:VAM_CONFIG.DAT file, to determine the location of the LDAP server, the filter to be used for lookups, etc. In this way, it presents the maximum flexibility for integration into the user’s existing LDAP environment. The VAM LDAP support must be configured for both the callable module and LOGINOUT callout support.

The VAM LDAP LGI Callouts

VAM may be incorporated into the OpenVMS login mechanism to control access to the entire system. VAM provides an OpenVMS shareable image, which the system manager can incorporate, using supported OpenVMS mechanisms, into the OpenVMS LOGINOUT mechanism. This image uses the LDAP protocols to supplement the standard OpenVMS login processing and provides the necessary user authentication to access the system as part of the login process.

This section assumes the user has basic knowledge of how LDAP directories are constructed and work.

Sample VAM LDAP Login

The following example shows a login to a system:

```
$ SET HOST VOODOO
```

```
Welcome to OpenVMS (TM) IA64 Operating System, Version V8.2-1
```

```
Username: johndoe
```

```
Password:
```

```
Welcome to OpenVMS IA64 V8.2-1
```

```
Last interactive login on Monday, 23-JAN-2006 12:04:50.21
```

```
Last non-interactive login on Friday, 2-DEC-2005 07:33:34.74
```

```
You have 1 new Mail message.
```

```
VOODOO_$
```

Controlling Access to the Callout

The system manager configures the system to use the LGI callouts. This may be done in two ways:

- Define the configuration keyword **REQUIRE_LDAP**. If set, all users are required to use LDAP authentication.
- Add the rights identifier **VAM_LGI_LDAP** to the system rights database. This identifier may then be granted to those users who will be required to use LDAP authentication.

VAM LDAP Configuration Keywords

Access to LDAP via VAM requires setting several configuration options in the configuration file VAM:VAM_CONFIG.DAT. This section describes those keywords and their usage.

LDAP_CERT

This configuration item is used when performing encrypted LDAP sessions. It is set to the file name of the PEM-formatted PKCS7 certificate containing the root certification chain for the trusted certification authority (CA) that will be used to establish the bonafides of the VAM system.

ALLOW_DECNET_LOGIN

If set to a non-zero value, determines DECnet CTERM (RTAnn:) devices are required log in using LDAP

ALLOW_DECTERM_LOGIN

If set to a non-zero value, determines that DECTerm (FTAnn:) devices are required log in using LDAP

LDAP_NOPASSWORD_SYNC

If set to 1, this will prevent VAM from updating the user's password and password change data in the VMS UAF file after a successful LDAP login. By default, VAM synchronizes this information in the UAF file to ensure that LDAP and VMS passwords are kept in sync.

LDAP_TIMELIMIT

This configuration item sets the maximum length of time an LDAP search will be allowed to take. The value is in seconds. If not specified, the default is 5 seconds.

Configuring VAM LDAP Server Search Criteria

VAM provides the ability to perform multiple searches on multiple LDAP servers. This is provided through the use of *stanzas*, which consist of an LDAP_SERVER section which describes a specific server (e.g., the server nodename and port), followed by one or more LDAP_SEARCH sections that describe the individual searches to be performed on that server.

Specifying Servers Using the LDAP_SERVER Keywords

The following configuration keywords are used to configure access to an LDAP server. These keywords are set in the file VAM:VAM_CONFIG.DAT.

LDAP_SERVER <servername URI>

This is the fully-qualified domain name of the LDAP server to be used in Uniform Resource Locator (URI) format. If prefaced by “ldap”, the URI indicates an unencrypted session will be done via port 389. If prefaced by “ldaps”, the URI indicates an encrypted session will be done via port 636. The port may also be explicitly specified in the URI.

For example:

```
ldap_server      ldaps://my.ldap.server.org:636/
```

Defines a server called *my.ldap.server.org*. Port 636 will be used to communicate to the server, and the session will be encrypted.

LDAP_USE_TLS

If your LDAP server supports LDAPS (LDAP-over-TLS), setting the value of this keyword to 1 will instruct VAM to attempt to use LDAPS for user authentication. If an LDAPS connection cannot be established, a standard LDAP connection will be used to authenticate the user.

Setting the value of this keyword to 2 will force an LDAPS connection. If an LDAPS connection cannot be established, the user will receive an error and will not be able to log in.

The value may never be used when using the ldaps form of the URI for a server to specify that the session should be encrypted.

Specifying Searches Using the LDAP_SEARCH Keywords

The following configuration keywords are used to configure searches on an LDAP server within the configuration stanza for that server. These keywords are set in the file VAM:VAM_CONFIG.DAT.

LDAP_AUTH_FILTER

Specifies the LDAP search filter used to find the directory entry for a user who is authenticating to the web user interface.

Both LDAP_BASE_DN and LDAP_AUTH_FILTER allow the following expansion tags to be used in their values:

Tag	Description
%u	The user's login name

For example, a site might set the values of LDAP_BASE_DN and LDAP_AUTH_FILTER as :

ldap_base_dn	o=%d
ldap_auth_filter	(&(objectclass=person)(uid=%u))

If a user logged in as jdoe@example.com, the values of these configuration variables would be expanded to:

ldap_base_dn:	o=example.com
ldap_auth_filter:	(&(objectclass=person)(uid=jdoe))

LDAP_AUTH_SERVER

Specifies the name of the LDAP host to search for authentication information. There is no default value.

LDAP_BASE_DN

Specifies the entry in the LDAP directory under which searches occur (sometimes also known as the search base). Consult your LDAP server's documentation set for more information specific to your implementation.

LDAP_BASE_DN supports the same tag expansions as LDAP_AUTH_FILTER.

LDAP_SEARCHACCT_DN

VAM must query the LDAP server to find the Distinguished Name of the user attempting to log in before the user can be authenticated. By default, this initial query will be done anonymously. Some directory servers (notably Microsoft's Active Directory) do not allow anonymous queries.

LDAP_SEARCHACCT_DN

Specifies the Distinguished Name of a user with search privileges on the directory server that VAM will connect as. By default, the value is NULL which indicates an anonymous login.

LDAP_SEARCHACCT_PASSWORD

Specifies the password for the search user whose Distinguished Name is specified in LDAP_SEARCHACCT_DN. By default, the value is NULL which indicates an anonymous login.

Fetching User Attributes

VAM provides the ability to fetch a list of named attributes for a user that are stored in an LDAP directory. The search for attributes is performed on the same server on which the user has been successfully authenticated.

The form of the attribute information returned depends on the VAM interface being used. When using the VMS LOGINOUT callouts, the information will be returned as a series of logical names created in the process's job logical name table. The form of each logical name will "VAM_ATTR_<attribute_name>"; for example, VAM_ATTR_logonCount would hold the *logonCount* attribute that was fetched for a user.

When using the VAM API, the user specifies the *UserAttributes* argument to the VMSAuthenticate call. This is a pointer to a *struct attr* structure pointer. A linked list of attributes and their values is returned in the *UserAttributes* argument. This structure is described in description of the VMSAuthenticate call in chapter 6.

To configure VAM to fetch attributes, the following keywords are used in the VAM_CONFIG.DAT file:

LDAP_ATTRIBUTE

Specifies an attribute to fetch. Each LDAP_ATTRIBUTE line is of the form "<attribute_name>,<attribute_type>". Multiple attribute lines are permitted.

The <attribute_name> is case-sensitive, and must be the same case as the attribute as stored in the LDAP directory.

Permitted values for <attribute_type> are:

- ATTRIBUTE_STRING for values that are stored in the LDAP directory as character strings. The value is returned as a null-terminated string.
- ATTRIBUTE_BINARY for values that are stored in the LDAP directory as binary values. The value is returned as a decimal number represented by a null-terminated string.

For example:

```
ldap_attribute   MyNamedAttribute,attribute_string
```

will cause the character string attribute MyNamedAttribute to be fetched.

LDAP_ATTRIBUTE_BASE_DN

Specifies the entry in the LDAP directory under which the search for the LDAP attributes occurs (sometimes also known as the search base). Consult your LDAP server's documentation set for more information specific to your implementation.

LDAP_ATTRIBUTE_BASE_DN supports the same tag expansions as LDAP_BASE_DN.

LDAP_ATTRIBUTE_FILTER

Specifies the LDAP search filter used to find the attribute entry for a user who is authenticating to the web user interface.

LDAP_ATTRIBUTE_BASE_DN supports the same tag expansions as LDAP_AUTH_FILTER:

Using TLS/SSL with VAM

TLS/SSL may be used to provide secure message transfer between VAM and the LDAP server. This is recommended as LDAP transactions by default are unencrypted and may contain clear-text username/password tuples. Thus, failure to use TLS/SSL can open a network security hole.

To enable TLS/SSL support:

- The trusted root certificate chain for the CA used to sign the LDAP server's certificate must be obtained. This certificate must be a PEM-formatted PKCS7 file.
- The VAM_CONFIG.DAT file must be edited to set the LDAP_CERT keyword. This keyword must point to the filename of the trusted root certificate chain.
- Ensure the SERVER URI(s) correctly use *ldaps* in the URI

Note that the *ldapsearch* and *openssl* utilities (supplied in the VAM distribution) may be used to help verify the certificate chain and search criteria..

Sample LDAP Configuration

The following is an excerpt from a VAM:VAM_CONFIG.DAT file that illustrate a sample VAM LDAP configuration.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!           LDAP Configuration Keywords
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
! If the next keyword is defined, then all users will be required
! to use LDAP authentication when using the LGIS callouts.
! This will override the checks for the LGI_LDAP
! rights identifier to determine who is required to use LDAP.
!
REQUIRE_LDAP      1
!
! The next keyword, if set to 1, will prevent VAM from updating the
! user's password and password change data in the VMS UAF file after a
! successful LDAP login.
!
LDAP_NOPASSWORD_SYNC  0
!
! Set the max time limit (in seconds) for LDAP searches. Defaults
```

```

! to 5 seconds if not defined.
!
LDAP_TIMELIMIT 10
!
! Define the name of the PEM-formatted PKCS7 file containing the
! root certificate chain for the trusted CA for LDAP sessions
!
LDAP_CERT MYSYS$DKA100:[CERTS]CA_ROOT_CERTS.PEM
!
! Define keywords for LDAP attributes to be fetched. Note that
! these are case-sensitive.
!
LDAP_ATTRIBUTE logonCount,attribute_binary
LDAP_ATTRIBUTE cn,attribute_string
!
! Define the search criteria for searching for attributes.
!
LDAP_ATTRIBUTE_BASE_DN "CN=Users,dc=limabeansdomain,dc=beans,dc=com"
LDAP_ATTRIBUTE_FILTER "(&(objectclass=userAttrs)(sAMAccountName=%u))"
!
! The next keywords define the parameters for performing LDAP
! authentication, for both the LGI interface and the programmatic
! interface. They should be set to values appropriate to your location.
!
! Multiple servers may be specified. Each server section starts with
! an "LDAP_SERVER" label, and within each server section, searches specific
! to that server are then defined in LDAP_SEARCH sections.
!
! Note that the port portion of the URI is optional. If not specified,
! the port will be defined to 389 for ldap and 636 for ldaps.
!!
LDAP_SERVER LDAP://LIMA.BEANS.COM
LDAP_SEARCH
LDAP_AUTH_FILTER "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN "CN=Users,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN "cn=Admin,CN=Users,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
LDAP_SEARCH
LDAP_AUTH_FILTER "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN "CN=OtherUsers,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN "cn=Mgr,CN=Users,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
LDAP_SEARCH
LDAP_AUTH_FILTER "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN "CN=MoreUsers,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN "cn=JohnDoe,CN=Users,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
!
LDAP_SERVER LDAPS://PINTO.BEANS.COM
LDAP_SEARCH

```

```
LDAP_AUTH_FILTER      "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN          "CN=Users,dc=domain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN    "cn=Admin,CN=Users,dc=pdomain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
LDAP_SEARCH
LDAP_AUTH_FILTER      "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN          "CN=MoreUsers,dc=pdomain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN    "cn=SYSMAN,CN=Users,dc=pdomain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
LDAP_SEARCH
LDAP_AUTH_FILTER      "(&(objectclass=user)(sAMAccountName=%u))"
LDAP_BASE_DN          "CN=MoreUsers,dc=pdomain,dc=beans,dc=com"
LDAP_SEARCHACCT_DN    "cn=SYSMAN,CN=Users,dc=pdomain,dc=beans,dc=com"
LDAP_SEARCHACCT_PASSWORD "secretpassword"
```

VAM LDAP Support Tools

The following unsupported tools, provided in the OpenLDAP distribution, are supplied in the VAM directory. These tools are supplied as a convenience to the user and are not supported by Process Software.

Documentation for these tools may be found at <http://www.openldap.org>. The supplied tools include:

- ldapcompare
- ldapdelete
- ldapmodify
- ldapmodrdn
- ldappasswd
- ldapsearch
- ldapwhoami
- openssl

Chapter 5

Using LOCALUAF and VAM

Introduction

The VMS Authentication Module (VAM) provides users of OpenVMS systems controlled access to user-written applications via an API that the user incorporates into a specific application to control access to that application. The VAM API is described in detail in chapter 6, “*Using the VAM API*”.

Note! LOCALUAF processing is not offered for the use of the LGI callouts for OpenVMS LOGINOUT.EXE, as this would be redundant with what is offered by OpenVMS.

Post-Installation Steps

The following sections describe the post-installation setup required to enable the various forms of authentication.

LOCALUAF authentication is supported only for using the VAM callable module. To use the VAM callable module, the system manager must add the line

```
@<install_device>: [VAM] VAM_STARTUP
```

to the SYSTARTUP_VMS.COM file.

Beyond that, no further configuration on the client system is required.

The user will be responsible for using the provided VAM API to integrate VAM into the desired application(s).

Controlling LOCALUAF Access to the Application

Some installations may have several applications protected via VAM and using LOCALUAF processing, but which they want to further restrict access to. For example, the company may want the PAYROLL application restricted to only people from the payroll department, while the INVENTORY application might be restricted to salespeople.

VAM provides a mechanism for restricting access in VAM-enabled applications by using VMS

rights ids. When adding the VAM interface to an application, the application programmers may add the *identifier* field to the VMSAuthenticate() function call (see chapter 6, *Using the VAM API*, for information on calling VMSAuthenticate). VAM then attempts to match *identifier* with a rights id in the UAF record for the username specified in the call to VMSAuthenticate. If a match is made, access is allowed; otherwise, access is denied.

If *identifier* is not specified or is blank when calling VMSAuthenticate, then *identifier* will default to **VAM_UAF_ID**. Therefore, the **VAM_UAF_ID** rights id must be granted to all VAM users using LOCALUAF processing if *identifier* is not specified in the call to VMSAuthenticate

Note! There is no equivalent functionality for use when performing SECURID or LDAP processing. Access in that case is solely determined by the RSA Authentication Manager or LDAP server, respectively.

For example, ABC corporation has three VAM-enabled applications using LOCALUAF processing: payroll, inventory and personnel. User John Doe will be allowed to access only INVENTORY, while Jane Doe will be allowed to access PERSONNEL and PAYROLL. To set these accounts up, the following steps may be used:

```
$ run sys$system:authorize
UAF> add/identifier payroll
%UAF-I-RDBADDMMSG, identifier PAYROLL value %X80010003 added to rights
database
UAF> add/identifier inventory
%UAF-I-RDBADDMMSG, identifier INVENTORY value %X80010004 added to rights
database
UAF> add/identifier personnel
%UAF-I-RDBADDMMSG, identifier PERSONNEL value %X80010005 added to rights
database
UAF> grant/identifier inventory johndoe
%UAF-I-GRANTMSG, identifier INVENTORY granted to JOHNDOE
UAF> grant/identifier payroll janedoe
%UAF-I-GRANTMSG, identifier PAYROLL granted to JANEDOE
UAF> grant/identifier personnel janedoe
%UAF-I-GRANTMSG, identifier PERSONNEL granted to JANEDOE
UAF> Exit
%UAF-I-NOMODS, no modifications made to system authorization file
%UAF-I-NAFNOMODS, no modifications made to network proxy database
%UAF-I-RDBDONEMSG, rights database modified
$
```

Then, when adding VAM to, for example, the payroll application, the call to VMSAuthenticate would be:

```
status = VMSAuthenticate("LOCALUAF", username, 0, &IOCallback,
                          &InfoCallback, &TimeoutCallback,
                          &ScreenClearCallback, 0, "payroll", 0, 0);
```

Chapter 6

Using the VAM API

Introduction

VAM provides an API for allowing user-written applications to use SecurID, LDAP or local UAF authentication for controlling access to the application. This can be implemented by a business that uses normal operating-system access for its internal functions, but which may need further authentication for specific applications that interface to counterparts on remote systems. In this case, VAM provides an additional layer of security for access to that application.

This chapter describes how to use the VAM API when using VAM as a front-end for an application.

The VAM API

The API allows VAM to be incorporated into user-written applications to control access to those applications. The API allows authentication via SecurID tokens, LDAP, or via the local system UAF.

This can be used by a business that uses normal operating-system access for its internal functions, but which may need further controlled access to specific applications that interface to counterparts on remote systems. In this case, VAM provides an additional layer of security for access to that application.

The API Authentication Philosophy

The authentication process begins with the user calling the VMSAuthenticate function, providing the username for the user, the type of authentication to perform and callbacks necessary to carry on a further dialog if needed.

For SECURID processing, the authentication routines carry on the dialog with the RSA Authentication Manager, handling all the internal processing necessary. This includes the capability to handle replicated servers, etc..

For LDAP processing, the authentication routines carry on the dialog with the LDAP server, handling all the internal processing necessary. The user must configure VAM to specify the correct LDAP server and search criteria (e.g., the LDAP filter to use) to be used for the queries.

For LOCALUAF processing, the authentication routines perform many of the same checks that the VMS LOGINOUT processing does in order to validate the user.

The authentication routines will not carry on the actual dialog with the user. The user program, by supplying the dialog callbacks, will be required to do the actual dialog, using prompts supplied by the authentication routines. In this way, the user may tailor this to the user's specific environment (video terminal, DECwindows application, etc).

When prompting for data via the dialog callbacks, the user is responsible for disabling terminal echo prior to reading the information, and re-enabling it after reading the information, and may be responsible (depending on the type of authentication being performed) for performing edits on the input data (such as being of proper length and type).

The basic processing will be as follows:

- The user is prompted for the username within the context of the user program.
- The user program calls `VMSAuthenticate()` to initialize processing. The first parameter to this function determines the authentication mechanism to use (SECURID, LDAP or LOCALUAF).
- `VMSAuthenticate` may use the callback routines to obtain more information from the user or to display information to the user.
- `VMSAuthenticate` will return to the original caller with a status indicating whether the user has been authenticated.

Compiling a VAM Application

When compiling a source module that will call the `VMSAuthenticate` function, include the file `VAM:VMSAUTHENTICATE.H`.

Linking A VAM Application

To link an application which uses the VAM API, include the file `VAM:[VAM]VAM_LINK.OPT`. For example:

```
$ LINK MYAPPLICATION, VAM: [VAM] VAM_LINK.OPT/OPTION
```

VAM Application Special Note

VAM-enabled programs must be installed with `CMKRNL` privileges. If this is not done, they will be unable to successfully parse the VAM configuration file. For example:

```
$ INSTALL ADD MYPROGRAM.EXE /PRIV=CMKRNL
```

VAM API Functions

The following sections describe each of the VAM API calls. It includes not only the VMSAuthenticate function, but also the callback functions that are supplied by the user.

VMSAuthenticate

The user application calls VMSAuthenticate to perform authentication. VMSAuthenticate must be supplied with an identifier that defines what type of authentication will take place and a username. A password may be supplied; however, it may be ignored (for example, in the case of performing SecurID authentication). The application must provide four callbacks to interact with the user.

VMSAuthenticate is a synchronous function; as such, it will not return until authentication completes successfully or fails.

Format

```
int VMSAuthenticate {
    char *   AuthenticationType,
    char *   Username,
    char *   Password,
    int *    (*IOCallback)(),
    int *    (*InfoCallback)(),
    void *   (*TimeoutCallback)(),
    void *   (*ScreenClearCallback)(),
    int *    UserData,
    char *   Identifier,
    struct vam_attr **UserAttributes,
    0
};
```

Inputs

- AuthenticationType - String (null-terminated) containing the type of authentication desired. Currently, must be "SECURID", "LDAP" or "LOCALUAF".
- Username - String (null-terminated) containing the username to be checked. The username is case-sensitive, and must match the case of the username when entered at the SecurID server.
- Password - String (null-terminated) containing the password to be checked. Ignored when AuthenticationType is "SECURID" or "LDAP". Required when AuthenticationType is "LOCALUAF".
- IOCallback - Pointer to the user-defined callback to be called when a prompt/response dialog must be performed with the user.
- InfoCallback - Pointer to the user-defined callback to be called when an informational message must be displayed to the user.
- TimeoutCallback - Pointer to the user-defined callback to be called when a prompt timeout occurs.
- ScreenClearCallback - Pointer to the user-defined callback to be called when the screen is to be cleared after a prompt.
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated). This pointer will be passed to all user-defined callback routines.
- Identifier - String (null-terminated) that contains the name of the application. This will be used

to match a VMS rights identifier when AuthenticationType is “LOCALUAF”. If this field is not specified for LOCALUAF processing, the identifier VAM_UAF_ID is used by default. This field is ignored for SECURID processing.

- UserAttributes - The address of a *struct vam_attr* pointer. When attributes for a user are fetched, a pointer to a linked list of *vam_attr* structures will be returned in this variable.

Note! The final parameter (denoted by “0” above) is reserved for future use but must be specified.

The *vam_attr* structure is defined in the VMSAUTHENTICATE.H file, and has the following form:

```
struct vam_attr {
    char *attribute_name;
    char *value;
    struct vam_attr *next;
};
```

The fields within this structure are:

attribute_name - pointer to a character string that will contain the name of the attribute that was specified in the *ATTRIBUTE* keyword in the VAM:VAM_CONFIG.DAT file.

value - pointer to a character string that contains the value fetched for *attribute_name*. This will be NULL if no value was fetched.

next - pointer to the next attribute structure. This will be zero if the end of the attribute chain has been reached.

Outputs

None.

Returns

SS\$_NORMAL

Authentication successful.

SS\$_ABORT

Authentication was aborted by the server

SS\$_BADPARAM

- No username was supplied
- Authentication type was not "SECURID", "LDAP" or "LOCALUAF"
- All callbacks were not supplied

SS\$_CANCEL

- Authentication was aborted by the user

SS\$_NOLICENSE

A valid license was not loaded.

Note! When performing authentication, the return status will never tell the user program (provided the arguments to the routine call were correct) why the authentication failed, only that it did fail. Providing this information to a user could provide an attacker with a clue as to what to try next.

IOCallback

This user-application-supplied routine is called when a prompt/response dialog (consisting of exactly one prompt and expecting exactly one response) must be conducted with the user. The callback will be called with the information necessary to prompt for and return the required information (for example, the prompt to use, the length characteristics of the expected response, and if the response should be echoed to the terminal screen). The callback is expected to prompt for the data and return the null-terminated data in the response field. The callback is responsible (when directed by the EchoFlag) for turning echo to the terminal off before prompting for the data, and turning echo back on after getting the data from the caller.

In the case of performing SecurID authentication, the callback routine may perform any necessary editing to ensure the format & type of the data is correct (for example, to ensure it doesn't exceed the maximum length and is of the correct - numeric or alphanumeric - type). However, this isn't required, as the VMSauthenticate routine will also perform these checks on behalf of the user. The benefit of the user program performing these checks may lie in providing the ability to instantly provide feedback to the user in the event the response violates the input parameters.

Format

```
int IOCallback(
    char *    Prompt,
    char *    Response,
    int      MinRespLen,
    int      MaxRespLen,
    int      RespType,
    int      EchoFlag,
    int      Timeout,
    int *    UserData
);
```

Inputs

- Prompt - String (null-terminated) that contains the prompt to display.
- MinRespLen - Minimum length of expected response.
- MaxRespLen - Maximum length of expected response.
- RespType - Type of data desired for the expected response, where 0 = numeric (0-9) and 1 = alphanumeric.
- EchoFlag - Set to 1 if the response should be echoed to the screen.
- Timeout - Time (in seconds) to display the prompt.
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

Outputs

- Response - character string (null-terminated) that contains the response returned by the user.

Returns

1 = successfully completed

0 = call was aborted. This will cause the authentication session to be terminated, with VMSAuthenticate returning a status of SS\$_CANCEL.

InfoCallback

This user application-supplied callback routine is used when an informational message must be displayed by the user application with no response required (save for possibly an "OK" button in, for example, a DECwindows application).

Format

```
int InfoCallback(  
    char *    Prompt,  
    int      Timeout,  
    Int *    UserData  
);
```

Inputs

- Prompt - Character string (null-terminated) that contains the prompt to display.
- Timeout - Time (in seconds) to display the prompt
- UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

Outputs

None.

Returns

1 = successfully completed

0 = call was aborted. This will cause the authentication session to be terminated, with VMSAuthenticate() returning a status of SSS_CANCEL.

TimeoutCallback

This user application-supplied callback routine is invoked when a timeout for a prompt has been exceeded. The user application is required to terminate the I/O operation that it invoked. This timer is started just prior to calling the user-supplied IOCallback or InfoCallback routines, and the RSA Authentication Manager supplies its value.

Note! The user program must not disable AST's via the VMS \$SETAST system service. If this is done, timeouts won't be enforced.

Format

```
void TimeoutCallback(  
    int * UserData  
);
```

Inputs

UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated)..

Outputs

None.

Returns

None.

ScreenClearCallback

This user application-supplied callback routine is used when the screen should be cleared subsequent to a call to IOCallback or InfoCallback.

Format

```
int ScreenClearCallback(  
    int *   UserData  
);
```

Inputs

UserData - Pointer to a user-defined data area. The contents and size of this data area are to be defined by the user, and may contain any context information desired by the user (for example, to identify the user or terminal being authenticated).

Outputs

None.

Returns

None.

Chapter 7

Using VAM with SSH

Introduction

VAM may be used with the SSH server offerings from Process Software, found in MultiNet, TCPware and SSH for OpenVMS. The SecurID LDAP modules are implemented in the SSH2 server in the form of “*plugins*” using KEYBOARD-INTERACTIVE authentication, and require a valid VAM license to use. Furthermore, the SSH client used must support KEYBOARD-INTERACTIVE authentication.

Note! This chapter assumes the user is familiar with configuring the SSH offerings from Process Software.

Configuring VAM in SSH

The following sections describe the post-installation setup required to enable the various forms of authentication.

Configuring VAM

In general, VAM is configured for SSH support via the use of the VAM_CONFIG.DAT file. However, due to restrictions of the SSH environment, not all VAM configuration keywords are honored by SSH. These unused configuration keywords are:

- LDAP_NO_PASSWORD_SYNC
- LGI_AUTH_METHODS
- ALLOW_DECNET_LOGIN
- ALLOW_DECTERM_LOGIN
- FALLTHROUGH_TO_VMS

Configuring SSH

The SSH2_DIR:SSHD2_CONFIG file must be modified to enable KEYBOARD-INTERACTIVE

support and the proper plugin support.

The following example illustrates enabling SecurID support:

```
AllowedAuthentications      keyboard-interactive
AuthKbdInt.Required        plugin
AuthKbdInt.Plugin          securidplugin
```

The next example illustrates enabling LDAP support:

```
AllowedAuthentications      keyboard-interactive
AuthKbdInt.Required        plugin
AuthKbdInt.Plugin          ldapplugin
```

A

API

- LDAP 6-2
 - LOCALUAF 6-2
 - SECURID 6-1
-

C

- conventions 1-xi
 - customer support
 - obtaining 1-ix
-

D

- disk space requirements 1-2
 - documentation set 1-x
-

E

- electronic mail 1-ix
-

F

File

- SDSTATUS.12 3-3
 - SECURID. 3-3
-

G

- general requirements 1-2
 - global page requirements 1-2
 - global pages 1-2
-

H

- hardware requirements 1-2
-

I

- InfoCallback 6-9
 - installation preparation 1-2
 - installing on mixed platform clusters 2-4
 - IOCallback 6-7
-

K

Keyword

- ALLOW_DECNET_LOGIN 3-3, 4-3
 - ALLOW_DECTERM_LOGIN 3-3, 4-3
 - FALLTHROUGH_TO_VMS 2-5
 - LDAP_ATTRIBUTE 4-5
 - LDAP_ATTRIBUTE_BASE_DN 4-5
 - LDAP_ATTRIBUTE_FILTER 4-6
 - LDAP_AUTH_FILTER 4-4
 - LDAP_AUTH_SERVER 4-4
 - LDAP_BASE_DN 4-4
 - LDAP_CERT 4-2
 - LDAP_NOPASSWORD_SYNC 4-3
 - LDAP_SEARCHACCT_DN 4-4
 - LDAP_SEARCHACCT_PASSWORD 4-5
 - LDAP_SERVER 4-3
 - LDAP_TIMELIMIT 4-3
 - LDAP_USE_TLS 4-3
 - LGI_AUTH_METHODS 2-5
 - REQUIRE_SECURID 3-2, 4-2
-

L

- license information 1-ix
- load the software 2-1

Logical

- RSATRACEDEST 3-3
 - RSATRACELEVEL 3-3
 - VAM 2-5
 - VAM_CURRENT_TRACE_LEVEL 2-5
 - VAM_LOGFILE 2-5
 - VAM_ROOT 2-5
-

M

- maintenance services 1-ix
-

O

- Online documentation 1-3
 - online help 1-viii
-

P

- post-installation tasks 2-4, 3-1, 5-9
-

R

reader's comments 1-ix
release notes 1-3
required disk space 1-2

S

ScreenClearCallback 6-11
software requirements 1-2
starting VMSINSTAL 2-1

T

telephone 1-ix
TimeoutCallback 6-10
Trace Level
 TRACE_ERROR 2-5
 TRACE_EXECUTION_DEEP 2-5
 TRACE_EXECUTION 2-5
 TRACE_INFO 2-5

U

Utility
 ldapcompare 4-8
 ldapdelete 4-8
 ldapmodify 4-8
 ldapmodrdn 4-8
 ldappasswd 4-8
 ldapsearch 4-8
 ldapwhoami 4-8
 openssl 4-8

V

VAM public mailing list 1-viii
vam_attr structure 6-5
VAM_LGI_SECURID 3-2, 4-2
VMSAuthenticate 6-4

W

where to install 1-2
World Wide Web 1-ix

Reader's Comments
VMS Authentication Module Version 2.0 Administration and User's Guide

Your comments and suggestions will help us to improve the quality of our future documentation. Please note that this form is for comments on documentation only.

I rate this guide's:	Excellent	Good	Fair	Poor
Accuracy	0	0	0	0
Completeness (enough information)	0	0	0	0
Clarity (easy to understand)	0	0	0	0
Organization (structure of subject matter)	0	0	0	0
Figures (useful)	0	0	0	0
Index (ability to find topic)	0	0	0	0
Ease of use	0	0	0	0

1. I would like to see more/less: _____
2. Does this guide provide the information you need to perform daily tasks? _____
3. What I like best about this guide: _____
4. What I like least about this guide: _____

My additional comments or suggestions for improving this guide: _____

I found the following errors in this guide:

Page	Description
_____	_____
_____	_____

Please indicate the type of user/reader that you most nearly represent:

System Manager	0	Educator/Trainer	0
Experienced Programmer	0	Sales	0
Novice Programmer	0	Scientist/Engineer	0
Computer Operator	0	Software Support	0
Administrative Support	0	Other (please specify)	0 _____

Name: _____ Dept. _____
 Company: _____ Date _____
 Mailing Address: _____

After filling out this form, FAX or mail it to:
Process Software, 959 Concord Street, Framingham, MA 01701-4682
Attention: Technical Publications Group FAX 508-879-0042 e-mail:techpubs@process.com

