

VMS Authorize Utility Manual

Order Number: AA-LA42A-TE

April 1988

This document describes the Authorize Utility for use on VAX processors.

Revision/Update Information: This document supersedes the
*VAX/VMS Authorize Utility Reference
Manual, Version 4.0.*

Software Version: VMS Version 5.0

**digital equipment corporation
maynard, massachusetts**

April 1988

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.


No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Copyright ©1988 by Digital Equipment Corporation

All Rights Reserved.
Printed in U.S.A.

The postpaid READER'S COMMENTS form on the last page of this document requests the user's critical evaluation to assist in preparing future documentation.

The following are trademarks of Digital Equipment Corporation:

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

ZK4533

**HOW TO ORDER ADDITIONAL DOCUMENTATION
DIRECT MAIL ORDERS**

USA & PUERTO RICO*

Digital Equipment Corporation
P.O. Box CS2008
Nashua, New Hampshire
03061

CANADA

Digital Equipment
of Canada Ltd.
100 Herzberg Road
Kanata, Ontario K2K 2A6
Attn: Direct Order Desk

INTERNATIONAL

Digital Equipment Corporation
PSG Business Manager
c/o Digital's local subsidiary
or approved distributor

In Continental USA and Puerto Rico call 800-258-1710.

In New Hampshire, Alaska, and Hawaii call 603-884-6660.

In Canada call 800-267-6215.

* Any prepaid order from Puerto Rico must be placed with the local Digital subsidiary (809-754-7575).

Internal orders should be placed through the Software Distribution Center (SDC), Digital Equipment Corporation, Westminister, Massachusetts 01473.

Production Note

This book was produced with the VAX DOCUMENT electronic publishing system, a software tool developed and sold by DIGITAL. In this system, writers use an ASCII text editor to create source files containing text and English-like code; this code labels the structural elements of the document, such as chapters, paragraphs, and tables. The VAX DOCUMENT software, which runs on the VMS operating system, interprets the code to format the text, generate a table of contents and index, and paginate the entire document. Writers can print the document on the terminal or line printer, or they can use DIGITAL-supported devices, such as the LN03 laser printer and PostScript[™] printers (PrintServer 40 or LN03R ScriptPrinter), to produce a typeset-quality copy containing integrated graphics.



Contents

PREFACE	vii
NEW AND CHANGED FEATURES	ix
AUTHORIZE Description	AUTH-1
1 UTILITY COMMANDS	AUTH-2
2 QUALIFIER SUMMARY	AUTH-3
3 RECREATING SYSUAF.DAT	AUTH-10
AUTHORIZE Usage Summary	AUTH-12
AUTHORIZE Commands	AUTH-13
ADD	AUTH-14
ADD/IDENTIFIER	AUTH-16
ADD/PROXY	AUTH-18
COPY	AUTH-20
CREATE/PROXY	AUTH-22
CREATE/RIGHTS	AUTH-23
DEFAULT	AUTH-24
EXIT	AUTH-26
GRANT/IDENTIFIER	AUTH-27
HELP	AUTH-28
LIST	AUTH-30
LIST/IDENTIFIER	AUTH-32
LIST/PROXY	AUTH-34
LIST/RIGHTS	AUTH-35
MODIFY	AUTH-36
MODIFY/IDENTIFIER	AUTH-37
MODIFY/PROXY	AUTH-39
MODIFY/SYSTEM_PASSWORD	AUTH-41
REMOVE	AUTH-42
REMOVE/IDENTIFIER	AUTH-43
REMOVE/PROXY	AUTH-44
RENAME	AUTH-45
RENAME/IDENTIFIER	AUTH-47
REVOKE/IDENTIFIER	AUTH-48

Contents

SHOW	AUTH-49
SHOW/IDENTIFIER	AUTH-52
SHOW/PROXY	AUTH-54
SHOW/RIGHTS	AUTH-55

INDEX

TABLES

AUTH-1	Summary of AUTHORIZE Commands	AUTH-2
AUTH-2	Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands	AUTH-4
AUTH-3	UIC Specification with the LIST Command	AUTH-30
AUTH-4	UIC Specification with the SHOW Command	AUTH-49

Preface

Intended Audience

This manual is intended for VMS system managers, operators, and system programmers.

Document Structure

This document consists of the following three sections:

- Description—Provides an overview and detailed usage information for the Authorize Utility (AUTHORIZE).
- Usage Summary—Outlines the following AUTHORIZE information:
 - Invoking the utility
 - Exiting from the utility
 - Directing output
 - Restrictions or privileges required
- Commands—Describes AUTHORIZE commands including format, parameters, and examples.

Associated Documents

For additional information on the topics covered in this document, refer to the *VMS DCL Dictionary*, the *Guide to Setting Up a VMS System*, and the *Guide to Maintaining a VMS System*.

Conventions

The following conventions are observed in this manual:

Convention	Meaning
<code>RET</code>	In examples, a key name (usually abbreviated) shown within a box indicates that you press a key on the keyboard; in text, a key name is not enclosed in a box. In this example, the key is the RETURN key. (Note that the RETURN key is not usually shown in syntax statements or in all examples; however, assume that you must press the RETURN key after entering a command or responding to a prompt.)
<code>CTRL/C</code>	A key combination, shown in uppercase with a slash separating two key names, indicates that you hold down the first key while you press the second key. For example, the key combination CTRL/C indicates that you hold down the key labeled CTRL while you press the key labeled C. In examples, a key combination is enclosed in a box.
<code>\$ SHOW TIME</code> <code>05-JUN-1988 11:55:22</code>	In examples, system output (what the system displays) is shown in black. User input (what you enter) is shown in red.
<code>\$ TYPE MYFILE.DAT</code> . . .	In examples, a vertical series of periods, or ellipsis, means either that not all the data that the system would display in response to a command is shown or that not all the data a user would enter is shown.
<code>input-file, . . .</code>	In examples, a horizontal ellipsis indicates that additional parameters, values, or other information can be entered, that preceding items can be repeated one or more times, or that optional arguments in a statement have been omitted.
<code>[logical-name]</code>	Brackets indicate that the enclosed item is optional. (Brackets are not, however, optional in the syntax of a directory name in a file specification or in the syntax of a substring specification in an assignment statement.)
quotation marks apostrophes	The term quotation marks is used to refer to double quotation marks ("). The term apostrophe (') is used to refer to a single quotation mark.

New and Changed Features

The following changes have been made to the Authorize Utility for VMS Version 5.0:

- New proxy login features:
 - Remote users can now be granted access to one default proxy account and up to 15 other proxy accounts on the local node. See the ADD/PROXY command for information on granting remote users access to multiple proxy accounts. Use the new MODIFY/PROXY command to redefine the default proxy account.
 - Proxy access is supported from non-VMS systems that implement DECnet Phase IV+. Remote users from non-VMS systems are identified in the network proxy database by a User Identification Code (UIC).
 - The name of the network proxy authorization file has changed from NETUAF.DAT to NETPROXY.DAT. The NETACP process maintains the volatile copy of the network proxy database on the running system. NETACP creates a new copy of NETPROXY from the permanent database each time the system is bootstrapped or whenever a proxy login change is made in AUTHORIZE.
- New login flag FORCE_EXP_PWD_CHANGE forces users to change expired passwords at login. This flag is set with the /FLAGS qualifier and is used in conjunction with the /PWDLIFETIME qualifier.
- New keyword NONE for the /MAXDETACH qualifier. Specifying /MAXDETACH=NONE prevents the user from creating detached processes.
- New support for command line recall. Press CTRL/B to display previously entered commands. Up to 20 previous commands can be displayed.



AUTHORIZE Description

The Authorize Utility (AUTHORIZE) is a system management tool you use to control access to the system and to allocate resources to users. Using AUTHORIZE, you control access to the system and its resources, as follows:

- By creating new records and modifying existing records in the system user authorization file (SYS\$SYSTEM:SYSUAF.DAT) and the network proxy authorization file (SYS\$SYSTEM:NETPROXY.DAT)
- By creating new records and modifying existing records in the rights database file (SYS\$SYSTEM:RIGHTSLIST.DAT)

If you want to store SYSUAF.DAT in an alternate directory, define the logical name SYSUAF in the system logical name table in executive mode to point to the system UAF, as shown in the following example:

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE SYSUAF file-spec
```

The SYSUAF logical name should be defined in the site-specific startup command procedure SYS\$MANAGER:SYSTARTUP.COM. Similarly, you should define system logical names NETPROXY and RIGHTSLIST if you move the files NETPROXY.DAT and RIGHTSLIST.DAT to an alternate directory.

Invoke AUTHORIZE by setting your default device and directory to SYS\$SYSTEM and entering the DCL command RUN AUTHORIZE. The system responds with the *UAF>* prompt. If no system UAF exists (that is, if it has been deleted), the system issues an error message:

```
%UAF-E-NAOFIL, unable to open SYSUAF.DAT
-RMS-E-FNF, file not found
Do you want to create a new file?
```

A response of YES (or Y) results in creation of a new system UAF containing a SYSTEM record and a DEFAULT record. These records are initialized with the same values set when the system was installed. See Section 3 for more information of recreating the system UAF.

Because certain images (such as MAIL and SET) require access to the system UAF and are normally installed with the SYSPRV privilege, make certain you always grant system access to SYSUAF.DAT.

The authorization files are owned by the system (UIC of [SYSTEM]) and are created with the following default protection:

```
SYSUAF.DAT      S:RWED, O:RWED, G, W
NETPROXY.DAT   S:RWED, O:RWED, G:RWE, W
RIGHTSLIST.DAT S:RWED, O:RWED, G:RWE, W:R
```

If you need to maximize the protection for SYSUAF.DAT or NETPROXY.DAT, use the following DCL command:

```
$ SET PROTECTION=(S:RWED,O,G,W) SYS$SYSTEM:filename
```

AUTHORIZE Description

1

Utility Commands

Table AUTH-1 summarizes the AUTHORIZE commands. The ADD, COPY, DEFAULT, MODIFY, and RENAME commands act upon individual fields of system UAF records through the specification of appropriate qualifiers.

Table AUTH-1 Summary of AUTHORIZE Commands

Command	Function
ADD	Adds a system UAF record
ADD/IDENTIFIER	Adds an identifier name to the rights database
ADD/PROXY	Adds proxy access for the specified user
COPY	Copies a system UAF record
CREATE/PROXY	Creates a network proxy authorization file
CREATE/RIGHTS	Creates a new rights database file
DEFAULT	Modifies the DEFAULT system UAF record
EXIT	Returns the user to DCL command level
GRANT/IDENTIFIER	Grants an identifier name to a UIC identifier
HELP	Displays HELP text for AUTHORIZE commands
LIST	Creates a listing file of system UAF records
LIST/IDENTIFIER	Creates a listing file of identifier names and values
LIST/PROXY	Creates a listing file of all proxy accounts and all remote users with proxy access to the accounts
LIST/RIGHTS	Creates a listing file of all identifiers held by the specified user
MODIFY	Modifies one or more system UAF records
MODIFY/IDENTIFIER	Modifies the named identifier in the rights database
MODIFY/PROXY	Modifies proxy access for the specified user
MODIFY/SYSTEM_PASSWORD	Sets the system password (equivalent to the DCL command SET PASSWORD/SYSTEM)
REMOVE	Deletes a system UAF record
REMOVE/IDENTIFIER	Removes an identifier from the rights database
REMOVE/PROXY	Deletes proxy access for the specified user
RENAME	Renames a system UAF record
RENAME/IDENTIFIER	Renames an identifier in the rights database
REVOKE/IDENTIFIER	Revokes an identifier name from a UIC identifier

Table AUTH-1 (Cont.) Summary of AUTHORIZE Commands

Command	Function
SHOW	Displays system UAF records
SHOW/IDENTIFIER	Displays identifier names and values on the current output device
SHOW/PROXY	Displays proxy access allowed for the specified user
SHOW/RIGHTS	Displays on the current output device the names of all identifiers held by the specified user

2

Qualifier Summary

Table AUTH-2 lists the qualifiers, describes the corresponding fields, and specifies the defaults (as provided in the DEFAULT record in the software distribution kit). Table AUTH-2 also lists the qualifiers for the ADD, COPY, DEFAULT, MODIFY, and REMOVE commands that affect the rights database.

The ADD/PROXY, CREATE/PROXY, LIST/PROXY, MODIFY/PROXY, REMOVE/PROXY, and SHOW/PROXY commands are used to build and maintain the network proxy authorization file (NETPROXY.DAT). Qualifiers for these commands are described in the Command Section.

A group of ten AUTHORIZE commands is used to create and maintain the rights database. (For a discussion of rights database management, refer to the *Guide to VMS System Security*.) These commands are ADD/IDENTIFIER, CREATE/RIGHTS, GRANT/IDENTIFIER, LIST/IDENTIFIER, LIST/RIGHTS, MODIFY/IDENTIFIER, REVOKE/IDENTIFIER, RENAME/IDENTIFIER, SHOW/IDENTIFIER, and SHOW/RIGHTS. Qualifiers for these commands are described in the Command Section.

AUTHORIZE Description

Table AUTH-2 Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/ACCESS [=(range[,...])]	<p>Specifies hours of access for all modes of access. Syntax for range specification is:</p> <p>/[NO]ACCESS=((PRIMARY), [n-m], [n], [...], [SECONDARY], [n-m], [n], [...])</p> <p>Specify hours as integers from 0 to 23, inclusive. Hours may be specified as single hours (n), or as ranges of hours (n-m). If the ending hour of a range is earlier than the starting hour, the range extends from the starting hour through midnight to the ending hour. The first set of hours after the keyword PRIMARY specifies hours on primary days; the second set of hours after the keyword SECONDARY specifies hours on secondary days. Note that hours are <i>inclusive</i>; that is, if you grant access during a given hour, access extends to the end of that hour.</p> <p>All of the list elements are optional. If no hours are specified for a day type, access is permitted for the entire day. If only primary hours or only secondary hours are given, no access is permitted for secondary or primary days, respectively. If hours are given with no day type, they apply to both types of days.</p> <p>Negating the qualifier denies the user access to the system for the specified period of time.</p> <p>Examples:</p> <p>/ACCESS Allows unrestricted access</p> <p>/NOACCESS=SECONDARY Allows access on primary days only</p> <p>/ACCESS=(9-17) Allows access from 9 A.M. through 5:59 P.M. on all days</p> <p>/NOACCESS=(PRIMARY, 9-17, SECONDARY, 18-8) Allows access from 9 through 5:59 on secondary days and all but 9 through 5:59 on primary days</p> <p>To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.</p>
/ACCOUNT=account-name	Specifies a 1 through 8 alphanumeric character string that is the default name for the account (for example, a billing name or number). By default, a blank account name is assigned.
/ADD_IDENTIFIER	Specifies whether an identifier with the user name and account name is to be added to the rights database. The default is /ADD_IDENTIFIER. This qualifier is used only with the ADD and COPY commands.
/ASTLM=value	Specifies an AST queue limit value for the ASTLM field of the UAF record. The AST queue limit is the maximum number of asynchronous system trap (AST) operations and scheduled wake-up requests that can be outstanding at one time.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/BATCH=(range[...])	Specifies hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier.
/BIOLM=value	Specifies a buffered I/O count limit for the BIOLM field of the UAF record. The buffered I/O count limit is the maximum number of buffered I/O operations, such as terminal I/O, that can be outstanding at one time.
/BYTLM=value	Specifies the buffered I/O byte limit for the BYTLM field of the UAF record. The buffered I/O byte limit is the maximum number of bytes of nonpaged system dynamic memory that a user's job may consume at one time. Nonpaged dynamic memory is used for operations such as I/O buffering, mailboxes, file-access windows.
/CLI=cli-name	Specifies the name of the default command language interpreter (CLI) for the CLI field of the UAF record. The cli-name is 1 through 12 alphanumeric characters and should be either DCL or MCR. By default, the DCL CLI is used.
/CLITABLES	Specifies user-defined CLI tables for the account, from 1 to 31 characters. If none is specified, LOGINOUT uses the default CLI.
/CPUTIME=time	Specifies the maximum process CPU time for the CPU field of the UAF record. The maximum process CPU time is the maximum CPU time a user's process can take per session. You must specify a delta-time value. For a discussion of delta-time values, see the <i>VMS DCL Concepts Manual</i> . The default value of 0 means infinite time.
/DEFPRIVILEGES =([NO]privname[...])	Specifies default privileges for the user; that is, those enabled at login time. A NO prefix removes a privilege from the user. The keyword [NO]ALL specified with the /DEFPRIVILEGES qualifier disables or enables all user privileges.
/DEVICE=device-name	Specifies the name of the default device, which must be a direct access device. The device-name is a 1 through 31 alphanumeric character string. If you omit the colon from the device-name value, a colon is appended. The default blank value is interpreted as SYSSYSDISK. Note that if you specify a logical name as the device-name (for example, DISK1: for DUA1:), an entry for the logical name must be made in <i>Executive mode</i> in the LNM\$SYSTEM_TABLE, using the DCL command DEFINE/SYSTEM/EXEC.
/DIALUP [(range[...])]	Specifies hours of access permitted for dial-up logins. For a description of the range specification, see the /ACCESS qualifier.
/DIOLM=value	Specifies the direct I/O count limit for the DIOLM field of the UAF record. The direct I/O count limit is the maximum number of direct I/O operations (usually disk) that can be outstanding at one time.
/DIRECTORY =directory-name	Specifies the default directory-name for the DIRECTORY field of the UAF record. The directory-name is 1 through 63 alphanumeric characters. Brackets are added to the directory name if omitted. By default, the directory-name [USER] is assigned.
/ENQLM=value	Specifies the lock queue limit for the ENQLM field of the UAF record. The lock queue limit is the maximum number of locks that can be queued at one time.
/EXPIRATION=time	Expiration date and time of the account. Default is 180 days for nonprivileged users.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/FILLM=value	Specifies the open file limit for the FILLM field of the UAF record. The open file limit is the maximum number of files that can be open at one time, including active network logical links.
/FLAGS =([NO]option[,...])	Specifies login flags for the user. The following are valid options: <ul style="list-style-type: none"> AUDIT Enables/disables security auditing of all auditable operations for a specific user. The default is NOAUDIT. AUTOLOGIN Restricts the user to using the autologin mechanism to log in to an account. When set, this flag disables login by any terminal that requires entry of user name and password. The default is NOAUTOLOGIN. CAPTIVE Restricts the user by disabling CTRL/Y interrupts and prohibiting user specification of a CLI using the /CLI qualifier. The user is not allowed to specify /DISK or /COMMAND when logging in. This flag is typically used to prevent an applications user from having unrestricted access to the CLI. NO in front of the flag clears the flag. The default is NOCAPTIVE. DEFCLI Restricts the user to using the default command interpreter by prohibiting use of the /CLI qualifier at login time (the MCR command can still be used). NO in front of the flag clears the flag. The default is NODEFCLI. DISCTLY Disables future CTRL/Y interrupts. If the intent of DISCTLY is only to force execution of the login command files, that procedure should issue a SET CONTROL_Y command before exiting. NO in front of the flag clears the flag. The default is NODISCTLY. DISMAIL Enables/disables mail delivery to the user. The default is NODISMAIL. DISNEWMAIL Suppresses announcements of new mail at login time. NO in front of the flag clears the flag. The default is NODISNEWMAIL. DISRECONNECT Disables automated reconnection to an existing process when a terminal connection has been interrupted. NO in front of the flag clears the flag. The default is DISRECONNECT. DISREPORT Disables reports for login information (last login date, login failures, and so on). NO in front of the flag clears the flag. The default is NODISREPORT. DISUSER Prevents the user from logging in. NO in front of the flag clears the flag. The default is NODISUSER.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
	DISWELCOME Suppresses the "Welcome to ..." login message. NO in front of the flag clears the flag. The default is NODISWELCOME.
	FORCE_EXP_PWD_CHANGE Requires the user to change expired passwords at login. NO in front of the flag clears the flag. The default is NOFORCE_EXP_PWD_CHANGE.
	GENPWD Requires the user to use generated passwords. NO in front of the flag clears the flag. The default is NOGENPWD.
	LOCKPWD Locks the user's password and prohibits the use of the SET PASSWORD command. NO in front of the flag clears the flag. The default is NOLOCKPWD.
	PWD_EXPIRED Marks password as expired. NO in front of the flag clears the flag. The default is NOPWD_EXPIRED.
	PWD2_EXPIRED Marks second password as expired. NO in front of the flag clears the flag. The default is NOPWD2_EXPIRED.
/GENERATE_PASSWORD [=keyword]	Invokes the password generator to generate user passwords. Specify one of the following keywords: ALL Generate primary and secondary passwords. BOTH Generate primary and secondary passwords (synonym for all). CURRENT Generate primary, secondary, both, or no passwords depending on account status. Current is the default keyword. PRIMARY Generate primary password only. SECONDARY Generate secondary password only. Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.
/INTERACTIVE [=(range[...])]	Specifies hours of access for interactive logins. For a description of the range specification, see the /ACCESS qualifier.
/JTQUOTA=value	Specifies the initial byte quota with which the job-wide logical name table is to be created. The default value is 1024.
/LGICMD=file-spec	Specifies the name of the default login command file for the LGICMD field of the UAF record. The file-spec value is a standard file specification (maximum length of 63 characters) with the following defaults: a default device as specified by the /DEVICE qualifier, a default directory as specified by the /DIRECTORY qualifier, and a default file type of COM if the default command interpreter is DCL, or of CMD if the default command interpreter is MCR. The default file-spec value is a blank string. Depending on the CLI specified for the account, a file-spec of either LOGIN.COM (DCL) or LOGIN.CMD (MCR) is supplied at login time.
/LOCAL [=(range[...])]	Specifies hours of access for interactive logins via local terminals. For a description of the range specification, see the /ACCESS qualifier.
/MAXACCTJOBS=value	Specifies the maximum number of batch, interactive, and detached processes which may be active at one time for all users of the same account. The default value of 0 represents an unlimited number.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/MAXDETACH=value	Specifies the maximum number of detached processes which may be active at one time for all users of the account. The keyword NONE indicates that the account users cannot create detached processes. The default value of 0 represents an unlimited number.
/MAXJOBS=value	Specifies the maximum number of processes (interactive, batch, detached, and network) which may be active at one time for the specified user. The first four network jobs are not counted. The default value of 0 represents an unlimited number.
/MODIFY_IDENTIFIER	Specifies whether the identifier associated with a user record is to be modified in the rights database. The qualifier only applies if the UIC or user name qualifier field in the UAF is modified. The default is /MODIFY_IDENTIFIER.
/NETWORK [(range[...])]	Specifies hours of access for network batch jobs. For a description of the range specification, see the /ACCESS qualifier.
/OWNER=owner-name	The owner-name specifies the name of the owner of the account. This name can be used, for example, for billing purposes. The owner-name is 1 through 31 characters and has a blank name for its default.
/PASSWORD=(password1 [,password2])	<p>Specifies up to two passwords for login. Passwords can be from 0 to 31 characters in length, and can include alphanumeric characters, dollar signs, and underscores.</p> <p>To set both passwords, specify the following: /PASSWORD=(password1, password2)</p> <p>To set only the first password and nullify the second, specify the following: /PASSWORD=password</p> <p>To change the first password without affecting the second, specify the following: /PASSWORD=(password, "")</p> <p>To set only the second password, specify the following: /PASSWORD=("", password)</p> <p>To set both passwords to null, specify the following: /NOPASSWORD</p> <p>If you omit the qualifier in the ADD command, the password defaults to USER. Note, however, that you <i>must</i> specify a password when creating a new UAF record with the COPY or RENAME command.</p>
/PGFLQUOTA=value	Specifies the paging file limit for the PGFLQUOTA field of the UAF record. The paging file limit is the maximum number of pages that the user's process can use in the system paging file.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/PRCLM=value	Specifies the subprocess creation limit for the PRCLM field of the UAF record. The subprocess creation limit is the maximum number of subprocesses that can exist at one time for the user's process.
/PRIMEDAYS =([NO]day[,...])	Defines the primary and secondary days of the week for the PRIMARY DAYS and SECONDARY DAYS fields of the UAF record. Specify the primary and secondary days as a list of days separated by commas and enclosed in parentheses. If you omit the qualifier, default primary days are Monday through Friday and the secondary days are Saturday and Sunday. To designate a day as a secondary day, use the prefix NO with the day name. Unique abbreviations of day names are acceptable. Any days omitted from the list take their default value.
/PRIORITY=value	Specifies the default base priority for the PRIO field of the UAF record. The value is an integer in the range of 0 through 31 with a default value of 4 for timesharing users.
/PRIVILEGES =([NO]privname[,...])	<p>Specifies one or more privileges for the PRIVILEGES field of the UAF record. When used with the ADD command, the specified privileges are added to the UAF record. If you specify a single privname value, you can omit the parentheses. If you specify more than one privname, separate them with commas and enclose the list in parentheses. The NO prefix removes the specified privilege from the user. The keyword [NO]ALL specified with the /PRIVILEGES qualifier disables or enables all user privileges.</p> <p>For a list of privileges and their functions, see the <i>Guide to Setting Up a VMS System</i>.</p>
/[NO]PWDEXPIRED	Specifies whether a password is valid only for the first login. In order to log in to the account after the first session, the user must specify a new password during this session with the DCL command SET PASSWORD. The /PWDEXPIRED qualifier only affects accounts which have a nonzero password lifetime.
/[NO]PWLIFETIME=time	Specifies or negates the length of time a password is valid. You must specify a delta-time value. For a discussion of delta-time values, see the <i>VMS DCL Concepts Manual</i> . If a period longer than the specified time has elapsed when the user logs in, a warning message is displayed, and the password is marked as expired. The default is 180 00:00.
/PWDMINIMUM=value	Specifies minimum password length in characters (default is 6). Note that this value is enforced only by the DCL command SET PASSWORD. Passwords in violation of this value may be specified to AUTHORIZE.
/REMOTE =[range[,...]]	Specifies hours of access permitted for interactive login via network remote terminals (that is, SET HOST). For a description of the range specification, see the /ACCESS qualifier.
/REMOVE_IDENTIFIER	Specifies whether the user name and account name identifiers should be removed from the rights database when a UAF record is removed from SYSUAF.DAT. This qualifier is used only with the REMOVE command. The account name identifier is removed only if there are no remaining UAF records with the same group as the deleted record. If identifiers should not be removed, specify /NOREMOVE_IDENTIFIER. The default is /REMOVE_IDENTIFIER.

AUTHORIZE Description

Table AUTH-2 (Cont.) Summary of Qualifiers for the ADD, COPY, DEFAULT, and MODIFY Commands

Qualifier	Function
/SHRFILLM=value	Specifies the maximum number of shared files the user may have open at one time. The default value of 0 represents an infinite number.
/TQELM	Specifies the total number of entries in the timer queue, plus the number of temporary common event flag clusters that the user can have at one time.
/UIC=uic	Specifies the user identification code (UIC) for the UIC field of the UAF record. The UIC value, specified in octal, is a group and member number separated by a comma and enclosed in brackets. The group number must be in the range 1-37776 (octal), the member number in the range 0-177776 (octal). The default UIC value is [200,200].
/WSDEFAULT=value	Specifies the default working set size for the WSDEFAULT field of the UAF record. The default working set size represents the default number of physical pages the process can use. The minimum value is 50 pages. The user can alter the default quantity up to WSQUOTA with the DCL command SET WORKING_SET. A value of 150 is satisfactory for most applications.
/WSEXTENT=value	Specifies the working set extent for the WSEXTENT field of the UAF record. The working set extent represents the absolute limit of physical memory allowed to the process. The memory over and above WSQUOTA is available to the process only when the system has excess free pages. The additional memory is taken back by the system if needed. The value is an integer equal to at least the WSQUOTA. Values of 512 and up are typical.
/WSQUOTA=value	Specifies the working set quota for the WSQUOTA field of the UAF record. The working set quota is the limit for the amount of physical memory a user process can lock into its working set. It also represents an upper limit on the amount of swap space the system reserves for this process and the upper limit on physical memory that the system allows the process to consume if the system-wide memory demand is significant. The minimum value is 50 pages.

3

Recreating SYSUAF.DAT

When you install a new VMS system, the software distribution kit provides the following AUTHORIZE records in the system user authorization file (SYSUAF.DAT) in SYS\$SYSTEM: DEFAULT, FIELD, SYSTEM, SYSTEST, and SYSTEST_CLIG.

If SYSUAF.DAT gets corrupted or accidentally deleted, you can use the template file SYSUAF.TEMPLATE in the SYS\$SYSTEM directory to recreate the file, as shown in the following example:

```
$ SET DEFAULT SYS$SYSTEM
$ RENAME SYSUAF.TEMPLATE SYSUAF.DAT
```

The qualifier defaults for these AUTHORIZE records (DEFAULT, FIELD, SYSTEM, SYSTEST, and SYSTEST_CLIG) stored in SYSUAF.TEMPLATE are identical to the defaults defined when the system was installed.

AUTHORIZE Description

You may want to create a private copy of SYSUAF.DAT in a directory other than SYS\$SYSTEM as an emergency backup for the system SYSUAF.DAT file. To affect user processes, copy any private version of SYSUAF.DAT to the SYS\$SYSTEM directory, as shown in the following example:

```
$ COPY MYSYSUAF.DAT SYS$SYSTEM:SYSUAF.DAT -  
_$/PROTECTION=(S:RWED,O:REWD,G,W)
```

AUTHORIZE Usage Summary

The Authorize Utility (AUTHORIZE) is a system management tool that allows you to control access to the system and to allocate user resources.

FORMAT RUN AUTHORIZE

PARAMETERS *None.*

usage summary

To invoke AUTHORIZE, set your process default device and directory to SYS\$SYSTEM, and type RUN AUTHORIZE. To terminate AUTHORIZE, enter the EXIT command at the UAF> prompt, or press CTRL/Z.

To create a listing file of reports for selected UAF records, enter the LIST command at the UAF> prompt. For more information on listing reports, see the description of the LIST command.

Note: Use of the Authorize Utility requires write access to SYSUAF.DAT, NETPROXY.DAT, or RIGHTSLIST.DAT in the SYS\$SYSTEM directory. Write access to these files is normally restricted to users with the system UIC or the SYSPRV or BYPASS privilege.

AUTHORIZE

AUTHORIZE Commands

AUTHORIZE COMMANDS

This section describes the AUTHORIZE commands and provides examples of their use. The commands follow the standard rules of DCL grammar, as specified in the *VMS DCL Concepts Manual*. You can abbreviate any command, keyword, or qualifier as long as the abbreviation is not ambiguous. The asterisk and the percent sign can be used as wildcard characters in the specification of user names, node names, and UICs.

The following commands are described in this section:

- ADD
- ADD/IDENTIFIER
- ADD/PROXY
- COPY
- CREATE/PROXY
- CREATE/RIGHTS
- DEFAULT
- EXIT
- GRANT/IDENTIFIER
- HELP
- LIST
- LIST/IDENTIFIER
- LIST/PROXY
- LIST/RIGHTS
- MODIFY
- MODIFY/IDENTIFIER
- MODIFY/PROXY
- MODIFY/SYSTEM_PASSWORD
- REMOVE
- REMOVE/PROXY
- RENAME
- REVOKE/PROXY
- SHOW
- SHOW/IDENTIFIER
- SHOW/PROXY
- SHOW/RIGHTS

AUTHORIZE

ADD

ADD

Adds a user record to the system UAF and corresponding identifiers to the rights database.

FORMAT **ADD** *newusername*

PARAMETER *newusername*

Specifies the name of the user record to be included in the system UAF. The **newusername** parameter is a string of 1 through 12 alphanumeric characters and may contain underscores. Although dollar signs are permitted, they are usually reserved for system names.

While fully numeric **newusernames** are permitted, fully numeric identifiers are not. Numeric **newusernames** do not receive corresponding identifiers and should be avoided.

QUALIFIERS *See Table AUTH-2.*

Qualifiers not specified take their values from the DEFAULT record, except that the default password is always USER. Typically, you take defaults on the limits, priority, privileges, command interpreter, and sometimes device; as a result, you type only the password, UIC, directory, owner, account, and sometimes device.

Note: When you add a new record to the UAF and a rights database exists, an identifier with the user name is added to the rights database (unless you specify the /NOADD_IDENTIFIER qualifier). If the record is the first member of a new UIC group, and you specify an account name with the record, a group identifier corresponding to the account name is also added to the rights database.

DESCRIPTION

When you add a record to the UAF, you should also create a first-level directory for the new user specifying the device name, directory name, and UIC of the UAF record. The following DCL command creates a first-level directory for user ROBIN:

```
$ CREATE/DIRECTORY SYS$USER:[ROBIN] /OWNER_UIC=[014,006]
```

EXAMPLES

1 UAF> ADD ROBIN /PASSWORD=SP0152/UIC=[014,006] -
_/_DEVICE=SYS\$USER/DIRECTORY=[ROBIN]/CLITABLES=DCLTABLES -
_/_OWNER="JOSEPH ROBIN" /ACCOUNT=INV
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier ROBIN value: [000014,000006] added to RIGHTSLLIST.DAT
%UAF-I-RDBADDMSGU, identifier INV value: [000014,177777] added to RIGHTSLLIST.DAT

This example illustrates the typical ADD command and qualifiers. The record that results from this command appears in the description of the SHOW command.

The commands in the next example add a record for a restricted account. Note that, because of the number of qualifiers required, a MODIFY command is used in conjunction with the ADD command to minimize the possibility of typing errors.

2 UAF> ADD WELCH /PASSWORD=SP0158/UIC=[014,051] -
_/_DEVICE=SYS\$USER/DIRECTORY=[WELCH]/OWNER="ROB WELCH"/FLAGS=DISUSER -
_/_ACCOUNT=INV/LGICMD=SECUREIN
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier WELCH value: [000014,000051] added to RIGHTSLLIST.DAT
UAF> MODIFY WELCH/FLAGS=(CAPTIVE,DISNEWMAIL,DISWELCOME,NODISUSER) -
_/_NODIALUP=SECONDARY/NETWORK=PRIMARY/CLITABLES=DCLTABLES -
_/_NOACCESS=(PRIMARY, 9-16, SECONDARY, 18-8)
%UAF-I-MDFYMSG, user records updated

The record that results from these commands and an explanation of the restrictions the record imposes appear in the description of the SHOW command.

Note that the DISUSER flag appears twice in the previous example. In the first command, setting the DISUSER flag prevents the user from logging in until all the account parameters are set up. In the second command, the DISUSER flag is disabled (by specifying NODISUSER) to allow access to the account.

AUTHORIZE

ADD/IDENTIFIER

ADD/IDENTIFIER

Adds an identifier to the rights database.

FORMAT **ADD/IDENTIFIER** *[id-name]*

PARAMETER *id-name*
Specifies the name of the identifier to be added to the rights database. If you omit the name, you must specify the /USER qualifier. The identifier name is a string of 1 through 31 alphanumeric characters that may contain underscores and dollar signs. The name must contain at least one nonnumeric character.

QUALIFIERS **/ATTRIBUTES=(keyword[,...])**
Specifies attributes to be associated with the new identifier. The following are valid keywords:

[NO]RESOURCE Determines whether holders of the identifier may charge resources to it. The default is NORESOURCE.

[NO]DYNAMIC Determines whether unprivileged holders of the identifier may add or remove it from the process rights list. The default is NODYNAMIC.

/USER=user-spec
Scans the UAF record for the specified user and creates the corresponding identifier. Specify **user-spec** by user name or UIC. You can use the asterisk wildcard to specify multiple user names or UICs. Full use of the asterisk and percent wildcards is permitted for user names; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard user name specification (*) creates identifiers alphabetically by user name; a wildcard UIC specification ([*,*]) creates them in numerical order by UIC.

/VALUE=value-specifier
Specifies the value to be attached to the identifier. The following are valid formats for the value-specifier:

IDENTIFIER:integer An integer value in the range of 65,536 to 268,435,455. You may also specify the value in hexadecimal (precede the value with %X) or octal (precede the value with %O).

Note that %X80000000 is added to the value you specify in order to differentiate general identifiers from UIC identifiers.

UIC:uic A UIC value in the standard UIC format

If the /VALUE qualifier is not specified, AUTHORIZE assigns an unused identifier value.

AUTHORIZE

ADD/IDENTIFIER

EXAMPLES

1 UAF> ADD/IDENTIFIER/VALUE=UIC:[300,011] INVENTORY
%UAF-I-RDBADMSGU, identifier INVENTORY value: [000300,000011] added to RIGHTSLLIST.DAT

The command in this example adds an identifier named INVENTORY to the rights database. By default, the identifier is not marked as a resource.

2 UAF> ADD/IDENTIFIER/ATTRIBUTES=(RESOURCE) -
_/_VALUE=IDENTIFIER:%X80011 PAYROLL
%UAF-I-RDBADMSGU, identifier PAYROLL value: %X80080011 added to RIGHTSLLIST.DAT

This command adds the identifier PAYROLL and marks it as a resource. Note that %X80000000 is added to the specified code for identifiers with integer values in order to differentiate them from identifiers with UIC values.

AUTHORIZE

ADD/PROXY

ADD/PROXY

Adds user entries to the network proxy authorization file.

FORMAT **ADD/PROXY** *node::remote-user local-user[,...]*

PARAMETERS **node**
Specifies a node name (1 through 6 alphanumeric characters). If you specify an asterisk, the specified remote user on all nodes is served by the account specified as **local-user**.

remote-user
Specifies the user name or UIC of a user at a remote node. If you specify an asterisk, all users at the specified node are served by the local user. You can also specify a wildcard asterisk in the group and member fields of the UIC.

local-user
Specifies the user names of from 1 to 16 users on the local node. If you specify an asterisk, a local-user name equal to remote-user name will be used.

POSITIONAL QUALIFIER **/DEFAULT**
Establishes the specified user name as the default proxy account. The remote user can request proxy access to an authorized account other than the default proxy account by specifying the name of the proxy account in the access control string of the network operation.

DESCRIPTION The ADD/PROXY command adds an entry to the network proxy authorization file, NETPROXY.DAT.

You can grant a remote user access to one default proxy account and up to 15 other local accounts. Remote users access proxy accounts other than the default proxy account by specifying the desired account in the access control string of the DCL command used to perform the DECnet file operation. System managers can change the default proxy account with the AUTHORIZE command MODIFY/PROXY.

The following command gives user WALTER on remote node SAMPLE proxy access to user ROBIN's account on local node AXEL.

```
UAF> ADD/PROXY SAMPLE::WALTER ROBIN/DEFAULT
%UAF-I-NAFADDMSG, record successfully added to NETPROXY.DAT
```

Through proxy login, user WALTER on remote node SAMPLE receives the default privileges of user ROBIN when performing network operations with node AXEL (the local node).

Note: Proxy login is an effective means of circumventing password specification and eliminates the need for users to reveal their passwords to users on remote systems. Always use caution in granting such access powers to remote users. Remember that the remote user can apply the full DCL command set, with the exception of SET HOST, while "logged on" to your

AUTHORIZE

ADD/PROXY

system in this fashion. Furthermore, the remote user receives the default privileges of the local user and, therefore, becomes the owner of the local user's files when executing any DCL commands.

To avoid potential security compromises, DIGITAL recommends that you create proxy accounts on the local node that are less privileged than a user's normal account on the remote node. By adding an extension such as `_NET`, you can identify the account as belonging to a remote user, while distinguishing it from a native account with the same name on the local node. See the *Guide to VMS System Security* for more information on creating proxy accounts.

When a number of users have accounts on a remote node with the same user name as on your system and require ready access to their local files, you might want to create an authorization record with the following form of the `ADD/PROXY` command:

```
UAF> ADD/PROXY SAMPLE::JONES JONES_NET/DEFAULT
%UAF-I-NAFADDMMSG, record successfully added to NETPROXY.DAT
```

This command establishes a proxy account for the user `JONES` on node `AXEL`. Note that `JONES_NET` on `AXEL` would probably be a less privileged account than `JONES` on `SAMPLE`. Nevertheless, `JONES` on `SAMPLE` has full access to any files available to `JONES_NET` on `AXEL`.

```
UAF> ADD/PROXY SAMPLE::WOODY */DEFAULT
%UAF-I-NAFADDMMSG, record successfully added to NETPROXY.DAT
```

In this command, the user `WOODY` on node `SAMPLE` can use the `WOODY` account on the local node for DECnet tasks such as remote file access.

EXAMPLES

1 UAF> ADD/PROXY MISHA::* MARCO/DEFAULT, OSCAR
%UAF-I-NAFADDMMSG, record successfully added to NETPROXY.DAT

The command in this example specifies that any user on the remote node `MISHA` can, by default, use the `MARCO` account on the local node for DECnet tasks such as remote file access. Remote users can also access the `OSCAR` proxy account by specifying the user name `OSCAR` in the access control string when remote node access is attempted.

2 UAF> ADD/PROXY MISHA::MARCO */DEFAULT
%UAF-I-NAFADDMMSG, record successfully added to NETPROXY.DAT

The command in this example specifies that user `MARCO` on the remote node `MISHA` can only use the `MARCO` account on the local node for remote file access.

AUTHORIZE

COPY

COPY

Creates a new system UAF record that duplicates an existing UAF record.

FORMAT **COPY** *oldusername newusername*

PARAMETERS ***oldusername***

Old user name for an existing user record.

newusername

New user name for a new user record. The user name is a string of 1 through 12 alphanumeric characters.

QUALIFIERS ***See Table AUTH-2.***

Qualifiers not specified in the command remain unchanged. However, since password verification includes the user name as well as the password, it will generally fail when you attempt to use a new user name with an old password. (Only null passwords can be effectively transferred from one user record to another by the COPY command.) Include the password whenever you use the COPY command.

DESCRIPTION

The COPY command creates a new system UAF record that duplicates an existing system UAF record.

You could add a new record for a new user named Thomas Sparrow that would be identical to that of Joseph Robin (but presumably different from the default record), as shown in the following example:

```
UAF> COPY ROBIN SPARROW /PASSWORD=SP0152
```

However, if you wanted to add a record for Thomas Sparrow that was the same as Joseph Robin's but differed in the UIC, directory name, password, and owner, you could use the following command:

```
UAF> COPY ROBIN SPARROW /UIC=[200,13]/DIRECTORY=[SPARROW] -  
_/PASSWORD=THOMAS/OWNER="THOMAS SPARROW"
```

You can also use the copy command to implement a system of multiple "default" records to meet the specific needs of various user groups. If, for example, you have programmers, administrators, and data entry personnel working on the same system, and the system default record uses "general-purpose" defaults, you can create "template" or "dummy" records such as PROGRAMMER, ADMINISTRATOR, and DATA_ENTRY, each tailored to the needs of a particular group. To add an account for a new user in one of these groups, you would copy the appropriate "template" record and specify a new user name, password, UIC, directory, and owner.

EXAMPLES

1 UAF> COPY ROBIN SPARROW /PASSWORD=SP0152
%UAF-I-COPMSG, user record copied
%UAF-E-RDBADDERRU, unable to add SPARROW value: [000014,00006] to RIGHTSLLIST.DAT
-SYSTEM-F-DUIDENT, duplicate identifier

The command in this example adds a record for Thomas Sparrow that is identical, except for the password, to that of Joseph Robin. Note that since there is no change in the UIC value, no identifier is added to RIGHTSLLIST.DAT. AUTHORIZE issues a "duplicate identifier" error message.

2 UAF> COPY ROBIN SPARROW /UIC=[200,13]/DIRECTORY=[SPARROW] -
_/PASSWORD=THOMAS/OWNER="THOMAS SPARROW"
%UAF-I-COPMSG, user record copied
%UAF-I-RDBADMSGU, identifier SPARROW value: [000200,000013] added to RIGHTSLLIST.DAT

The command in this example adds a record for Thomas Sparrow that is the same as Joseph Robin's except for the UIC, directory name, password, and owner. Note that you could use a similar command to copy a "template" record when adding a record for a new user in a particular user group.

AUTHORIZE

CREATE/PROXY

CREATE/PROXY

Creates and initializes the network proxy authorization file, NETPROXY.DAT.

FORMAT **CREATE/PROXY**

PARAMETERS *None.*

QUALIFIERS *None.*

DESCRIPTION NETPROXY.DAT is created with no records and is assigned the following protection:
(S:RWED,O:RWED,G:RWE,W)
If NETPROXY.DAT already exists, AUTHORIZE reports the following error message:
%UAF-W-NAFAEX, NETPROXY.DAT already exists
To create a new file, you must either delete or rename the old one.

EXAMPLE

```
UAF> CREATE/PROXY
UAF>
```

The command in this example creates and initializes the network proxy authorization file.

CREATE/RIGHTS

Creates and initializes the rights database, RIGHTSLIST.DAT.

FORMAT	CREATE/RIGHTS
---------------	----------------------

PARAMETERS	<i>None.</i>
-------------------	--------------

QUALIFIERS	<i>None.</i>
-------------------	--------------

DESCRIPTION	RIGHTSLIST.DAT is created with no records and is assigned the following protection:
--------------------	---

(S:RWED,O:RWED,G:R,W:R)

Note that the file is created only if the file does not already exist.

EXAMPLE

```
UAF> CREATE/RIGHTS
%UAF-E-RDBCREERR, unable to create RIGHTSLIST.DAT
-RMS-E-FEX, file already exists, not superseded
```

You can use the command in this example to create and initialize a new rights database. Note, however, that RIGHTSLIST.DAT is created automatically during the installation process. Thus you must delete or rename the existing file before creating a new one. For more information on rights database management, refer to the *Guide to VMS System Security*.

AUTHORIZE

DEFAULT

DEFAULT

Modifies the system UAF's DEFAULT record.

FORMAT	DEFAULT
---------------	----------------

PARAMETERS	<i>None.</i>
-------------------	--------------

QUALIFIERS	<i>See Table AUTH-2.</i> Qualifiers not specified in the command remain unchanged.
-------------------	--

DESCRIPTION	Modify the DEFAULT record when qualifiers normally assigned to a new user differ from the DIGITAL-supplied values. The following qualifiers most often need modification:
--------------------	---

- /CLI—If the command interpreter is MCR.
- /DEVICE—If most users have the same default device.
- /LGICMD—When automation of initial housekeeping chores at login time is desired through a specific login command file. VMS automates the execution of login command file in the following way:

First the system checks whether the logical name SYS\$SYLOGIN has been defined. If it has, the name is translated (in most cases to SYLOGIN.COM), and the named command file is executed. (This command file can call other login command files.) However, when it completes, the system makes another check. If the user's LGICMD field in the UAF specifies a command file, that file is executed. If LGICMD is blank, the user's file LOGIN.COM is executed automatically if the command interpreter is DCL. (In this case, all users must name their login command files LOGIN.COM.) If the command interpreter is MCR, the user's file LOGIN.COM is executed automatically.

Thus, the login protocol generally consists of a systemwide login command file followed by a user-specific login command file.

- /PRIVILEGES—When users are given different privileges than those supplied by DIGITAL.
- Quota qualifiers—When the default quotas are insufficient or inappropriate for mainstream work.

EXAMPLE

```
UAF> DEFAULT /DEVICE=SYS$USER/LGICMD=SYS$MANAGER:SECURELGN -  
_/_PRIVILEGES=(TMPMBX, GRPNAM, GROUP)  
%-UAF-MDFYMSG, user record(s) updated
```

The command in this example modifies the DEFAULT record, changing the default device, default login command file, and default privileges.

AUTHORIZE

EXIT

EXIT

Enables you to exit from AUTHORIZE and return to DCL command level. You can also return to command level by pressing CTRL/Z.

FORMAT **EXIT**

PARAMETERS *None.*

QUALIFIERS *None.*

EXAMPLES

1 UAF> EXIT
 %UAF-I-DONEMSG, system authorization file modified
 %UAF-I-NAFNOMODS, no modifications made to network authorization file
 %UAF-I-RDBDONEMSG, rights data base modified

The command in this example terminates the AUTHORIZE session and returns control to the DCL command level. Note that the utility reports any modifications made during the session.

2 UAF> CTRL/Z

In this example, CTRL/Z is pressed to terminate the AUTHORIZE session.

GRANT/IDENTIFIER

Grants the specified identifier to the user.

FORMAT **GRANT/IDENTIFIER** *id-name user-spec*

PARAMETERS *id-name*
Specifies the identifier name. Specify the name in identifier ID format (see the ADD/IDENTIFIER command).

user-spec
Specifies the UIC identifier corresponding to the user (see the ADD/IDENTIFIER command).

QUALIFIER **/ATTRIBUTES=(keyword[,...])**
Specifies attributes to be associated with the identifier. The following are valid keywords:

[NO]RESOURCE Determines whether holders of the identifier may charge resources to it. The default is NORESOURCE.

[NO]DYNAMIC Determines whether unprivileged holders of the identifier can add or remove it from the process rights list. The default is NODYNAMIC.

EXAMPLE

```
UAF> GRANT/IDENTIFIER INVENTORY [300,015]
%UAF-I-GRANTMSG, identifier INVENTORY granted to CRAMER
```

The command in this example grants the identifier INVENTORY to a user with the UIC [300,015]. The user Cramer becomes the holder of the identifier and any resources associated with it. The following command produces the same result:

```
UAF> GRANT/IDENTIFIER INVENTORY CRAMER
```

AUTHORIZE

HELP

HELP

Lists and explains AUTHORIZE commands and qualifiers.

FORMAT **HELP** [*command-name*]

PARAMETER *command-name*
Specifies the name of an AUTHORIZE command (see Table AUTH-1).

QUALIFIERS *None.*

DESCRIPTION If you do not specify a command name, HELP displays general information on the commands for which help is available. It then prompts with "Topic?". You can supply a command name or press RETURN. When you specify a command name and qualifiers, you get detailed information about that command. If you respond by pressing RETURN, you exit from the HELP command. You can also exit from the HELP command by pressing CTRL/Z.

If the command you request accepts qualifiers, the display of the help information on the command is followed by the prompt "Subtopic?". Respond to this prompt with a qualifier name, or press RETURN. If you respond by pressing RETURN, HELP prompts with "Topic?". If you want to exit from the HELP command directly from this level, press CTRL/Z.

EXAMPLES

1 UAF> HELP ADD

The HELP command in this example displays information about the ADD command:

ADD

The ADD command will create a new entry in the user authorization file.

Format for creating new entries in SYSUAF.DAT:

ADD newusername [/qualifiers]

Additional information available:

/IDENTIFIER	/PROXY	Parameters	Qualifiers			
/ACCESS	/ACCOUNT	/ASTLM	/BATCH	/BIOLM	/BYTLM	/CLI
/CLITABLES	/CPUTIME	/DEFPRIVILEGES		/DEVICE	/DIALUP	/DIOLM
/DIRECTORY	/ENQLM	/EXPIRATION		/FILLM	/FLAGS	/GENERATE
/INTERACTIVE		/JTQUOTA	/LGICMD	/LOCAL	/MAXACCTJOBS	
/MAXDETACH	/MAXJOBS	/NETWORK	/OWNER	/PASSWORD	/PBYTLM	
/PGFLQUOTA	/PRCLM	/PRIMEDAYS	/PRIORITY	/PRIVILEGES		/PWDEXPIRED
/PWDLIFETIME		/PWDMINIMUM		/QUEPRIORITY		/REMOTE
/SHRFILLM	/TQELM	/UIC	/WSDEFAULT	/WSEXTENT	/WSQUOTA	

ADD Subtopic?

AUTHORIZE

HELP

2 UAF> HELP MODIFY/WSDEFAULT

The command in this example displays information about the /WSDEFAULT qualifier:

MODIFY

/WSDEFAULT=n

Initial limit of a working set for the user process.

AUTHORIZE

LIST

LIST

Writes reports for selected UAF records to a listing file, SYSUAF.LIS.

FORMAT **LIST** [*user-spec*]

PARAMETER ***user-spec***
Specifies the user name or UIC of the desired UAF record. If you omit the user-spec parameter, the user records of all users are listed. The asterisk and percent sign wildcards are permitted in the user name.

QUALIFIERS ***/BRIEF***
Specifies that a brief report be written to SYSUAF.LIS. */BRIEF* is the default qualifier.

/FULL
Specifies that a full report be written to SYSUAF.LIS, including identifiers held by the user.

DESCRIPTION The LIST command creates a listing file of reports for selected UAF records. Print the listing file, SYSUAF.LIS, with the DCL command PRINT.

Specification of a user name results in a single-user report. Specification of the asterisk wildcard character following the LIST command results in reports for all users in ascending sequence by user name. Specification of a UIC results in reports for all users with that UIC. (DIGITAL recommends that you assign each user a unique UIC, but if users share a UIC, the report will show all users with that UIC.) You can use the asterisk wildcard character in specifying the UIC.

Table AUTH-3 shows how you specify a UIC with the LIST command and use the asterisk wildcard character with the UIC specification to produce various types of reports.

Table AUTH-3 UIC Specification with the LIST Command

Command	Description
LIST [14,6]	Lists a full report for the user (or users) with member number 6 in group 14.
LIST [14,*] /BRIEF	Lists a brief report for all users in group 14, in ascending sequence by member number.
LIST [* ,6] /BRIEF	Lists a brief report for all users with a member number of 6.
LIST [* ,*] /BRIEF	Lists a brief report for all users, in ascending sequence by UIC.

AUTHORIZE

LIST

Although you are encouraged to provide separate UICs for each user, if there are users with the same UIC, the LIST command reports users in the order in which they were added to the UAF. Full reports list the details of the limits, privileges, login flags, and command interpreter. Brief reports do not include the limits, login flags, or command interpreter, nor do they summarize the privileges. The password is never listed. See the SHOW command for examples of brief and full reports.

EXAMPLES

1 UAF> LIST ROBIN/FULL
%UAF-I-LSTMSG1, writing listing file
%UAF-I-LSTMSG2, listing file SYSUAF.LIS complete

This command lists a full report for the user record ROBIN.

2 UAF> LIST *
%UAF-I-LSTMSG1, writing listing file
%UAF-I-LSTMSG2, listing file SYSUAF.LIS complete

This command results in brief reports for all users in ascending sequence by user name. Note, however, that this is the same result you would produce had you omitted the asterisk wildcard.

3 UAF> LIST [300.*]
%UAF-I-LSTMSG1, writing listing file
%UAF-I-LSTMSG2, listing file SYSUAF.LIS complete

This command lists a brief report for all user records with a group UIC of 300.

AUTHORIZE

LIST/IDENTIFIER

LIST/IDENTIFIER

Creates a listing file (RIGHTSLIST.LIS) to which identifier information is written.

FORMAT **LIST/IDENTIFIER** *[id-name]*

PARAMETER ***id-name***
Specifies an identifier name. You can specify the wildcard character * to list all identifiers. If you omit the identifier name, you must specify /USER or /VALUE.

QUALIFIERS ***/BRIEF***
Specifies a brief listing in which only the identifier name, value and attributes appear.

/FULL
Specifies a full listing, in which the names of the identifier's holders are displayed along with the identifier's name, value, and attributes. /FULL is the default listing format.

/USER=user-spec
Specifies one or more users whose identifiers are to be listed. **User-spec** may be a user name or UIC. You can use the asterisk wildcard to specify multiple user names or UICs. Full use of the asterisk and percent wildcards is permitted for user names; UICs must be in the form [*,*], [n,*], [*n], or [n,n]. A wildcard user name specification (*) lists identifiers alphabetically by user name; a wildcard UIC specification ([*,*]) lists them numerically by UIC.

/VALUE=value-specifier
Specifies the value of the identifier to be listed. The following are valid formats for the value-specifier:

IDENTIFIER:integer An integer value in the range of 65,536 to 268,435,455. You may also specify the value in hexadecimal (precede the value with %X) or octal (precede the value with %O).

Note that %X80000000 is added to the value you specify in order to differentiate general identifiers from UIC identifiers.

UIC:uic A UIC value in the standard UIC format.

DESCRIPTION The LIST/IDENTIFIER command creates a listing file in which identifier names, attributes, values, and holders are displayed in various formats depending on the qualifiers specified. Two of these formats are illustrated in the description of the SHOW/IDENTIFIER command.

Print the listing file named RIGHTSLIST.LIS with the DCL command PRINT.

EXAMPLES

1 UAF> LIST/IDENTIFIER INVENTORY
%UAF-I-LSTMSG1, writing listing file
%UAF-I-RLSTMSG, listing file RIGHTSLLIST.LIS complete

The command in this example generates a full listing for the identifier INVENTORY, including its value (in hexadecimal), holders, and attributes.

2 UAF> LIST/IDENTIFIER/USER=ANDERSON
%UAF-I-LSTMSG1, writing listing file
%UAF-I-RLSTMSG, listing file RIGHTSLLIST.LIS complete

This command lists an identifier associated with the user ANDERSON, along with its value and attributes. Note, however, that this is the same result you would produce had you specified ANDERSON's UIC with the following forms of the command:

UAF> LIST/IDENTIFIER/USER=[300,015]

UAF> LIST/IDENTIFIER/VALUE=UIC:[300,015]

AUTHORIZE

LIST/PROXY

LIST/PROXY

Creates a listing file of the network proxy database entries.

FORMAT **LIST/PROXY**

PARAMETERS *None.*

QUALIFIERS *None.*

DESCRIPTION Use the DCL command PRINT to print the listing file, NETPROXY.LIS. The output assumes the same format as that of the SHOW/PROXY command. For an example of the output format, see the description of the SHOW/PROXY command.

EXAMPLE

```
UAF> LIST/PROXY
%UAF-I-LSTMSG1, writing listing file
%UAF-I-NETLSTMSG, listing file NETPROXY.LIS complete
```

The command in this example creates a listing file of all the entries in the network proxy database.

LIST/RIGHTS

Lists identifiers held by the specified identifier or, if /USER is specified, all identifiers held by the specified users.

FORMAT **LIST/RIGHTS** *[id-name]*

PARAMETER *[id-name]*
Specifies the name of the identifier associated with the user. Specify the identifier in UIC format. If you omit the identifier name, you must specify the /USER qualifier.

QUALIFIER */USER=user-spec*
Specifies a user whose identifiers are to be listed. **User-spec** may be a user name or UIC. You can use the asterisk wildcard to specify multiple user names or UICs. Full use of the asterisk and percent wildcards is permitted for user names; UICs must be in the form *[*,*]*, *[n,*]*, *[*,n]*, or *[n,n]*. A wildcard user name specification (***) or wildcard UIC specification (*[*,*]*) lists all identifiers held by users. The wildcard user name specification lists holders' user names alphabetically; the wildcard UIC specification lists them in the numerical order of their UICs.

DESCRIPTION Use the DCL command PRINT to print the listing file (RIGHTSLIST.LIS) produced by the LIST/RIGHTS command. For an example of the output format, see the description of the SHOW/RIGHTS command.

EXAMPLE

```
UAF> LIST/RIGHTS PAYROLL
%UAF-I-LSTMSG1, writing listing file
%UAF-I-RLSTMSG, listing file RIGHTSLIST.LIS complete
```

The command in this example lists identifiers held by PAYROLL, providing PAYROLL is the name of a UIC format identifier.

AUTHORIZE

MODIFY

MODIFY

Changes values in a system UAF user record.

FORMAT **MODIFY** *username /qualifier[,...]*

PARAMETER ***username***
Specifies the name of a user in the system UAF. The asterisk and percent sign wild card characters are permitted in the user name. When you specify a single asterisk for the user name, you modify the records of all users.

QUALIFIERS ***See Table AUTH-2.***
Qualifiers not specified in the command remain unchanged.

DESCRIPTION The MODIFY command changes values in a system UAF user record. Values not specified in the command remain unchanged.

Note that modifications to system UAF records do not affect users already logged in. The modifications take effect the next time the user logs in. If the UIC is changed, the value of the corresponding identifier is also changed.

EXAMPLES

1 UAF> MODIFY ROBIN /PASSWORD=SP0172
 %UAF-I-MDFYMSG, user record(s) updated

The command in this example changes the password for user ROBIN without altering any other values in the record.

2 UAF> MODIFY ROBIN/FLAGS=CAPTIVE
 %UAF-I-MDFYMSG, user record(s) updated

The command in this example modifies the UAF record for user ROBIN by adding the login flag CAPTIVE.

MODIFY/IDENTIFIER

Modifies an identifier in the rights database.

FORMAT **MODIFY/IDENTIFIER** *id-name*

PARAMETER *id-name*
Specifies the name of an identifier to be modified.

QUALIFIERS ***/ATTRIBUTES=(keyword[,...])***
Specifies attributes to be associated with the modified identifier. The following are valid keywords:

- [NO]RESOURCE Determines whether holders of the identifier can charge resources to it.
- If you specify RESOURCE, a holder named with the /HOLDER qualifier gains the right to charge resources to the identifier. If you specify NORESOURCE, the holder loses the right to charge resources. If you specify NORESOURCE and do not name any holder (if /HOLDER is not specified), all holders lose the right to charge resources. The default is NORESOURCE.
- [NO]DYNAMIC Determines whether unprivileged holders of the identifier can add or remove it from the process rights list. The default is NODYNAMIC.

/HOLDER=username
Specifies the holder of an identifier whose attributes are to be modified. The /HOLDER qualifier is used only in conjunction with the /ATTRIBUTES qualifier. If you specify /HOLDER, the /NAME and /VALUE qualifiers are ignored.

/NAME=id-name
Specifies a new identifier name to be associated with the identifier.

/VALUE=value-specifier
Specifies a new identifier value. Note that an identifier value cannot be modified from a UIC to a non-UIC format or vice versa. The following are valid formats for the value-specifier:

- IDENTIFIER:integer An integer value in the range of 65,536 to 268,435,455. You can also specify the value in hexadecimal (precede the value with %X) or octal (precede the value with %O).
- Note that %X80000000 is added to the value you specify in order to differentiate general identifiers from UIC identifiers.
- UIC:uic A UIC value in the standard UIC format.

AUTHORIZE

MODIFY/IDENTIFIER

DESCRIPTION The MODIFY/IDENTIFIER command changes identifier names, associated values, and attributes in the rights database. Values not specified in the command remain unchanged.

EXAMPLES

1 UAF> MODIFY/IDENTIFIER/VALUE=UIC:[300,21] ACCOUNTING
%UAF-I-RDBMDFYMSG, identifier ACCOUNTING modified

The command in this example changes the old UIC value of the identifier ACCOUNTING to a new value.

2 UAF> MODIFY/IDENTIFIER/ATTRIBUTES=NORESOURCE/HOLDER=CRAMER ACCOUNTING
%UAF-I-RDBMDFYMSG, identifier ACCOUNTING modified

The command in this example associates the attribute NORESOURCE with the identifier ACCOUNTING in CRAMER's holder record. The identifier ACCOUNTING is not changed.

MODIFY/PROXY

Modifies an entry in the network proxy authorization file (NETPROXY.DAT).

FORMAT **MODIFY/PROXY** *node::remote-user*

PARAMETERS *node*

Specifies a node name (1 through 6 alphanumeric characters). If you specify an asterisk, the specified remote user on all nodes is served by the local user.

remote-user

Specifies the user name of a user at a remote node. If you specify an asterisk, all users at the specified node are served by the local-user.

For non-VMS systems which implement DECnet Phase IV+, specifies the UIC of a user at a remote node. You can specify a wildcard asterisk in the group and member fields of the UIC.

QUALIFIER ***/DEFAULT[=local-user]***
/NODEFAULT

Designates the default user name on the local node through which proxy access from the remote user is directed. If */NODEFAULT* is specified, removes the default designation.

DESCRIPTION

Use the **MODIFY/PROXY** command to specify a different local account as the default proxy account for the remote user or to specify that there is no default proxy account for the remote user.

The first command in the following example grants remote user STIR::YETTA proxy access to the PROXY1 and PROXY2 local accounts. The default proxy account is PROXY1. The second command is used to change the default proxy account to PROXY2.

```
UAF> ADD/PROXY STIR::YETTA PROXY1/DEFAULT, PROXY2
```

```
  .
```

```
UAF> MODIFY/PROXY STIR::YETTA /DEFAULT=PROXY2
```

The next example shows the command used to remove the default proxy designation.

```
UAF> MODIFY/PROXY STIR::YETTA /NODEFAULT
```

If you remove the default proxy designation as shown in the last command, remote user STIR::YETTA must include the name of the proxy account (PROXY1 or PROXY2) in the access control string of each network operation to gain proxy access to the local system.

AUTHORIZE

MODIFY/PROXY

If no default proxy account is specified either in the network proxy database or in the access control string of the DCL command, VMS attempts to perform the network operation using the default DECnet account.

EXAMPLE

```
UAF> MODIFY/PROXY MISHA::MARCO /DEFAULT=JOHNSON
%UAF-I-NAFADMSG, record successfully modified in NETPROXY.DAT
```

The command in this example changes the default proxy account for user MARCO on the remote node MISHA to the JOHNSON account.

MODIFY/SYSTEM_PASSWORD

Changes the system password.

FORMAT **MODIFY/SYSTEM_PASSWORD=***system-password*

PARAMETER *system-password*
Specifies the new system password.

QUALIFIERS *None.*

DESCRIPTION For a detailed description of the effects of this command, refer to the discussion of the SET PASSWORD/SYSTEM command in the *VMS DCL Concepts Manual*.

EXAMPLE

UAF> MODIFY/SYSTEM_PASSWORD=ABRACADABRA
UAF>

This command changes the system password to ABRACADABRA.

AUTHORIZE

REMOVE

REMOVE

Deletes a system UAF user record and corresponding identifiers in the rights database. The DEFAULT and SYSTEM records cannot be deleted.

FORMAT **REMOVE** *username*

PARAMETER *username*
Specifies the name of a user in the system UAF.

QUALIFIER ***[/[NO]REMOVE_IDENTIFIER***
Specifies whether the user name and account name identifiers should be removed from the rights database when a record is removed from the UAF. If there are two UAF records with the same UIC, the user name identifier is removed only when the second record is deleted. Similarly, the account name identifier is removed only if there are no remaining UAF records with the same group as the deleted record.

DESCRIPTION If you remove a system UAF record for a user who also appears as a local user in the network UAF, every network UAF record for that user is also removed.

EXAMPLE

```
UAF> REMOVE ROBIN
%UAF-I-REMMSG, record removed from SYSUAF.DAT
%UAF-I-RDBREMSGU, identifier ROBIN value: [000014,000006] removed from RIGHTSLIST.DAT
```

The command in this example deletes the record for user ROBIN from the system UAF and ROBIN's UIC identifier from RIGHTSLIST.DAT.

REMOVE/IDENTIFIER

Removes an identifier from the rights database.

FORMAT **REMOVE/IDENTIFIER** *id-name*

PARAMETER *id-name*
Specifies the name of an identifier in the rights database.

QUALIFIERS *None.*

EXAMPLE

```
UAF> REMOVE/IDENTIFIER Q1SALES
%UAF-I-RDBREMSGU, identifier Q1SALES value %X80010024 removed from RIGHTSLLIST.DAT
```

The command in this example removes the identifier Q1SALES from the rights database. All of its holder records are removed with it.

AUTHORIZE

REMOVE/PROXY

REMOVE/PROXY

Deletes network proxy access for the specified remote user. The /PROXY qualifier is required.

FORMAT **REMOVE/PROXY** *node::remote-user [local-user,...]*

PARAMETERS

node

Specifies the name of a network node in the network UAF.

remote-user

Specifies the user name or UIC of a user on a remote node. The asterisk wildcard character is permitted in the remote-user specification.

local-user

Specifies the user name of from 1 to 16 users on the local node. If no local user is specified, proxy access to all local accounts is removed.

QUALIFIERS

None.

EXAMPLE

```
UAF> REMOVE/PROXY MISHA::MARCO
%UAF-I-NAFDONEMSG, record removed from NETPROXY.DAT
```

The command in this example deletes the record for MISHA::MARCO from the network proxy authorization file, removing all proxy access to the local node for user MARCO on node MISHA.

RENAME

Renames a system UAF record.

FORMAT **RENAME** *oldusername newusername*

PARAMETERS ***oldusername***
Specifies the name of a user currently in the system UAF.

newusername
Specifies the new user name.

QUALIFIERS ***/[NO]MODIFY_IDENTIFIER***
Specifies whether the corresponding identifier is renamed.

/[NO]PASSWORD[=(password[,password2])]
See Table AUTH-2.

 Because password verification includes the user name as well as the password, it will generally fail when you attempt to use a new user name with an old password. You must include a new password whenever you use the RENAME command unless you specify a null password with /NOPASSWORD.

/GENERATE_PASSWORD
See Table AUTH-2.

DESCRIPTION The RENAME command renames a system UAF record.

 The new user name must follow the user name conventions. It can consist of 1 through 12 alphanumeric characters and underscores. Although dollar signs are permitted, they are usually reserved for system names.

 The RENAME command changes the user name of the system UAF record (and, if specified, the corresponding identifier) while retaining the characteristics of the old record. Retention of these characteristics can be particularly helpful when a user's name changes.

 Note that since password verification includes the user name as well as the password, an attempted login will fail when the user whose name has been changed attempts to log in with an old password. (Only null passwords can be effectively transferred from one user record to another by the RENAME command.) Make it a practice to include a new password when you use the RENAME command, and notify the user of the change. If you omit the /PASSWORD qualifier, you receive a warning message reminding you that the old password must be changed.

 The user's network authorization records are automatically changed to the new name.

AUTHORIZE

RENAME

EXAMPLES

1 UAF> RENAME HAWKES KRAMERDOVE/PASSWORD=MARANNKRA
%UAF-I-ZZPRACREN, proxies to HAWKES renamed
%UAF-I-RENMSG, user record renamed
%UAF-I-RDBMDFYMSG, identifier HAWKES modified

The command in this example changes the name of the account Hawkes to Kramerdove, modifies the user name identifier for the account, and renames all proxies to the account.

2 UAF> RENAME HAWKES KRAMERDOVE
%UAF-I-ZZPRACREN, proxies to HAWKES renamed
%UAF-I-RENMSG, user record renamed
%UAF-W-DEFPWD, Warning: copied or renamed records must receive new password
%UAF-I-RDBMDFYMSG, identifier HAWKES modified

This example shows the warning message that the system displays if you fail to specify a new password with the RENAME command.

RENAME/IDENTIFIER

Renames an identifier in the rights database.

FORMAT **RENAME/IDENTIFIER** *old-id-name new-id-name*

PARAMETERS *old-id-name*
Specifies the name of an identifier to be renamed.

new-id-name
Specifies the new identifier name.

QUALIFIERS *None.*

DESCRIPTION The RENAME/IDENTIFIER command is functionally equivalent to the following form of the MODIFY/IDENTIFIER command:

MODIFY/IDENTIFIER/NAME=new-id-name old-id-name

EXAMPLE

```
UAF> RENAME/IDENTIFIER Q1SALES Q2SALES
%UAF-I-RDBMDFYMSG, identifier Q1SALES modified
```

The command in this example renames the identifier Q1SALES to Q2SALES.

AUTHORIZE

REVOKE/IDENTIFIER

REVOKE/IDENTIFIER

Revokes an identifier held by a user.

FORMAT **REVOKE/IDENTIFIER** *id-name user-spec*

PARAMETERS ***id-name***
The identifier name. Specify the name in identifier ID format (see the ADD/IDENTIFIER command).

user-spec
An identifier (UIC or non-UIC format) that specifies the user (see the ADD/IDENTIFIER command).

EXAMPLE

```
UAF> REVOKE/IDENTIFIER INVENTORY CRAMER
%UAF-I-REVOKEMSG, identifier INVENTORY revoked from CRAMER
```

The command in this example revokes the identifier INVENTORY from the user Cramer. Cramer loses the identifier and any resources associated with it.

Note that, since rights identifiers are stored in numeric format, it is not necessary to change records for users holding a renamed identifier.

SHOW

Displays reports for selected UAF records on the current SYS\$OUTPUT device.

FORMAT **SHOW** *user-spec*

PARAMETER *user-spec*
Specifies the user name or UIC of the desired UAF record. If you omit the user-spec parameter, the UAF records of all users are listed. The asterisk and percent sign wildcard characters are permitted in the user name.

QUALIFIERS */BRIEF*
Specifies that a brief report be displayed. If you omit the */BRIEF* qualifier, a full report is displayed.

/FULL
Specifies that a full report be displayed, including identifiers held by the user.

DESCRIPTION Specification of a user name results in a single-user report. Specification of an asterisk wildcard character results in reports for all users in ascending sequence by user name. Specification of a UIC results in reports for all users with the UIC. You can use the asterisk wildcard character in specifying the UIC, as illustrated in the following table:

Table AUTH-4 UIC Specification with the SHOW Command

Command	Description
SHOW [14,6]	Displays a full report for the user (or users) with member number 6 in group 14.
SHOW [14,*] /BRIEF	Displays a brief report for all users in group 14, in ascending sequence by member number.
SHOW [* ,6] /BRIEF	Displays a brief report for all users with a member number of 6.
SHOW [* ,*] /BRIEF	Displays a brief report for all users, in ascending sequence by UIC.

Users with the same UIC are listed in the order that they were added to the system UAF. Full reports include the details of the limits, privileges, login flags, and the command interpreter, and show identifiers held by users. The password is never listed.

AUTHORIZE

SHOW

EXAMPLES

1 UAF> SHOW ROBIN

The command in this example displays a full report for the user ROBIN. The display corresponds to the first example in the description of the ADD command. Note that most defaults are in effect.

```
Username: ROBIN                               Owner: JOSEPH ROBIN
Account: VMS                                  UIC: [14,6] ([INV,ROBIN])
CLI: DCL                                       Tables: DCLTABLES
Default: SYS$USER:[ROBIN]
LGICMD:
Login Flags:
Primary days: Mon Tue Wed Thu Fri
Secondary days:                               Sat Sun
No access restrictions
Expiration: (none) Pwdminimum: 6 Login Fails: 0
Pwdlifetime: (none) Pwdchange: 15-APR-1987 14:08
Last Login: (none) (interactive), (none) (non-interactive)
Maxjobs: 0 Fillm: 20 Byt1m: 12480
Maxacctjobs: 0 Shrfillm: 0 Pbyt1m: 0
Maxdetach: 0 BIO1m: 6 JTquota: 1024
Prclm: 2 DIO1m: 6 WSdef: 300
Prio: 4 AST1m: 10 WSquo: 350
Queprio: 0 TQE1m: 10 WSextent: 700
CPU: (none) Enqlm: 30 Pgflquo: 12480
Authorized Privileges:
  TMPMBX NETMBX
Default Privileges:
  TMPMBX NETMBX
Identifier Value Attributes
CLASS_CA101 %X80010032 NORESOURCE NODYNAMIC
CLASS_PY102 %X80010049 NORESOURCE NODYNAMIC
```

Note: The quotas Pbyt1m and Queprio are not implemented for Version 5.0 and thus are not documented in this manual.

2 UAF> SHOW [360,*] /BRIEF

The command in this example displays a brief report for every user with a group UIC of 360.

Owner	Username	UIC	Account	Privs	Pri	Default	Directory
JOHN SMITH	SMITH	[360,201]	USER	Normal	4	DOCD\$:	[SMITH]
MARY JONES	JONES	[360,203]	DOC	Devour	4	DOCD\$:	[JONES]
STEVE BROWN	BROWN	[360,021]	DOC	All	4	DOCD\$:	[BROWN]
SUE CARTER	CARTER	[360,005]	DOCSEC	Group	4	DOCD\$:	[CARTER]

AUTHORIZE SHOW

3 UAF> SHOW WELCH

This command displays a full report for the restricted user WELCH. The display corresponds to the second example in the description of the ADD command.

```
Username: WELCH                               Owner: ROB WELCH
Account: INV                                   UIC: [14,51] ([14,51])
CLI: DCL                                       Tables: DCLTABLES
Default: SYS$USER:[WELCH]
LGICMD: SECUREIN
Login Flags: Captive Diswelcome Disnewmail
Primary days: Mon Tue Wed Thu Fri
Secondary days:                               Sat Sun
Primary 000000000011111111112222 Secondary 000000000011111111112222
Day Hours 012345678901234567890123 Day Hours 012345678901234567890123
Network: ---- No access ----                ##### Full access #####
Batch: #####-----#####                -----#####-----
Local: #####-----#####                -----#####-----
Dialup: ##### Full access #####           ---- No access ----
Remote: #####-----#####                -----#####-----
Expiration: (none) Pwdminimum: 6 Login Fails: 0
Pwdlifetime: (none) Pwdchange: (pre-expired)
Last Login: (none) (interactive), (none) (non-interactive)
Maxjobs: 0 Fillm: 20 Byt1m: 4096
Maxacctjobs: 0 Shrfillm: 0 Pbyt1m: 0
Maxdetach: 0 BI01m: 6 JTquota: 1024
Prclm: 2 DI01m: 6 WSdef: 150
Prio: 4 AST1m: 10 WSquo: 200
Queprio: 4 TQE1m: 10 WSextent: 500
CPU: (none) Enqlm: 10 Pgflquo: 10000
Authorized Privileges:
TMPMBX NETMBX
Default Privileges:
TMPMBX NETMBX
```

Note that WELCH is a captive user who does not receive announcements of new mail or the welcome message when logging in. His login command file, SECUREIN.COM, is presumably a captive command file that controls all of his operations. (Such a command file never exits, but performs operations for its user and logs him out when appropriate.) The CAPTIVE flag prevents WELCH from escaping control of the command file by using CTRL/Y or other means. Furthermore, he is restricted to logging in between the hours of 5:00 P.M. and 8:59 A.M. on weekdays and 9:00 A.M. and 5:59 P.M. on weekends. Although he is allowed to use dial-up lines at all times during the week, he is not allowed then to log in over the network. On weekends he is further restricted so that he cannot dial in at any time or use the DCL command SET HOST between the hours of 6:00 P.M. and 8:59 A.M.

AUTHORIZE

SHOW/IDENTIFIER

SHOW/IDENTIFIER

Displays information about the identifier on the current SYS\$OUTPUT device.

FORMAT **SHOW/IDENTIFIER** *[id-name]*

PARAMETER ***id-name***
Specifies an identifier name. If you omit the identifier name, you must specify /USER or /VALUE.

QUALIFIERS ***/BRIEF***
Specifies a brief listing, in which only the identifier name, value, and attributes are displayed. /BRIEF is the default format for the SHOW/IDENTIFIER command.

/FULL
Specifies a full listing in which the names of the identifier's holders are displayed along with the identifier's name, value, and attributes.

/USER=user-spec
Specifies one or more users whose identifiers are to be displayed. **User-spec** can be a user name or UIC. You can use the asterisk wildcard to specify multiple user names or UICs. Full use of the asterisk and percent wildcards is permitted for user names; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard user name specification (*) displays identifiers alphabetically by user name; a wildcard UIC specification ([*,*]) displays them numerically by UIC.

/VALUE=value-specifier
Specifies a value in any valid format (see the LIST/IDENTIFIER command).

DESCRIPTION The SHOW/IDENTIFIER command displays identifier names, values, attributes, and holders in various formats depending on the qualifiers specified. Two of these formats are illustrated in the following examples.

EXAMPLES

1 UAF> SHOW/IDENTIFIER/FULL INVENTORY

The command in this example would produce output similar to the following:

Name	Value	Attributes
INVENTORY	%X80010006	NORESOURCE NODYNAMIC
Holder	Attributes	
ANDERSON	NORESOURCE	NODYNAMIC
BROWN	NORESOURCE	NODYNAMIC
CRAMER	NORESOURCE	NODYNAMIC

AUTHORIZE SHOW/IDENTIFIER

2 UAF> SHOW/IDENTIFIER/USER=ANDERSON

This command displays the identifier associated with the user ANDERSON, as follows:

Name	Value	Attributes
ANDERSON	[000300,000015]	NORESOURCE NODYNAMIC

The identifier is shown, along with its value and attributes. Note, however, that this is the same result you would produce had you specified ANDERSON's UIC with the following forms of the command:

UAF> SHOW/IDENTIFIER/USER=[300,015]

UAF> SHOW/IDENTIFIER/VALUE=UIC:[300,015]

AUTHORIZE

SHOW/PROXY

SHOW/PROXY

Displays all authorized proxy access for the specified remote user. The /PROXY qualifier is required.

FORMAT **SHOW/PROXY** *node::remote-user*

PARAMETERS *node*
Specifies the name of a network node in the network UAF. The asterisk wildcard is permitted in the node specification.

remote-user
Specifies the user name or UIC of a user on a remote node. The asterisk wildcard is permitted in the remote-user specification.

QUALIFIERS *None.*

EXAMPLE

UAF> SHOW/PROXY SAMPLE::[200,100]

Default proxies are flagged with an *

SAMPLE:: [200,100]

MARCO *
PROXY3

PROXY2

The command in this example displays all authorized proxy access for the user on node SAMPLE with a UIC of [200,100]. The default proxy account can be changed from MARCO to PROXY2 or PROXY3 with the MODIFY/PROXY command.

SHOW/RIGHTS

Displays the identifiers held by the specified identifiers or, if /USER is specified, all identifiers held by the specified users.

FORMAT **SHOW/RIGHTS** *[user-spec]*

PARAMETER *[user-spec]*
The name of the identifier associated with the user. Specify the identifier in UIC format. If you omit the identifier name, you must specify the /USER qualifier.

QUALIFIER */USER=user-spec*
Specifies one or more users whose identifiers are to be listed. **User-spec** can be a user name or UIC. You can use the asterisk wildcard to specify multiple user names or UICs. Full use of the asterisk and percent wildcards is permitted for user names; UICs must be in the form *[*,*]*, *[n,*]*, *[*,n]*, or *[n,n]*. A wildcard user name specification (***) or wildcard UIC specification (*[*,*]*) displays all identifiers held by users. The wildcard user name specification displays holders' user names alphabetically; the wildcard UIC specification displays them in the numerical order of their UICs.

DESCRIPTION Output displayed from the SHOW/RIGHTS command is identical to that written to RIGHTSLIST.LIS when you use the LIST/RIGHTS command.

EXAMPLE

UAF> SHOW/RIGHTS ANDERSON

This command displays all identifiers held by the user ANDERSON. For example:

Name	Value	Attributes
INVENTORY	%X80010006	NORESOURCE NODYNAMIC
PAYROLL	%X80010022	NORESOURCE NODYNAMIC

Note that the following formats of the command produce the same result:

SHOW/RIGHTS/USER=ANDERSON
SHOW/RIGHTS/USER=[300,015]



Index

A

ADD/IDENTIFIER command • AUTH-16
ADD/PROXY command • AUTH-18
ADD command • AUTH-14
Authorize Utility (AUTHORIZE)
 commands • AUTH-13 to AUTH-55
 DCL qualifiers • AUTH-3 to AUTH-10
 default password • AUTH-14
 DEFAULT record • AUTH-14
 directing output from • AUTH-12
 exiting from • AUTH-12
 invoking • AUTH-12
 login flags • AUTH-6
 restrictions • AUTH-12

C

Command summary • AUTH-2
COPY command • AUTH-20
CREATE/PROXY command • AUTH-22
CREATE/RIGHTS command • AUTH-23

D

DEFAULT command • AUTH-24
Default protection
 for NETPROXY.DAT • AUTH-1
 for RIGHTSLIST.DAT • AUTH-1
 for SYSUAF.DAT • AUTH-1
Default user authorization record
 modifying • AUTH-24
Directory
 creating • AUTH-14

E

EXIT command • AUTH-26

F

Flags
 login • AUTH-6

G

GRANT/IDENTIFIER command • AUTH-27

H

HELP command • AUTH-28

I

Identifiers
 default • AUTH-14
 granting • AUTH-27
 renaming • AUTH-47
 revoking • AUTH-48

L

List
 of network proxy database • AUTH-34
 of rights database • AUTH-32, AUTH-35
 of system user authorization file (SYSUAF) • AUTH-30
LIST/IDENTIFIER command • AUTH-32
LIST/PROXY command • AUTH-34
LIST/RIGHTS command • AUTH-35
LIST command • AUTH-30
Login command file • AUTH-24
 LOGIN.COM • AUTH-24
 LOGIN.COM • AUTH-24

Index

M

MODIFY/IDENTIFIER command • AUTH-37
MODIFY/PROXY command • AUTH-39
MODIFY/SYSTEM_PASSWORD command •
AUTH-41
MODIFY command • AUTH-36

N

NETPROXY.DAT
See Network proxy authorization file
(NETPROXY)
Network proxy authorization file (NETPROXY)
creating • AUTH-22
displaying proxy access • AUTH-54
modifying • AUTH-1

P

Proxy accounts
deleting • AUTH-44
how to add • AUTH-18
modifying • AUTH-39
Proxy login • AUTH-18, AUTH-39

Q

Qualifier summary • AUTH-3

R

Records
duplicating • AUTH-20
REMOVE/IDENTIFIER command • AUTH-43
REMOVE/PROXY command • AUTH-44
REMOVE command • AUTH-42
RENAME/IDENTIFIER command • AUTH-47
RENAME command • AUTH-45
REVOKE/IDENTIFIER command • AUTH-48
Rights database
adding identifiers to • AUTH-16

Rights database (cont'd.)
altering identifiers in • AUTH-37
creating • AUTH-1
creation • AUTH-23
deleting identifiers from • AUTH-43
displaying identifiers in • AUTH-52
displaying records in • AUTH-55
modifying • AUTH-1
renaming identifiers • AUTH-47

S

SHOW/IDENTIFIER command • AUTH-52
SHOW/PROXY command • AUTH-54
SHOW/RIGHTS command • AUTH-55
SHOW command • AUTH-49
System password • AUTH-41
System user authorization file (SYSUAF)
creating • AUTH-1
default directory entry • AUTH-14
displaying records in • AUTH-49
modifying • AUTH-1
recreating • AUTH-10
renaming records • AUTH-45

U

UAF
See System user authorization file (SYSUAF)
User accounts
altering • AUTH-36
creating • AUTH-14
deleting • AUTH-42
User directory
creating • AUTH-14

Reader's Comments

VMS Authorize Utility Manual
AA-LA42A-TE

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

Thank you for your assistance.

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

I would like to see more/less _____

What I like best about this manual is _____

What I like least about this manual is _____

I found the following errors in this manual:

Page	Description
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Additional comments or suggestions to improve this manual:

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

Name/Title _____ Dept. _____

Company _____ Date _____

Mailing Address _____

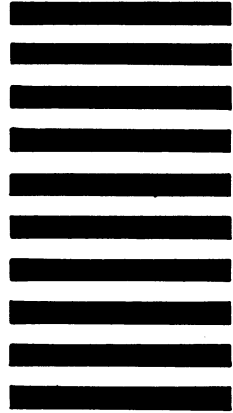
Phone _____

--- Do Not Tear - Fold Here and Tape ---

digital™



No Postage
Necessary
if Mailed
in the
United States



BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

DIGITAL EQUIPMENT CORPORATION
Corporate User Publications—Spit Brook
ZK01-3/J35 110 SPIT BROOK ROAD
NASHUA, NH 03062-9987



--- Do Not Tear - Fold Here ---

Cut Along Dotted Line

Reader's Comments

VMS Authorize Utility Manual
AA-LA42A-TE

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

Thank you for your assistance.

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

I would like to see more/less _____

What I like best about this manual is _____

What I like least about this manual is _____

I found the following errors in this manual:

Page	Description
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Additional comments or suggestions to improve this manual:

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

Name/Title _____ Dept. _____
Company _____ Date _____
Mailing Address _____
Phone _____

--- Do Not Tear - Fold Here and Tape ---

digital™

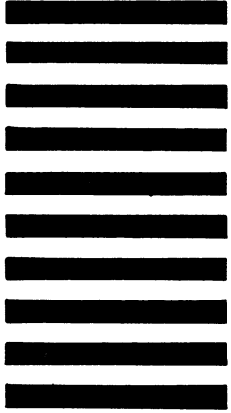


No Postage
Necessary
if Mailed
in the
United States

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

DIGITAL EQUIPMENT CORPORATION
Corporate User Publications—Spit Brook
ZK01-3/J35 110 SPIT BROOK ROAD
NASHUA, NH 03062-9987



--- Do Not Tear - Fold Here ---

Cut Along Dotted Line