VAX/VMS Authorize Utility Reference Manual

Order Number: AA–Z406A–TE

September 1984

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

Revision/Update Information: This is a new manual.

Software Version: VAX/VMS Version 4.0

digital equipment corporation
maynard, massachusetts

September 1984

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.

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
DEC/CMS
DEC/MMS
DECnet
DECsystem–10
DECSYSTEM–20
DECUS
DECwriter

DIBOL
EduSystem
IAS
MASSBUS
PDP
PDT
RSTS
RSX

UNIBUS
VAX
VAXcluster
VMS
VT

digital

ZK–2305

This document was prepared using an in-house documentation production system. All page composition and make-up was performed by TeX, the typesetting system developed by Donald E. Knuth at Stanford University. TeX is a registered trademark of the American Mathematical Society.

AUTHORIZE Contents

TABLES

Preface

Intended Audience

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

Structure of This Document

This document is composed of three major sections.

The Format Section is an overview of AUTHORIZE and is intended as a quick reference guide. The format summary contains the DCL command that invokes AUTHORIZE, listing all commands and qualifiers. The usage summary describes how to invoke and exit from AUTHORIZE, how to direct output, and any restrictions you should be aware of.

The Description Section explains how to use Authorize.

The Commands Section describes each AUTHORIZE command. Commands appear in alphabetical order.

Associated Documents

For additional information on the topics covered in this document, refer to the *VAX/VMS DCL Dictionary* and the *Guide to VAX/VMS System Management and Daily Operations.*

Conventions Used in This Document

Convention	Meaning
RET	A symbol with a one- to six-character abbreviation indicates that you press a key on the terminal, for example, RET .
CTRL/x	The phrase CTRL/x indicates that you must press the key labeled CTRL while you simultaneously press another key, for example, CTRL/C, CTRL/Y, CTRL/O.
$ SHOW TIME 05-JUN-1985 11:55:22	Command examples show all output lines or prompting characters that the system prints or displays in black letters. All user-entered commands are shown in red letters.
$ TYPE MYFILE.DAT . . .	Vertical series of periods, or ellipsis, mean either that not all the data that the system would display in response to the particular command is shown or that not all the data a user would enter is shown.

Convention	Meaning
file-spec,...	Horizontal ellipsis indicates that additional parameters, values, or information can be entered.
[logical-name]	Square brackets indicate that the enclosed item is optional. (Square 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 Authorize Utility has been extensively revised for Version 4.0. This document provides a complete description of the revised utility.

AUTHORIZE

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

FORMAT

RUN AUTHORIZE

Command Qualifiers	**Defaults**
None.	*None.*

Command Parameters

None.

usage summary

Invoking

Before you invoke the Authorize Utility, set your process default device and directory to that of SYS$SYSTEM by specifying SET DEFAULT SYS$SYSTEM. Then, to invoke AUTHORIZE, type RUN AUTHORIZE in response to the DCL prompt.

If you do not set your default device and directory to SYS$SYSTEM, the Authorize Utility will let you create a version of SYSUAF.DAT in your default directory. However, records you create or modify in a such a "private copy" of SYSUAF.DAT do not affect user processes.

Note: **System managers may want to create a private copy of SYSUAF.DAT in a directory other than SYS$SYSTEM as an emergency backup for the system SYSUAF.DAT file. To affect user processes, they must copy any private version of SYSUAF.DAT to the SYS$SYSTEM directory using the system UIC.**

Exiting

To terminate AUTHORIZE, issue the EXIT command at the UAF> prompt or press CTRL/Z.

Directing Output

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

Privileges/Restrictions

Use of the Authorize Utility to affect user processes requires write access to SYSUAF.DAT, NETUAF.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 privilege.

commands

Syntax

```
UAF> command [parameter]
```

AUTHORIZE Commands

```
ADD
   /[NO]ACCESS[=(range[,...])]
   /ACCOUNT=account-name
   /[NO]ADD_IDENTIFER
   /ATTRIBUTES=(keyword[,...])
   /[NO]BATCH[=(range[,...])]
   /BIOLM=value
   /BYTLM=value
   /CLI=cli-name
   /CLITABLES=clitable-name
   /CPUTIME=time
   /DEFPRIVILEGES=([NO]privname[,...])
   /DEVICE=name
   /[NO]DIALUP[=(range[,...])]
   /DIOLM=value
   /DIRECTORY=directory-name
   /ENQLM=value
   /EXPIRATION=time
   /FILLM=value
   /GENERATE_PASSWORD[=keyword]
   /FLAGS=([NO]option[,...])
   /[NO]INTERACTIVE[=(range[,...])]
   /JTQUOTA=value
   /LGICMD=file-spec
   /[NO]LOCAL[=(range[,...])]
   /MAXACCTJOBS=value
   /MAXDETACH=value
   /MAXJOBS=value
   /[NO]NETWORK[=(range[,...])]
   /OWNER=owner-name
   /[NO]PASSWORD=(password [,password2])
   /PFLAGS=([NO]option[,...])
   /PGFLQUOTA=value
   /PRCLM=value
   /P_RESTRICT=(range[,...])
   /PRIMEDAYS=([NO]day[,...])
   /PRIORITY=value
   /PRIVILEGES=([NO]privname[,...])
   /[NO]PWDEXPIRED
   /[NO]PWDLIFETIME=time
   /PWDMINIMUM=value
   /QUEPRIORITY=value
   /[NO]REMOTE[=(range[,...])]
   /SFLAGS=([NO]option[,...])
   /SHRFILLM=value
   /S_RESTRICT=(range[,...])
   /TQELM=value
   /UIC=uic
   /WSDEFAULT=value
   /WSEXTENT=value
   /WSQUOTA=value
```

```
ADD/IDENTIFIER
    /ATTRIBUTES=(keyword[,...])
    /USER=user-spec
    /VALUE=value-specifier
ADD/PROXY
COPY
    (Same qualifiers as ADD)
CREATE/PROXY
CREATE/RIGHTS
DEFAULT
    (Same qualifiers as ADD)
EXIT
GRANT/IDENTIFIER
    /ATTRIBUTES=(keyword[,...])
HELP
    (All commands and qualifiers)
LIST
    /BRIEF
    /FULL
LIST/IDENTIFIER
    /BRIEF
    /FULL
    /USER=user-spec
    /VALUE=value-specifier
LIST/PROXY
LIST/RIGHTS
    /USER=user-spec
MODIFY
    /[NO]ACCESS[=(range[,...])]
    /ACCOUNT=account-name
    /ASTLM=value
    /[NO]BATCH[=(range[,...])]
    /BIOLM=value
    /BYTLM=value
    /CLI=cli-name
    /CLITABLES=clitable-name
    /CPUTIME=time
    /DEFPRIVILEGES=([NO]privname[,...])
    /DEVICE=name
    /[NO]DIALUP[=(range[,...])]
    /DIOLM=value
    /DIRECTORY=directory-name
    /ENQLM=value
    /EXPIRATION=time
    /FILLM=value
    /FLAGS=([NO]option[,...])
    /[NO]INTERACTIVE[=(range[,...])]
    /JTQUOTA=value
    /LGICMD=file-spec
    /[NO]LOCAL[=(range[,...])]
    /MAXACCTJOBS=value
    /MAXDETACH=value
    /MAXJOBS=value
    /[NO]MODIFY_IDENTIFIER
    /[NO]NETWORK[=(range[,...])]
    /OWNER=owner-name
    /PASSWORD[=(password[,password2])]
    /PFLAGS=([NO]option[,...])
```

```
   /PGFLQUOTA=value
   /PRCLM=value
   /P_RESTRICT=(range[,...])
   /PRIMEDAYS=([NO]day[,...])
   /PRIORITY=value
   /PRIVILEGES=([NO]privname[,...])
   /[NO]PWDEXPIRED
   /[NO]PWDLIFETIME=time
   /PWDMINIMUM=value
   /QUEPRIORITY=value
   /[NO]REMOTE[=(range[,...])]
   /SFLAGS=([NO]option[,...])
   /SHRFILLM=value
   /S_RESTRICT=(range[,...])
   /TQELM=value
   /UIC=uic
   /WSDEFAULT=value
   /WSEXTENT=value
   /WSQUOTA=value
MODIFY/IDENTIFIER
   /ATTRIBUTES=(keyword[,...])
   /HOLDER=holder-name
   /NAME=id-name
   /VALUE=value-specifier
MODIFY/SYSTEM_PASSWORD=system-password
REMOVE
   /[NO]REMOVE_IDENTIFIER
REMOVE/PROXY
RENAME
   /PASSWORD[=(password[,password2])]
   /[NO]MODIFY_IDENTIFIER
RENAME/IDENTIFIER
REVOKE/IDENTIFIER
SHOW
   /BRIEF
SHOW/IDENTIFIER
   /BRIEF
   /FULL
   /USER=user-spec
   /VALUE=value-specifier
SHOW/PROXY
SHOW/RIGHTS
   /USER=user-spec
```

DESCRIPTION

Using AUTHORIZE, you control access to the system and its resources by

- Creating new records and modifying existing records in the system user authorization file (SYS$SYSTEM:SYSUAF.DAT) and the network user authorization file (SYS$SYSTEM:NETUAF.DAT)
- Creating new records and modifying existing records in the rights database file (SYS$SYSTEM:RIGHTSLIST.DAT)

1 Invoking and Terminating the Utility

The following commands invoke the utility:

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
```

Your default device and directory must be that of SYS$SYSTEM to access the system UAF or the network UAF. (Alternatively, you can define the logical name SYSUAF to point to the system UAF.)

If a system UAF exists in SYS$SYSTEM, the system responds with the following prompt:

```
UAF>
```

You can then enter any of the commands listed in Table AUTH–1.

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 values shown in Tables AUTH–3 and AUTH–4.

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 created with the following default protection:

```
SYSUAF.DAT      S:RWED, O:RWED, G, W
NETUAF.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 NETUAF.DAT, the following DCL command is recommended:

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

Caution: RIGHTSLIST.DAT must be world-readable.

You can terminate AUTHORIZE with the EXIT command or by pressing CTRL/Z.

2 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–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, REMOVE/PROXY, and SHOW/PROXY commands are used to build and maintain the records in NETUAF.DAT. None of the qualifiers in Table AUTH–2 apply to these AUTHORIZE commands.

Tables AUTH–3 and AUTH–4 show the values of the qualifiers in the SYSTEM, FIELD, SYSTEST, SYSTEST_CLIG, and DEFAULT records as provided with the software distribution kit. (The SYSTEST_CLIG account is used for testing of VAXclusters.)

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 VAX/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 not listed in Table AUTH–2. They are described in the Command Section.

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 a network UAF record
COPY	Copies a system UAF record
CREATE/PROXY	Creates a network UAF 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	Lists identifier names and values in a listing file
LIST/PROXY	Creates a listing file of network UAF records
LIST/RIGHTS	Lists names 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/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 a network UAF record
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
SHOW	Displays system UAF records
SHOW/IDENTIFIER	Displays identifier names and values on the current output device
SHOW/PROXY	Displays network UAF records
SHOW/RIGHTS	Displays on the current output device the names of all identifiers held by the specified user

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

Qualifier	Function
/ACCESS [=(range[,...])]	Specifies hours of access for all modes of access. Syntax for range specification is: `/[NO]ACCESS=([PRIMARY], [n-m], [n], [,...], [SECONDARY], [n-m], [n], [,...])` 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 *inclusive*; that is, if you grant access during a given hour, access extends to the end of that hour. All the list elements are optional. If no hours are specified for a day type, access is permitted 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. Negating the qualifier by specifying /NOACCESS completely inverts the sense of the access hours. **Examples:** */ACCESS* Allows unrestricted access */NOACCESS=SECONDARY* Allows access on primary days only */ACCESS=(9-17)* Allows access from 9 A.M. through 5:59 P.M. on all days */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 To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.
/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 username 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. The value is an integer of at least 2, and has a default of 10.
/BATCH[=(range[,...])]	Specifies hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier.

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

Qualifier	Function
/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. The value is an integer of at least 2 and has a default of 6.
/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 I/O buffering, mailboxes, file-access windows, and so forth. The value is an integer of at least 1024 and has a default of 4096.
/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 are 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 *VAX/VMS DCL Dictionary*. A value of 0 means infinite time and is the default.
/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.
/DEVICE=device-name	Specifies the name of the default device (must be a direct cess device). The device-name is a 1 through 15 alphanumeric character string. If you omit the colon from the device-name value, a colon is appended. A blank value is interpreted as SYS$SYSDISK and is the default.
/DIALUP [=(range[,...])]	Specifies hours of access permitted for dialup 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. The value is an integer of at least 2 and has a default of 18.
/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 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. The value is an integer of at least 2 and has a default of 30.
/EXPIRATION=time	Expiration date and time of the account. Default is 180 days for nonprivileged.
/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. The value is an integer of at least 2 and has a default of 20.

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

Qualifier	Function	
/FLAGS =([NO]option[,...])	Specifies login flags for the user. The following are valid options:	
	AUDIT	Enables/disables auditing of all security relevant actions. The default is NOAUDIT.
	CAPTIVE	Restricts the user by disabling CTRL/Y interrupts and prohibiting user specification of a CLI using the /CLI qualifier. Also, 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.
	DISWELCOME	Suppresses the "Welcome to ..." login message. NO in front of the flag clears the flag. The default is NODISWELCOME.
	GENPWD	Requires the user to use generated passwords. NO in front of the flag clears the flag. The default is NOGENPWD.

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

Qualifier	Function	
	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.
	PWDEXPIRED	Marks password as expired. NO in front of the flag clears the flag. The default is NOPWDEXPIRED.
	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. You may 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.	
/MAXDETACH=value	Specifies the active process limit for the MAXDETACH field of the UAF record. The active process limit is the total number of detached processes permitted at one time. The value is an integer. The default value of 0 represents an unlimited number.	

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

Qualifier	Function
/MAXJOBS=value	Specifies the active process limit for the MAXJOBS field of the UAF record. The active process limit is the total number of active processes (interactive, batch, and detached) permitted at one time. The value is an integer. 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 username qualifier field in the UAF is modifed. The default is /MODIFY_IDENTIFIER.
/NETWORK [=(range[,...])]	Specifies hours of access for batch network 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])
	Specifies up to two passwords for login. These must be from 0 to 31 characters in length, and must be composed of alphanumeric characters, dollar signs, and underscores.
	To set both passwords, specify
	`/PASSWORD=(password1, password2)`
	To set only the first password and nullify the second, specify
	`/PASSWORD=password`
	To change the first password without affecting the second, specify
	`/PASSWORD=(password, "")`
	To set only the second password, specify
	`/PASSWORD=("", password)`
	To set both passwords to null, specify
	`/NOPASSWORD`
	If you omit the qualifier in the ADD command, the password defaults to USER. Note however, that you *must* specify a password when creating a new UAF record with the COPY or RENAME command.

/PFLAGS =([NO]option[,...])	Specifies certain login flags for the PRIMARY DAYS field of the UAF record. This qualifier is obsolete and is retained for compatibility purposes. For current usage, see the description of the /ACCESS and related qualifiers.
/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. The value is an integer of at least 2048 for typical interactive processes and has a default of 10000.
/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. The value is an integer of at least 0 and has a default of 2.
/P_RESTRICT =(range[,...])	Specifies login time restrictions for the PRIMARY DAYS field of the UAF record. This qualifier is obsolete and is retained for compatibility purposes. For current usage, see the description of the /ACCESS and related qualifiers.

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

Qualifier	Function
/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. The default value is 4.
/PRIVILEGES =([NO]privname[,...])	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. For a list of privileges and their functions, See Chapter 6 in the *Guide to VAX/VMS System Management and Daily Operations*.
/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.
/PWDLIFETIME=time	Specifies or negates a password lifetime. You must specify a delta-time value. For a discussion of delta-time values, see the *VAX/VMS DCL Dictionary*. 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. 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 username 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.
/SFLAGS =([NO]option[,...])	Specifies certain login flags for the SECONDARY DAYS field of the UAF record. This qualifier is obsolete and is retained for compatibility purposes. For current usage, see the description of the /ACCESS and related qualifiers.
/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.

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

Qualifier	Function
/S_RESTRICT =(range[,...])	Specifies login time restrictions for the SECONDARY DAYS field of the UAF record. This qualifier is obsolete and is retained for compatibility purposes. For current usage, see the description of the /ACCESS and related qualifiers.
/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. The default value is 10.
/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 0–1777776 (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 value is an integer of at least 50 and has a default value of 150. 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 on physical memory that the system will allow the process to have. The memory over and above WSQUOTA is available to the process only when the system has an excess of free pages. The additional memory will be taken back by the system if needed. The value is an integer equal to at least the WSQUOTA and has a default value of 500. Values of 500 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 may lock into its working set. It also represents an upper limit on the amount of swap space the system will reserve for this process and the upper limit on physical memory that the system will allow the process to consume if the system-wide memory demand is significant. The value is an integer of at least 50 and has a default value of 500. Values in the range 200–400 are suitable for most applications. If you omit the qualifier, the WSQUOTA value is taken from the DEFAULT record.

Table AUTH–3 Initial Values of SYSTEM, FIELD, and SYSTEST Records

Qualifier	SYSTEM	FIELD	SYSTEST
/ACCESS	no restrictions	no restrictions	no restrictions
/ACCOUNT	SYSTEM	FIELD	SYSTEST
/ASTLM	24	24	24
/BIOLM	18	18	18
/BYTLM	20480	10240	4096
/CLI	DCL	DCL	DCL
/CLITABLES	blanks	blanks	blanks
/CPU	(none)	(none)	(none)
/DEFPRIVILEGES	all	GRPNAM ALLSPOOL GROUP DIAGNOSE PRMCEB LOG_IO SETPRV TMPMBX PRMMBX PHY_IO NETMBX	CMKRNL CMEXEC SYSNAM GRPNAM DETACH LOG_IO GROUP PRMCEB PRMMBX TMPMBX NETMBX VOLPRO SYSPRV PHY_IO DIAGNOSE
/DEVICE	blanks	blanks	blanks
/DIOLM	18	18	18
/DIRECTORY	[SYSMGR]	[SYSMAINT]	[SYSTEST]
/ENQLM	30	10	20
/FILLM	20	20	20
/FLAGS	no restrictions	no restrictions	no restrictions
/JTQUOTA	1024	1024	1024
/LGICMD	LOGIN	LOGIN	LOGIN
/MAXDETACH	0	0	0
/MAXJOBS	0	0	0
/OWNER	SYSTEM MANAGER	FIELD SERVICE	SYSTEST-UETP
/PASSWORD	MANAGER	SERVICE	UETP
/PGFLQUOTA	10000	10000	10000
/PRCLM	10	2	8
/PRIMEDAYS	MON,TUE,WED, THU,FRI	MON,TUE,WED, THU,FRI	MON,TUE,WED, THU,FRI
/PRIO	4	4	4
/PRIVILEGES	all	GRPNAM ALLSPOOL GROUP DIAGNOSE PRMCEB LOG_IO SETPRV TMPMBX PRMMBX PHY_IO	CMKRNL CMEXEC SYSNAM GRPNAM DETACH LOG_IO GROUP PRMCEB PRMMBX TMPMBX

Table AUTH–3 (Cont.) Initial Values of SYSTEM, FIELD, and SYSTEST Records

Qualifier	SYSTEM	FIELD	SYSTEST
		NETMBX	NETMBX VOLPRO SYSPRV PHY_IO DIAGNOSE
/SHRFILLM	0	0	0
/TQELM	20	20	20
/UIC	[001,004]	[001,010]	[001,007]
/WSDEFAULT	150	150	150
/WSEXTENT	1024	0	1024
/WSQUOTA	350	1024	350

Table AUTH–4 Initial Values of SYSTEST_CLIG and DEFAULT Records

Qualifier	SYSTEST_CLIG	DEFAULT
/ACCESS	network only	no restrictions
/ACCOUNT	SYSTEST-UETP	USER
/ASTLM	24	24
/BIOLM	18	18
/BYTLM	20480	4096
/CLI	DCL	DCL
/CLITABLES	blanks	blanks
/CPU	(none)	(none)
/DEFPRIVILEGES	CMKRNL CMEXEC SYSNAM GRPNAM PRMCEB LOG_IO NETMBX TMPMBX PRMMBX PHY_IO SYSPRV SETPRV GROUP DETACH DIAGNOSE VOLPRO	TMPMBX NETMBX
/DEVICE	blanks	blanks
/DIOLM	18	18
/DIRECTORY	[SYSTEST]	[USER]
/ENQLM	30	10
/FILLM	20	20
/FLAGS	Disctrly Defcli Lockpwd Captive	no restrictions
/JTQUOTA	1024	1024

Table AUTH–4 Initial Values of SYSTEST_CLIG and DEFAULT Records (Cont.)

Qualifier	SYSTEST_CLIG	DEFAULT
/LGICMD	UETCLIG00.COM	LOGIN
/MAXDETACH	0	0
/MAXJOBS	0	0
/OWNER	SYSTEST-UETP	USER
/PASSWORD		USER
/PGFLQUOTA	10000	10000
/PRCLM	10	2
/PRIMEDAYS	MON,TUE,WED, THU,FRI	MON,TUE,WED, THU,FRI
/PRIO	4	4
/PRIVILEGES	CMKRNL CMEXEC SYSNAM GRPNAM PRMCEB LOG_IO NETMBX TMPMBX PRMMBX PHY_IO SYSPRV SETPRV GROUP DETACH DIAGNOSE VOLPRO	TMPMBX NETMBX
/SHRFILLM	0	0
/TQELM	20	10
/UIC	[001,007]	[200,200]
/WSDEFAULT	150	150
/WSEXTENT	1024	500
/WSQUOTA	350	200

3 Error Messages

The *VAX/VMS System Messages and Recovery Procedures Reference Manual* lists the messages issued by AUTHORIZE and provides explanations and suggested user actions.

COMMANDS

The following sections present the AUTHORIZE commands. The commands follow the standard rules of DCL grammar, as specified in the *VAX/VMS DCL Dictionary*. Thus, 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.

ADD

Adds a user record to the system UAF and corresponding identifier(s) to the rights database.

FORMAT

ADD *newusername*

command parameter

newusername

Specifies the name of the user record to be included in the system UAF. The newusername 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.

Note that while fully numeric newusernames are permitted, fully numeric identifiers are not. Such newusernames, therefore, do not receive corresponding identifiers and should be avoided.

command qualifiers

See Table AUTH–2.

Qualifiers not specified take their values from the DEFAULT record, except that the default password is always USER (no matter what the password in the DEFAULT record is). 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 username is added to the rights database (unless you specify the /NOADD_IDENTIFIER qualifier). If a new record is the first in a group and the first record with an account name, an identifier with the account name is also added.**

DESCRIPTION

Whenever 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. Protection for the "ordinary" user is normally read, write, execute, and delete access for the system and owner processes, read and execute access for group processes, and no access for world processes. 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 RIGHTSLIST.DAT
%UAF-I-RDBADDMSGU, identifier INV value: [000014,177777] added to RIGHTSLIST.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" -
_/ACCOUNT=INV/LGICMD=SECUREIN/NOACCESS=(PRIMARY, 9-16, SECONDARY, 18-8)
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier WELCH value: [000014,000051] added to RIGHTSLIST.DAT
UAF> MODIFY WELCH/FLAGS=(CAPTIVE,DISNEWMAIL,DISWELCOME) -
_/NODIALUP=SECONDARY/NONETWORK=PRIMARY/CLITABLES=DCLTABLES
%UAF-I-MDFYMSG, user records updated
```

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

ADD/IDENTIFIER

Adds an identifier to the rights database.

FORMAT

ADD/IDENTIFIER *[id-name]*

command 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 id-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.

command qualifiers

/ATTRIBUTES=(keyword[,...])

Specifies atttributes to be associated with the new identifier. Valid keywords are:

RESOURCE	Holders of the identifier may charge resources to it.
NORESOURCE	Holders of the identifier may not charge resources to it.

The default is NORESOURCE.

/USER=user-spec

Scans the UAF record(s) of the specified user(s) and creates the appropriate identifier(s). Specify user-spec by username or UIC. You can use the asterisk wildcard to specify multiple usernames or UICs: full use of the asterisk and percent wildcards is permitted for usernames; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard username specification (*) creates identifiers alphabetically by username; a wildcard UIC specification ([*,*]) creates them in numerical order by UIC.

/VALUE=value-specifier

Specifies the value to be attached to the identifier. Valid formats for the value-specifier are:

IDENTIFIER:integer	An integer value in the range of 32,768 to 268,435,455. You may also specify the value in hexadecimal (%X) or octal (%O).
UIC:uic	A uic value in the standard UIC format

If the /VALUE qualfier is not specified, AUTHORIZE will assign an unused identifier value by default.

EXAMPLES

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

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

2

```
UAF> ADD/IDENTIFIER/ATTRIBUTES=(RESOURCE) -
_/VALUE=IDENTIFIER:%X80011 PAYROLL
%UAF-I-RDBADDMSGU, identifier PAYROLL value: %X80080011 added to RIGHTSLIST.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.

ADD/PROXY

Adds a user record to the network UAF.

FORMAT

ADD/PROXY *node::remote-user local-user*

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

local-user

Specifies the username of a user on a local node. If you specify an asterisk, a local-username equal to remote-username will be used.

DESCRIPTION

The ADD/PROXY command adds a user record to the network UAF.

You cannot add a record that duplicates a pair of remote node and user names that already exist in the network UAF. In other words, each user at a remote node is allowed access to the files of only one user on the local node. However, your users may wish to permit access to their files to multiple users on remote nodes.

The following command adds a network authorization record to permit access for the user WALTER on the remote node SAMPLE to the user ROBIN on the local node AXEL.

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

As a result of this network authorization record, user WALTER on SAMPLE will be permitted to issue any DCL command to act on data located in ROBIN's files on AXEL, without either logging in on AXEL as user ROBIN or including an access control string in the file specification.

Caution: **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. However, you should 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 system in this fashion. Furthermore, the remote user receives the default privileges of the local user, and for all practical purposes 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.

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

```
UAF> ADD/PROXY SAMPLE::JONES JONES_NET
%UAF-I-NAFADDMSG, record successfully added to NETUAF.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::*  *
%UAF-I-NAFADDMSG, record successfully added to NETUAF.DAT
```

This command authorizes any user on the remote node SAMPLE to access any account with the same username on your system.

Similarly, you might want to permit this sort of access for just one user.

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

In this case, 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 *
%UAF-I-NAFADDMSG, record successfully added to NETUAF.DAT
```

The command in this example specifies that the user MARCO on the remote node MISHA can use the MARCO account on the local node for DECnet tasks such as remote file access.

2

```
UAF> ADD/PROXY MISHA::* MARCO
%UAF-I-NAFADDMSG, record successfully added to NETUAF.DAT
```

The command in this example specifies that any user on the remote node MISHA can use the MARCO account on the local node for DECnet tasks such as remote file access.

COPY

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

FORMAT

COPY *oldusername newusername*

command parameters

oldusername
Oldusername for an existing user record.

newusername
Newusername for a new user record. The username is a string of 1 through 12 alphanumeric characters.

command qualifiers

See Table AUTH–2.
Qualifiers not specified in the command remain unchanged. However, since password verification includes the username as well as the password, it will generally fail when you attempt to use a new username with an old password. (Only null passwords can be effectively transferred from one user record to another by the COPY command.) Thus, you will probably want to make it a practice to 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.

As shown in Example 1, 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).

However, if you wanted to add a record for Thomas Sparrow that was essentially the same as Joseph Robin's but differed in the UIC, directory name, password, and owner, you could use the command shown in Example 2.

You can also use the copy command to implement a system of multiple "default" records to meet the specific needs of various user groups. Suppose, for example, that you have programmers, administrators, and data entry personnel working on the same system, and that 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. Then, to add an account for a new user in one of these groups, you can copy the appropriate "template" record and specify a new username, 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 RIGHTSLIST.DAT
-SYSTEM-F-DUPIDENT, duplicate identifier
```

The command in this example adds a record for Thomas Sparrow that is identical to that of Joseph Robin except for the password. Note that since there is no change in the UIC value, no identifier is added to RIGHTSLIST.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-RDBADDMSGU, identifier SPARROW value: [000200,000013] added to RIGHTSLIST.DAT
```

The command in this example adds a record for Thomas Sparrow that is essentially 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.

CREATE/PROXY

Creates and initializes a network UAF, NETUAF.DAT.

FORMAT

CREATE/PROXY

command parameters

None.

command qualifiers

None.

DESCRIPTION

NETUAF.DAT is created with no records and is assigned the following protection:

```
(S:RWED,O:RWED,G:RWE,W)
```

If NETUAF.DAT already exists, AUTHORIZE reports the following error message:

```
%UAF-W-NAFAEX, NETUAF.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 UAF.

CREATE/RIGHTS

Creates and initializes the rights database, RIGHTSLIST.DAT.

FORMAT

CREATE/RIGHTS

command parameters

None.

command qualifiers

None.

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 VAX/VMS System Security*.

DEFAULT

Modifies the system UAF's DEFAULT record.

FORMAT

DEFAULT

command parameters

None.

command qualifiers

See Table AUTH–2.
Qualifiers not specified in the command remain unchanged.

DESCRIPTION

You typically modify the DEFAULT record when qualifiers normally assigned to a new user differ from the DIGITAL-supplied values. The qualifiers most often needing modification are as follows:

- /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. VAX/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 even 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 it exists and the command interpreter is DCL. (Of course, in this case, all users must name their login command files LOGIN.COM.) If the command interpreter is MCR, the user's file LOGIN.CMD is executed automatically.

  Thus, the login protocol generally consists of a system-wide login command file followed by a user-specific login command file.
- /PRIVILEGES—When users are normally given different privileges than the DIGITAL-supplied ones
- Quota qualifiers—When the default quotas are insufficient or inappropriate for mainstream work

After modifying the default value record, you should pencil in the changes in Table AUTH–4.

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.

EXIT

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

FORMAT

EXIT

command parameters

None.

command 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*

command parameters

id-name
Is the identifier name. You must specify the name in identifier ID format (see the ADD/IDENTIFIER command).

user-spec
Is an identifier name in UIC format that specifies the user. Wildcard specifications are permitted.

command qualifier

/ATTRIBUTES=(keyword[,...])
Specifies atttributes to be associated with the new identifier. Valid keywords are:

RESOURCE	Holders of the identifier may charge resources to it.
NORESOURCE	Holders of the identifier may not charge resources to it.

The default is NORESOURCE.

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
```

HELP

Lists and explains the AUTHORIZE commands and qualifiers.

FORMAT

HELP *[command-name]*

command parameter

command-name

Name of an AUTHORIZE command (see Table AUTH–1).

command 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. Specification of command names and qualifiers obtains more detailed information. If you respond with RETURN, the HELP command exits. You can also exit from the HELP command by pressing CTRL/Z.

If the command you seek help on accepts qualifiers, the display of the help information on the command is followed by the prompt "Subtopic?". You can respond to this prompt with a qualifier name or press RETURN. If you respond with 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    /PFLAGS
  /PGFLQUOTA /P_RESTRICT           /PRCLM     /PRIMEDAYS /PRIORITY
  /PRIVILEGES           /PWDEXPIRED           /PWDLIFETIME
  /PWDMINIMUM           /QUEPRIORITY          /REMOTE    /SFLAGS
  /S_RESTRICT           /SHRFILLM  /TQELM     /UIC       /WSDEFAULT /WSEXTENT
  /WSQUOTA
ADD Subtopic?
```

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.
```

LIST

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

FORMAT

LIST *[user-spec]*

command parameter

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

command qualifiers

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

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

DESCRIPTION

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

Specification of a username 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 username. 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–5 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–5 UIC Specification with the LIST Command

Command	Description
LIST [014,006]	Lists a full report for the user (or users) with member number 006 in group 014.
LIST [014,*] /BRIEF	Lists a brief report for all users in group 014, in ascending sequence by member number.
LIST [*,006] /BRIEF	Lists a brief report for all users with a member number of 006.
LIST [*,*] /BRIEF	Lists a brief report for all users, in ascending sequence by UIC.

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-LSTMSG1, listing file SYSUAF.LIS complete
```

This command results in brief reports for all users in ascending sequence by username. 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-LSTMSG1, listing file SYSUAF.LIS complete
```

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

LIST/IDENTIFIER

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

FORMAT

LIST/IDENTIFIER *[id-name]*

command parameter

id-name

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

command 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 username or UIC. You can use the asterisk wildcard to specify multiple usernames or UICs: full use of the asterisk and percent wildcards is permitted for usernames; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard username specification (*) lists identifiers alphabetically by username; a wildcard UIC specification ([*,*]) lists them numerically by UIC.

/VALUE=value-specifier

Specifies the value of the identifier to be listed. Valid formats for the value-specifier are:

IDENTIFIER:integer	An integer value in the range of 32,768 to 268,435,455. You may also specify the value in hexadecimal (%X) or octal (%O).
UIC:uic	A uic value in the standard UIC format

If the /VALUE qualfier is not specified, AUTHORIZE will assign an unused identifier value by default.

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.

You can print the listing file, named RIGHTSLIST.LIS, with the DCL command PRINT.

EXAMPLES

1

```
UAF> LIST/IDENTIFIER INVENTORY
%UAF-I-RLSTMSG, writing listing file
%UAF-I-RLSTMSG, listing file RIGHTSLIST.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-RLSTMSG, writing listing file
%UAF-I-RLSTMSG, listing file SYSUAF.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]
```

LIST/PROXY

Creates a listing file of all the network UAF records.

FORMAT

LIST/PROXY

command parameters

None.

command qualifiers

None.

DESCRIPTION

You can use the DCL command PRINT to print the listing file, NETUAF.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-NETLSTMSG, writing listing file
%UAF-I-NETLSTMSG, listing file NETUAF.LIS complete
```

The command in this example creates a listing file of all the network UAF records.

LIST/RIGHTS

Lists identifiers held by the specified identifier, or, if /USER is specified, all identifiers held by the specified user(s).

FORMAT

LIST/RIGHTS *[id-name]*

command parameter

[id-name]

Is the name of the identifier associated with the user. Specify the identifier in UIC format. If you omit the id-name, you must specify the /USER qualifier.

command qualifier

/USER=user-spec

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

DESCRIPTION

You can 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-RLSTMSG, 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.

MODIFY

Changes values in a system UAF user record.

RMAT

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

command parameter

username

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

command 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 logged in. The modifications take effect the next time the user logs in. If the UIC is changed, then 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*

command parameter

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

command qualifiers

/ATTRIBUTES=(keyword[,...])
Specifies attributes to be associated with the modified identifier. Valid keywords are:

RESOURCE	Holders of the identifier may charge resources to it.
NORESOURCE	Holders of the identifier may not 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.

/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 id-name to be associated with the identifier.

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

IDENTIFIER:integer	An integer value in the range of 32,768 to 268,435,455. You may also specify the value in hexadecimal (%X) or octal (%O).
UIC:uic	A uic value in the standard UIC format

If the /VALUE qualfier is not specified, AUTHORIZE will assign an unused identifier value by default.

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, however.

MODIFY/SYSTEM_PASSWORD

Changes the system password.

FORMAT

MODIFY/SYSTEM_PASSWORD=*system-password*

command parameter

system-password

Specifies the new system password.

command 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 *VAX/VMS DCL Dictionary*.

EXAMPLE

```
UAF> MODIFY/SYSTEM_PASSWORD=ABRACADABRA
UAF>
```

This command changes the system password to ABRACADABRA.

REMOVE

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

FORMAT

REMOVE *username*

command parameter

username

Specifies the name of a user in the system UAF.

command qualifier

/[NO]REMOVE_IDENTIFIER

Specifies whether the username 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 username 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-RDBREMMSGU, 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*

command parameter

id-name

Specifies the name of an identifier in the rights database.

command qualifiers

None.

EXAMPLE

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

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

REMOVE/PROXY

Deletes a network UAF record. The /PROXY qualifier is required.

FORMAT

REMOVE/PROXY *node::remote-user*

command parameters

node

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

remote-user

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

command qualifiers

None.

EXAMPLE

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

The command in this example deletes the record for MISHA::MARCO from the network UAF.

RENAME

Renames a system UAF record.

FORMAT

RENAME *oldusername newusername*

command parameters

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

newusername
Specifies the changed name desired by the user.

command qualifiers

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

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

/GENERATE_PASSWORD
See Table AUTH–2.

DESCRIPTION

The RENAME command renames a system UAF record.

The new username must adhere to the username conventions. That is, 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 username 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 whenever a user's name changes, as perhaps in the case of marriage or divorce.

Note, however, that since password verification includes the username 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.) Thus, you will probably want to make it a practice to include a new password whenever you use the RENAME command and to notify the 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.

If the user possessed one or more network authorization records with the old name, they are automatically changed to the new name.

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 username 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*

command parameters

old-id-name
Specifies the name of an identifer to be renamed.

new-id-name
Specifies the new identifier name.

command 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.

REVOKE/IDENTIFIER

Revokes the specified identifier from a user.

FORMAT

REVOKE/IDENTIFIER *id-name user-spec*

command parameters

id-name
Is the identifier name (see the ADD/IDENTIFIER command).

user-spec
Is 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 it not necessary to change records for users holding a renamed identifier.

SHOW

Displays reports for selected UAF records.

FORMAT

SHOW *user-spec*

command parameter

user-spec

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

command 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 username results in a single-user report; specification of an asterisk wildcard character results in reports for all users in ascending sequence by username; 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 accompanying table.

Table AUTH–6 UIC Specification with the SHOW Command

Command	Description
SHOW [014,006]	Displays a full report for the user (or users) with member number 006 in group 014.
SHOW [014,*] /BRIEF	Displays a brief report for all users in group 014, in ascending sequence by member number.
SHOW [*,006] /BRIEF	Displays a brief report for all users with a member number of 006.
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. Brief reports do not include the limits, login flags, command interpreter, nor do they summarize the privileges. The password is never listed.

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-1984 14:08
Last Login:            (none) (interactive),            (none) (non-interactive)
Maxjobs:         0  Fillm:        20  Bytlm:        12480
Maxacctjobs:     0  Shrfillm:      0  Pbytlm:           0
Maxdetach:       0  BIOlm:         6  JTquota:       1024
Prclm:           2  DIOlm:         6  WSdef:          300
Prio:            4  ASTlm:        10  WSquo:          350
Queprio:         0  TQElm:        10  WSextent:       700
CPU:        (none)  Enqlm:        30  Pgflquo:      12480
Authorized Privileges:
  TMPMBX NETMBX
Default Privileges:
  TMPMBX NETMBX
  Name                                   Value                 Attributes
Identifiers held by ROBIN:
  INVENTORY                              %X80010006            NORESOURCE
```

Note: The quotas Pbytlm and Queprio are not implemented for Version 4.0 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]
```

```
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   Bytlm:         4096
Maxacctjobs:     0  Shrfillm:      0   Pbytlm:           0
Maxdetach:       0  BIOlm:         6   JTquota:       1024
Prclm:           2  DIOlm:         6   WSdef:          150
Prio:            4  ASTlm:        10   WSquo:          200
Queprio:         4  TQElm:        10   WSextent:       500
CPU:        (none)  Enqlm:        10   Pgflquo:      10000
Authorized Privileges:
  TMPMBX NETMBX
Default Privileges:
  TMPMBX NETMBX
```

Observe 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 dialup lines at all times during the week, he is not allowed to log in over the network then. 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.

SHOW/IDENTIFIER

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

FORMAT

SHOW/IDENTIFIER *[id-name]*

command parameter

id-name

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

command 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 may be a username or UIC. You can use the asterisk wildcard to specify multiple usernames or UICs: full use of the asterisk and percent wildcards is permitted for usernames; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard username specification (*) displays identifiers alphabetically by username; a wildcard UIC specification ([*,*]) displays them numerically by UIC.

/VALUE=value-specifier

Specifies a value in any valid format (see the ADD/IDENTIFIER command).

DESCRIPTION

The SHOW/IDENTIFIER command displays identifier names, values, and attributes, and holders in various formats depending on the qualifiers specified. Two of these formats are illustrated in the accompanying 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
  Holder                                 Attributes
  ANDERSON                               NORESOURCE
  BROWN                                  NORESOURCE
  CRAMER                                 NORESOURCE
```

2

```
UAF> SHOW/IDENTIFIER/USER=ANDERSON
```

This command displays the identifier associated with the user ANDERSON; for example:

```
Name                                     Value                     Attributes
ANDERSON                                 [000300,000015]           NORESOURCE
```

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]
```

SHOW/PROXY

Displays one or all records in the network UAF. The /PROXY qualifier is required.

FORMAT

SHOW/PROXY *node::remote-user*

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

command qualifiers

None.

EXAMPLES

1

```
UAF> SHOW/PROXY SAMPLE::MARCO

Node    Remote User     Local User
SAMPLE ::MARCO            MARCO_N
```

The command in this example displays the network UAF record for user MARCO on node SAMPLE.

2

```
UAF> SHOW/PROXY SAMPLE::*

Node     Remote User     Local User
SAMPLE   ::SMITH           SMITH_N
SAMPLE   ::JONES           DOCUMENT
SAMPLE   ::MARCO           MARCO_N
SAMPLE   ::SYSBUILD        SYSBUILD_N
```

The command in this example displays all records in the network UAF on node SAMPLE.

3

```
UAF> SHOW/PROXY *::MARCO

Node     Remote User     Local User
CURLEY   ::MARCO           MARCO_N
LARRY    ::MARCO           MARCO_N
MOE      ::MARCO           MARCO_N
SAMPLE   ::MARCO           MARCO_N
```

This command lists all proxy entries for the remote user MARCO.

SHOW/RIGHTS

Displays the identifiers held by the specified identifiers, or, if /USER is specified, all identifiers held by the specified user(s).

FORMAT

SHOW/RIGHTS *[user-spec]*

command parameter

[user-spec]

Is the name of the identifier associated with the user. Specify the identifier in UIC format. If you omit the id-name, you must specify the /USER qualifier.

command qualifier

/USER=user-spec

Specifies one or more user(s) whose identifiers are to be listed. User-spec may be a username or UIC. You can use the asterisk wildcard to specify multiple usernames or UICs: full use of the asterisk and percent wildcards is permitted for usernames; UICs must be in the form [*,*], [n,*], [*,n], or [n,n]. A wildcard username specification (*) or wildcard UIC specification ([*,*]) displays all identifiers held by users. The wildcard username specification displays holders' usernames 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
PAYROLL                               %X80010022          NORESOURCE
```

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

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

Index

VAX/VMS
Authorize Utility
Reference Manual
AA-Z406A-TE

READER'S COMMENTS

Note: This form is for document comments only. DIGITAL will use comments submitted on this form at the company's discretion. If you require a written reply and are eligible to receive one under Software Performance Report (SPR) service, submit your comments on an SPR form.

Did you find this manual understandable, usable, and well organized? Please make suggestions for improvement.

Did you find errors in this manual? If so, specify the error and the page number.

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

- □ Assembly language programmer
- □ Higher-level language programmer
- □ Occasional programmer (experienced)
- □ User with little programming experience
- □ Student programmer
- □ Other (please specify) ____________________

Name ____________________ Date ____________________

Organization ____________________

Street ____________________

City ____________________ State ____________________ Zip Code ____________________
or Country

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

SSG PUBLICATIONS ZK1-3/J35
DIGITAL EQUIPMENT CORPORATION
110 SPIT BROOK ROAD
NASHUA, NEW HAMPSHIRE 03062-2698

Do Not Tear - Fold Here

Cut Along Dotted Line