VMS AUTHORIZE (UAF) Help

1 Usage_Summary

To invoke AUTHORIZE, set your default device and directory to SYS$SYSTEM and enter RUN AUTHORIZE at the DCL command prompt. At the UAF> prompt, you can enter any of the AUTHORIZE commands.

To exit from AUTHORIZE, enter the EXIT command at the UAF> prompt or press Ctrl/Z.

If you move the SYSUAF.DAT file, be sure the logical name SYSUAF is defined and points to an existing file. If AUTHORIZE is unable to locate the SYSUAF.DAT file, it displays the following 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 results in creation of a new SYSUAF file containing a SYSTEM record and a DEFAULT record. These records are initialized with the same values set when the system was installed.

VMS AUTHORIZE (UAF) Help

1 Command_Summary

Command	Description
	Managing System Resources and User Accounts with SYSUAF
ADD	Adds a user record to the SYSUAF and corresponding identifiers to the rights database.
COPY	Creates a new SYSUAF record that duplicates an existing record.
DEFAULT	Modifies the default SYSUAF record.
LIST	Writes reports for selected UAF records to a listing file, SYSUAF.LIS.
MODIFY	Changes values in a SYSUAF user record. Qualifiers not specified in the command remain unchanged.
REMOVE	Deletes a SYSUAF user record and corresponding identifiers in the rights database. The DEFAULT and SYSTEM records cannot be deleted.
RENAME	Changes the user name of the SYSUAF record (and, if specified, the corresponding identifier) while retaining the characteristics of the old record.
SHOW	Displays reports for selected SYSUAF records.
	Managing Network Proxies with NETPROXY.DAT or NET$PROXY.DAT
ADD/PROXY	Adds proxy access for the specified user.
CREATE/PROXY	Creates a network proxy authorization file.
LIST/PROXY	Creates a listing file of all proxy accounts and all remote users with proxy access to the accounts.
MODIFY/PROXY	Modifies proxy access for the specified user.
REMOVE/PROXY	Deletes proxy access for the specified user.
SHOW/PROXY	Displays proxy access allowed for the specified user.
	Managing Identifiers with RIGHTSLIST.DAT
ADD/IDENTIFIER	Adds an identifier name to the rights database.
CREATE/RIGHTS	Creates a new rights database file.
GRANT/IDENTIFIER	Grants an identifier name to a UIC identifier.
LIST/IDENTIFIER	Creates a listing file of identifier names and values.
LIST/RIGHTS	Creates a listing file of all identifiers held by the specified user.
MODIFY/IDENTIFIER	Modifies the named identifier in the rights database.
REMOVE/IDENTIFIER	Removes an identifier from the rights database.
RENAME/IDENTIFIER	Renames an identifier in the rights database.
REVOKE/IDENTIFIER	Revokes an identifier name from a UIC identifier.
SHOW/IDENTIFIER	Displays identifier names and values on the current output device.
SHOW/RIGHTS	Displays on the current output device the names of all identifiers held by the specified user.
	General Commands
EXIT	Returns the user to DCL command level.
HELP	Displays HELP text for AUTHORIZE commands.
MODIFY/SYSTEM_ PASSWORD	Sets the system password (equivalent to the DCL command SET PASSWORD/SYSTEM).

VMS AUTHORIZE (UAF) Help

1 ADD

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

Format

ADD newusername

2 Parameter

newusername

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

Avoid using fully numeric user names (for example, 89560312). A fully numeric user name cannot receive a corresponding identifier because fully numeric identifiers are not permitted.

2 Qualifiers

/ACCESS

/ACCESS[=(range[,...])]

Specifies hours of access for all modes of access. The syntax for specifying the range is:

/[NO]ACCESS=([PRIMARY], [n-m], [n], [,...],[SECONDARY], [n-m], [n], [,...])

Specify hours as integers from 0 to 23, inclusive. You can specify single hours (n) or 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.

By default, a user has full access every day. See the DCL command SET DAY in the OpenVMS DCL Dictionary for information on overriding the defaults for primary and secondary day types.

All the list elements are optional. Unless you specify hours for a day type, access is permitted for the entire day. By specifying an access time, you prevent access at all other times. Adding NO to the qualifier denies the user access to the system for the specified period of time.

Examples:

/ACCESS	Allows unrestricted access
/NOACCESS=SECONDARY	Allows access on primary days only
/ACCESS=(9-17)	Allows access from 9 A.M. to 5:59 P.M. on all days
/NOACCESS=(PRIMARY, 9-17, SECONDARY, 18-8)	Disallows access between 9 A.M. to 5:59 P.M. on primary days but allows access during these hours on secondary days

To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.

/ACCOUNT

/ACCOUNT=account-name

Specifies the default name for the account (for example, a billing name or number). The name can be a string of 1 to 8 alphanumeric characters. By default, AUTHORIZE does not assign an account name.

/ADD_IDENTIFIER

/ADD_IDENTIFIER (default)
/NOADD_IDENTIFIER

Adds a user (user name and account name) to the rights database. The /NOADD_IDENTIFIER does not create a rights list identifier (user name and account name).

/ALGORITHM

/ALGORITHM=keyword=type [=value]

Sets the password encryption algorithm for a user. The keyword VMS refers to the algorithm used in the operating system version that is running on your system, whereas a customer algorithm is one that is added through the $HASH_PASSWORD system service by a customer site, by a layered product, or by a third party. The customer algorithm is identified in $HASH_PASSWORD by an integer in the range of 128 to 255. It must correspond with the number used in the AUTHORIZE command MODIFY/ALGORITHM. By default, passwords are encrypted with the VMS algorithm for the current version of the operating system.

Keyword	Function
BOTH	Set the algorithm for primary and secondary passwords.
CURRENT	Set the algorithm for the primary, secondary, both, or no passwords, depending on account status. CURRENT is the default value.
PRIMARY	Set the algorithm for the primary password only.
SECONDARY	Set the algorithm for the secondary password only.

The following table lists password encryption algorithms:

Type	Definition
VMS	The algorithm used in the version of the operating system that is running on your system.
CUSTOMER	A numeric value in the range of 128 to 255 that

identifies a customer algorithm.

The following example selects the VMS algorithm for Sontag's primary password:

```
UAF>  MODIFY SONTAG/ALGORITHM=PRIMARY=VMS
```

If you select a site-specific algorithm, you must give a value to identify the algorithm, as follows:

```
UAF>  MODIFY SONTAG/ALGORITHM=CURRENT=CUSTOMER=128
```

/ASTLM

/ASTLM=value

Specifies the AST queue limit, which is the total number of asynchronous system trap (AST) operations and scheduled wake-up requests that the user can have queued at one time. The default is 40 on VAX systems and 250 on Alpha systems.

/BATCH

/BATCH[=(range[,...])]

Specifies the hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier. By default, a user can submit batch jobs any time.

/BIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/BYTLM

/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 can consume at one time. Nonpaged dynamic memory is used for operations such as I/O buffering, mailboxes, and file-access windows. The default is 32768 on VAX systems and 64000 on Alpha systems.

/CLI

/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 a string of 1 to 31 alphanumeric characters and should be either DCL or MCR. The default is DCL. This setting is ignored for network jobs.

/CLITABLES

/CLITABLES=filespec

Specifies user-defined CLI tables for the account. The filespec can contain 1 to 31 characters. The default is SYS$LIBRARY:DCLTABLES. Note that this setting is ignored for network jobs to guarantee that the system-supplied command procedures used to implement network objects function properly.

/CPUTIME

/CPUTIME=time

Specifies the maximum process CPU time for the CPU field of the UAF record. The maximum process CPU time is the maximum amount of 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 OpenVMS User's Manual. The default is 0, which means an infinite amount of time.

/DEFPRIVILEGES

/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. By specifying the keyword [NO]ALL with the /DEFPRIVILEGES qualifier, you can disable or enable all user privileges. The default privileges are TMPMBX and NETMBX. Privname is the name of the privilege.

/DEVICE

/DEVICE=device-name

Specifies the name of the user's default device at login. The device-name is a string of 1 to 31 alphanumeric characters. If you omit the colon from the device-name value, AUTHORIZE appends a colon. The default device is SYS$SYSDISK.

If you specify a logical name as the device-name (for example, DISK1: for DUA1:), you must make an entry for the logical name in the LNM$SYSTEM_TABLE in executive mode by using the DCL command DEFINE/SYSTEM/EXEC.

/DIALUP

/DIALUP[=(range[,...])]

Specifies hours of access permitted for dialup logins. For a description of the range specification, see the /ACCESS qualifier. The default is full access.

/DIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/DIRECTORY

/DIRECTORY=directory-name

Specifies the default directory name for the DIRECTORY field of the UAF record. The directory-name can be 1 to 39 alphanumeric characters. If you do not enclose the directory name in brackets, AUTHORIZE adds the brackets for you. The default directory name is [USER].

/ENQLM

/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 by the user at one time. The default is 200 on VAX systems and 2000 on Alpha systems.

/EXPIRATION

/EXPIRATION=time (default)
/NOEXPIRATION

Specifies the expiration date and time of the account. The /NOEXPIRATION qualifier removes the expiration date on the account or resets the expiration time for expired accounts. The default expiration time period is 90 days for nonprivileged users.

/FILLM

/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 default is 300 on VAX systems and 100 on Alpha systems.

/FLAGS

/FLAGS=([NO]option[,...])

Specifies login flags for the user. The prefix NO clears the flag. The options are as follows:

AUDIT	Enables or disables mandatory security auditing for a specific user. By default, the system does not audit the activities of specific users (NOAUDIT).
AUTOLOGIN	Restricts the user to the automatic login mechanism when logging in to an account. When set, the flag disables login by any terminal that requires entry of a user name and password. The default is to require a user name and password (NOAUTOLOGIN).
CAPTIVE	Prevents the user from changing any defaults at login, for example, /CLI or /LGICMD. It prevents the user from escaping the captive login command procedure specified by the /LGICMD qualifier and gaining access to the DCL command level. See Guidelines for Captive Command Procedures in the OpenVMS Guide to System Security. The CAPTIVE flag also establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. By default, an account is not captive (NOCAPTIVE).
DEFCLI	Restricts the user to the default command interpreter by prohibiting the use of the /CLI qualifier at login; the MCR command can still be used. By default, a user can choose a CLI (NODEFCLI).
DISCTLY	Establishes an environment where Ctrl/Y interrupts are initially turned off and are invalid until a SET CONTROL=Y is encountered. This could happen in SYLOGIN.COM or in a procedure called by SYLOGIN.COM. Once a SET CONTROL=Y is executed (which requires no privilege), a user can enter a Ctrl/Y and reach the DCL prompt ($). If the intent of DISCTLY is to force execution of the login command files, then SYLOGIN.COM should issue the DCL command SET CONTROL=Y to turn on Ctrl /Y interrupts before exiting. By default, Ctrl /Y is enabled (NODISCTLY).
DISFORCE_PWD_ CHANGE	Removes the requirement that a user must change an expired password at login. By default, a person can use an expired password only once (NODISFORCE_PWD_CHANGE) and then is forced to change the password after logging in. If the user does not select a new password, the user is locked out of the system. To use this feature, set a password expiration date with the /PWDLIFETIME qualifier.
DISIMAGE	Prevents the user from executing RUN, MCR, and foreign commands. By default, a user can execute RUN, MCR, and foreign commands (NODISIMAGE).
DISMAIL	Disables mail delivery to the user. By default, mail delivery is enabled (NODISMAIL).
DISNEWMAIL	Suppresses announcements of new mail at login. By default, the system announces new mail (NODISNEWMAIL).
DISPWDDIC	Disables automatic screening of new passwords against a system dictionary. By default, passwords are automatically screened (NODISPWDDIC).
DISPWDHIS	Disables automatic checking of new passwords against a list of the user's old passwords. By default, the system screens new passwords (NODISPWDHIS).
DISRECONNECT	Disables automatic reconnection to an existing

process when a terminal connection has been interrupted. By default, automatic reconnection is enabled (NODISRECONNECT).

DISREPORT	Suppresses reports of the last login time, login failures, and other security reports. By default, login information is displayed (NODISREPORT).
DISUSER	Disables the account so the user cannot log in. For example, the DEFAULT account is disabled. By default, an account is enabled (NODISUSER).
DISWELCOME	Suppresses the welcome message (an informational message displayed during a local login). This message usually indicates the version number of the operating system that is running and the name of the node on which the user is logged in. By default, a system login message appears (NODISWELCOME).
EXTAUTH	Considers user to be authenticated by an external user name and password, not by the SYSUAF user name and password. (The system still uses the SYSUAF record to check a user's login restrictions and quotas and to create the user's process profile.)
GENPWD	Restricts the user to generated passwords. By default, users choose their own passwords (NOGENPWD).
LOCKPWD	Prevents the user from changing the password for the account. By default, users can change their passwords (NOLOCKPWD).
PWD_EXPIRED	Marks a password as expired. The user cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not expired after login (NOPWD_EXPIRED).
PWD2_EXPIRED	Marks a secondary password as expired. Users cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not set to expire after login (NOPWD2_EXPIRED).
RESTRICTED	Prevents the user from changing any defaults at login (for example, by specifying /LGICMD) and prohibits user specification of a CLI with the /CLI qualifier. The RESTRICTED flag establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. Typically, this flag is used to prevent an applications user from having unrestricted access to the CLI. By default, a user can change defaults (NORESTRICTED).

/GENERATE_PASSWORD

/GENERATE_PASSWORD[=keyword]
/NOGENERATE_PASSWORD (default)

Invokes the password generator to create user passwords. Generated passwords can consist of 1 to 10 characters. Specify one of the following keywords:

BOTH	Generate primary and secondary passwords.
CURRENT	Do whatever the DEFAULT account does (for example, generate primary, secondary, both, or no passwords). This is the default keyword.
PRIMARY	Generate primary password only.
SECONDARY	Generate secondary password only.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, users are forced to change their passwords (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/INTERACTIVE

/INTERACTIVE[=(range[,...])]
/NOINTERACTIVE

Specifies the hours of access for interactive logins. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on interactive logins.

/JTQUOTA

/JTQUOTA=value

Specifies the initial byte quota with which the jobwide logical name table is to be created. By default, the value is 4096 on VAX systems and 4096 on Alpha systems.

/LGICMD

/LGICMD=filespec

Specifies the name of the default login command file. The file name defaults to the device specified for /DEVICE, the directory specified for /DIRECTORY, a file name of LOGIN, and a file type of .COM. If you select the defaults for all these values, the file name is SYS$SYSTEM:[USER]LOGIN.COM.

/LOCAL

/LOCAL[=(range[,...])]

Specifies hours of access for interactive logins from local terminals. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on local logins.

/MAXACCTJOBS

/MAXACCTJOBS=value

Specifies the maximum number of batch, interactive, and detached processes that can be active at one time for all users of the same account. By default, a user has a maximum of 0, which represents an unlimited number.

/MAXDETACH

/MAXDETACH=value

Specifies the maximum number of detached processes with the cited user name that can be active at one time. To prevent the user from creating detached processes, specify the keyword NONE. By default, a user has a value of 0, which represents an unlimited number.

/MAXJOBS

/MAXJOBS=value

Specifies the maximum number of processes (interactive, batch, detached, and network) with the cited user name that can be active simultaneously. The first four network jobs are not counted. By default, a user has a maximum value of 0, which represents an unlimited number.

/NETWORK

/NETWORK[=(range[,...])]

Specifies hours of access for network batch jobs. For a description of how to specify the range, see the /ACCESS qualifier. By default, network logins have no access restrictions.

/OWNER

/OWNER=owner-name

Specifies the name of the owner of the account. You can use this name for billing purposes or similar applications. The owner name is 1 to 31 characters. No default owner name exists.

/PASSWORD

/PASSWORD=(password1[,password2])
/NOPASSWORD

Specifies up to two passwords for login. Passwords can be from 0 to 32 characters in length and can include alphanumeric characters, dollar signs, and underscores. Avoid using the word password as the actual password. Use the /PASSWORD qualifier as follows:

- To set only the first password and clear the second, specify /PASSWORD=password.
- To set both the first and second password, specify /PASSWORD=(password1, password2).
- To change the first password without affecting the second, specify /PASSWORD=(password, "").
- To change the second password without affecting the first, specify /PASSWORD=("", password).
- To set both passwords to null, specify /NOPASSWORD.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, the user is forced to change the password (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

By default, the ADD command assigns the password USER. When you create a new UAF record with the COPY or RENAME command, you must specify a password. Avoid using the word password as the actual password.

/PBYTLM

This flag is reserved for Digital.

/PGFLQUOTA

/PGFLQUOTA=value

Specifies the paging file limit. This is the maximum number of pages that the person's process can use in the system paging file. By default, the value is 32768 pages on VAX systems and 50000 pagelets on Alpha systems.

If decompressing libraries, make sure to set PGFLQUOTA to twice the size of the library.

/PRCLM

/PRCLM=value

Specifies the subprocess creation limit. This is the maximum number of subprocesses that can exist at one time for the specified user's process. By default, the value is 2 on VAX systems and 8 on Alpha systems.

/PRIMEDAYS

/PRIMEDAYS=([NO]day[,...])

Defines the primary and secondary days of the week for logging in. Specify the days as a list separated by commas, and enclose the list in parentheses. To specify a secondary day, prefix the day with NO (for example, NOFRIDAY). To specify a primary day, omit the NO prefix.

By default, primary days are Monday through Friday and secondary days are Saturday and Sunday. If you omit a day from the list, AUTHORIZE uses the default value. (For example, if you omit Monday from the list, AUTHORIZE defines Monday as a primary day.)

Use the primary and secondary day definitions in conjunction with such qualifiers as /ACCESS, /INTERACTIVE, and /BATCH.

/PRIORITY

/PRIORITY=value

Specifies the default base priority. The value is an integer in the range of 0 to 31 on VAX systems and 0 to 63 on Alpha systems. By default, the value is set to 4 for timesharing users.

/PRIVILEGES

/PRIVILEGES=([NO]privname[,...])

Specifies which privileges the user is authorized to hold, although these privileges are not necessarily enabled at login. (The /DEFPRIVILEGES qualifier determines which ones are enabled.) A NO prefix removes the privilege from the user. The keyword NOALL disables all user privileges. Many privileges have varying degrees of power and potential system impact (see the OpenVMS Guide to System Security for a detailed discussion). By default, a user holds TMPMBX and NETMBX privileges. Privname is the name of the privilege.

/PWDEXPIRED

/PWDEXPIRED (default)
/NOPWDEXPIRED

Specifies the password is valid for only one login. A user must change a password immediately after login or be locked out of the system. The system warns users of password expiration. A user can either specify a new password, with the DCL command SET PASSWORD, or wait until expiration and be forced to change. By default, a user must change a password when first logging in to an account. The default is applied to the account only when the password is being modified.

/PWDLIFETIME

/PWDLIFETIME=time (default)
/NOPWDLIFETIME

Specifies the length of time a password is valid. Specify a delta time value in the form [dddd-] [hh:mm:ss.cc]. For example, for a lifetime of 120 days, 0 hours, and 0 seconds, specify /PWDLIFETIME="120-". For a lifetime of 120 days 12 hours, 30 minutes and 30 seconds, specify /PWDLIFETIME="120-12:30:30". If a period longer than the specified time elapses before the user logs in, the system displays a warning message. The password is marked as expired.

To prevent a password from expiring, specify the time as NONE. By default, a password expires in 90 days.

/PWDMINIMUM

/PWDMINIMUM=value

Specifies the minimum password length in characters. Note that this value is enforced only by the DCL command SET PASSWORD. It does not prevent you from entering a password shorter than the minimum length when you use AUTHORIZE to create or modify an account. By default, a password must have at least 6 characters. The value specified by the /PWDMINIMUM qualifier conflicts with the value used by the /GENERATE_PASSWORD qualifier or the DCL command SET PASSWORD/GENERATE, the operating system chooses the lesser value. The maximum value for generated passwords is 10.

/QUEPRIO

/QUEPRIO=value

Reserved for future use.

/REMOTE

/REMOTE[=(range[,...])]

Specifies hours during which access is permitted for interactive logins from network remote terminals (with the DCL command SET HOST). For a description of the range specification, see the /ACCESS qualifier. By default, remote logins have no access restrictions.

/SHRFILLM

/SHRFILLM=value

Specifies the maximum number of shared files that the user can have open at one time. By default, the system assigns a value of 0, which 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. By default, a user can have 10.

/UIC

/UIC=value

Specifies the user identification code (UIC). The UIC value is a group number in the range from 1 to 37776 (octal) and a member number in the range from 0 to 177776 (octal), which are separated by a comma and enclosed in brackets. Digital reserves group 1 and groups 300-377 for its own use.

Each user must have a unique UIC. By default, the UIC value is [200,200].

/WSDEFAULT

/WSDEFAULT=value

Specifies the default working set limit. This represents the initial limit to the number of physical pages the process can

use. (The user can alter the default quantity up to WSQUOTA with the DCL command SET WORKING_SET.) By default, a user has 256 pages on VAX systems and 2000 pagelets on Alpha systems.

The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSDEFAULT.

/WSEXTENT

/WSEXTENT=value

Specifies the working set maximum. This represents the maximum amount of physical memory allowed to the process. The system provides memory to a process beyond its working set quota only when it has excess free pages. The additional memory is recalled by the system if needed.

The value is an integer equal to or greater than WSQUOTA. By default, the value is 1024 pages on VAX systems and 16384 pagelets on Alpha systems. The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSEXTENT.

/WSQUOTA

/WSQUOTA=value

Specifies the working set quota. This is the maximum amount of physical memory a user process can lock into its working set. It also represents the maximum amount of swap space that the system reserves for this process and the maximum amount of physical memory that the system allows the process to consume if the systemwide memory demand is significant.

The value cannot be greater than the value of WSMAX and cannot exceed 64K pages. This quota value replaces smaller values of PQL_MWSQUOTA.

2 Examples

```
1.UAF> ADD ROBIN /PASSWORD=SP0152/UIC=[014,006] -
  _/DEVICE=SYS$USER/DIRECTORY=[ROBIN]/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.

```
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
        RIGHTSLIST.DAT
  UAF> MODIFY WELCH/FLAGS=(RESTRICTED,DISNEWMAIL,DISWELCOME,NODISUSER,EXTAUTH)-
  _/NODIALUP=SECONDARY/NONETWORK=PRIMARY/CLITABLES=DCLTABLES -
  _/NOACCESS=(PRIMARY, 9-16, SECONDARY, 18-8)
  %UAF-I-MDFYMSG, user records updated
```

The commands in this example add a record for a restricted account. Because of the number of qualifiers required, a MODIFY command is used in conjunction with the ADD command. This helps to minimize the possibility of typing errors.

In the ADD command line, setting the DISUSER flag prevents the user from logging in until all the account parameters are set up. In the MODIFY command line, the DISUSER flag is disabled (by specifying NODISUSER) to allow access to the account. The EXTAUTH flag causes the system to consider the user as authenticated by an external user name and password, not by the SYSUAF user name and password.

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

2 /IDENTIFIER

Adds only an identifier to the rights database. It does not add a user account.

Format

ADD/IDENTIFIER [id-name]

3 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 to 31 alphanumeric characters. The name can contain underscores and dollar signs. It must contain at least one nonnumeric character.

3 Qualifiers

/ATTRIBUTES

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

Specifies attributes to be associated with the new identifier. The following are valid keywords:

DYNAMIC	Allows unprivileged holders of the identifier to remove and to restore the identifier from the process rights list by using the DCL command SET RIGHTS_LIST.
HOLDER_HIDDEN	Prevents people from getting a list of users who hold an identifier, unless they own the identifier themselves.
NAME_HIDDEN	Allows holders of an identifier to have it translated, either from binary to ASCII or from ASCII to binary, but prevents unauthorized users from translating the identifier.
NOACCESS	Makes any access rights of the identifier null and void. If a user is granted an identifier with the No Access attribute, that identifier has no effect on the user's access rights

to objects. This attribute is a modifier for an identifier with the Resource or Subsystem attribute.

RESOURCE — Allows holders of an identifier to charge disk space to the identifier. Used only for file objects.

SUBSYSTEM — Allows holders of the identifier to create and maintain protected subsystems by assigning the Subsystem ACE to the application images in the subsystem. Used only for file objects.

By default, none of these attributes is associated with the new identifier.

/USER

/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=value-specifier

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

IDENTIFIER:n — 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).

The system displays this type of identifier in hexadecimal. To differentiate general identifiers from UIC identifiers, the system adds %X80000000 to the value you specify.

UIC:uic — A UIC value in standard UIC format consists of a member name and, optionally, a group name enclosed in brackets. For example, [360,031].

In numeric UICs, the group number is an octal number in the range of 1 to 37776; the member number is an octal number in the range of 0 to 177776. You can omit leading zeros when you are specifying group and member numbers.

Regardless of the UIC format you use, the system translates a UIC to a 32-bit numeric value.

Alphanumeric UICs are not allowed.

Typically, system managers add identifiers as UIC values to represent system users; the system applies identifiers in integer format to system resources.

3 Examples

1.UAF> ADD/IDENTIFIER/VALUE=UIC:[300,011] INVENTORY
%UAF-I-RDBADDMSGU, identifier INVENTORY value: [000300,000011] added to RIGHTSLIST.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-RDBADDMSGU, identifier PAYROLL value: %X80080011 added to RIGHTSLIST.DAT

This command adds the identifier PAYROLL and marks it as a resource. To differentiate identifiers with integer values from identifiers with UIC values, %X80000000 is added to the specified code.

2 /PROXY

Adds an entry to the network proxy authorization files, NETPROXY.DAT and NET$PROXY.DAT, and signals DECnet to update its volatile database. Proxy additions take effect immediately on all nodes in a cluster that share the proxy database.

Format

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

3 Parameters

node

Specifies a DECnet node name. If you provide a wildcard character (*), the specified remote user on all nodes is served by the account defined as 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 systems that are not OpenVMS and that implement DECnet, specifies the UIC of a user at a remote node. You can specify a wildcard character (*) in the group and member fields of the UIC.

local-user

Specifies the user names of 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.

3 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.

3 Examples

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

  Specifies that user WALTER on remote node SAMPLE has proxy access to user ROBIN's account on local node AXEL. Through proxy login, WALTER receives the default privileges of user ROBIN when he accesses node AXEL remotely.

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

  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.

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

  Specifies that user MARCO on the remote node MISHA can use only the MARCO account on the local node for remote file access.

4.UAF> ADD/PROXY TAO::MARTIN MARTIN/D,SALES_READER
  %UAF-I-NAFADDMSG, proxy from TAO:.TWA.RAN::MARTIN to MARTIN added
  %UAF-I-NAFADDMSG, proxy from TAO:.TWA.RAN::MARTIN to SALES_READER added

  Adds a proxy from TAO::MARTIN to the local accounts MARTIN (the default) and SALES_READER on a system running DECnet-Plus.

VMS AUTHORIZE (UAF) Help

1 COPY

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

Format

```
COPY  oldusername newusername
```

2 Parameters

oldusername

Name of an existing user record to serve as a template for the new record.

newusername

Name for the new user record. The user name is a string of 1 to 12 alphanumeric characters.

2 Qualifiers

/ACCESS

```
/ACCESS[=(range[,...])]
```

Specifies hours of access for all modes of access. The syntax for specifying the range is:

```
/[NO]ACCESS=([PRIMARY], [n-m], [n], [,...],[SECONDARY], [n-m], [n], [,...])
```

Specify hours as integers from 0 to 23, inclusive. You can specify single hours (n) or 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.

By default, a user has full access every day. See the DCL command SET DAY in the OpenVMS DCL Dictionary for information on overriding the defaults for primary and secondary day types.

All the list elements are optional. Unless you specify hours for a day type, access is permitted for the entire day. By specifying an access time, you prevent access at all other times. Adding NO to the qualifier denies the user access to the system for the specified period of time.

Examples:

/ACCESS	Allows unrestricted access
/NOACCESS=SECONDARY	Allows access on primary days only
/ACCESS=(9-17)	Allows access from 9 A.M. to 5:59 P.M. on all days
/NOACCESS=(PRIMARY, 9-17, SECONDARY, 18-8)	Disallows access between 9 A.M. to 5:59 P.M. on primary days but allows access during these hours on secondary days

To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.

/ACCOUNT

```
/ACCOUNT=account-name
```

Specifies the default name for the account (for example, a billing name or number). The name can be a string of 1 to 8 alphanumeric characters. By default, AUTHORIZE does not assign an account name.

/ADD_IDENTIFIER

```
/ADD_IDENTIFIER (default)
/NOADD_IDENTIFIER
```

Adds a user (user name and account name) to the rights database. The /NOADD_IDENTIFIER does not create a rights list identifier (user name and account name).

/ALGORITHM

```
/ALGORITHM=keyword=type [=value]
```

Sets the password encryption algorithm for a user. The keyword VMS refers to the algorithm used in the operating system version that is running on your system, whereas a customer algorithm is one that is added through the $HASH_PASSWORD system service by a customer site, by a layered product, or by a third party. The customer algorithm is identified in $HASH_PASSWORD by an integer in the range of 128 to 255. It must correspond with the number used in the AUTHORIZE command MODIFY/ALGORITHM. By default, passwords are encrypted with the VMS algorithm for the current version of the operating system.

Keyword	Function
BOTH	Set the algorithm for primary and secondary passwords.
CURRENT	Set the algorithm for the primary, secondary, both, or no passwords, depending on account status. CURRENT is the default value.
PRIMARY	Set the algorithm for the primary password only.
SECONDARY	Set the algorithm for the secondary password only.

The following table lists password encryption algorithms:

Type	Definition
VMS	The algorithm used in the version of the operating system that is running on your system.
CUSTOMER	A numeric value in the range of 128 to 255 that identifies a customer algorithm.

The following example selects the VMS algorithm for Sontag's primary password:

```
UAF>  MODIFY SONTAG/ALGORITHM=PRIMARY=VMS
```

If you select a site-specific algorithm, you must give a value to identify the algorithm, as follows:

```
UAF>  MODIFY SONTAG/ALGORITHM=CURRENT=CUSTOMER=128
```

/ASTLM

/ASTLM=value

Specifies the AST queue limit, which is the total number of asynchronous system trap (AST) operations and scheduled wake-up requests that the user can have queued at one time. The default is 40 on VAX systems and 250 on Alpha systems.

/BATCH

/BATCH[=(range[,...])]

Specifies the hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier. By default, a user can submit batch jobs any time.

/BIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/BYTLM

/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 can consume at one time. Nonpaged dynamic memory is used for operations such as I/O buffering, mailboxes, and file-access windows. The default is 32768 on VAX systems and 64000 on Alpha systems.

/CLI

/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 a string of 1 to 31 alphanumeric characters and should be either DCL or MCR. The default is DCL. This setting is ignored for network jobs.

/CLITABLES

/CLITABLES=filespec

Specifies user-defined CLI tables for the account. The filespec can contain 1 to 31 characters. The default is SYS$LIBRARY:DCLTABLES. Note that this setting is ignored for network jobs to guarantee that the system-supplied command procedures used to implement network objects function properly.

/CPUTIME

/CPUTIME=time

Specifies the maximum process CPU time for the CPU field of the UAF record. The maximum process CPU time is the maximum amount of 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 OpenVMS User's Manual. The default is 0, which means an infinite amount of time.

/DEFPRIVILEGES

/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. By specifying the keyword [NO]ALL with the /DEFPRIVILEGES qualifier, you can disable or enable all user privileges. The default privileges are TMPMBX and NETMBX. Privname is the name of the privilege.

/DEVICE

/DEVICE=device-name

Specifies the name of the user's default device at login. The device-name is a string of 1 to 31 alphanumeric characters. If you omit the colon from the device-name value, AUTHORIZE appends a colon. The default device is SYS$SYSDISK.

If you specify a logical name as the device-name (for example, DISK1: for DUA1:), you must make an entry for the logical name in the LNM$SYSTEM_TABLE in executive mode by using the DCL command DEFINE/SYSTEM/EXEC.

/DIALUP

/DIALUP[=(range[,...])]

Specifies hours of access permitted for dialup logins. For a description of the range specification, see the /ACCESS qualifier. The default is full access.

/DIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/DIRECTORY

/DIRECTORY=directory-name

Specifies the default directory name for the DIRECTORY field of the UAF record. The directory-name can be 1 to 39 alphanumeric characters. If you do not enclose the directory name in brackets, AUTHORIZE adds the brackets for you. The default directory name is [USER].

/ENQLM

/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 by the user at one time. The default is 200 on VAX systems and 2000 on Alpha systems.

/EXPIRATION

/EXPIRATION=time (default)
/NOEXPIRATION

Specifies the expiration date and time of the account. The /NOEXPIRATION qualifier removes the expiration date on the account or resets the expiration time for expired accounts. The default expiration time period is 90 days for nonprivileged users.

/FILLM

/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 default is 300 on VAX systems and 100 on Alpha systems.

/FLAGS

/FLAGS=([NO]option[,...])

Specifies login flags for the user. The prefix NO clears the flag. The options are as follows:

AUDIT	Enables or disables mandatory security auditing for a specific user. By default, the system does not audit the activities of specific users (NOAUDIT).
AUTOLOGIN	Restricts the user to the automatic login mechanism when logging in to an account. When set, the flag disables login by any terminal that requires entry of a user name and password. The default is to require a user name and password (NOAUTOLOGIN).
CAPTIVE	Prevents the user from changing any defaults at login, for example, /CLI or /LGICMD. It prevents the user from escaping the captive login command procedure specified by the /LGICMD qualifier and gaining access to the DCL command level. See Guidelines for Captive Command Procedures in the OpenVMS Guide to System Security. The CAPTIVE flag also establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. By default, an account is not captive (NOCAPTIVE).
DEFCLI	Restricts the user to the default command interpreter by prohibiting the use of the /CLI qualifier at login; the MCR command can still be used. By default, a user can choose a CLI (NODEFCLI).
DISCTLY	Establishes an environment where Ctrl/Y interrupts are initially turned off and are invalid until a SET CONTROL=Y is encountered. This could happen in SYLOGIN.COM or in a procedure called by SYLOGIN.COM. Once a SET CONTROL=Y is executed (which requires no privilege), a user can enter a Ctrl/Y and reach the DCL prompt ($). If the intent of DISCTLY is to force execution of the login command files, then SYLOGIN.COM should issue the DCL command SET CONTROL=Y to turn on Ctrl /Y interrupts before exiting. By default, Ctrl /Y is enabled (NODISCTLY).
DISFORCE_PWD_ CHANGE	Removes the requirement that a user must change an expired password at login. By default, a person can use an expired password only once (NODISFORCE_PWD_CHANGE) and then is forced to change the password after logging in. If the user does not select a new password, the user is locked out of the system. To use this feature, set a password expiration date with the /PWDLIFETIME qualifier.
DISIMAGE	Prevents the user from executing RUN, MCR, and foreign commands. By default, a user can execute RUN, MCR, and foreign commands (NODISIMAGE).
DISMAIL	Disables mail delivery to the user. By default, mail delivery is enabled (NODISMAIL).
DISNEWMAIL	Suppresses announcements of new mail at login. By default, the system announces new mail (NODISNEWMAIL).
DISPWDDIC	Disables automatic screening of new passwords against a system dictionary. By default, passwords are automatically screened (NODISPWDDIC).
DISPWDHIS	Disables automatic checking of new passwords against a list of the user's old passwords. By default, the system screens new passwords (NODISPWDHIS).
DISRECONNECT	Disables automatic reconnection to an existing process when a terminal connection has

been interrupted. By default, automatic reconnection is enabled (NODISRECONNECT).

DISREPORT — Suppresses reports of the last login time, login failures, and other security reports. By default, login information is displayed (NODISREPORT).

DISUSER — Disables the account so the user cannot log in. For example, the DEFAULT account is disabled. By default, an account is enabled (NODISUSER).

DISWELCOME — Suppresses the welcome message (an informational message displayed during a local login). This message usually indicates the version number of the operating system that is running and the name of the node on which the user is logged in. By default, a system login message appears (NODISWELCOME).

EXTAUTH — Considers user to be authenticated by an external user name and password, not by the SYSUAF user name and password. (The system still uses the SYSUAF record to check a user's login restrictions and quotas and to create the user's process profile.)

GENPWD — Restricts the user to generated passwords. By default, users choose their own passwords (NOGENPWD).

LOCKPWD — Prevents the user from changing the password for the account. By default, users can change their passwords (NOLOCKPWD).

PWD_EXPIRED — Marks a password as expired. The user cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not expired after login (NOPWD_EXPIRED).

PWD2_EXPIRED — Marks a secondary password as expired. Users cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not set to expire after login (NOPWD2_EXPIRED).

RESTRICTED — Prevents the user from changing any defaults at login (for example, by specifying /LGICMD) and prohibits user specification of a CLI with the /CLI qualifier. The RESTRICTED flag establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. Typically, this flag is used to prevent an applications user from having unrestricted access to the CLI. By default, a user can change defaults (NORESTRICTED).

/GENERATE_PASSWORD

/GENERATE_PASSWORD[=keyword]
/NOGENERATE_PASSWORD (default)

Invokes the password generator to create user passwords. Generated passwords can consist of 1 to 10 characters. Specify one of the following keywords:

BOTH — Generate primary and secondary passwords.
CURRENT — Do whatever the DEFAULT account does (for example, generate primary, secondary, both, or no passwords). This is the default keyword.
PRIMARY — Generate primary password only.
SECONDARY — Generate secondary password only.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, users are forced to change their passwords (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/INTERACTIVE

/INTERACTIVE[=(range[,...])]
/NOINTERACTIVE

Specifies the hours of access for interactive logins. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on interactive logins.

/JTQUOTA

/JTQUOTA=value

Specifies the initial byte quota with which the jobwide logical name table is to be created. By default, the value is 4096 on VAX systems and 4096 on Alpha systems.

/LGICMD

/LGICMD=filespec

Specifies the name of the default login command file. The file name defaults to the device specified for /DEVICE, the directory specified for /DIRECTORY, a file name of LOGIN, and a file type of .COM. If you select the defaults for all these values, the file name is SYS$SYSTEM:[USER]LOGIN.COM.

/LOCAL

/LOCAL[=(range[,...])]

Specifies hours of access for interactive logins from local terminals. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on local logins.

/MAXACCTJOBS

/MAXACCTJOBS=value

Specifies the maximum number of batch, interactive, and detached processes that can be active at one time for all users of the same account. By default, a user has a maximum of 0, which represents an unlimited number.

/MAXDETACH

/MAXDETACH=value

Specifies the maximum number of detached processes with the cited user name that can be active at one time. To prevent the user from creating detached processes, specify the keyword NONE. By default, a user has a value of 0, which represents an unlimited number.

/MAXJOBS

/MAXJOBS=value

Specifies the maximum number of processes (interactive, batch, detached, and network) with the cited user name that can be active simultaneously. The first four network jobs are not counted. By default, a user has a maximum value of 0, which represents an unlimited number.

/NETWORK

/NETWORK[=(range[,...])]

Specifies hours of access for network batch jobs. For a description of how to specify the range, see the /ACCESS qualifier. By default, network logins have no access restrictions.

/OWNER

/OWNER=owner-name

Specifies the name of the owner of the account. You can use this name for billing purposes or similar applications. The owner name is 1 to 31 characters. No default owner name exists.

/PASSWORD

/PASSWORD=(password1[,password2])
/NOPASSWORD

Specifies up to two passwords for login. Passwords can be from 0 to 32 characters in length and can include alphanumeric characters, dollar signs, and underscores. Avoid using the word password as the actual password. Use the /PASSWORD qualifier as follows:

- To set only the first password and clear the second, specify /PASSWORD=password.
- To set both the first and second password, specify /PASSWORD=(password1, password2).
- To change the first password without affecting the second, specify /PASSWORD=(password, "").
- To change the second password without affecting the first, specify /PASSWORD=("", password).
- To set both passwords to null, specify /NOPASSWORD.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, the user is forced to change the password (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

When you create a new UAF record with the COPY command, you must specify a password.

/PBYTLM

This flag is reserved for Digital.

/PGFLQUOTA

/PGFLQUOTA=value

Specifies the paging file limit. This is the maximum number of pages that the person's process can use in the system paging file. By default, the value is 32768 pages on VAX systems and 50000 pagelets on Alpha systems.

If decompressing libraries, make sure to set PGFLQUOTA to twice the size of the library.

/PRCLM

/PRCLM=value

Specifies the subprocess creation limit. This is the maximum number of subprocesses that can exist at one time for the specified user's process. By default, the value is 2 on VAX systems and 8 on Alpha systems.

/PRIMEDAYS

/PRIMEDAYS=([NO]day[,...])

Defines the primary and secondary days of the week for logging in. Specify the days as a list separated by commas, and enclose the list in parentheses. To specify a secondary day, prefix the day with NO (for example, NOFRIDAY). To specify a primary day, omit the NO prefix.

By default, primary days are Monday through Friday and secondary days are Saturday and Sunday. If you omit a day from the list, AUTHORIZE uses the default value. (For example, if you omit Monday from the list, AUTHORIZE defines Monday as a primary day.)

Use the primary and secondary day definitions in conjunction with such qualifiers as /ACCESS, /INTERACTIVE, and /BATCH.

/PRIORITY

/PRIORITY=value

Specifies the default base priority. The value is an integer in the range of 0 to 31 on VAX systems and 0 to 63 on Alpha systems. By default, the value is set to 4 for timesharing users.

/PRIVILEGES

/PRIVILEGES=([NO]privname[,...])

Specifies which privileges the user is authorized to hold, although these privileges are not necessarily enabled at login. (The /DEFPRIVILEGES qualifier determines which ones are enabled.) A NO prefix removes the privilege from the user. The keyword NOALL disables all user privileges. Many privileges have varying degrees of power and potential system impact (see the OpenVMS Guide to System Security for a detailed discussion). By default, a user holds TMPMBX and NETMBX privileges. Privname is the name of the privilege.

/PWDEXPIRED

/PWDEXPIRED (default)
/NOPWDEXPIRED

Specifies the password is valid for only one login. A user must change a password immediately after login or be locked out of the system. The system warns users of password expiration. A user can either specify a new password, with the DCL command SET PASSWORD, or wait until expiration and be forced to change. By default, a user must change a password when first logging in to an account. The default is applied to the account only when the password is being modified.

/PWDLIFETIME

/PWDLIFETIME=time (default)
/NOPWDLIFETIME

Specifies the length of time a password is valid. Specify a delta time value in the form [dddd-] [hh:mm:ss.cc]. For example, for a lifetime of 120 days, 0 hours, and 0 seconds, specify /PWDLIFETIME="120-". For a lifetime of 120 days 12 hours, 30 minutes and 30 seconds, specify /PWDLIFETIME="120-12:30:30". If a period longer than the specified time elapses before the user logs in, the system displays a warning message. The password is marked as expired.

To prevent a password from expiring, specify the time as NONE. By default, a password expires in 90 days.

/PWDMINIMUM

/PWDMINIMUM=value

Specifies the minimum password length in characters. Note that this value is enforced only by the DCL command SET PASSWORD. It does not prevent you from entering a password shorter than the minimum length when you use AUTHORIZE to create or modify an account. By default, a password must have at least 6 characters. The value specified by the /PWDMINIMUM qualifier conflicts with the value used by the /GENERATE_PASSWORD qualifier or the DCL command SET PASSWORD/GENERATE, the operating system chooses the lesser value. The maximum value for generated passwords is 10.

/QUEPRIO

/QUEPRIO=value

Reserved for future use.

/REMOTE

/REMOTE[=(range[,...])]

Specifies hours during which access is permitted for interactive logins from network remote terminals (with the DCL command SET HOST). For a description of the range specification, see the /ACCESS qualifier. By default, remote logins have no access restrictions.

/SHRFILLM

/SHRFILLM=value

Specifies the maximum number of shared files that the user can have open at one time. By default, the system assigns a value of 0, which 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. By default, a user can have 10.

/UIC

/UIC=value

Specifies the user identification code (UIC). The UIC value is a group number in the range from 1 to 37776 (octal) and a member number in the range from 0 to 177776 (octal), which are separated by a comma and enclosed in brackets. Digital reserves group 1 and groups 300-377 for its own use.

Each user must have a unique UIC. By default, the UIC value is [200,200].

/WSDEFAULT

/WSDEFAULT=value

Specifies the default working set limit. This represents the initial limit to the number of physical pages the process can use. (The user can alter the default quantity up to WSQUOTA with the DCL command SET WORKING_SET.) By default, a user has 256 pages on VAX systems and 2000 pagelets on Alpha systems.

The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSDEFAULT.

/WSEXTENT

/WSEXTENT=value

Specifies the working set maximum. This represents the maximum amount of physical memory allowed to the process. The system provides memory to a process beyond its working set quota only when it has excess free pages. The additional memory is recalled by the system if needed.

The value is an integer equal to or greater than WSQUOTA. By default, the value is 1024 pages on VAX systems and 16384 pagelets on Alpha systems. The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSEXTENT.

/WSQUOTA

/WSQUOTA=value

Specifies the working set quota. This is the maximum amount of physical memory a user process can lock into its working set. It also represents the maximum amount of swap space that the system reserves for this process and the maximum amount of physical memory that the system allows the process to consume if the systemwide memory demand is significant.

The value cannot be greater than the value of WSMAX and cannot exceed 64K pages. This quota value replaces smaller values of PQL_MWSQUOTA.

2 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, except for the password, to that of Joseph Robin. Note that because the UIC value has no change, 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 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.

VMS AUTHORIZE (UAF) Help

1 CREATE

2 /PROXY
Creates and initializes the network proxy authorization files.
The primary network proxy authorization file is NET$PROXY.DAT.
The file NETPROXY.DAT is maintained for compatibility.

NOTE

Do not delete NETPROXY.DAT because DECnet Phase IV and many layered products still use it.

Format

CREATE/PROXY

3 Example

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

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

2 /RIGHTS
Creates and initializes the rights database, RIGHTSLIST.DAT.

Format

CREATE/RIGHTS

3 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 OpenVMS Guide to System Security.

VMS AUTHORIZE (UAF) Help

1 DEFAULT

Modifies the SYSUAF's DEFAULT record.

Format

DEFAULT

2 Qualifiers

/ACCESS

/ACCESS[=(range[,...])]

Specifies hours of access for all modes of access. The syntax for specifying the range is:

/[NO]ACCESS=([PRIMARY], [n-m], [n], [,...],[SECONDARY], [n-m], [n], [,...])

Specify hours as integers from 0 to 23, inclusive. You can specify single hours (n) or 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.

By default, a user has full access every day. See the DCL command SET DAY in the OpenVMS DCL Dictionary for information on overriding the defaults for primary and secondary day types.

All the list elements are optional. Unless you specify hours for a day type, access is permitted for the entire day. By specifying an access time, you prevent access at all other times. Adding NO to the qualifier denies the user access to the system for the specified period of time.

Examples:

/ACCESS	Allows unrestricted access
/NOACCESS=SECONDARY	Allows access on primary days only
/ACCESS=(9-17)	Allows access from 9 A.M. to 5:59 P.M. on all days
/NOACCESS=(PRIMARY, 9-17, SECONDARY, 18-8)	Disallows access between 9 A.M. to 5:59 P.M. on primary days but allows access during these hours on secondary days

To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.

/ACCOUNT

/ACCOUNT=account-name

Specifies the default name for the account (for example, a billing name or number). The name can be a string of 1 to 8 alphanumeric characters. By default, AUTHORIZE does not assign an account name.

/ALGORITHM

/ALGORITHM=keyword=type [=value]

Sets the password encryption algorithm for a user. The keyword VMS refers to the algorithm used in the operating system version that is running on your system, whereas a customer algorithm is one that is added through the $HASH_PASSWORD system service by a customer site, by a layered product, or by a third party. The customer algorithm is identified in $HASH_PASSWORD by an integer in the range of 128 to 255. It must correspond with the number used in the AUTHORIZE command MODIFY/ALGORITHM. By default, passwords are encrypted with the VMS algorithm for the current version of the operating system.

Keyword	Function
BOTH	Set the algorithm for primary and secondary passwords.
CURRENT	Set the algorithm for the primary, secondary, both, or no passwords, depending on account status. CURRENT is the default value.
PRIMARY	Set the algorithm for the primary password only.
SECONDARY	Set the algorithm for the secondary password only.

The following table lists password encryption algorithms:

Type	Definition
VMS	The algorithm used in the version of the operating system that is running on your system.
CUSTOMER	A numeric value in the range of 128 to 255 that identifies a customer algorithm.

The following example selects the VMS algorithm for Sontag's primary password:

```
UAF>  MODIFY SONTAG/ALGORITHM=PRIMARY=VMS
```

If you select a site-specific algorithm, you must give a value to identify the algorithm, as follows:

```
UAF>  MODIFY SONTAG/ALGORITHM=CURRENT=CUSTOMER=128
```

/ASTLM

/ASTLM=value

Specifies the AST queue limit, which is the total number of asynchronous system trap (AST) operations and scheduled wake-up requests that the user can have queued at one time. The default is 40 on VAX systems and 250 on Alpha systems.

/BATCH

/BATCH[=(range[,...])]

Specifies the hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier. By default, a user can submit batch jobs any time.

/BIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/BYTLM

/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 can consume at one time. Nonpaged dynamic memory is used for operations such as I/O buffering, mailboxes, and file-access windows. The default is 32768 on VAX systems and 64000 on Alpha systems.

/CLI

/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 a string of 1 to 31 alphanumeric characters and should be either DCL or MCR. The default is DCL. This setting is ignored for network jobs.

/CLITABLES

/CLITABLES=filespec

Specifies user-defined CLI tables for the account. The filespec can contain 1 to 31 characters. The default is SYS$LIBRARY:DCLTABLES. Note that this setting is ignored for network jobs to guarantee that the system-supplied command procedures used to implement network objects function properly.

/CPUTIME

/CPUTIME=time

Specifies the maximum process CPU time for the CPU field of the UAF record. The maximum process CPU time is the maximum amount of 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 OpenVMS User's Manual. The default is 0, which means an infinite amount of time.

/DEFPRIVILEGES

/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. By specifying the keyword [NO]ALL with the /DEFPRIVILEGES qualifier, you can disable or enable all user privileges. The default privileges are TMPMBX and NETMBX. Privname is the name of the privilege.

/DEVICE

/DEVICE=device-name

Specifies the name of the user's default device at login. The device-name is a string of 1 to 31 alphanumeric characters. If you omit the colon from the device-name value, AUTHORIZE appends a colon. The default device is SYS$SYSDISK.

If you specify a logical name as the device-name (for example, DISK1: for DUA1:), you must make an entry for the logical name in the LNM$SYSTEM_TABLE in executive mode by using the DCL command DEFINE/SYSTEM/EXEC.

/DIALUP

/DIALUP[=(range[,...])]

Specifies hours of access permitted for dialup logins. For a description of the range specification, see the /ACCESS qualifier. The default is full access.

/DIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/DIRECTORY

/DIRECTORY=directory-name

Specifies the default directory name for the DIRECTORY field of the UAF record. The directory-name can be 1 to 39 alphanumeric characters. If you do not enclose the directory name in brackets, AUTHORIZE adds the brackets for you. The default directory name is [USER].

/ENQLM

/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 by the user at one time. The default is 200 on VAX systems and 2000 on Alpha systems.

/EXPIRATION

/EXPIRATION=time (default)
/NOEXPIRATION

Specifies the expiration date and time of the account. The /NOEXPIRATION qualifier removes the expiration date on the account or resets the expiration time for expired accounts. The default expiration time period is 90 days for nonprivileged users.

/FILLM

/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 default is 300 on VAX systems and 100 on Alpha systems.

/FLAGS

/FLAGS=([NO]option[,...])

Specifies login flags for the user. The prefix NO clears the flag. The options are as follows:

AUDIT	Enables or disables mandatory security auditing for a specific user. By default, the system does not audit the activities of specific users (NOAUDIT).
AUTOLOGIN	Restricts the user to the automatic login mechanism when logging in to an account. When set, the flag disables login by any terminal that requires entry of a user name and password. The default is to require a user name and password (NOAUTOLOGIN).
CAPTIVE	Prevents the user from changing any defaults at login, for example, /CLI or /LGICMD. It prevents the user from escaping the captive login command procedure specified by the /LGICMD qualifier and gaining access to the DCL command level. See Guidelines for Captive Command Procedures in the OpenVMS Guide to System Security. The CAPTIVE flag also establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. By default, an account is not captive (NOCAPTIVE).
DEFCLI	Restricts the user to the default command interpreter by prohibiting the use of the /CLI qualifier at login; the MCR command can still be used. By default, a user can choose a CLI (NODEFCLI).
DISCTLY	Establishes an environment where Ctrl/Y interrupts are initially turned off and are invalid until a SET CONTROL=Y is encountered. This could happen in SYLOGIN.COM or in a procedure called by SYLOGIN.COM. Once a SET CONTROL=Y is executed (which requires no privilege), a user can enter a Ctrl/Y and reach the DCL prompt ($). If the intent of DISCTLY is to force execution of the login command files, then SYLOGIN.COM should issue the DCL command SET CONTROL=Y to turn on Ctrl /Y interrupts before exiting. By default, Ctrl /Y is enabled (NODISCTLY).
DISFORCE_PWD_ CHANGE	Removes the requirement that a user must change an expired password at login. By default, a person can use an expired password only once (NODISFORCE_PWD_CHANGE) and then is forced to change the password after logging in. If the user does not select a new password, the user is locked out of the system. To use this feature, set a password expiration date with the /PWDLIFETIME qualifier.
DISIMAGE	Prevents the user from executing RUN, MCR, and foreign commands. By default, a user can execute RUN, MCR, and foreign commands (NODISIMAGE).
DISMAIL	Disables mail delivery to the user. By default, mail delivery is enabled (NODISMAIL).
DISNEWMAIL	Suppresses announcements of new mail at login. By default, the system announces new mail (NODISNEWMAIL).
DISPWDDIC	Disables automatic screening of new passwords against a system dictionary. By default, passwords are automatically screened (NODISPWDDIC).
DISPWDHIS	Disables automatic checking of new passwords against a list of the user's old passwords. By default, the system screens new passwords (NODISPWDHIS).
DISRECONNECT	Disables automatic reconnection to an existing process when a terminal connection has been interrupted. By default, automatic reconnection is enabled (NODISRECONNECT).
DISREPORT	Suppresses reports of the last login time, login failures, and other security reports. By default, login information is displayed (NODISREPORT).
DISUSER	Disables the account so the user cannot log in. For example, the DEFAULT account is disabled. By default, an account is enabled (NODISUSER).
DISWELCOME	Suppresses the welcome message (an informational message displayed during a local login). This message usually indicates the version number of the operating system that is running and the name of the node on which the user is logged in. By default, a system login message appears (NODISWELCOME).
EXTAUTH	Considers user to be authenticated by an external user name and password, not by the SYSUAF user name and password. (The system still uses the SYSUAF record to check a user's login restrictions and quotas and to create the user's process profile.)
GENPWD	Restricts the user to generated passwords. By default, users choose their own passwords (NOGENPWD).

LOCKPWD — Prevents the user from changing the password for the account. By default, users can change their passwords (NOLOCKPWD).

PWD_EXPIRED — Marks a password as expired. The user cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not expired after login (NOPWD_EXPIRED).

PWD2_EXPIRED — Marks a secondary password as expired. Users cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not set to expire after login (NOPWD2_EXPIRED).

RESTRICTED — Prevents the user from changing any defaults at login (for example, by specifying /LGICMD) and prohibits user specification of a CLI with the /CLI qualifier. The RESTRICTED flag establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. Typically, this flag is used to prevent an applications user from having unrestricted access to the CLI. By default, a user can change defaults (NORESTRICTED).

/GENERATE_PASSWORD

/GENERATE_PASSWORD[=keyword]
/NOGENERATE_PASSWORD (default)

Invokes the password generator to create user passwords. Generated passwords can consist of 1 to 10 characters. Specify one of the following keywords:

BOTH — Generate primary and secondary passwords.

CURRENT — Do whatever the DEFAULT account does (for example, generate primary, secondary, both, or no passwords). This is the default keyword.

PRIMARY — Generate primary password only.

SECONDARY — Generate secondary password only.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, users are forced to change their passwords (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/INTERACTIVE

/INTERACTIVE[=(range[,...])]
/NOINTERACTIVE

Specifies the hours of access for interactive logins. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on interactive logins.

/JTQUOTA

/JTQUOTA=value

Specifies the initial byte quota with which the jobwide logical name table is to be created. By default, the value is 4096 on VAX systems and 4096 on Alpha systems.

/LGICMD

/LGICMD=filespec

Specifies the name of the default login command file. The file name defaults to the device specified for /DEVICE, the directory specified for /DIRECTORY, a file name of LOGIN, and a file type of .COM. If you select the defaults for all these values, the file name is SYS$SYSTEM:[USER]LOGIN.COM.

/LOCAL

/LOCAL[=(range[,...])]

Specifies hours of access for interactive logins from local terminals. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on local logins.

/MAXACCTJOBS

/MAXACCTJOBS=value

Specifies the maximum number of batch, interactive, and detached processes that can be active at one time for all users of the same account. By default, a user has a maximum of 0, which represents an unlimited number.

/MAXDETACH

/MAXDETACH=value

Specifies the maximum number of detached processes with the cited user name that can be active at one time. To prevent the user from creating detached processes, specify the keyword NONE. By default, a user has a value of 0, which represents an unlimited number.

/MAXJOBS

/MAXJOBS=value

Specifies the maximum number of processes (interactive, batch, detached, and network) with the cited user name that can be active simultaneously. The first four network jobs are not counted. By default, a user has a maximum value of 0, which represents an unlimited number.

/MODIFY_IDENTIFIER

/MODIFY_IDENTIFIER (default)
/NOMODIFY_IDENTIFIER

Specifies whether the identifier associated with the user is to be modified in the rights database. This qualifier applies only when you modify the UIC or user name in the UAF record. By default, the associated identifiers are modified.

/NETWORK

/NETWORK[=(range[,...])]

Specifies hours of access for network batch jobs. For a description of how to specify the range, see the /ACCESS qualifier. By default, network logins have no access restrictions.

/OWNER

/OWNER=owner-name

Specifies the name of the owner of the account. You can use this name for billing purposes or similar applications. The owner name is 1 to 31 characters. No default owner name exists.

/PASSWORD

/PASSWORD=(password1[,password2])
/NOPASSWORD

Specifies up to two passwords for login. Passwords can be from 0 to 32 characters in length and can include alphanumeric characters, dollar signs, and underscores. Avoid using the word password as the actual password. Use the /PASSWORD qualifier as follows:

- To set only the first password and clear the second, specify /PASSWORD=password.
- To set both the first and second password, specify /PASSWORD=(password1, password2).
- To change the first password without affecting the second, specify /PASSWORD=(password, "").
- To change the second password without affecting the first, specify /PASSWORD=("", password).
- To set both passwords to null, specify /NOPASSWORD.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, the user is forced to change the password (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/PBYTLM

This flag is reserved for Digital.

/PGFLQUOTA

/PGFLQUOTA=value

Specifies the paging file limit. This is the maximum number of pages that the person's process can use in the system paging file. By default, the value is 32768 pages on VAX systems and 50000 pagelets on Alpha systems.

If decompressing libraries, make sure to set PGFLQUOTA to twice the size of the library.

/PRCLM

/PRCLM=value

Specifies the subprocess creation limit. This is the maximum number of subprocesses that can exist at one time for the specified user's process. By default, the value is 2 on VAX systems and 8 on Alpha systems.

/PRIMEDAYS

/PRIMEDAYS=([NO]day[,...])

Defines the primary and secondary days of the week for logging in. Specify the days as a list separated by commas, and enclose the list in parentheses. To specify a secondary day, prefix the day with NO (for example, NOFRIDAY). To specify a primary day, omit the NO prefix.

By default, primary days are Monday through Friday and secondary days are Saturday and Sunday. If you omit a day from the list, AUTHORIZE uses the default value. (For example, if you omit Monday from the list, AUTHORIZE defines Monday as a primary day.)

Use the primary and secondary day definitions in conjunction with such qualifiers as /ACCESS, /INTERACTIVE, and /BATCH.

/PRIORITY

/PRIORITY=value

Specifies the default base priority. The value is an integer in the range of 0 to 31 on VAX systems and 0 to 63 on Alpha systems. By default, the value is set to 4 for timesharing users.

/PRIVILEGES

/PRIVILEGES=([NO]privname[,...])

Specifies which privileges the user is authorized to hold, although these privileges are not necessarily enabled at login. (The /DEFPRIVILEGES qualifier determines which ones are enabled.) A NO prefix removes the privilege from the user. The keyword

NOALL disables all user privileges. Many privileges have varying degrees of power and potential system impact (see the OpenVMS Guide to System Security for a detailed discussion). By default, a user holds TMPMBX and NETMBX privileges. Privname is the name of the privilege.

/PWDEXPIRED

/PWDEXPIRED (default)
/NOPWDEXPIRED

Specifies the password is valid for only one login. A user must change a password immediately after login or be locked out of the system. The system warns users of password expiration. A user can either specify a new password, with the DCL command SET PASSWORD, or wait until expiration and be forced to change. By default, a user must change a password when first logging in to an account. The default is applied to the account only when the password is being modified.

/PWDLIFETIME

/PWDLIFETIME=time (default)
/NOPWDLIFETIME

Specifies the length of time a password is valid. Specify a delta time value in the form [dddd-] [hh:mm:ss.cc]. For example, for a lifetime of 120 days, 0 hours, and 0 seconds, specify /PWDLIFETIME="120-". For a lifetime of 120 days 12 hours, 30 minutes and 30 seconds, specify /PWDLIFETIME="120-12:30:30". If a period longer than the specified time elapses before the user logs in, the system displays a warning message. The password is marked as expired.

To prevent a password from expiring, specify the time as NONE. By default, a password expires in 90 days.

/PWDMINIMUM

/PWDMINIMUM=value

Specifies the minimum password length in characters. Note that this value is enforced only by the DCL command SET PASSWORD. It does not prevent you from entering a password shorter than the minimum length when you use AUTHORIZE to create or modify an account. By default, a password must have at least 6 characters. The value specified by the /PWDMINIMUM qualifier conflicts with the value used by the /GENERATE_PASSWORD qualifier or the DCL command SET PASSWORD/GENERATE, the operating system chooses the lesser value. The maximum value for generated passwords is 10.

/QUEPRIO

/QUEPRIO=value

Reserved for future use.

/REMOTE

/REMOTE[=(range[,...])]

Specifies hours during which access is permitted for interactive logins from network remote terminals (with the DCL command SET HOST). For a description of the range specification, see the /ACCESS qualifier. By default, remote logins have no access restrictions.

/SHRFILLM

/SHRFILLM=value

Specifies the maximum number of shared files that the user can have open at one time. By default, the system assigns a value of 0, which 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. By default, a user can have 10.

/UIC

/UIC=value

Specifies the user identification code (UIC). The UIC value is a group number in the range from 1 to 37776 (octal) and a member number in the range from 0 to 177776 (octal), which are separated by a comma and enclosed in brackets. Digital reserves group 1 and groups 300-377 for its own use.

Each user must have a unique UIC. By default, the UIC value is [200,200].

/WSDEFAULT

/WSDEFAULT=value

Specifies the default working set limit. This represents the initial limit to the number of physical pages the process can use. (The user can alter the default quantity up to WSQUOTA with the DCL command SET WORKING_SET.) By default, a user has 256 pages on VAX systems and 2000 pagelets on Alpha systems.

The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSDEFAULT.

/WSEXTENT

/WSEXTENT=value

Specifies the working set maximum. This represents the maximum amount of physical memory allowed to the process. The system provides memory to a process beyond its working set quota only when it has excess free pages. The additional memory is recalled by the system if needed.

The value is an integer equal to or greater than WSQUOTA. By default, the value is 1024 pages on VAX systems and 16384 pagelets on Alpha systems. The value cannot be greater than

WSMAX. This quota value replaces smaller values of PQL_MWSEXTENT.

/WSQUOTA

/WSQUOTA=value

Specifies the working set quota. This is the maximum amount of physical memory a user process can lock into its working set. It also represents the maximum amount of swap space that the system reserves for this process and the maximum amount of physical memory that the system allows the process to consume if the systemwide memory demand is significant.

The value cannot be greater than the value of WSMAX and cannot exceed 64K pages. This quota value replaces smaller values of PQL_MWSQUOTA.

2 Example

```
UAF> DEFAULT /DEVICE=SYS$USER/LGICMD=SYS$MANAGER:SECURELGN -
_UAF> /PRIVILEGES=(TMPMBX,GRPNAM,GROUP)
%UAF-I-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.

VMS AUTHORIZE (UAF) Help

1 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

VMS AUTHORIZE (UAF) Help

1 GRANT

2 /IDENTIFIER
Assigns the specified identifier to the user and documents the user as a holder of the identifier in the rights database.

Format

```
GRANT/IDENTIFIER  id-name user-spec
```

3 Parameters

id-name

Specifies the identifier name. The identifier name is a string of 1 to 31 alphanumeric characters that can contain underscores and dollar signs. The name must contain at least one nonnumeric character.

user-spec

Specifies the UIC identifier that uniquely identifies the user on the system. This type of identifier appears in alphanumeric format. For example: [GROUP1,JONES].

3 Qualifier

/ATTRIBUTES

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

Specifies attributes to be associated with the identifier. The following are valid keywords:

DYNAMIC	Allows unprivileged holders of the identifier to remove and to restore the identifier from the process rights list by using the DCL command SET RIGHTS_LIST.
HOLDER_HIDDEN	Prevents people from getting a list of users who hold an identifier, unless they own the identifier themselves.
NAME_HIDDEN	Allows holders of an identifier to have it translated, either from binary to ASCII or from ASCII to binary, but prevents unauthorized users from translating the identifier.
NOACCESS	Makes any access rights of the identifier null and void. If a user is granted an identifier with the No Access attribute, that identifier has no effect on the user's access rights to objects. This attribute is a modifier for an identifier with the Resource or Subsystem attribute.
RESOURCE	Allows holders of an identifier to charge disk space to the identifier. Used only for file objects.
SUBSYSTEM	Allows holders of the identifier to create and maintain protected subsystems by assigning the Subsystem ACE to the application images in the subsystem. Used only for file objects.

To remove an attribute from the identifier, add a NO prefix to the attribute keyword. For example, to remove the Resource attribute, specify /ATTRIBUTES=NORESOURCE.

3 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 the user named Cramer who has UIC [300,015]. 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
```

VMS AUTHORIZE (UAF) Help

1 HELP

Displays information concerning the use of AUTHORIZE, including formats and explanations of commands, parameters, and qualifiers.

Format

HELP [keyword[,...]]

2 Parameter

keyword[,...]

Specifies one or more keywords that refer to the topic, command, qualifier, or parameter on which you want information from the AUTHORIZE HELP command.

VMS AUTHORIZE (UAF) Help

1 LIST

Writes reports for selected UAF records to a listing file, SYSUAF.LIS, which is placed in the SYS$SYSTEM directory.

Format

LIST [user-spec]

2 Parameter

user-spec

Specifies the user name or UIC of the requested UAF record. Without the user-spec parameter, AUTHORIZE lists the user records of all users. The asterisk (*) and percent sign (%) wildcards are permitted in the user name.

2 Qualifiers

/BRIEF

Specifies that a brief report be written to SYSUAF.LIS. The /BRIEF qualifier is the default qualifier. SYSUAF.LIS is placed in the SYS$SYSTEM directory.

/FULL

Specifies that a full report be written to SYSUAF.LIS, including identifiers held by the user. SYSUAF.LIS is placed in the SYS$SYSTEM directory.

2 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.
Creates a listing file (RIGHTSLIST.LIS) in which identifier names, attributes, values, and holders are written.

Format

LIST/IDENTIFIER [id-name]

3 Parameter

id-name

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

3 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. The /FULL qualifier specifies the default listing format.

/USER

/USER=user-spec

Specifies one or more users whose identifiers are to be listed. The user-spec can be a user name or UIC. You can use the asterisk wildcard character (*) to specify multiple user names or UICs. 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=value-specifier

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

IDENTIFIER:n	An integer value in the range 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).
	To differentiate general identifiers from UIC identifiers, %X80000000 is added to the value you specify.
UIC:uic	A UIC value in the standard UIC format.

3 Examples

1.UAF> LIST/IDENTIFIER INVENTORY
%UAF-I-LSTMSG1, 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-LSTMSG1, writing listing file
%UAF-I-RLSTMSG, listing file RIGHTSLIST.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]

2 /PROXY

Creates a listing file of the network proxy database entries from the network database file NET$PROXY.DAT.

Format

LIST/PROXY

3 Qualifiers

/OLD

Directs AUTHORIZE to display information from the NETPROXY.DAT file rather than from the default file NET$PROXY.DAT.

If someone modifies the proxy database on a cluster node that is not running the current OpenVMS VAX system, then you can use the /OLD qualifier to list the contents of the old database: NETPROXY.DAT.

3 Example

```
UAF> LIST/PROXY/OLD
%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 NETPROXY.DAT.

2 /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]

3 Parameter

id-name

Specifies the name of the identifier associated with the user. If you omit the identifier name, you must specify the /USER qualifier.

3 Qualifier

/USER

/USER=user-spec

Specifies a user whose identifiers are to be listed. The user-spec can be a user name or UIC. You can use the asterisk wildcard character (*) to specify multiple UICs or all 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.

3 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.

VMS AUTHORIZE (UAF) Help

1 MODIFY

Changes values in a SYSUAF user record. Qualifiers not specified in the command remain unchanged.

Format

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

2 Parameter

username

Specifies the name of a user in the SYSUAF. The asterisk (*) and percent sign (%) wildcard characters are permitted in the user name. When you specify a single asterisk for the user name, you modify the records of all users.

2 Qualifiers

/ACCESS

```
/ACCESS[=(range[,...])]
```

Specifies hours of access for all modes of access. The syntax for specifying the range is:

```
/[NO]ACCESS=([PRIMARY], [n-m], [n], [,...],[SECONDARY], [n-m], [n], [,...])
```

Specify hours as integers from 0 to 23, inclusive. You can specify single hours (n) or 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.

By default, a user has full access every day. See the DCL command SET DAY in the OpenVMS DCL Dictionary for information on overriding the defaults for primary and secondary day types.

All the list elements are optional. Unless you specify hours for a day type, access is permitted for the entire day. By specifying an access time, you prevent access at all other times. Adding NO to the qualifier denies the user access to the system for the specified period of time.

Examples:

/ACCESS	Allows unrestricted access
/NOACCESS=SECONDARY	Allows access on primary days only
/ACCESS=(9-17)	Allows access from 9 A.M. to 5:59 P.M. on all days
/NOACCESS=(PRIMARY, 9-17, SECONDARY, 18-8)	Disallows access between 9 A.M. to 5:59 P.M. on primary days but allows access during these hours on secondary days

To specify access hours for specific types of access, see the /BATCH, /DIALUP, /INTERACTIVE, /LOCAL, /NETWORK, and /REMOTE qualifiers.

/ACCOUNT

```
/ACCOUNT=account-name
```

Specifies the default name for the account (for example, a billing name or number). The name can be a string of 1 to 8 alphanumeric characters. By default, AUTHORIZE does not assign an account name.

/ALGORITHM

```
/ALGORITHM=keyword=type [=value]
```

Sets the password encryption algorithm for a user. The keyword VMS refers to the algorithm used in the operating system version that is running on your system, whereas a customer algorithm is one that is added through the $HASH_PASSWORD system service by a customer site, by a layered product, or by a third party. The customer algorithm is identified in $HASH_PASSWORD by an integer in the range of 128 to 255. It must correspond with the number used in the AUTHORIZE command MODIFY/ALGORITHM. By default, passwords are encrypted with the VMS algorithm for the current version of the operating system.

Keyword	Function
BOTH	Set the algorithm for primary and secondary passwords.
CURRENT	Set the algorithm for the primary, secondary, both, or no passwords, depending on account status. CURRENT is the default value.
PRIMARY	Set the algorithm for the primary password only.
SECONDARY	Set the algorithm for the secondary password only.

The following table lists password encryption algorithms:

Type	Definition
VMS	The algorithm used in the version of the operating system that is running on your system.
CUSTOMER	A numeric value in the range of 128 to 255 that identifies a customer algorithm.

The following example selects the VMS algorithm for Sontag's primary password:

```
UAF>  MODIFY SONTAG/ALGORITHM=PRIMARY=VMS
```

If you select a site-specific algorithm, you must give a value to identify the algorithm, as follows:

```
UAF>  MODIFY SONTAG/ALGORITHM=CURRENT=CUSTOMER=128
```

/ASTLM

/ASTLM=value

Specifies the AST queue limit, which is the total number of asynchronous system trap (AST) operations and scheduled wake-up requests that the user can have queued at one time. The default is 40 on VAX systems and 250 on Alpha systems.

/BATCH

/BATCH[=(range[,...])]

Specifies the hours of access permitted for batch jobs. For a description of the range specification, see the /ACCESS qualifier. By default, a user can submit batch jobs any time.

/BIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/BYTLM

/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 can consume at one time. Nonpaged dynamic memory is used for operations such as I/O buffering, mailboxes, and file-access windows. The default is 32768 on VAX systems and 64000 on Alpha systems.

/CLI

/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 a string of 1 to 31 alphanumeric characters and should be either DCL or MCR. The default is DCL. This setting is ignored for network jobs.

/CLITABLES

/CLITABLES=filespec

Specifies user-defined CLI tables for the account. The filespec can contain 1 to 31 characters. The default is SYS$LIBRARY:DCLTABLES. Note that this setting is ignored for network jobs to guarantee that the system-supplied command procedures used to implement network objects function properly.

/CPUTIME

/CPUTIME=time

Specifies the maximum process CPU time for the CPU field of the UAF record. The maximum process CPU time is the maximum amount of 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 OpenVMS User's Manual. The default is 0, which means an infinite amount of time.

/DEFPRIVILEGES

/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. By specifying the keyword [NO]ALL with the /DEFPRIVILEGES qualifier, you can disable or enable all user privileges. The default privileges are TMPMBX and NETMBX. Privname is the name of the privilege.

/DEVICE

/DEVICE=device-name

Specifies the name of the user's default device at login. The device-name is a string of 1 to 31 alphanumeric characters. If you omit the colon from the device-name value, AUTHORIZE appends a colon. The default device is SYS$SYSDISK.

If you specify a logical name as the device-name (for example, DISK1: for DUA1:), you must make an entry for the logical name in the LNM$SYSTEM_TABLE in executive mode by using the DCL command DEFINE/SYSTEM/EXEC.

/DIALUP

/DIALUP[=(range[,...])]

Specifies hours of access permitted for dialup logins. For a description of the range specification, see the /ACCESS qualifier. The default is full access.

/DIOLM

/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 default is 40 on VAX systems and 150 on Alpha systems.

/DIRECTORY

/DIRECTORY=directory-name

Specifies the default directory name for the DIRECTORY field of the UAF record. The directory-name can be 1 to 39 alphanumeric characters. If you do not enclose the directory name in brackets, AUTHORIZE adds the brackets for you. The default directory name

is [USER].

/ENQLM

/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 by the user at one time. The default is 200 on VAX systems and 2000 on Alpha systems.

/EXPIRATION

/EXPIRATION=time (default)
/NOEXPIRATION

Specifies the expiration date and time of the account. The /NOEXPIRATION qualifier removes the expiration date on the account or resets the expiration time for expired accounts. The default expiration time period is 90 days for nonprivileged users.

/FILLM

/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 default is 300 on VAX systems and 100 on Alpha systems.

/FLAGS

/FLAGS=([NO]option[,...])

Specifies login flags for the user. The prefix NO clears the flag. The options are as follows:

AUDIT	Enables or disables mandatory security auditing for a specific user. By default, the system does not audit the activities of specific users (NOAUDIT).
AUTOLOGIN	Restricts the user to the automatic login mechanism when logging in to an account. When set, the flag disables login by any terminal that requires entry of a user name and password. The default is to require a user name and password (NOAUTOLOGIN).
CAPTIVE	Prevents the user from changing any defaults at login, for example, /CLI or /LGICMD. It prevents the user from escaping the captive login command procedure specified by the /LGICMD qualifier and gaining access to the DCL command level. See Guidelines for Captive Command Procedures in the OpenVMS Guide to System Security. The CAPTIVE flag also establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. By default, an account is not captive (NOCAPTIVE).
DEFCLI	Restricts the user to the default command interpreter by prohibiting the use of the /CLI qualifier at login; the MCR command can still be used. By default, a user can choose a CLI (NODEFCLI).
DISCTLY	Establishes an environment where Ctrl/Y interrupts are initially turned off and are invalid until a SET CONTROL=Y is encountered. This could happen in SYLOGIN.COM or in a procedure called by SYLOGIN.COM. Once a SET CONTROL=Y is executed (which requires no privilege), a user can enter a Ctrl/Y and reach the DCL prompt ($). If the intent of DISCTLY is to force execution of the login command files, then SYLOGIN.COM should issue the DCL command SET CONTROL=Y to turn on Ctrl /Y interrupts before exiting. By default, Ctrl /Y is enabled (NODISCTLY).
DISFORCE_PWD_ CHANGE	Removes the requirement that a user must change an expired password at login. By default, a person can use an expired password only once (NODISFORCE_PWD_CHANGE) and then is forced to change the password after logging in. If the user does not select a new password, the user is locked out of the system. To use this feature, set a password expiration date with the /PWDLIFETIME qualifier.
DISIMAGE	Prevents the user from executing RUN, MCR, and foreign commands. By default, a user can execute RUN, MCR, and foreign commands (NODISIMAGE).
DISMAIL	Disables mail delivery to the user. By default, mail delivery is enabled (NODISMAIL).
DISNEWMAIL	Suppresses announcements of new mail at login. By default, the system announces new mail (NODISNEWMAIL).
DISPWDDIC	Disables automatic screening of new passwords against a system dictionary. By default, passwords are automatically screened (NODISPWDDIC).
DISPWDHIS	Disables automatic checking of new passwords against a list of the user's old passwords. By default, the system screens new passwords (NODISPWDHIS).
DISRECONNECT	Disables automatic reconnection to an existing process when a terminal connection has been interrupted. By default, automatic reconnection is enabled (NODISRECONNECT).
DISREPORT	Suppresses reports of the last login time, login failures, and other security reports. By default, login information is displayed (NODISREPORT).
DISUSER	Disables the account so the user cannot log in. For example, the DEFAULT account is disabled. By default, an account is enabled (NODISUSER).
DISWELCOME	Suppresses the welcome message (an informational message displayed during a local login). This message usually indicates the version number of the operating system that is

running and the name of the node on which the user is logged in. By default, a system login message appears (NODISWELCOME).

EXTAUTH — Considers user to be authenticated by an external user name and password, not by the SYSUAF user name and password. (The system still uses the SYSUAF record to check a user's login restrictions and quotas and to create the user's process profile.)

GENPWD — Restricts the user to generated passwords. By default, users choose their own passwords (NOGENPWD).

LOCKPWD — Prevents the user from changing the password for the account. By default, users can change their passwords (NOLOCKPWD).

PWD_EXPIRED — Marks a password as expired. The user cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not expired after login (NOPWD_EXPIRED).

PWD2_EXPIRED — Marks a secondary password as expired. Users cannot log in if this flag is set. The LOGINOUT.EXE image sets the flag when both of the following conditions exist: a user logs in with the DISFORCE_PWD_CHANGE flag set, and the user's password expires. A system manager can clear this flag. By default, passwords are not set to expire after login (NOPWD2_EXPIRED).

RESTRICTED — Prevents the user from changing any defaults at login (for example, by specifying /LGICMD) and prohibits user specification of a CLI with the /CLI qualifier. The RESTRICTED flag establishes an environment where Ctrl/Y interrupts are initially turned off; however, command procedures can still turn on Ctrl/Y interrupts with the DCL command SET CONTROL=Y. Typically, this flag is used to prevent an applications user from having unrestricted access to the CLI. By default, a user can change defaults (NORESTRICTED).

/GENERATE_PASSWORD

/GENERATE_PASSWORD[=keyword]
/NOGENERATE_PASSWORD (default)

Invokes the password generator to create user passwords. Generated passwords can consist of 1 to 10 characters. Specify one of the following keywords:

BOTH — Generate primary and secondary passwords.

CURRENT — Do whatever the DEFAULT account does (for example, generate primary, secondary, both, or no passwords). This is the default keyword.

PRIMARY — Generate primary password only.

SECONDARY — Generate secondary password only.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, users are forced to change their passwords (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/INTERACTIVE

/INTERACTIVE[=(range[,...])]
/NOINTERACTIVE

Specifies the hours of access for interactive logins. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on interactive logins.

/JTQUOTA

/JTQUOTA=value

Specifies the initial byte quota with which the jobwide logical name table is to be created. By default, the value is 4096 on VAX systems and 4096 on Alpha systems.

/LGICMD

/LGICMD=filespec

Specifies the name of the default login command file. The file name defaults to the device specified for /DEVICE, the directory specified for /DIRECTORY, a file name of LOGIN, and a file type of .COM. If you select the defaults for all these values, the file name is SYS$SYSTEM:[USER]LOGIN.COM.

/LOCAL

/LOCAL[=(range[,...])]

Specifies hours of access for interactive logins from local terminals. For a description of the range specification, see the /ACCESS qualifier. By default, there are no access restrictions on local logins.

/MAXACCTJOBS

/MAXACCTJOBS=value

Specifies the maximum number of batch, interactive, and detached processes that can be active at one time for all users of the same account. By default, a user has a maximum of 0, which represents an unlimited number.

/MAXDETACH

/MAXDETACH=value

Specifies the maximum number of detached processes with the cited user name that can be active at one time. To prevent the user from creating detached processes, specify the keyword NONE. By default, a user has a value of 0, which represents an unlimited

number.

/MAXJOBS

/MAXJOBS=value

Specifies the maximum number of processes (interactive, batch, detached, and network) with the cited user name that can be active simultaneously. The first four network jobs are not counted. By default, a user has a maximum value of 0, which represents an unlimited number.

/MODIFY_IDENTIFIER

/MODIFY_IDENTIFIER (default)
/NOMODIFY_IDENTIFIER

Specifies whether the identifier associated with the user is to be modified in the rights database. This qualifier applies only when you modify the UIC or user name in the UAF record. By default, the associated identifiers are modified.

/NETWORK

/NETWORK[=(range[,...])]

Specifies hours of access for network batch jobs. For a description of how to specify the range, see the /ACCESS qualifier. By default, network logins have no access restrictions.

/OWNER

/OWNER=owner-name

Specifies the name of the owner of the account. You can use this name for billing purposes or similar applications. The owner name is 1 to 31 characters. No default owner name exists.

/PASSWORD

/PASSWORD=(password1[,password2])
/NOPASSWORD

Specifies up to two passwords for login. Passwords can be from 0 to 32 characters in length and can include alphanumeric characters, dollar signs, and underscores. Avoid using the word password as the actual password. Use the /PASSWORD qualifier as follows:

- To set only the first password and clear the second, specify /PASSWORD=password.
- To set both the first and second password, specify /PASSWORD=(password1, password2).
- To change the first password without affecting the second, specify /PASSWORD=(password, "").
- To change the second password without affecting the first, specify /PASSWORD=("", password).
- To set both passwords to null, specify /NOPASSWORD.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, the user is forced to change the password (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/PBYTLM

This flag is reserved for Digital.

/PGFLQUOTA

/PGFLQUOTA=value

Specifies the paging file limit. This is the maximum number of pages that the person's process can use in the system paging file. By default, the value is 32768 pages on VAX systems and 50000 pagelets on Alpha systems.

If decompressing libraries, make sure to set PGFLQUOTA to twice the size of the library.

/PRCLM

/PRCLM=value

Specifies the subprocess creation limit. This is the maximum number of subprocesses that can exist at one time for the specified user's process. By default, the value is 2 on VAX systems and 8 on Alpha systems.

/PRIMEDAYS

/PRIMEDAYS=([NO]day[,...])

Defines the primary and secondary days of the week for logging in. Specify the days as a list separated by commas, and enclose the list in parentheses. To specify a secondary day, prefix the day with NO (for example, NOFRIDAY). To specify a primary day, omit the NO prefix.

By default, primary days are Monday through Friday and secondary days are Saturday and Sunday. If you omit a day from the list, AUTHORIZE uses the default value. (For example, if you omit Monday from the list, AUTHORIZE defines Monday as a primary day.)

Use the primary and secondary day definitions in conjunction with such qualifiers as /ACCESS, /INTERACTIVE, and /BATCH.

/PRIORITY

/PRIORITY=value

Specifies the default base priority. The value is an integer in

the range of 0 to 31 on VAX systems and 0 to 63 on Alpha systems. By default, the value is set to 4 for timesharing users.

/PRIVILEGES

/PRIVILEGES=([NO]privname[,...])

Specifies which privileges the user is authorized to hold, although these privileges are not necessarily enabled at login. (The /DEFPRIVILEGES qualifier determines which ones are enabled.) A NO prefix removes the privilege from the user. The keyword NOALL disables all user privileges. Many privileges have varying degrees of power and potential system impact (see the OpenVMS Guide to System Security for a detailed discussion). By default, a user holds TMPMBX and NETMBX privileges. Privname is the name of the privilege.

/PWDEXPIRED

/PWDEXPIRED (default)
/NOPWDEXPIRED

Specifies the password is valid for only one login. A user must change a password immediately after login or be locked out of the system. The system warns users of password expiration. A user can either specify a new password, with the DCL command SET PASSWORD, or wait until expiration and be forced to change. By default, a user must change a password when first logging in to an account. The default is applied to the account only when the password is being modified.

/PWDLIFETIME

/PWDLIFETIME=time (default)
/NOPWDLIFETIME

Specifies the length of time a password is valid. Specify a delta time value in the form [dddd-] [hh:mm:ss.cc]. For example, for a lifetime of 120 days, 0 hours, and 0 seconds, specify /PWDLIFETIME="120-". For a lifetime of 120 days 12 hours, 30 minutes and 30 seconds, specify /PWDLIFETIME="120-12:30:30". If a period longer than the specified time elapses before the user logs in, the system displays a warning message. The password is marked as expired.

To prevent a password from expiring, specify the time as NONE. By default, a password expires in 90 days.

/PWDMINIMUM

/PWDMINIMUM=value

Specifies the minimum password length in characters. Note that this value is enforced only by the DCL command SET PASSWORD. It does not prevent you from entering a password shorter than the minimum length when you use AUTHORIZE to create or modify an account. By default, a password must have at least 6 characters. The value specified by the /PWDMINIMUM qualifier conflicts with the value used by the /GENERATE_PASSWORD qualifier or the DCL command SET PASSWORD/GENERATE, the operating system chooses the lesser value. The maximum value for generated passwords is 10.

/QUEPRIO

/QUEPRIO=value

Reserved for future use.

/REMOTE

/REMOTE[=(range[,...])]

Specifies hours during which access is permitted for interactive logins from network remote terminals (with the DCL command SET HOST). For a description of the range specification, see the /ACCESS qualifier. By default, remote logins have no access restrictions.

/SHRFILLM

/SHRFILLM=value

Specifies the maximum number of shared files that the user can have open at one time. By default, the system assigns a value of 0, which 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. By default, a user can have 10.

/UIC

/UIC=value

Specifies the user identification code (UIC). The UIC value is a group number in the range from 1 to 37776 (octal) and a member number in the range from 0 to 177776 (octal), which are separated by a comma and enclosed in brackets. Digital reserves group 1 and groups 300-377 for its own use.

Each user must have a unique UIC. By default, the UIC value is [200,200].

/WSDEFAULT

/WSDEFAULT=value

Specifies the default working set limit. This represents the initial limit to the number of physical pages the process can use. (The user can alter the default quantity up to WSQUOTA with the DCL command SET WORKING_SET.) By default, a user has 256 pages on VAX systems and 2000 pagelets on Alpha systems.

The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSDEFAULT.

/WSEXTENT

/WSEXTENT=value

Specifies the working set maximum. This represents the maximum amount of physical memory allowed to the process. The system provides memory to a process beyond its working set quota only when it has excess free pages. The additional memory is recalled by the system if needed.

The value is an integer equal to or greater than WSQUOTA. By default, the value is 1024 pages on VAX systems and 16384 pagelets on Alpha systems. The value cannot be greater than WSMAX. This quota value replaces smaller values of PQL_MWSEXTENT.

/WSQUOTA

/WSQUOTA=value

Specifies the working set quota. This is the maximum amount of physical memory a user process can lock into its working set. It also represents the maximum amount of swap space that the system reserves for this process and the maximum amount of physical memory that the system allows the process to consume if the systemwide memory demand is significant.

The value cannot be greater than the value of WSMAX and cannot exceed 64K pages. This quota value replaces smaller values of PQL_MWSQUOTA.

2 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=RESTRICTED
%UAF-I-MDFYMSG, user record(s) updated

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

2 /IDENTIFIER

Modifies an identifier name, its associated value, or its attributes in the rights database.

Format

MODIFY/IDENTIFIER id-name

3 Parameter

id-name

Specifies the name of an identifier to be modified.

3 Qualifiers

/ATTRIBUTES

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

Specifies attributes to be associated with the modified identifier. The following are valid keywords:

DYNAMIC	Allows unprivileged holders of the identifier to remove and to restore the identifier from the process rights list by using the DCL command SET RIGHTS_LIST.
HOLDER_HIDDEN	Prevents people from getting a list of users who hold an identifier, unless they own the identifier themselves.
NAME_HIDDEN	Allows holders of an identifier to have it translated, either from binary to ASCII or from ASCII to binary, but prevents unauthorized users from translating the identifier.
NOACCESS	Makes any access rights of the identifier null and void. If a user is granted an identifier with the No Access attribute, that identifier has no effect on the user's access rights to objects. This attribute is a modifier for an identifier with the Resource or Subsystem attribute.
RESOURCE	Allows holders of an identifier to charge disk space to the identifier. Used only for file objects.
SUBSYSTEM	Allows holders of the identifier to create and maintain protected subsystems by assigning the Subsystem ACE to the application images in the subsystem. Used only for file objects.

To remove an attribute from the identifier, add a NO prefix to the attribute keyword. For example, to remove the Resource attribute, specify /ATTRIBUTES=NORESOURCE.

NOTE

If you specify the NORESOURCE keyword without naming any holder with the /HOLDER qualifier, all holders lose the right to charge resources.

/HOLDER

/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

/NAME=new-id-name

Specifies a new identifier name to be associated with the identifier.

/VALUE

/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:n	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). To differentiate general identifiers from UIC identifiers, %X80000000 is added to the value you specify.
UIC:uic	A UIC value in the standard UIC format.

3 Examples

1.UAF> MODIFY/IDENTIFIER OLD_ID /NAME=NEW_ID
%UAF-I-RDBMDFYMSG, identifier OLD_ID modified

The command in this example changes the name of the OLD_ID identifier to NEW_ID.

2.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.

3.UAF> MODIFY/IDENTIFIER/ATTRIBUTES=NORESOURCE-
_UAF> /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.

2 /PROXY

Modifies an entry in the network proxy authorization file to specify a different local account as the default proxy account for the remote user or to specify no default proxy account for the remote user.

The command modifies an entry in the network proxy authorization file NET$PROXY.DAT and, to maintain compatibility with other systems, modifies an entry in NETPROXY.DAT.

NOTE

You must modify the proxy database from a system running the current OpenVMS system.

Format

MODIFY/PROXY node::remote-user

3 Parameters

node

Specifies a node name. If you specify an asterisk wildcard character (*), 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 wildcard character, all users at the specified node are served by the local user.

For systems that are not OpenVMS systems that implement DECnet, specifies the UIC of a user at a remote node. You can specify an asterisk wildcard in the group and member fields of the UIC.

3 Qualifier

/DEFAULT

/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.

3 Example

```
UAF> MODIFY/PROXY MISHA::MARCO /DEFAULT=JOHNSON
%UAF-I-NAFADDMSG, 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.

2 /SYSTEM_PASSWORD

Changes the systemwide password (which, however, is different from the password for the SYSTEM username). This command operates similarly to the DCL command SET PASSWORD/SYSTEM.

Format

MODIFY/SYSTEM_PASSWORD=system-password

3 Parameter

system-password

Specifies the new systemwide password.

3 Example

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

This command changes the systemwide password to ABRACADABRA.

VMS AUTHORIZE (UAF) Help

1 REMOVE

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

Format

```
REMOVE  username
```

2 Parameter

username

Specifies the name of a user in the SYSUAF.

2 Qualifier

/REMOVE_IDENTIFIER

```
/REMOVE_IDENTIFIER (default)
/NOREMOVE_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 two UAF records have 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.

2 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 SYSUAF and ROBIN's UIC identifier from RIGHTSLIST.DAT.

2 /IDENTIFIER

Removes an identifier from the rights database.

Format

```
REMOVE/IDENTIFIER  id-name
```

3 Parameter

id-name

Specifies the name of an identifier in the rights database.

3 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 of its holder records are removed with it.

2 /PROXY

Deletes network proxy access for the specified remote user.

Format

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

3 Parameters

node

Specifies the name of a network node in the network proxy authorization file.

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.

3 Example

```
 UAF> REMOVE/PROXY MISHA::MARCO
 %UAF-I-NAFREMMSG, proxy from MISHA::MARCO to * removed
```

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.

VMS AUTHORIZE (UAF) Help

1 RENAME

Changes the user name of the SYSUAF record (and, if specified, the corresponding identifier) while retaining the characteristics of the old record.

Format

```
RENAME  oldusername newusername
```

2 Parameters

oldusername

Specifies the current user name in the SYSUAF.

newusername

Specifies the new name for the user. It can contain 1 to 12 alphanumeric characters and underscores. Although dollar signs are permitted, they are usually reserved for system names.

2 Qualifiers

/GENERATE_PASSWORD

```
/GENERATE_PASSWORD[=keyword]
/NOGENERATE_PASSWORD (default)
```

Invokes the password generator to create user passwords. Generated passwords can consist of 1 to 10 characters. Specify one of the following keywords:

BOTH	Generate primary and secondary passwords.
CURRENT	Do whatever the DEFAULT account does (for example, generate primary, secondary, both, or no passwords). This is the default keyword.
PRIMARY	Generate primary password only.
SECONDARY	Generate secondary password only.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, users are forced to change their passwords (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

/MODIFY_IDENTIFIER

```
/MODIFY_IDENTIFIER (default)
/NOMODIFY_IDENTIFIER
```

Specifies whether the identifier associated with the user is to be modified in the rights database. This qualifier applies only when you modify the UIC or user name in the UAF record. By default, the associated identifiers are modified.

/PASSWORD

```
/PASSWORD=(password1[,password2])
/NOPASSWORD
```

Specifies up to two passwords for login. Passwords can be from 0 to 32 characters in length and can include alphanumeric characters, dollar signs, and underscores. Avoid using the word password as the actual password. Use the /PASSWORD qualifier as follows:

- To set only the first password and clear the second, specify /PASSWORD=password.
- To set both the first and second password, specify /PASSWORD=(password1, password2).
- To change the first password without affecting the second, specify /PASSWORD=(password, "").
- To change the second password without affecting the first, specify /PASSWORD=("", password).
- To set both passwords to null, specify /NOPASSWORD.

When you modify a password, the new password expires automatically; it is valid only once (unless you specify /NOPWDEXPIRED). On login, the user is forced to change the password (unless you specify /FLAGS=DISFORCE_PWD_CHANGE).

Note that the /GENERATE_PASSWORD and /PASSWORD qualifiers are mutually exclusive.

When you create a new UAF record with the RENAME command, you must specify a password.

2 Examples

```
1.UAF> RENAME HAWKES KRAMERDOVE/PASSWORD=MARANNKRA
  %UAF-I-PRACREN, 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-PRACREN, 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.
```

2 /IDENTIFIER

Renames an identifier in the rights database.

Format

RENAME/IDENTIFIER current-id-name new-id-name

3 Parameters

current-id-name

Specifies the name of an identifier to be renamed.

new-id-name

Specifies the new name for the identifier.

3 Example

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

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

VMS AUTHORIZE (UAF) Help

1 REVOKE

2 /IDENTIFIER
Takes an identifier away from a user.

Format

REVOKE/IDENTIFIER id-name user-spec

3 Parameters

id-name

Specifies the identifier name. The identifier name is a string of 1 to 31 alphanumeric characters. The name can contain underscores and dollar signs. It must contain at least one nonnumeric character.

user-spec

Specifies the UIC identifier that uniquely identifies the user on the system. This type of identifier appears in alphanumeric format, not numeric format; for example, [GROUP1,JONES].

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

VMS AUTHORIZE (UAF) Help

1 SHOW

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

Format

```
SHOW  user-spec
```

2 Parameter

user-spec

Specifies the user name or UIC of the requested 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.

2 Qualifiers

/BRIEF

Specifies that a brief report be displayed. In the report, the Directory field displays one of the following items:

- Disuser-The account has been disabled.
- Expired-The account has expired.
- A device and directory name-The login device and directory for the account (for example, DOCD$:[SMITH]).

If you omit the /BRIEF qualifier, AUTHORIZE displays a full report.

/FULL

Specifies that a full report be displayed, including identifiers held by the user. Full reports include the details of the limits, privileges, login flags, and the command interpreter as well as the identifiers held by the user. The password is not listed.

/EXACT

Controls whether the SHOW command matches the search string exactly or treats uppercase and lowercase letters as equivalents. Enclose the specified string within quotation marks (" "). Use /EXACT with the /PAGE=SAVE and /SEARCH qualifiers.

/HIGHLIGHT

```
/HIGHLIGHT[=keyword]
/NOHIGHLIGHT (default)
```

Identifies how to display the line that contains a string once it is found. The following keywords are valid:

```
BLINK
BOLD (default)
REVERSE
UNDERLINE
```

Use the /HIGHLIGHT qualifier with the /PAGE=SAVE and /SEARCH qualifiers.

/PAGE

```
/PAGE[=keyword]
/NOPAGE (default)
```

Controls the information display on a screen. The following keywords are valid:

CLEAR_SCREEN	Clear the screen before displaying the next page.
SCROLL	Display a continuous stream of information.
SAVE[=n]	Store information and enable the navigational keys listed in Screen Control Keys. By default, the command saves 5 pages. The maximum page width is 255 columns.

Table 4 Screen Control Keys

Key or Key Sequence	Action Taken When Key or Key Sequence Is Pressed
v	Scroll the display down one line
< -	Scroll the display one column to the left
- >	Scroll the display one column to the right
^	Scroll the display up one line
Find (E1)	Search for a new string in the information being displayed
Insert Here (E2)	Move the display to the right by half a screen
Remove (E3)	Move the display to the left by half a screen
Select (E4)	Switch from 80-column displays to 132-column displays
Prev Screen (E5)	Return to the previous page
Next Screen (E6)	Display the next page
CTRL/Z	Return to the UAF> prompt
Help	Display AUTHORIZE help text
F16 (Do)	Switch from the oldest to the newest page
Ctrl/W	Refresh the display

/SEARCH

```
/SEARCH=string
```

Used with the /PAGE=SAVE qualifier to specify a string to find in the information being displayed. You can dynamically change the search string by pressing the Find key (E1) while the information is being displayed.

/WRAP

```
   /WRAP
   /NOWRAP (default)

Used with the /PAGE=SAVE qualifier to limit the number of columns
to the width of the screen and wrap lines that extend beyond the
width of the screen to the next line.

The /NOWRAP qualifier extends lines beyond the width of the
screen. Use the /PAGE=SAVE qualifier and the screen control keys
listed in Screen Control Keys to view the entire screen.


2  Examples

1.UAF> SHOW ROBIN

  The command in this VAX example displays a full report for the
  user ROBIN. The display corresponds to the first example in the
  description of the ADD command. 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-JAN-1996 14:08
    Last Login:            (none) (interactive),      (none) (non-interactive)
    Maxjobs:         0  Fillm:       300  Bytlm:        32768
    Maxacctjobs:     0  Shrfillm:      0  Pbytlm:           0
    Maxdetach:       0  BIOlm:        40  JTquota:       4096
    Prclm:           2  DIOlm:        40  WSdef:          256
    Prio:            4  ASTlm:        40  WSquo:          512
    Queprio:         0  TQElm:        10  WSextent:      1024
    CPU:        (none)  Enqlm:       200  Pgflquo:      32768
    Authorized Privileges:
      TMPMBX NETMBX
    Default Privileges:
      TMPMBX NETMBX
    Identifier                      Value           Attributes
      CLASS_CA101                   %X80010032      NORESOURCE NODYNAMIC
      CLASS_PY102                   %X80010049      NORESOURCE NODYNAMIC

                              NOTE

   The quotas Pbytlm and Queprio are placeholders only.

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 JAMES          JAMES      [360,201] USER     Normal  4 DOCD$:[JAMES]
    SUSY JONES          JONES      [360,203] DOC      Devour  4 DOCD$:[JONES]
    CLIFF BROWN         BROWN      [360,021] DOC      All     4 disuser
    JOY CARTER          CARTER     [360,005] DOCSEC   Group   4 expired

3.UAF> SHOW WELCH

  This command displays a full report for the restricted user
  WELCH. This 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:  Restricted Diswelcome Disnewmail ExtAuth
    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:       300  Bytlm:        32768
    Maxacctjobs:     0  Shrfillm:      0  Pbytlm:           0
    Maxdetach:       0  BIOlm:        40  JTquota:       4096
    Prclm:           2  DIOlm:        40  WSdef:          256
    Prio:            4  ASTlm:        40  WSquo:          512
    Queprio:         4  TQElm:        10  WSextent:      1024
    CPU:        (none)  Enqlm:       200  Pgflquo:      32768
    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 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.


2  /IDENTIFIER
   Displays information about an identifier, such as its name,
   value, attributes, and holders, on the current SYS$OUTPUT device.

   Format

     SHOW/IDENTIFIER  [id-name]


3  Parameter


id-name
```

Specifies an identifier name. The identifier name is a string of 1 to 31 alphanumeric characters. The name can contain underscores and dollar signs. It must contain at least one nonnumeric character. If you omit the identifier name, you must specify /USER or /VALUE.

3 Qualifiers

/BRIEF

Specifies a brief listing in which only the identifier name, value, and attributes are displayed. The default format is /BRIEF.

/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=user-spec

Specifies one or more users whose identifiers are to be displayed. The user-spec can be a user name or a UIC. You can use the asterisk wildcard character (*) to specify multiple UICs or all 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=value-specifier

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

IDENTIFIER:n	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). To differentiate general identifiers from UIC identifiers, %X80000000 is added to the value you specify.
UIC:uic	A UIC value in the standard UIC format.

/EXACT

Controls whether the SHOW command matches the search string exactly or treats uppercase and lowercase letters as equivalents. Enclose the specified string within quotation marks (" "). Use /EXACT with the /PAGE=SAVE and /SEARCH qualifiers.

/HIGHLIGHT

/HIGHLIGHT[=keyword]
/NOHIGHLIGHT (default)

Identifies how to display the line that contains a string once it is found. The following keywords are valid:

BLINK
BOLD (default)
REVERSE
UNDERLINE

Use the /HIGHLIGHT qualifier with the /PAGE=SAVE and /SEARCH qualifiers.

/PAGE

/PAGE[=keyword]
/NOPAGE (default)

Controls the information display on a screen. The following keywords are valid:

CLEAR_SCREEN	Clear the screen before displaying the next page.
SCROLL	Display a continuous stream of information.
SAVE[=n]	Store information and enable the navigational keys listed in Screen Control Keys. By default, the command saves 5 pages. The maximum page width is 255 columns.

Table 4 Screen Control Keys

Key or Key Sequence	Action Taken When Key or Key Sequence Is Pressed
v	Scroll the display down one line
< -	Scroll the display one column to the left
- >	Scroll the display one column to the right
^	Scroll the display up one line
Find (E1)	Search for a new string in the information being displayed
Insert Here (E2)	Move the display to the right by half a screen
Remove (E3)	Move the display to the left by half a screen
Select (E4)	Switch from 80-column displays to 132-column displays
Prev Screen (E5)	Return to the previous page
Next Screen (E6)	Display the next page
CTRL/Z	Return to the UAF> prompt
Help	Display AUTHORIZE help text
F16 (Do)	Switch from the oldest to the newest page
Ctrl/W	Refresh the display

/SEARCH

/SEARCH=string

Used with the /PAGE=SAVE qualifier to specify a string to find in the information being displayed. You can dynamically change the search string by pressing the Find key (E1) while the information is being displayed.

/WRAP

/WRAP
/NOWRAP (default)

Used with the /PAGE=SAVE qualifier to limit the number of columns to the width of the screen and wrap lines that extend beyond the width of the screen to the next line.

The /NOWRAP qualifier extends lines beyond the width of the screen. Use the /PAGE=SAVE qualifier and the screen control keys listed in Screen Control Keys to view the entire screen.

3 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
```

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]
```

2 /PROXY

Displays all authorized proxy access for the specified remote user.

Format

```
  SHOW/PROXY  node::remote-user
```

3 Parameters

node

Specifies the name of a network node in the network proxy authorization file. The asterisk wildcard character (*) is permitted in the node specification.

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.

3 Qualifiers

/OLD

Directs AUTHORIZE to display information from NETPROXY.DAT rather than the default file NET$PROXY.DAT.

If someone modifies the proxy database on a cluster node that is running an OpenVMS system prior to Version 6.1, then you can use the /OLD qualifier to display the contents of the old database: NETPROXY.DAT.

/EXACT

Controls whether the SHOW command matches the search string exactly or treats uppercase and lowercase letters as equivalents. Enclose the specified string within quotation marks (" "). Use /EXACT with the /PAGE=SAVE and /SEARCH qualifiers.

/HIGHLIGHT

/HIGHLIGHT[=keyword]
/NOHIGHLIGHT (default)

Identifies how to display the line that contains a string once it is found. The following keywords are valid:

BLINK
BOLD (default)
REVERSE
UNDERLINE

Use the /HIGHLIGHT qualifier with the /PAGE=SAVE and /SEARCH qualifiers.

/PAGE

/PAGE[=keyword]
/NOPAGE (default)

Controls the information display on a screen. The following keywords are valid:

CLEAR_SCREEN	Clear the screen before displaying the next page.
SCROLL	Display a continuous stream of information.
SAVE[=n]	Store information and enable the navigational keys listed in Screen Control Keys. By default, the command saves 5 pages. The maximum page width is 255 columns.

Table 4 Screen Control Keys

Key or Key

Sequence	Action Taken When Key or Key Sequence Is Pressed
v	Scroll the display down one line
< -	Scroll the display one column to the left
- >	Scroll the display one column to the right
^	Scroll the display up one line
Find (E1)	Search for a new string in the information being displayed
Insert Here (E2)	Move the display to the right by half a screen
Remove (E3)	Move the display to the left by half a screen
Select (E4)	Switch from 80-column displays to 132-column displays
Prev Screen (E5)	Return to the previous page
Next Screen (E6)	Display the next page
CTRL/Z	Return to the UAF> prompt
Help	Display AUTHORIZE help text
F16 (Do)	Switch from the oldest to the newest page
Ctrl/W	Refresh the display

/SEARCH

/SEARCH=string

Used with the /PAGE=SAVE qualifier to specify a string to find in the information being displayed. You can dynamically change the search string by pressing the Find key (E1) while the information is being displayed.

/WRAP

/WRAP
/NOWRAP (default)

Used with the /PAGE=SAVE qualifier to limit the number of columns to the width of the screen and wrap lines that extend beyond the width of the screen to the next line.

The /NOWRAP qualifier extends lines beyond the width of the screen. Use the /PAGE=SAVE qualifier and the screen control keys listed in Screen Control Keys to view the entire screen.

3 Examples

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

Default proxies are flagged with an *

```
SAMPLE::[200,100]
     MARCO *                          PROXY2
     PROXY3
```

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.

2.UAF> SHOW/PROXY *::*

Default proxies are flagged with (D)

```
TAO:.TWA.RANCH::MARTINEZ
    MARTINEZ (D)                      SALES_READER

UAF> show/proxy/old *::*

 Default proxies are flagged with (D)

RANCH::MARTINEZ
    MARTINEZ (D)                      SALES_READER
```

The command in this example displays information about local authorized proxy access on a system running DECnet-Plus. The first command draws information from the file NET$PROXY.DAT. By including the /OLD qualifier on the SHOW/PROXY command, AUTHORIZE displays information from the file NETPROXY.DAT.

2 /RIGHTS

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

Format

SHOW/RIGHTS [id-name]

3 Parameter

id-name

Specifies the name of the identifier associated with the user. If you omit the identifier name, you must specify the /USER qualifier.

3 Qualifier

/USER

/USER=user-spec

Specifies one or more users whose identifiers are to be listed. The user-spec can be a user name or a UIC. You can use the asterisk wildcard character (*) to specify multiple UICs or all 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.

/EXACT

Controls whether the SHOW command matches the search string exactly or treats uppercase and lowercase letters as equivalents. Enclose the specified string within quotation marks (" "). Use /EXACT with the /PAGE=SAVE and /SEARCH qualifiers.

/HIGHLIGHT

/HIGHLIGHT[=keyword]
/NOHIGHLIGHT (default)

Identifies how to display the line that contains a string once it is found. The following keywords are valid:

BLINK
BOLD (default)
REVERSE
UNDERLINE

Use the /HIGHLIGHT qualifier with the /PAGE=SAVE and /SEARCH qualifiers.

/PAGE

/PAGE[=keyword]
/NOPAGE (default)

Controls the information display on a screen. The following keywords are valid:

CLEAR_SCREEN	Clear the screen before displaying the next page.
SCROLL	Display a continuous stream of information.
SAVE[=n]	Store information and enable the navigational keys listed in Screen Control Keys. By default, the command saves 5 pages. The maximum page width is 255 columns.

Table 4 Screen Control Keys

Key or Key Sequence	Action Taken When Key or Key Sequence Is Pressed
v	Scroll the display down one line
< -	Scroll the display one column to the left
- >	Scroll the display one column to the right
^	Scroll the display up one line
Find (E1)	Search for a new string in the information being displayed
Insert Here (E2)	Move the display to the right by half a screen
Remove (E3)	Move the display to the left by half a screen
Select (E4)	Switch from 80-column displays to 132-column displays
Prev Screen (E5)	Return to the previous page
Next Screen (E6)	Display the next page
CTRL/Z	Return to the UAF> prompt
Help	Display AUTHORIZE help text
F16 (Do)	Switch from the oldest to the newest page
Ctrl/W	Refresh the display

/SEARCH

/SEARCH=string

Used with the /PAGE=SAVE qualifier to specify a string to find in the information being displayed. You can dynamically change the search string by pressing the Find key (E1) while the information is being displayed.

/WRAP

/WRAP
/NOWRAP (default)

Used with the /PAGE=SAVE qualifier to limit the number of columns to the width of the screen and wrap lines that extend beyond the width of the screen to the next line.

The /NOWRAP qualifier extends lines beyond the width of the screen. Use the /PAGE=SAVE qualifier and the screen control keys listed in Screen Control Keys to view the entire screen.

3 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]
```